Centro Universitário de Brasília – UniCEUB
Faculdade de Tecnologia e Ciências Sociais Aplicadas – FATECS
Engenharia de Computação
Disciplina: Projeto Final

SUPERVISIONAMENTO DE FIREWALL IPTABLES PARA PEQUENAS EMPRESAS DE INFORMÁTICA

Marcelo de Souza Mendonça
RA: 2041672/6

Orientador: Marco Antônio Araújo

BRASÍLIA - DF
2009

MARCELO DE SOUZA MENDONÇA

SUPERVISIONAMENTO DE FIREWALL IPTABLES PARA PEQUENAS EMPRESAS DE INFORMÁTICA

Monografia apresentada como requisito para conclusão do Curso de Bacharelado em Engenharia de Computação realizado no Centro Universitário de Brasília - UniCEUB.

Orientador: Marco Antônio Araújo.

BRASÍLIA - DF
2009

SUPERVISIONAMENTO DE FIREWALL IPTABLES PARA PEQUENAS EMPRESAS DE INFORMÁTICA

por

Marcelo de Souza Mendonça

Monografia apresentada como requisito para conclusão do Curso de Bacharelado em Engenharia de Computação realizado no Centro Universitário de Brasília - UniCEUB.

Brasília – DF, 2009

Banca Examinadora

Prof. Msc. Antônio Barbosa Júnior
Examinador

Prof. Msc. Luigi Silva Mota
Examinador

Prof. Msc. Roberto Avila Paldês
Examinador

Prof. Msc. Roberto Schaefer de Azeredo
Examinador

AGRADECIMENTOS

Meus sinceros agradecimentos...

...à minha Família que, mesmo distante, sempre esteve comigo;

...à minha mãe Cláudia Inês, que está sempre presente nos momentos mais difíceis;

...ao meu pai Orlandilson, por todo seu esforço para tornar tudo isto possível;

...aos meus tios Pedro e Suely, pelo carinho e oportunidade;

...ao meu irmão Felipe, grande amigo que sempre torceu por mim;

...às minhas irmãs Lara e Camila, por todo o carinho;

...à Lana, pessoa querida, que aconteceu em minha vida e deixou muitas coisas boas;

...ao grande amigo Welligton, pelos valiosos ensinamentos;

...ao meu orientador Marco Antônio, pelas valiosas sugestões;

...a Deus, por estar sempre comigo.

“Por mais longa que seja a caminhada o mais importante é dar o primeiro passo.”

(Vinícius de Moraes)

RESUMO

Este projeto consiste na criação de uma interface para realizar a supervisão e gestão das funções de Firewall do Iptables com enfoque em pequenas Empresas de Informática. Posto isto, caracteriza o estudo de uma solução para estabelecer o relacionamento entre os módulos de configuração do Iptables e o usuário administrador de rede de modo simples e amigável.

O trabalho é todo desenvolvido utilizando a linguagem Shell Script. Portanto, tanto as regras de filtragem do Iptables quanto as telas de menu da interface foram programadas dentro de Scripts que são executados a partir de um Shell. O programa utilizado para desenhar as telas da interface, chama-se Dialog.

Palavras-Chave: Firewall; Iptables; Shell Script; Interface; Supervisionamento.

ABSTRACT

This project is based on the creation of an interface to perform the supervision and management functions of the Firewall from Iptables focusing on small computer companies. Therefore is characterized by the study of a solution to establish the relation between the configuration modules from Iptables and the network administrator in a simple and friendly way.

The whole work was developed using the Shell Script language, thus the filter rules of Iptables and the menu screens of the interface were programmed in Scripts that run from a Shell. The program used to design the screens interface is called Dialog.

Keywords: Firewall; Iptables; Shell Script; Interface; Management.

LISTA DE FIGURAS

LISTA DE ABREVIATURAS

DDoS	*Distributed Denial of Service*
DNS	*Domain Name System*
DoS	*Denial of Service*
FTP	*File Transfer Protocol*
HTTP	*HyperText Transfer Protocol*
HTTPS	*HyperText Transfer Protocol Secure*
ICMP	*Internet Control Message Protocol*
IDS	*Intrusion Detection System*
IMAP	*Internet Message Access Protocol*
IP	*Internet Protocol*
IPS	*Intrusion Prevention System*
NAT	*Network Address Translation*
POP	*Post Office Protocol*
SMTP	*Simple Mail Transfer Protocol*
SSH	*Secure Shell*
TCP	*Transmission Control Protocol*
UDP	*User Datagram Protocol*
URL	*Universal Resource Locator*
WWW	*World Wide Web*

SUMÁRIO

1 INTRODUÇÃO

A enorme carência de segurança, atualmente, é algo que ultrapassa a própria produtividade do homem nos mais distintos meios de criação. A velocidade com que as tecnologias são criadas, hoje em dia, em busca de obter vantagem competitiva e reconhecimento no mercado de trabalho aumenta tanto quanto a falta de segurança e as ameaças que rondam esses ambientes corporativos.

Quando se trata de segurança, seja ela relacionada à violência urbana ou à criminalidade virtual, que não deixa de ser um crime real, ainda sim, seu processo de evolução acontece de forma semelhante. A evolução acontece no desenvolvimento de novas formas de ataques as quais em resposta se têm a criação de novas formas de proteção, estabelecendo-se um ciclo.

Desta forma, é importante que sejam implementados meios de segurança tanto em grandes ambientes corporativos quanto em pequenas empresas que prestam os mais diversos tipos de serviços e que possuem informações que precisam ser resguardadas.

Existem diversas ferramentas com maior ou menor grau de configuração, muitas delas precisando de verdadeiros especialistas na sua implementação e configuração. Uma das formas de se facilitar bastante a utilização e configuração de certas ferramentas consiste na adoção de uma interface gráfica, que estabeleça um relacionamento entre o usuário e a ferramenta muito mais amigável.

Assim, neste trabalho propõe-se o desenvolvimento de uma interface de gestão da ferramenta Iptables, em função de ser uma ferramenta composta por vários módulos que precisam ser muito estudados antes de serem implementados em um ambiente computacional de redes. O Iptables é o programa responsável por configurar as regras de filtragem de pacotes do Netfilter, que é o Firewall do Linux em nível de kernel. Uma pessoa que nunca trabalhou com o Iptables, por exemplo, se tivesse a necessidade de implementar essa ferramenta de filtragem de pacotes (Firewall) dentro de sua rede, na certa teria algumas dificuldades porque não é algo pronto para ser utilizado, é necessário se ter os conhecimentos necessários de redes bem como dos módulos de configuração da própria ferramenta. Portanto, a criação de uma interface gráfica ajuda bastante no processo de configuração dessa ferramenta, de modo, que

não precisaria ser um especialista de fato, bastaria alguns conhecimentos de redes, segurança, protocolos e os principais serviços.

Nos seguintes capítulos, serão apresentadas as principais ameaças e formas de proteção de modo a garantir que os pequenos ambientes organizacionais desempenhem suas tarefas com maior tranqüilidade e seguridade.

1.1 Motivação

Durante o período em que cursei a disciplina Estágio Profissional, assim como todos os alunos, teve-se que buscar por um estágio que se relacionasse de alguma forma com a área de atuação do curso, a Tecnologia da Informação. O estágio que consegui foi de Técnico de Suporte em uma Empresa que fornece cursos de informática ao mercado. Percebi que lá, assim como em muitas empresas que atuam neste ramo no mercado, existiam alguns problemas que precisavam ser solucionados de alguma forma.

O que me motivou no desenvolvimento deste Projeto de conclusão de curso, foi estudar formas de solucionar esses problemas através da criação de uma interface que gerenciasse o Firewall do GNU/Linux Iptables, e que de alguma forma facilitasse o desempenho de certas práticas de segurança, realizadas por esta ferramenta, para determinados membros da equipe de Tecnologia, de modo geral, que não sabiam realizar as configurações necessárias da ferramenta manualmente.

1.2 Objetivo Geral e Específicos

Em muitas escolas de informática existem alguns problemas como, alunos utilizando grande parte da banda de rede para baixar filmes, jogos, fotos, músicas, alunos tentando

acessar sites proibidos, alunos tentando utilizar MSN, Orkut, etc. Na maioria dessas empresas, por que não dizer em todas, existe um software chamado Firewall, que em alguns casos auxiliado por um Proxy, bloqueia exatamente esses acessos acima mencionados. No entanto, nessas empresas, geralmente o tecnólogo de redes reserva uma classe de endereços IPs (Equipe Suporte) que tem acesso livre a internet sem passar pelas regras e rotinas do Firewall. Dessa forma, surge o problema que alguns alunos descobrem, ou por acaso, ou porque o técnico modificou as configurações do protocolo TCP/IP e esqueceu-se de retornar ao padrão, e ficam com acesso direto a internet e a banda de rede sem sofrer nenhum tipo de bloqueio por parte do Firewall. Outro problema, não tão comum, mas extremamente crítico em determinados casos, é quando o tecnólogo responsável por ter implementado todas as rotinas e regras do firewall precisa sair, e surge de repente, enquanto ele está fora, a necessidade de liberar um recurso para um laboratório ou para administração que necessita de uma configuração específica e manual do Firewall que somente ele poderá resolver, e mais ninguém da equipe de Suporte Técnico. Nesse sentido uma interface gráfica com algumas funções predefinidas ajudaria muito.

Objetivo Geral

O objetivo deste projeto consiste no desenvolvimento de uma Interface de supervisionamento do Firewall Iptables que permita a implantação de uma boa política de segurança dentro de um ambiente corporativo, como também fornecer maior facilidade de tratamento e configuração de seus módulos.

Objetivos Específicos

Dentre os objetivos específicos, tem-se:

- Facilitar a configuração das regras e módulos do Iptables;
- Estabelecer a liberação de serviços específicos condizentes com a relação de atividades desenvolvidas pelo ambiente organizacional;

- Estabelecimento de uma política de segurança empresarial mais organizada.

1.3 Estrutura do Trabalho

Este trabalho está dividido em seis capítulos, de acordo com o detalhamento a seguir:

Capítulo 1: Trata-se do capítulo atual, onde contém a introdução, os objetivos e a estrutura do trabalho.

Capítulo 2: São apresentados aspectos relativos à segurança organizacional, tais como os alvos de ataque, as ameaças e as ferramentas de proteção.

Capítulo 3: Traz as principais abordagens sobre Firewalls, e as principais características do Iptables.

Capítulo 4: Apresenta o desenvolvimento da parte de implementação do Projeto. Traz as principais abordagens sobre a linguagem utilizada e a ferramenta utilizada para o desenvolvimento do projeto, como Shell Script e Dialog, respectivamente.

Capítulo 5: Aborda os testes realizados com a Interface de Supervisionamento do Iptables, desenvolvida neste Projeto. Após a abordagem dos testes, apresenta as considerações finais do trabalho, como as vantagens e desvantagens da ferramenta e sugestões para projetos futuros.

Capítulo 6: Traz as conclusões finais acerca do Projeto.

2 SEGURANÇA ORGANIZACIONAL

A tecnologia da informação estabeleceu-se fundamental para os mais diversos tipos de empresas. Com o passar dos anos, tornou-se cada vez maior a necessidade da informática e da telecomunicação como meio de garantir o sucesso nas atividades desenvolvidas nos ambientes empresariais. No entanto, em resposta a essa evolução, novos problemas surgiram e passaram a fazer parte do dia-a-dia dessas organizações, cujos quais destacamos, primordialmente a segurança de seus recursos.

Quando se utiliza um padrão ou norma como meio de garantir a segurança nos mais distintos aspectos dentro de uma empresa, fica mais simples de conseguir atender a todas as possíveis vulnerabilidades que aquela empresa teria no desempenho de suas atividades e funções.

Dentro da norma NBR ISO/IEC 17799 - 27002, o pilar que aborda a Segurança Organizacional objetiva aportar a estrutura de uma supervisão voltada para segurança da informação, caracterizada por definir as responsabilidades dos usuários pela segurança da informação, envolvendo agentes externos, assim como prestadores de serviços.

De acordo com a norma,

> Objetivo: Gerenciar a segurança das informações dentro da organização.
> Deve ser estabelecida uma estrutura gerencial para iniciar e controlar a implementação da segurança de informações dentro da organização.
> Foros gerenciais adequados com liderança da administração devem ser estabelecidos para aprovar a política de segurança de informações, atribuir papéis de segurança e coordenar a implementação da segurança em toda a organização. Se necessário, um canal de aconselhamento especializado em segurança de informações deve ser estabelecido e disponibilizado dentro da organização. Contatos com especialistas em segurança externos devem ser desenvolvidos para acompanhar as tendências da indústria, monitorar padrões e métodos de avaliação e prover pontos de contato adequados para quando se lidar com incidentes de segurança. Um enfoque multidisciplinar quanto à segurança de informações deve ser encorajado; por exemplo, envolvendo a cooperação e colaboração de gerentes, usuários, administradores, projetistas de aplicações, auditores e equipe de segurança e especialistas em áreas tais como seguro e gestão de riscos. (Padrão Internacional ISO/IEC 17799, 2000, p. 3).

Portanto, tem como meta garantir uma estrutura de gestão para dar início, bem como controlar, a implementação da segurança da informação dentro de um ambiente

organizacional. Deve ser feita a realização de fóruns para análise e aprovação da política de segurança, de forma que sejam atribuídas as funções da segurança para garantir uma melhor coordenação da mesma.

No capítulo em questão será abordada a importância da segurança em ambientes corporativos.

2.1 Fatores a Serem Protegidos

Dentro de um Ambiente Organizacional, constituído de redes de computadores, existe uma série de fatores que são de suma importância para o desenvolvimento das atividades empresariais. Fatores estes que, em muitos casos secretos ou indispensáveis para as funções desempenhadas pelas empresas, não podem correr certos riscos de serem perdidos, corrompidos ou mesmo cair em mãos de pessoas que não deveriam ter acesso a tal informação. Tais fatores são:

- Proteção dos Dados – São as informações contidas nas máquinas da Empresa;
- Proteção dos Recursos – São as máquinas, banda da rede, entre outros.
- Proteção da Reputação – Diz respeito ao nome da empresa, sua reputação. (PEREIRA, 2002)

2.1.1 Proteção dos Dados

Segundo consta na norma,

> **2.1 Segurança de informações**
> Preservação da confidencialidade, integridade e disponibilidade das informações.
> **- Confidencialidade**
> Garantir que as informações sejam acessíveis apenas para aqueles que estão autorizados a acessá-las.
> **- Integridade**
> Salvaguardar a exatidão e a inteireza das informações e métodos de processamento.
> **- Disponibilidade**
> Assegurar que os usuários autorizados tenham acesso às informações e aos ativos associados quando necessário. (Padrão Internacional ISO/IEC 17799, 2000, p. 1).

O banco de dados, ou seja, as informações mais importantes contidas dentro de uma empresa são geralmente os alvos de maior risco e preocupação dentro de um ambiente corporativo. Para evitar os riscos com essas informações, as empresas isolam as máquinas que contém esses dados dentro da rede interna, de forma que máquinas externas a rede não tem acesso a elas.

No entanto, torna-se insuficiente apenas isolar essas informações, atendendo ao pilar da confidencialidade, a partir do momento em que se esquece que existem outros dois aspectos que precisam ser contemplados. Trata-se da integridade e da disponibilidade. Se uma informação precisa ser isolada é porque se trata de algo fundamental e secreto para a organização, e assim sendo, é necessário que esteja protegida para que permaneça íntegra e não sofra nenhuma alteração, bem como disponível para aquele usuário que tem livre acesso a ela quando se fizer necessário.

2.1.2 Proteção dos Recursos

A maioria dos ambientes corporativos, atualmente, é dotada de alguns recursos que são essenciais no desempenho de suas atividades. No caso em questão, de que se trata este

trabalho, as pequenas Empresas de Informática, que prestam serviços através de seus cursos especializantes, são dotadas de inúmeros recursos sem os quais sacrificaria bastante o seu desempenho no mercado.

Para que uma informação esteja bem protegida dentro de um ambiente de redes de computadores, é necessário que se isole a máquina que contem estas informações de todos os fatores externos a esta rede, bem como fatores internos a ela. Essa prática se faz necessária, pois se alguém de fora da Empresa, ou mesmo uma pessoa que é parte integrante da empresa, mas que, no entanto, não tem os respectivos privilégios de acesso aquela informação, tente fazer uso daquela informação de alguma forma, a mesma estará resguardada em um ambiente seguro. Desta forma, quando se fala em recursos remete-se aos computadores que possuem dados importantes e secretos, aos acessos à rede, etc.

Outro recurso muito importante para uma Empresa de Informática é a sua banda de acesso a Internet. Muitos cursos ministrados nesses Centros de Informática precisam de uma largura de banda boa para desempenhar certas atividades específicas, como o curso de Web Designer por exemplo. Entretanto, existem alguns alunos que durante as aulas tentam ficar utilizando a banda da rede para baixar músicas, filmes, seriados entre outros arquivos que são extremamente pesados e que, de fato, comprometem o desempenho e velocidade dos acessos.

Enfim, a segurança sobre os recursos de uma empresa não se caracteriza apenas por impedir que um usuário indesejado acesse as máquinas principais para roubar, alterar, ou mesmo apagar dados do sistema. É importante garantir, também, que esses usuários não utilizem dos recursos de que a organização dispõe a favor de seus benefícios próprios.

2.1.3 Proteção da Reputação

A reputação é o que representa, no caso em questão, uma organização dentro de um ambiente relacional. É o nome da Empresa, ou seja, é a avaliação da sociedade em relação às atividades desempenhadas por uma organização. Desta forma, para toda corporação é de extrema importância que sua reputação esteja sempre limpa diante dos olhos do mercado em

que atua. Mas para tal, é preciso que se tenha uma ótima política de segurança tanto externa quanto interna, para garantir que este aspecto não seja abalado.

Fatores bem simples podem contribuir para a perda de reputação de uma empresa. Um simples exemplo disso é o caso de um invasor que tem problemas pessoais com a empresa ou com alguém que faz parte da mesma e manda e-mails ofendendo pessoas em nome da organização.

Nesse sentido existem dois tipos de invasores: externos e internos. Existe possibilidade de um invasor externo forjar um e-mail em nome de uma empresa sem ter acesso ao site. No entanto, se realmente for uma mensagem falsa advinda de fora do site torna-se mais fácil de comprovar sua ilegitimidade. Quando o invasor é interno e, por assim ser, tem acesso direto a máquina de e-mail, a mensagem que for enviada por ele será tal como uma mensagem legítima.

Portanto, esse é um simples exemplo de como a reputação de uma empresa precisa de políticas de segurança que garantam que seu nome não seja ferido através de certos atos de pessoas maliciosas.

2.2 Ameaças

O surgimento da internet foi algo extraordinário para o cenário das telecomunicações mundiais. Este meio foi capaz de globalizar e distribuir uma gama de informações importantes para os mais diversos ramos do mundo todo. Desta forma, a internet tornou-se o meio mais prático e rápido utilizado pelas pessoas para se relacionarem globalmente, seja na busca por informações ou na necessidade de comunicação. No entanto, existem algumas informações que precisam de cuidados especiais, são sigilosas, extremamente importantes para àqueles que as preservam e, se por ventura, caírem em mãos erradas podem resultar em prejuízos muitas vezes irreparáveis. É neste ambiente que surgem os chamados crackers.

Os próximos tópicos apresentarão as ameaças e riscos fornecidos pelos tão famosos crackers.

2.2.1 *Malwares*

Segundo Fernando Melis Neto,

> A expressão "*Malware*" nasceu da justaposição das palavras *Malicious Software* (programas maliciosos) e é utilizada quando se pretende fazer referências genéricas a pragas virtuais. (NETO, 2005, p. 13)

De acordo com a Cartilha sobre Segurança na Internet desenvolvida pelo CERT.Br,

> Código malicioso ou *Malware (Malicious Software)* é um termo genérico que abrange todos os tipos de programa especificamente desenvolvidos para executar ações maliciosas em um computador. Na literatura de segurança o termo *malware* também é conhecido por "*software* malicioso".[1]

Desta forma, um *malware* é caracterizado por todo e qualquer *software* que mesmo que desempenhe tarefas interessantes para um determinado público de usuários, são executados, também, alguns algoritmos com funções maliciosas.

Dentre estes softwares podemos citar: Vírus, Worms, Cavalo de Tróia, Adware e Spyware.

2.2.2 Invasões

São as práticas utilizadas pelos crackers. Esses quando invadem corporações ou máquinas buscam por informações confidenciais como números de conta, senhas de banco, dados pessoais, etc. As práticas dos crackers, desde o momento que passaram a ser desempenhadas, nunca mudou, apenas aperfeiçoam-se. Segundo pesquisa, no ano de 2008 no

[1] Texto extraído da Cartilha de Segurança para Internet, desenvolvida pelo CERT.br, mantido pelo NIC.br, com inteiro teor em http://cartilha.cert.br/. Parte I: Conceitos de Segurança. **Pag**. 9

Brasil, foram notificados 327 ataques de invasão propriamente ditos, fora as intenções referentes à scaneamento de portas que somaram 43822 ataques. (CERT.Br, 2008)

Dentre alguns métodos de intrusão que de forma direta ou indireta, configuram tentativas de invasão de redes e sistemas, tem-se: Varredura de portas, *Spoofing*, *Sniffer* e *DoS* (*Denial of Service* – Negação de Serviço).

A varredura de portas é classificada como um ataque de coleta de informações. Todo ataque de coleta de informações, diretamente, não causa nenhum dano ao sistema atacado, pois consiste exclusivamente na coleta de informações necessárias para se realizar uma invasão de fato.

Segundo o livro "Segurança Máxima":

> O spoofing pode ser resumido em uma única frase: é uma técnica sofisticada de autenticar uma máquina para outra forjando pacotes de um endereço de origem confiável. (ANÔNIMO, 2001, p. 96)

O spoofing permite a comunicação entre duas máquinas através de uma autenticação forjada. Portanto, para entrar em detalhes de como ocorre o ataque de spoofing é preciso se reportar a dois aspectos de extrema importância para segurança na internet, confiança e autenticação. O livro "Segurança Máxima" (ANÔNIMO, 2001), define confiança como a relação entre máquinas que possuem acesso autorizado entre si, e autenticação a forma com que essas máquinas utilizam para se identificarem.

O *Sniffer* ou *packet sniffing*, é classificado como um ataque para obtenção e coleta de informações acerca de uma máquina alvo, de preferência, de forma imperceptível, para se caracterizar como um ataque de sucesso. (GEUS; NAKAMURA, 2003)

Por ultimo, têm-se os famosos ataques de Negação de Serviço. GEUS e NAKAMURA fizeram a seguinte definição no livro "Segurança de Redes em Ambientes Cooperativos, 2003":

> Os ataques de negação de serviços (*Denial-of-Service Attack* – DoS) fazem com que recursos sejam explorados de maneira agressiva, de modo que usuários legítimos ficam impossibilitados de utilizá-los. (GEUS;NAKAMURA, 2003, p.87).

Para o Anônimo que escreveu “Segurança Máxima”:

> A negação de serviço é a categoria de ataques que causa uma perda de serviço ou uma incapacidade de funcionamento. Esses ataques surgem de muitas formas e atacam muitos alvos diferentes. Os resultados podem durar minutos, horas ou dias e influenciar o desempenho da rede, a integridade dos dados e a operação do sistema. (ANÔNIMO, 2001, p. 242).

Com base nas definições, o DoS se caracteriza na sobrecarga de uma máquina ou servidor com excessivas solicitações de serviço no objetivo de congestioná-la e causar a tão famosa negação de serviço.

Lógico que esse conceito foi estabelecido de forma abrangente. Os ataques de negação de serviço são explorados dos defeitos de programação em softwares. O funcionamento da negação de serviço se dá por meio de uma das três formas: Através do consumo de largura de banda, através da saturação de recursos ou da queda de sistema e aplicativo. (ANÔNIMO, 2001)

2.2.3 Panorama Atual

As diversas ameaças e ataques abordados estão presentes no mundo das comunicações virtuais, o mundo da informática. Este ambiente tornou-se extremamente importante, porque foi capaz de globalizar e unificar todas as relações mundiais nos mais diversos ramos. A informática cresceu e se difundiu em praticamente todos os setores automatizando as atividades empresariais, bem como permitindo que essas empresas estabelecessem contatos entre si através da maior rede mundial de comunicação, a internet. Entretanto, junto com tantos benefícios e facilidades surgiram grandes dificuldades em aspectos de segurança.

As mesmas pragas virtuais abordadas neste capítulo continuam assombrando as redes de computadores do mundo inteiro através da internet. Alexandre Freire em seu artigo “A Convergência das Tecnologias de Proteção de Perímetros, 2009” revela que segundo indicadores de institutos como SANS e CERT é possível visualizar o aumento da quantidade de códigos maliciosos trafegados na internet que contribuem para o aumento do número de

contaminações de máquinas de usuários ou corporações. As pragas virtuais são, entre algumas variações, as mesmas como: vírus, worms, cavalos-de-tróia, spywares, phishing, entre outras. Para Alexandre, a causa dos principais problemas de segurança é a falta de conhecimentos por parte dos usuários domésticos, ou corporativos, sobre os malwares que se proliferam cada vez mais a cada dia. Outro ataque, atualmente em evidência, segundo o artigo, é o chamado ataque de negação distribuído, uma variante do DoS (Denial of Service – Negação de Serviço).

Em artigo publicado pela redação da iMasters consta que segundo relatório da McAfee acerca de spam, empresas pelo mundo inteiro pagam altos custos gerados por essa ameaça. Segundo pesquisa, os ataques de spam, em média, podem custar US$ 182. 500 dólares anualmente. O artigo faz a seguinte citação:

> "O spam está custando às empresas mais do que elas imaginam. Por isso, é mais importante que nunca que elas se protejam contra esse tipo de ameaça", diz Jeff Green, vice-presidente sênior do McAfee Avert Labs.[2]

Outro artigo que chamou bastante atenção foi o "Conficker: o que muda depois do super-vírus, 2009", de Vicente Sloboda. O artigo relata que o mundo das comunicações virtuais foi afetado em dimensões alarmantes poucas vezes vistas, por infecções decorrentes de vírus de computador. Muitas empresas pararam suas atividades e de acordo com as previsões de alguns, não restabelecerão facilmente por determinado período. A causa desse desastre é o novo vírus Downad, também conhecido como Conficker ou Kido. Segundo o artigo, o vírus tornou-se um verdadeiro pesadelo para segurança organizacional em função de sua versatilidade, variedade de métodos de infecção e extrema dificuldade de remoção. Por isso, foram receitadas algumas providencias para reduzir ou evitar este tipo de ataque, que com certeza é a nova tendência, tais como: Atualizações de segurança regulares, usuário logado sem privilégios de administrador, investimento em antivírus, padronização de hardware e software, preferência no uso da plataforma Linux ao invés de Windows, etc. (SLOBODA, 2009)

---

[2] Texto extraído do Artigo "Spam custa anualmente às empresas mais de 180 mil dólares", redigido pela equipe de Redação iMasters, disponível em: http://imasters.uol.com.br/noticia/12036/seguranca/spam_custa_anualmente_as_empresas_mais_de_180_mil_dolares/. Acesso em: 08/03/2009.

2.3 Ferramentas de Segurança

Foi visto nas seções anteriores, que o surgimento da internet trouxe uma série de benefícios para o mundo das comunicações mundiais. Atualmente, a internet estabeleceu-se como principal meio utilizado para troca de informações pelo mundo todo. As informações trocadas neste ambiente são as mais diversas, desde simples mensagens de afeto através de correios eletrônicos, até informações confidenciais, pessoais e intransferíveis. Desta forma, a necessidade de segurança passa a ser fazer presente.

Assim, ainda nas seções anteriores, foram abordadas as principais ameaças e riscos existentes na internet, tais como *malwares* e ataques de invasão. Cada ataque realizado na internet tem sua particularidade. Diferem em vários aspectos como métodos de infecção, formas de se replicar, objetivos, etc. Assim como diferem em seus métodos de intrusão, diferem na forma que são prevenidos e combatidos. Para cada tipo de ameaça existe um modelo de ferramenta responsável por combater os riscos por ela oferecidos.

As ferramentas de segurança mais utilizadas são o Antivírus, Antispam, IDS/IPS e o Firewall que será objeto de análise no capítulo 3.

2.3.1 Antivírus

Segundo a "Cartilha de Segurança para Internet" desenvolvida pelo CERT.Br a definição de antivírus é:

> Os antivírus são programas que procuram detectar e, então, anular ou remover os vírus de computador. Atualmente, novas funcionalidades têm sido adicionadas aos programas antivírus, de modo que alguns procuram detectar e remover cavalos de tróia e outros tipos de código malicioso, barrar programas hostis e verificar e-mails.[3]

[3] Texto extraído da Cartilha de Segurança para Internet, desenvolvida pelo CERT.br, mantido pelo NIC.br, com inteiro teor em http://cartilha.cert.br/. Parte II: Riscos Envolvidos no Uso da Internet e Métodos de Prevenção. **Pág**. 8

Através da definição acima mencionada, pode-se dizer que antivírus são programas responsáveis por detectar vírus e realizar algumas ações específicas como anular ou removê-los de um computador.

A "Cartilha de Segurança para Internet" do CERT.Br enumera algumas funcionalidades que um bom antivírus deve possuir, tais como:

> - identificar e eliminar a maior quantidade possível de vírus e outros tipos de malware;
> - analisar os arquivos que estão sendo obtidos pela Internet;
> - verificar continuamente os discos rígidos (HDs), flexíveis (disquetes) e unidades removíveis, como CD, DVDs e pen drivers, de forma transparente ao usuário;
> - procurar vírus, cavalos de tróia e outros tipos de malware em arquivos anexados aos e-mails;
> - criar, sempre que possível, uma mídia de verificação (disquete ou CD de boot) que possa ser utilizado caso um vírus desative o antivírus que está instalado no computador;
> - atualizar as assinaturas de vírus e malwares conhecidos, pela rede, de preferência diariamente.[4]

Enfim, o termo antivírus, no campo da informática, transmite a idéia de um software responsável por detectar e eliminar vírus de um computador. Entretanto, como foi visto o antivírus não protege seu sistema apenas contra vírus. Ele também protege contra diversos tipos de malwares criados diariamente, como spyware, adware, rootkits, cavalos de tróia, etc. Desta forma, cabe ao usuário procurar por uma ferramenta antivírus com ótima aceitação no mercado e que se atualize diariamente. Só assim, será capaz de realizar suas atividades pela internet com o mínimo de segurança recomendado.

[4] Texto extraído da Cartilha de Segurança para Internet, desenvolvida pelo CERT.br, mantido pelo NIC.br, com inteiro teor em http://cartilha.cert.br/. Parte II: Riscos Envolvidos no Uso da Internet e Métodos de Prevenção. **Pág**. 8

2.3.2 Anti Spam

De acordo com a "Cartilha de Segurança para Internet" elaborada pelo CERT.Br:

> *Spam* é o termo usado para se referir aos *e-mails* não solicitados, que geralmente são enviados para um grande número de pessoas. Quando o conteúdo é exclusivamente comercial, este tipo de mensagem também é referenciada como UCE (do inglês *Unsolicited Commercial E-mail*).[5]

Por meio das definições acima mencionadas, o spam é caracterizado pelo recebimento de e-mails não solicitados. No entanto, existem vários tipos de spam com características particulares.

O Antispam.br que faz parte do Comitê Gestor da Internet no Brasil estabelece os tipos de spam da seguinte forma:

- Correntes (chain letters)
- Boatos (hoaxes) e lendas urbanas
- Propagandas
- Ameaças brincadeiras e difamação
- Pornografia
- Códigos maliciosos
- Fraudes
- Spit e spim
- Spam via redes de relacionamento[6]

O spam é uma prática muito freqüente na Internet. Como foi em seção anterior, muitas empresas perdem grandes quantias financeiras em conseqüência deste tipo de ataque. Fora os incômodos proporcionados ao usuário com suas caixas postais eletrônicas abarrotadas de mensagens não solicitadas impedindo o recebimento de mensagens legais e importantes. Sem dúvida, o spam, assim como os malwares, é um dos ataques mais usuais realizados na internet, porém, se forem utilizadas as devidas precauções, como as enumeradas acima,

---

[5] Texto extraído da Cartilha de Segurança para Internet, desenvolvida pelo CERT.br, mantido pelo NIC.br, com inteiro teor em http://cartilha.cert.br/. Parte IV: *Spam*. **Pág**. 3

[6] Comitê Gestor da Internet no Brasil – Antispam.br. **Tipos de spam** Disponível em: http://www.antispam.br/tipos/. Acesso em: 03.04.2009.

elaboradas pelo Antispam.Br, evitar-se-ia em grandes proporções os índices de freqüência relacionadas a este tipo de ataque.

2.3.3 IDS e IPS

De acordo com o livro “Firewalls e Segurança na Internet”

> Há vários tipos de sistemas de detecção de intrusão. Os *IDSs de rede* (NIDSs) bisbilhotam o tráfego da rede, procurando indicação de uma invasão. Vários sistemas baseados em host examinam arquivos ou trafego em busca de vírus recebidos; alguns analisam padrões de chamada de sistema ou procuram por arquivos alterados. (CHESWICK; BELLOVIN; RUBIN, 2005, p. 271)

O IDS é responsável por analisar e detectar possíveis invasões ou comportamentos anômalos dentro de uma rede, principalmente em um ambiente organizacional. Se tais anomalias forem detectadas, este sistema é capaz de fornecer aos administradores da rede todas as possíveis tentativas de ataques ou invasões. Dentro de um ambiente organizacional, torna-se muito útil, também, contra possíveis invasores internos. (GEUS; NAKAMURA, 2003)

No entanto, apesar de ser uma ferramenta essencial para defesa contra invasões, o IDS é somente capaz de detectar as intrusões, de forma que o administrador tem que analisar as formas cujas quais está sendo atacado, e realizar ações para impedir aquele ataque. Portanto, seria interessante existir uma ferramenta que além de detectar tais intrusões, pudesse preveni-las evitando-as antes que ocorram. Para isso foi criado o sistema de prevenção de intrusão, IPS (*Intrusion Prevention System*).

Para Neil (DESAI, 2003), IPS é qualquer dispositivo (hardware ou software), que tem a capacidade de detectar ataques, ambos conhecidos ou desconhecidos, e impedir que o mesmo seja bem sucedido.

Muitos autores classificam o IPS como uma evolução do IDS pelo fato de realizar medidas preventivas contra as invasões. Assim como, existem outros autores, que devido ao

fato do IPS realizar medidas preventivas, estabelecem que o IPS deva ser classificado de forma diferente do IDS.

Entretanto, para implementar um IDS e, principalmente um IPS, dentro de um ambiente de rede precisa-se tomar alguns cuidados fundamentais para evitar certos equívocos. Esses equívocos são conhecidos como falso positivo e falso negativo.

Ocorre falso positivo quando o sistema de detecção de intrusão encontra um evento lícito dentro de um segmento de rede e o atribui como um ataque real. (CALETTI, 2006)

É ocasionado falso negativo, quando há algum ataque em procedimento ou realizado com sucesso e o sistema de detecção de intrusão detecta como uma atividade normal da rede. (CALETTI, 2006)

Enfim, os sistemas de detecção e prevenção de intrusão são ferramentas essenciais para o bom andamento e segurança de uma rede. Como foi visto, o IDS consegue apenas detectar e alertar tentativas de invasões. Cabe ao administrador da rede, com base na detecção, tomar as devidas ações para impedir eventual ataque. Porém, existe o IPS responsável por, não apenas detectar intrusões, assim como agir com medidas preventivas para evitar que elas ocorram. O mais importante de tudo, independente de qual ferramenta esteja em uso, é que o IDS ou IPS estejam devidamente configurados dentro da rede, de modo que possam detectar ou coagir simplesmente os ataques reais, e não deixar que eventos lícitos sejam confundidos com ataques e bloqueados por conseqüência.

2.3.4 Firewall

Segundo o livro “Firewalls e Segurança na Internet”

> Definimos um firewall como uma coleção de componentes colocados entre duas redes que coletivamente têm as seguintes propriedades:
>
> - Todo tráfego de dentro para fora, e vice-versa, deve passar pelo firewall.
> - Apenas tráfego autorizado, como definido pela política de segurança local, terá permissão de passar.
> - O próprio firewall é imune a penetrações. (CHESWICK; BELLOVIN; RUBIN, 2005, p. 32).

O firewall, sem dúvida, é uma das ferramentas de segurança mais importantes dentro de um ambiente de rede, principalmente, dentro de um ambiente organizacional. A maioria dos ambientes corporativos, por que não dizer todos, possui suas redes internas, onde armazenam certos dados de extrema importância para o desenvolvimento de suas atividades. Geralmente, essas corporações precisam que suas máquinas tenham acesso à Internet, para realizar certas operações que vão desde a necessidade de comunicação até operações bancárias. Como toda operação na internet conta com riscos, as empresas devem possuir alguma ferramenta que seja capaz de isolar sua rede interna da internet, como forma de se ver livre dessas ameaças. É nesse contexto que surge a necessidade de se ter um firewall.

O firewall é uma das ferramentas mais antigas e conhecidas para segurança de redes. Não existe um ambiente de rede razoavelmente seguro, se não houver um firewall. Um firewall pode ser entendido como um dispositivo de hardware ou software, localizado entre pelo menos duas redes, capaz de controlar, autenticar e guardar em *logs* todo o tráfego que entre elas circula. (GEUS; NAKAMURA, 2003)

Este tópico propõe citar a importância da utilização de um firewall como ferramenta de segurança. Não há como falar em ferramentas de segurança de redes, sem abordar a necessidade de se implementar um firewall como ponto de partida para a implantação de uma boa política interna de segurança. Como este trabalho é voltado diretamente para segurança de redes em ambientes organizacionais através da implementação de uma interface de supervisionamento de firewall, em específico Iptables, torna-se necessário a abordagem da ferramenta firewall em um único capítulo separado. Desta forma, o próximo capítulo trará as principais abordagens sobre esta ferramenta.

3 FIREWALLS

No capítulo anterior, foram citadas algumas definições do que é um firewall. Mas o termo firewall, segundo GEUS e NAKAMURA (2003), vem sofrendo algumas modificações com o passar do tempo, em função da própria evolução desta ferramenta.

Por ser um dos componentes mais utilizados e mais antigos de segurança de redes, sempre se criou uma expectativa muito grande em relação à proteção que o firewall proporciona. Antes, pensava-se que um firewall era a ferramenta de segurança capaz de proporcionar todas as condições necessárias para manter um ambiente de rede totalmente seguro. Com o passar do tempo, à medida que foram avaliadas questões como desempenho, mercado, testes e problemas encontrados, percebeu-se que o firewall, sozinho, não garante a total segurança de um ambiente organizacional. (GEUS; NAKAMURA, 2003)

No entanto, podemos pensar que o firewall é o ponto de partida para a implantação de uma boa política interna de segurança. Os próximos tópicos abordarão diversas questões a respeito dessa ferramenta, tais como sua importância, problemas que não podem ser resolvidos pelo firewall, os tipos de firewalls existentes, bem como as características e particularidades de cada um deles.

3.1 A Importância de um Firewall

Para Humberto Jucá (2005),

> O termo “firewall”, em português, quer dizer, “parede/muro de fogo” e sua função é barrar os acessos indesejados. A partir de uma política de segurança bem definida, estabelecemos as regras de acesso, definindo o que será acessado e por quem. Um firewall não deve ser encarado apenas como uma máquina que faz filtros, mas sim como um conjunto de ferramentas que ampliam a segurança de sua rede (segundo a política de segurança), e precisa ser constantemente “acompanhado”. (JUCÁ, 2005, p. 15).

Para GEUS e NAKAMURA (2003), o firewall é um ponto único entre duas ou mais redes, sendo um componente ou um conjunto de componentes, por onde ronda todo o tráfego, capaz de realizar o controle e a autenticação desse tráfego. Sua importante função é:

> Esse ponto único constitui um mecanismo utilizado para proteger, geralmente, uma rede confiável de uma rede pública não confiável. O firewall pode ser utilizado também para separar diferentes sub-redes, grupos de trabalho ou LANs dentro de uma organização. (GEUS; NAKAMURA, 2003, p. 207).

Portanto, a importância da utilização de um firewall está ligada diretamente a sua definição. Se imaginarmos uma organização que presta serviços a população, como bancos, locadoras de automóveis, locadoras de vídeos, etc., sabe-se que esse tipo de empresa sempre tem guardado certos dados do cliente como forma de garantir sucesso e segurança na realização de suas funções. Com o surgimento da Internet, a maioria das empresas passaram a disponibilizar seus serviços por meio de sites, como forma de simplificar a vida do cliente, assim como atrair nova clientela no mercado. Entretanto, a Internet assim como trouxe inúmeros benefícios, trouxe, também, inúmeros riscos.

Se eventualmente, alguma dessas empresas sofresse um ataque que as fizesse perder dados e informações fundamentais sobre seus clientes, na certa isso iria trazer prejuízos enormes para suas atividades, bem como para sua reputação no mercado.

Assim, criou-se a necessidade de que as organizações separassem seus bancos de dados da internet. Para isso, as empresas dividiram sua rede em interna (banco de dados e informações) e externa (internet). No entanto, não bastava apenas dividir a rede. Era necessário que entre a rede interna e a rede externa houvesse alguma ferramenta de segurança capaz de realizar a filtragem dos acessos permitidos e não permitidos entre as mesmas. Para isso, criou-se o firewall.

3.2 Limitações

Primeiramente, é importante se ter consciência de que um firewall faz parte de um conjunto de ferramentas de segurança necessário dentro de um ambiente organizacional. Isso quer dizer, ao contrário do que muitos dizem, que o firewall, somente, não é capaz de assegurar a segurança total de uma organização.

Na verdade, como já foi dito, o firewall é o ponto de partida para a adoção de uma boa política de segurança. Assim, fica claro que o firewall é a primeira base de defesa, o que torna essencial a sua presença dentro de uma infra-estrutura envolvendo segurança de redes. Por ser a primeira base de defesa, o firewall tem por objetivo bloquear todos os acessos suspeitos, que não condizem com a política de segurança da corporação. (GEUS; NAKAMURA, 2003)

Segundo CHESWICK, BELLOVIN e RUBIN (2005)

"Os firewalls são inúteis contra ataques internos." (CHESWICK; BELLOVIN; RUBIN, 2005, p. 194).

Os firewalls são capazes, embora não totalmente, de garantir a segurança das informações e recursos da rede interna de uma organização contra ataques originados da rede externa. Desta forma, a rede interna é objeto de proteção do firewall e não caracteriza uma ameaça. Assim, a afirmação de Cheswick, Bellovin e Rubin é completamente pertinente, e caracteriza exatamente um problema que os firewalls não podem resolver.

Os ataques internos podem ser feitos tanto por usuários legítimos insatisfeitos, assim como por alguma pessoa que obteve acesso a uma máquina interna por outros meios. Além dessas duas formas, se alguma máquina for infectada por um código malicioso adquirido por meio de uma mensagem de correio eletrônico, ou mesmo por exploração de um estouro de *buffer* na máquina, da mesma maneira será considerado como um ataque de procedência interna. (CHESWICK; BELLOVIN; RUBIN, 2005)

A carência de segurança contra ameaças internas presente nos firewalls levou algumas empresas a adotarem regimentos com procedimentos mais sérios em relação a estes tipos de

ameaças. As empresas que possuem sérios riscos de ataques de pessoal, como bancos, por exemplo, monitoram freqüentemente suas redes internas, com todo cuidado, e desmontam as máquinas dos usuários quando existe alguma espécie de suspeita. Eles buscam pelos prejuízos causados por essas pessoas. (CHESWICK; BELLOVIN; RUBIN, 2005)

De acordo com Cheswick, Bellovin e Rubin (2005)

> Se seu *firewall* é seu único mecanismo de segurança e alguém entra por algum outro mecanismo, você está com problemas. (CHESWICK; BELLOVIN; RUBIN, 2005, p. 195).

Ainda, segundo eles

> A noção de um exterior impiedoso e selvagem com um interior tranqüilo e civilizado [Cheswick, 1990] somente fornece segurança se não houver maneira alguma de entrar no interior. Hoje, isso pode ser irreal. (CHESWICK; BELLOVIN; RUBIN, 2005, p. 195).

Pelas citações acima, evidenciamos que o firewall não é capaz de assegurar segurança total a qualquer ambiente organizacional por si só.

Além das limitações citadas, temos que lembrar que o equipamento também possui vulnerabilidades

- **Firewall-1** – Foi descoberto, em maio de 1998, que esta ferramenta tinha diversas palavras-chaves pré-definidas, que se eventualmente fossem utilizadas como objeto de rede, automaticamente abriam diversas possibilidades de intrusão.
- **Ipchains** – Em julho de 1999, foram encontrados alguns problemas no código de firewall do Linux, que permitiam que invasores remotos pudessem enviar dados para portas supostamente bloqueadas.
- **Network Associates Gauntlet** – Em maio de 2000, descobriu-se um estouro de buffer nesta ferramenta, possibilitando aos invasores a execução de código malicioso no firewall. Posteriormente, descobriu-se que o problema não era parte integrante do código original do firewall, e que na verdade foi introduzido pelo sistema de filtragem de conteúdo que a NAI havia integrado aos produtos Gauntlet.

- Em junho de 2000 descobriram que um ataque de negação de serviço utilizando pacotes fragmentados, foi capaz de tornar indisponível todos os firewalls Checkpoint Firewall-1. Ainda neste mesmo mês e ano, John Mcdonald e Thomas Lopatic destacaram diversas vulnerabilidades encontradas no Firewall-1.

(ANÔNIMO, 2001).

3.3 Tipos de Firewall

As tecnologias de firewall evoluíram bastante, desde os primeiros anos de surgimento da internet. Atualmente, é possível comprar excelentes dispositivos e construí-los fazendo uso de software livre. Mesmo se houver a necessidade de pagar por um firewall, o usuário poderá contar com interfaces sofisticadas, assim como obter uma ferramenta com excelente capacidade de filtragem em nível de aplicação. Outra vantagem é a obtenção de suporte técnico, caso haja necessidade, item cujo qual não será disponível se a ferramenta tiver sido projetada por conta própria. (CHESWICK; BELLOVIN; RUBIN, 2005)

Os firewalls são capazes de realizar a filtragem de pacotes em diferentes níveis dentro de uma pilha de protocolos de rede. Dessa forma, existem diversos tipos de firewalls e recursos. O livro "Segurança Máxima" destaca alguns desses recursos:

- **Filtragem de conteúdo.** Algumas organizações querem que seus usuários parem de navegar por determinados sites da Web: sites de correio eletrônico baseados na Web, sites "underground", portais de compra e venda de ações, sites com pornografia e assim por diante. Os recursos e serviços de filtragem de conteúdo podem ajudar a bloquear esses sites, bem como a proteger contra alguns tipos de códigos e applets hostis baseados em Java e ActiveX.
- **Virtual Private Networking (VPN).** As VPNs são utilizadas para envelopar tráfego seguramente do ponto A para o ponto B, normalmente em redes hostis (como a Internet). Embora haja um amplo espectro de appliances de VPN dedicados no mercado hoje, fornecedores como a Checkpoint e a Cisco estão alegremente integrando os serviços de VPN em suas promoções de firewall. Muitos produtos de firewall agora oferecem funcionalidade de VPN tanto de cliente para empresa como de rede local para rede local.
- **Network Address Translation (NAT).** A conversão de endereço de rede (Network Address Translation – NAT) é freqüentemente utilizada para mapear blocos de endereços ilegais ou reservados (veja a RFC 1918) para aqueles válidos (por exemplo, mapear 10.0.100.3 para 206.246.131.227). Embora a

> NAT não seja necessariamente um recurso de segurança, os primeiros dispositivos de NAT que aparecem em ambientes corporativos normalmente são produtos de firewall.
> - **Equilíbrio de carga.** Mais genérico que qualquer outro termo, equilíbrio de carga é a arte de segmentar tráfego de maneira distribuída. Embora o equilíbrio de carga de firewall seja uma coisa, alguns produtos de firewall agora estão suportando recursos que ajudarão a direcionar trafego de Web e trafego de FTP de uma maneira distribuída.
> - **Tolerância a falhas.** Alguns firewalls mais sofisticados como o Cisco PIX e a combinação de Nokia/Checkpoint suportam alguns recursos de tolerância a falhas relativamente complexos. Muitas vezes referido como funcionalidade de alta disponibilidade (High-Availability – HA), os recursos de tolerância a falhas avançados com freqüência permitem que os firewalls executem em pares, com um dispositivo funcionando como um "hot standby" ("reserva instantânea") se o outro falhar.
> - **Detecção de invasão.** O "termo detecção de invasão" pode significar muitas coisas, mas, nesse caso, alguns fornecedores estão começando a integrar um tipo inteiramente diferente de produto com suas promoções de firewall. Embora isso não represente um problema por si só, as pessoas devem estar cientes do tipo de carga de trabalho que isso poderia impor ao firewall. (ANÔNIMO, 2001, p. 153).

Como foi dito e citado, existem diversos tipos de Firewall com seus respectivos recursos. Este capítulo pretende abordar três deles: Firewall baseado em Proxy, Firewall NAT e Firewall Filtro de Pacotes.

3.3.1 Firewall NAT

À medida que foram sendo construídas grandes empresas de informática passou a haver uma demanda por endereços IP privados muito maior que a própria capacidade disponibilizada pelas classes de endereços privados. Esse problema precisava ser solucionado de alguma forma, então, criou-se o NAT (*Network Address Translation*).

O NAT é capaz de converter os endereços IP da rede interna privados em endereços IP públicos únicos utilizados para navegação na internet. Portanto, embora esta ferramenta tenha sido criada para disponibilizar uma gama maior de endereços IP privados para rede interna, observou-se que aliado a isso o NAT trouxe um aspecto relativo à segurança tão importante quanto o objetivo real de sua criação: a capacidade de ocultar os hosts da rede interna. (STREBE; PERKINS, 2002)

De fato, o NAT consegue omitir todas as informações dos hosts internos em nível de TCP/IP, dando a impressão de que todo o tráfego é oriundo de um único endereço IP, apenas. Além disso, o NAT permite que seja usado qualquer intervalo de endereço IP na rede interna, mesmo que esse endereço já esteja sendo utilizado por outro host na Internet. (STREBE; PERKINS, 2002)

De acordo com GEUS e NAKAMURA (2003)

> O NAT não foi criado com a intenção de ser usado como um componente de segurança, mas sim para tratar de problemas em redes de grande porte, nas quais a escassez de endereços IP representa um problema. Dessa maneira, a rede interna pode utilizar endereços IP reservados (*Request For Comments*, RFC 1918), sendo o NAT o responsável pela conversão desses endereços inválidos e reservados para endereços válidos e roteáveis, quando a rede externa é acessada. Sob o ponto de vista da segurança, o NAT pode, assim, esconder os endereços dos equipamentos da rede interna e, conseqüentemente, sua topologia de rede, dificultando os eventuais ataques externos. (GEUS; NAKAMURA, 2003, p. 209-210).

3.3.1.1 Funcionamento

Para explicar o funcionamento do NAT será utilizado um exemplo retirado do livro "Firewalls" (STREBE; PERKINS, 2002).

Supõe-se que o host interno 10.1.1.7 deseja estabelecer uma conexão Web com o host externo 192.168.13.15. Portanto, utilizando a próxima porta disponível, 10.1.1.7:1234 envia um pacote TCP para 192.168.13.15:80.

Após isso, o endereço interno do roteador/Firewall recebe o pacote e registra da seguinte maneira em sua tabela de conversão:

Origem	10.1.1.7:1234
Host Público	192.168.13.15:80
Conversão	128.110.121.1:15465

Desta forma, o roteador/Firewall transmite o pacote pela Internet utilizando o endereço IP e o número convertidos, de forma que o 192.168.13.15:15465 recebe uma tentativa de conexão oriunda de 128.110.121.1:15465. No momento em que o host público responder, ele

transmitirá a resposta para a origem que ele pensa que originou o pacote: 128.110.121.1:15465 (correspondente ao endereço externo do Firewall).

Quando o Firewall recebe o pacote, ele verifica em sua tabela de conversão se existe um soquete correspondente e o encontra. Após isso, ele constata se a origem do pacote é, de fato, a mesma que a do host público encontrado na tabela de conversão no momento em que a entrada foi realizada. O fato de existir uma entrada na tabela ratifica que o pacote foi solicitado por um host interno. Assim, se não fosse encontrada nenhuma entrada registrada na tabela de conversão, o pacote seria descartado e a tentativa de conexão registrada.

Finalmente, o Firewall faz modificações no pacote com o número do soquete do cliente de origem interno e o passa para rede interna até que seja recebido pelo cliente final.

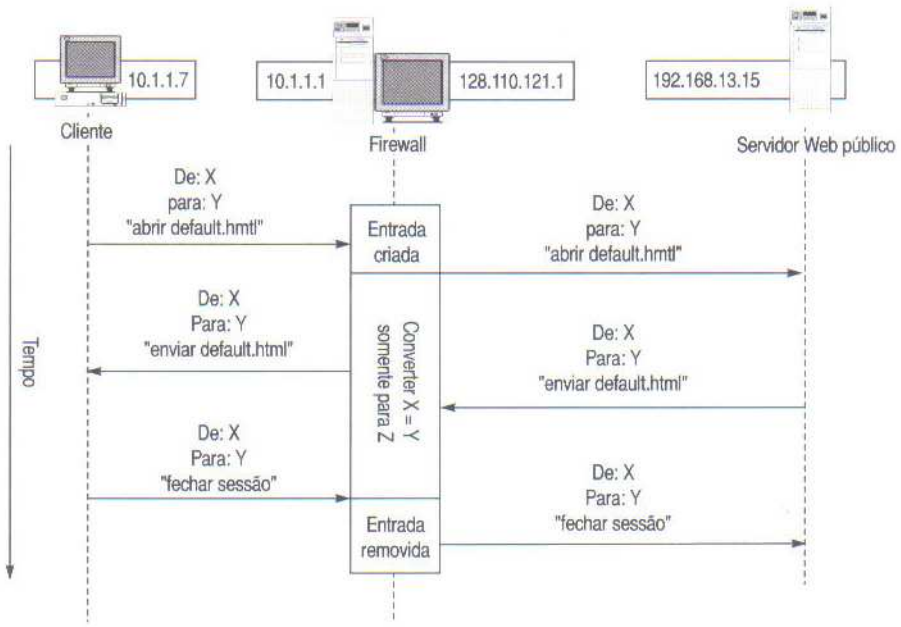

Figura 1: Nat. Fonte: (STREBE;PERKINS, 2002, p. 139).

3.3.1.2 Problemas

Existem alguns protocolos que não podem ser usados com o NAT, apesar de serem poucos, pois exigem a capacidade de que seja estabelecido um canal de retorno para o cliente, agregar a informação de endereço TCP/IP dentro do protocolo de mais alto nível, fazer

criptografia do cabeçalho TCP ou mesmo usar o endereço IP original para algum fim que se relacione à segurança. (STREBE; PERKINS, 2002)

De acordo com Matthew Strebe e Charles Perkins (2002), os principais problemas do NAT são:

> - Os canais de retorno não funcionam porque não existe nenhuma rota de retorno separada para os hosts internos. Isso acontece com a teleconferência de vídeo H.323.
> - Software que incorpora informações sobre o endereço TCP/IP dentro dos pacotes TCP/IP e depois depende dessa informação não funcionará porque as informações sobre o endereço TCP/IP no interior do pacote estarão incorretas.
> - Software que criptografa informações sobre o cabeçalho TCP não funcionará corretamente com a NAT porque a informação precisa estar acessível para o Firewall. Esses problemas podem ser resolvidos fazendo o Firewall ser o ponto final da criptografia. Isso ocorre com o PPTP.
> - Software que depende de informações sobre o endereço TCP/IP para verificação da segurança falhará porque a informação sobre o endereço IP terá sido alterada. Isso ocorre com o sqlnet2. (STREBE; PERKINS, 2002, p. 146).

Para os protocolos acima citados, é preciso utilizar um firewall capaz de inspecionar as conexões de saída e estabelecer uma entrada de conversão para aguardar a resposta do host externo de destino com o pedido de abertura do canal de retorno. A maioria dos firewalls não dá suporte à conversão NAT específica para serviços em geral. Eles utilizam um proxy específico para cada serviço auxiliado pelo NAT para realizar essas funções.

Enfim, a próxima seção abordará um dos modelos de firewall considerado dos mais sofisticados que trabalha em nível de aplicação, o firewall baseado em proxy.

3.3.2 Firewall baseado em Proxy

A função pela qual foram desenvolvidos os servidores proxy visava armazenar em cache todas as páginas Web que eram freqüentemente acessadas pelos usuários. Logo que a Internet surgiu, ainda nos seus primeiros meses de surgimento, os enlaces de longa distância remotos eram bastante lentos, existiam pouquíssimas páginas Web além de serem todas estáticas. A Internet era mais utilizada para o compartilhamento de sites Web entre cientistas e

acadêmicos. Dessa forma, o que ocorria era sempre que fosse adicionado algum elemento novo em algum site, diversos cientistas da mesma organização acessavam tal página. Assim, o site era armazenado em cache do servidor local da empresa, onde por meio do proxy todos os acessos a mesma página seriam eliminados por serem redundantes. (STREBE; PERKINS, 2002)

À medida que a Internet cresceu, juntamente com seus milhares de sites Web, a função original pela qual o proxy foi desenvolvido deixou de ser eficaz. Isto ocorreu devido ao fato do número de sites ter aumentado de forma explosiva e das páginas terem se tornado, na maioria, dinâmicas. Estes dois motivos representaram um problema de cache, realmente, muito complicado de ser resolvido. No entanto, assim como surgiram algumas dificuldades, também surgiram inovações. Dentre algumas delas, o proxy passou a ter o poder de ocultar todos os usuários reais de uma rede através de uma única máquina, realizar filtragem de URLs além de bloquear a passagem de conteúdo suspeito ou ilegal. (STREBE; PERKINS, 2002)

Segundo Matthew Strebe e Charles Perkins (2002)

> A finalidade principal da maioria dos servidores proxy atuais é operar como Firewall em vez de cache de páginas Web. (STREBE; PERKINS, 2002, p. 151).

Para GEUS e NAKAMURA (2003)

> Os *proxies* são sistemas que atuam como um gateway entre duas redes, permitindo as requisições dos usuários internos e as respostas dessas requisições, de acordo com a política de segurança definida. Eles podem atuar simplesmente como um *relay*, podendo também realizar uma filtragem mais apurada dos pacotes, por atuar na camada de aplicação do modelo *International Organization for Standadization/Open Systems Interconnection* (ISO/OSI). (GEUS; NAKAMURA, 2003, p. 209).

De acordo com o Anônimo, que escreveu o livro “Segurança Máxima” (2001)

> Quando um usuário remoto entra em contato com uma rede que executa um firewall baseado em proxy, o firewall faz triagem da conexão pelo proxy. Com essa técnica, pacotes de IP não são encaminhados diretamente à rede interna. Em vez disso, ocorre um tipo de tradução, com o gateway agindo como condutor e interpretador. (ANÔNIMO, 2001, p. 157).

Essa capacidade adquirida pelo gateway de conduzir e interpretar os pacotes trafegados auxilia bastante na filtragem de conteúdo de certas aplicações como correio eletrônico. Desta forma, o correio eletrônico pode ser filtrado em busca de palavras obscenas assim como a capacidade de eliminar anexos considerados perigosos. (CHESWICK; BELLOVIN; RUBIN, 2005)

3.3.2.1 Funcionamento

Segundo JUCÁ (2005)

> É possível afirmar que o papel principal de um servidor *Proxy* é intermediar a comunicação entre um cliente qualquer e o servidor de destino responsável pelo serviço solicitado. (JUCÁ, 2005, p. 266).

Os proxies atuam recebendo as solicitações de serviços feitas pelos usuários da rede interna enviando-as para a rede externa como se fosse o próprio usuário de origem. Assim que recebe a resposta enviada pelo servidor externo, o proxy responde a solicitação feita, anteriormente, ao usuário interno como se fosse o próprio servidor externo de origem. Desta forma, o proxy localiza-se exatamente entre as redes interna e externa. Esta localização, permite o proxy atuar como um firewall oferecendo diversas vantagens relativas à segurança. (STREBE; PERKINS, 2002)

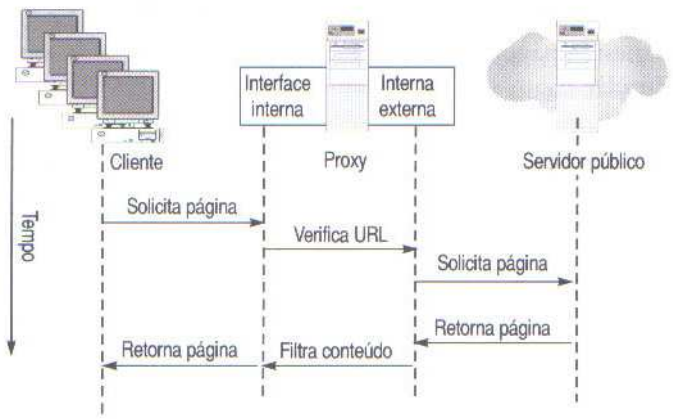

Figura 2: Um servidor proxy. Fonte: (STREBE;PERKINS, 2002, p. 152).

3.3.2.2 Vantagens

De acordo com Matthew Strebe e Charles Perkins (2002)

- Os proxies ocultam os clientes privados de serem expostos externamente.
- Os proxies podem bloquear URLs suspeitos ou considerados perigosos.
- Os proxies podem filtrar conteúdo suspeito ou perigoso como vírus e cavalos de Tróia antes de passá-los para o cliente.
- Os proxies podem conferir a consistência do conteúdo retornado.
- Os proxies podem eliminar a necessidade de roteamento da camada de transporte entre rede.
- Os proxies fornecem um único ponto de acesso, controle e monitoração (STREBE; PERKINS, 2002, p. 152).

Portanto, a utilização de um firewall baseado em proxy traz uma série de quesitos importantes para o estabelecimento de segurança dentro de um ambiente organizacional. O primeiro aspecto citado acima é sem dúvida uma das maiores vantagens trazidas pela implementação de um firewall baseado em proxy. O que ocorre é que os servidores proxy têm a capacidade de fazer com que todas as máquinas pertencentes a rede interna de uma organização sejam vistas como apenas uma máquina na Internet, pois é somente por uma única máquina que todas as solicitações por serviços são feitas. Assim, todos os clientes internos tornam-se ocultos para os servidores externos.

Outra vantagem, extremamente característica do firewall baseado em proxy é sua capacidade de estabelecer a filtragem entre sites a partir de uma lista de sites recusados de acordo com a política interna da empresa. Quando um usuário tenta acessar determinado site, imediatamente o proxy verifica se esse site está incluído na lista de sites recusados. Caso esteja, imediatamente o proxy bloqueia o acesso àquele site impossibilitando a solicitação de acesso feita pelo cliente. O proxy também é capaz de bloquear certas expressões que possam estar contidas no corpo do endereço Web. Verifica-se muito isto, quando dentro da empresa é proibida a utilização de programas de mensagem instantânea, como Messenger por exemplo. O usuário não consegue conectar o programa, pois o firewall da empresa está bloqueando a porta utilizada pelo programa para estabelecer comunicação externa. Assim, o usuário entra em algum site Web que disponibilize a conexão deste serviço. Nesse caso, existem inúmeros sites que oferecem o serviço de mensagem instantânea do Messenger, através de um browser Web e, tornar-se-ia inviável para o administrador do proxy incluir todos esses sites em uma lista bloqueando o acesso de todos eles. Desta forma, o administrador do proxy adiciona uma expressão que não deve conter no corpo de nenhuma URL de sites, “MSN” por exemplo. Todos os sites que contenham a expressão “MSN” em sua URL são bloqueados.

Em relação aos filtros de conteúdo, o proxy é capaz de filtrar e remover certas suspeitas de malwares antes que sejam acessados pelo cliente. Nesse caso, o administrador do proxy pode configurar o seu proxy HTTP, por exemplo, para remover controles ActiveX, applets Java ou certas imagens que considerar como possíveis ameaças à segurança. Outro aspecto, seria a configuração do proxy SMTP para remover anexos de e-mail com arquivos executáveis ou arquivos compactados caso caracterizassem uma possível tentativa de intrusão. (STREBE; PERKINS, 2002)

O firewall baseado em proxy é, sem dúvida, uma ferramenta muito requisitada em certas organizações que buscam pelas vantagens trazidas por esta ferramenta. Mas como garantir segurança total é uma tarefa quase impossível, esta ferramenta apresenta algumas desvantagens que valem a pena serem ressaltadas. A próxima seção abordará as principais desvantagens que o firewall baseado em proxy traz no uso de sua aplicação.

3.3.2.3 Desvantagens

Com base no livro “Segurança de redes em ambientes cooperativos”:

> - É mais lento do que os filtros de pacotes (somente o *application-level gateway*).
> - Requer um proxy específico para cada aplicação.
> - Não trata pacotes ICMP.
> - Não aceita todos os serviços.
> - Requer que os clientes internos saibam sobre ele. (GEUS; NAKAMURA, 2003, p. 223-224).

Mesmo sendo uma ferramenta essencial para estabelecer filtragem no nível de aplicação, os firewalls baseados em proxy apresentam algumas desvantagens. A primeira delas, como citado acima, é o fato de ser mais lento que o filtro de pacotes. Mas sem dúvida, a maior desvantagem desta ferramenta é o fato de ser preciso utilizar um proxy diferente para cada tipo de aplicação.

O que ocorre é que a NAT não funciona com protocolos que dependem de informações de endereços IP embutidas nos dados úteis ou que exigem a capacidade de abrir um canal de retorno com o cliente. Assim, os protocolos cujos quais não existe um serviço de proxy disponível não podem ser conectados por meio de um proxy, a menos que seja um proxy TCP genérico. No entanto, nenhum serviço que não houvesse um serviço de proxy disponível teria a vantagem de realizar a filtragem de conteúdo. Desta forma, muitos serviços não podem ser de modo simples, usados com proxies, pelo fato de exigirem o estabelecimento de um canal de retorno. Isto, estabelece a necessidade de um serviço de proxy diferente para cada protocolo de serviço suportado. (STREBE; PERKINS, 2002)

Enfim, fica evidente que os firewalls baseados em proxy são mais sofisticados que os firewalls baseados em filtragem de pacotes, até pelo fato de possuírem a capacidade de desempenhar sua filtragem em nível de aplicação. Como este projeto prevê a implementação de uma interface de gestão do firewall do Linux Iptables, que é uma ferramenta classificada como firewall baseado em filtragem de pacotes, deixou-se, por último, a abordagem desta tecnologia. A próxima seção abordará o modelo de firewall baseado em filtragem de pacotes.

3.3.3 Firewall Filtro de Pacotes

Os primeiros desenvolvimentos de Firewalls baseavam-se na filtragem de pacotes. O que ocorre é a verificação do cabeçalho dos pacotes TCP/IP pelo roteador que realiza a rejeição caso estes pacotes não estejam de acordo com os padrões de aceitação.

Porém, a tecnologia de filtro de pacotes possui algumas limitações que a torna insuficiente para estabelecer uma proteção completa a um ambiente organizacional. Por isso, os firewalls baseados em filtro de pacotes estão realizando suas filtragens aliados a servidores proxy bem como a conversores de endereços de rede como forma de preencher estas limitações.

Não se pode garantir proteção adequada utilizando apenas servidores proxy e conversores de endereços deixando de utilizar um filtro de pacotes, assim como utilizar apenas o filtro de pacotes sem o auxílio dos servidores proxy e conversores de endereço não se obtêm proteção completa. Somente a união desses três serviços é capaz de realizar uma função de proteção coerente e completa. Portanto, um bom Firewall só será capaz de proteger realmente a rede interna de uma corporação, se for capaz de utilizar os três métodos de segurança combinados. (STREBE; PERKINS, 2002)

Existem dois modelos de filtragem de pacotes:

- Filtragem de pacotes sem estados (stateless).
- Filtragem de pacotes com inspeção de estados.

(STREBE; PERKINS, 2002)

3.3.3.1 Filtro de Pacotes sem estados

Os firewalls baseados em filtragem de pacotes são, na verdade, roteadores que possuem a capacidade de realizar filtragem de pacotes. Fazendo uso de um modelo básico de roteador que realiza filtragem de pacotes torna-se possível permitir ou negar conexão ao seu site por meio de diversas variáveis. (ANÔNIMO, 2001)

Segundo Anônimo (ANÔNIMO, 2001), estas variáveis são

- Endereço de origem
- Endereço de destino
- Protocolo
- Número de porta (ANÔNIMO, 2001, p. 155)

De acordo com Geus e Nakamura, a tecnologia de filtragem de pacotes atua tanto na camada de rede quanto na camada de transporte do modelo TCP/IP, de forma que toma parte de todas as decisões de filtragem com base nas informações do cabeçalho dos pacotes. Estas informações incluem endereço de origem, endereço de destino, porta de origem, porta de destino e a direção do fluxo de conexões. (GEUS; NAKAMURA, 2003)

As figuras 3 e 4, ilustram o cabeçalho do protocolo IP e TCP respectivamente:

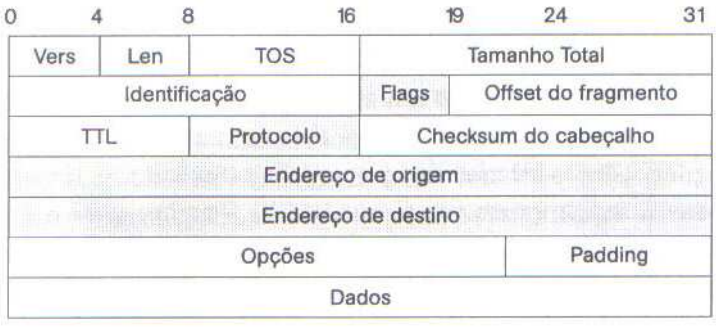

Figura 3: Campos do cabeçalho IP usados pelo *firewall*.
Fonte: (GEUS;NAKAMURA, 2003, p. 214).

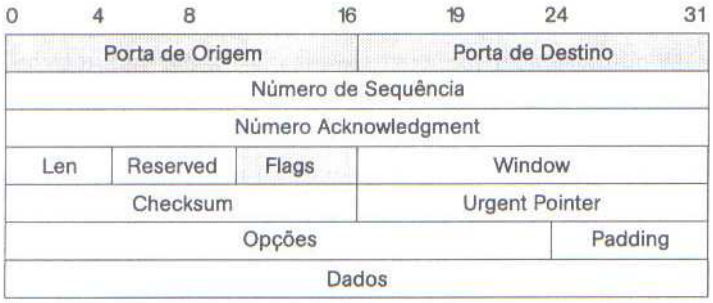

Figura 4: Campos do cabeçalho TCP usados pelo *firewall*.
Fonte: (GEUS;NAKAMURA, 2003, p. 214).

Vale ressaltar que a filtragem das conexões UDP e ICMP são um pouco diferentes das realizadas nas conexões TCP. O que difere a filtragem UDP da TCP é a impossibilidade do firewall distinguir o sentido das conexões uma vez que o protocolo UDP não é orientado a conexão. Já em relação ao ICMP, a filtragem se estabelece por meio dos códigos e tipos de mensagens. As figuras 5 e 6, do livro "Segurança de Redes em Ambientes Cooperativos" (GEUS; NAKAMURA, 2003) demonstra os campos dos cabeçalhos UDP e ICMP respectivamente:

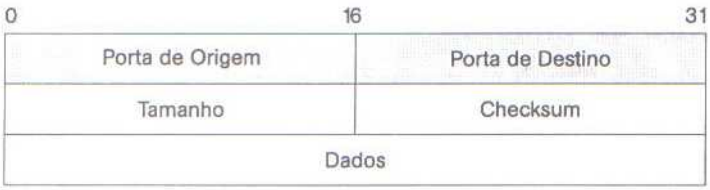

Figura 5: Campos do cabeçalho UDP usados pelo *firewall*.
Fonte: (GEUS;NAKAMURA, 2003, p. 214).

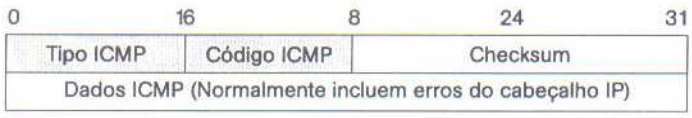

Figura 6: Campos do cabeçalho ICMP usados pelo *firewall*.
Fonte: (GEUS;NAKAMURA, 2003, p. 215).

3.3.3.1.1 *Filtro de endereços IP*

A filtragem de endereços IP estabelece a limitação das conexões origem e destino de hosts e rede específicos em função de seus endereços IP. Cada filtro utiliza uma política de segurança diferente, ou seja, enquanto existem filtros que recusam todos os acessos, com exceção de uma lista de endereços aceitos, existem filtros que permitem acesso a todos os hosts, com exceção de uma lista de recusados. (STREBE; PERKINS, 2002)

A utilização de uma política de segurança que aceite todas as conexões, exceto uma lista de recusados, sem dúvida, não é das mais seguras. Se analisarmos, ao aceitar todas as conexões e negarmos apenas a de certos hosts específicos, considerados, é claro, suspeitos conhecidos, deixaríamos livre acesso a todos, inclusive as possíveis ameaças ainda desconhecidas. Desta forma, hackers que utilizassem hosts que não estivessem na lista de exceções de acesso, teriam permissão livre para estabelecer conexão e praticar seus métodos de intrusão.

Portanto, a melhor política de segurança baseada em filtragem de endereços IP é aquela que rejeita toda e qualquer tentativa de conexão, com exceção de uma lista de hosts aceitos. Assim, a rede torna-se mais segura, rejeitando acesso para toda e qualquer possível ameaça e liberando conexão apenas a hosts conhecidos, que podem ser inclusive hosts internos.

Entretanto, como não existe segurança absoluta, é importante deixar claro que um filtro só pode estabelecer limites para os endereços IP por meio do conteúdo do campo que identifica estes endereços, e que infelizmente pode ser diferente do host de origem legítimo. O que ocorre é que os hackers têm facilidade de forjar o campo de endereço IP de um pacote. Desta forma, eles poderiam sem muitas dificuldades fazer com que um pacote forjado passasse pelo filtro de pacotes se soubessem um endereço IP que tivesse acesso permitido.

3.3.3.1.2 *Filtro de portas TCP/UDP*

Os dados relativos às portas TCP ou UDP são os mais utilizados na filtragem, pois seu campo indica especificamente a utilidade de determinado pacote. O fato do número da porta TCP ou UDP identificar os protocolos em seu mais alto nível, este modelo de filtragem também pode ser chamado de filtragem de protocolos. (STREBE; PERKINS, 2002)

De acordo com Matthew Strebe e Charles Perkins (STREBE; PERKINS, 2002)

> Os protocolos comuns que podem ser filtrados com base no campo TCP ou UDP são:
>
> | | | |
> |---|---|---|
> | Daytime | DNS | Sessão NetBIOS |
> | Echo | HTTP | IMAP |
> | Quote | Gopher | NFS |
> | FTP | POP | Whois |
> | Telnet | SNMP | RSH |
> | SMTP | NNTP | |
>
> (STREBE; PERKINS, 2002, p. 125).

Semelhante a filtragem de endereços IP, na filtragem de protocolos a política de segurança pode ser tanto liberar todos os protocolos, com exceção de uma lista de negados, quanto negar todos os protocolos, exceto uma lista de permitidos. Neste caso, diferente da filtragem de endereços IP, a solução ainda mais útil seria negar determinados protocolos, pois as tentativas de intrusão realizadas pelos hackers quase sempre utilizam protocolos específicos para cada fim.

GEUS e NAKAMURA (2003) destacam algumas vantagens e desvantagens na utilização de filtro de pacotes sem estados

> As vantagens do filtro de pacotes são:
>
> - Baixo *overhead*/alto desempenho da rede.
> - É barato, simples e flexível.
> - É bom para o gerenciamento de tráfego.
> - É transparente para o usuário.
>
> As desvantagens do filtro de pacotes são:
>
> - Permite a conexão direta para hosts internos de clientes externos.
> - É difícil de gerenciar em ambientes complexos.

- É vulnerável a ataques como o *IP spoofing*, a menos que seja configurado para que isso seja evitado (apenas falsificação de endereços internos).
- Não oferece a autenticação do usuário.
- Dificuldade de filtrar serviços que utilizam portas dinâmicas, como o RPC.
- Deixa 'brechas' permanentes abertas no perímetro da rede. (GEUS; NAKAMURA, 2003, p. 216).

Portanto, fica claro que as regras utilizadas na filtragem de pacotes não são suficientes para garantir a segurança completa de todos os tipos de sistemas. Acima, podem-se ver algumas desvantagens decorrentes da utilização da filtragem de pacotes sem estados como a abertura de 'brechas' no perímetro da rede que podem ser exploradas por um cavalo de Tróia que garante acesso remoto para a captura de senhas digitadas e de telas da vítima. No entanto, a filtragem de pacotes com inspeção em estados é, sem dúvida, uma solução mais sofisticada e será apresentada na próxima seção.

3.3.3.2 Filtro de Pacotes com inspeção de estados

A filtragem de pacotes sem estados possui várias falhas, que surgem do fato de que um único pacote em uma comunicação não possui todas as informações necessárias para determinar se este pacote deve ou não ser recusado. Os filtros de pacotes com inspeção de estados são capazes de solucionar este problema, pois guardam na memória os estados de todas as conexões que passam pelo Firewall e usam esse estado para determinar se os pacotes individuais devem ou não ser descartados. Portanto, são filtrados fluxos inteiros de conexão, e não apenas os pacotes. (STREBE; PERKINS, 2002)

Anônimo (ANÔNIMO, 2001), autor do livro "Segurança Máxima" tem sua abordagem em relação ao filtro de pacotes com inspeção de estados muito parecida com Matthew Strebe e Charles Perkins (STREBE, 2002). Para ele, a filtragem de pacotes com inspeção de estados é baseada na filtragem de pacotes sem estados, mas com alguns passos à frente. Os passos à frente que ele se refere dizem respeito à capacidade do modelo de filtragem de pacotes com estados monitorar sessões e conexões em tabelas de estado internas e podendo, portanto, reagir de acordo. Isso torna os filtros de pacotes com informações de

estado mais flexíveis, além de serem projetados para proteger contra certos tipos de ataques DoS, adicionar proteção ao correio baseado em SMTP e diversos outros recursos voltados especificamente para segurança. (ANÔNIMO, 2001)

Segundo Geus e Nakamura (GEUS; NAKAMURA, 2003)

> Os filtros de pacotes dinâmicos (*dynamic packet filter*), também conhecidos como filtros de pacotes baseados em estados (*stateful packet filter*), tomam as decisões de filtragem tendo como referencia dois elementos:
>
> - As informações dos cabeçalhos dos pacotes de dados, como no filtro de pacotes.
> - Uma tabela de estados, que guarda os estados de todas as conexões. (GEUS; NAKAMURA, 2003, p. 217).

É importante ressaltar que a maior parte dos filtros de pacotes sem estados permite que todas as portas acima de 1024 (portas altas) passem através do Firewall, em função de que essas portas são usadas para os soquetes de retorno das conexões iniciadas a partir do Firewall. Fica claro, que isso traz alguns problemas de segurança, pois nada impede que um cavalo de Tróia fique instalado na rede interna por meio de uma porta de serviço acima de 1024. Desta forma, os filtros de pacotes sem estados não conseguem evitar este tipo de intrusão, o que não ocorre com os filtros de pacotes baseados em informações de estados, pois estes não permitem nenhum serviço passar pelo Firewall, exceto os que estão autorizados para isso e que possuem suas conexões já mantidas nas tabelas de estado dos filtros. (STREBE; PERKINS, 2002)

GEUS e NAKAMURA (2003) destacam algumas vantagens e desvantagem dos filtros de pacotes com inspeção de estados

> As vantagens do filtro de pacotes baseado em estado são:
>
> - Aberturas apenas temporárias do perímetro da rede.
> - Baixo *overhead*/alto desempenho da rede.
> - Aceita quase todos os tipos de serviços.
>
> As desvantagens do filtro de pacotes baseado em estados são:
>
> - Permite a conexão direta para hosts internos a partir de redes externas.
> - Não oferece autenticação do usuário, a não ser via gateway de aplicação (*application gateway*). (GEUS; NAKAMURA, 2003, p. 222).

Apesar de ser mais sofisticado que o filtro de pacotes padrão, o filtro de pacotes com informações de estados também apresenta alguns fatores limitantes. Pode-se notar através das desvantagens acima citadas, que faltam exatamente dois elementos muito importantes para resolver certos problemas da filtragem com inspeção de estados: a necessidade de um conversor de endereços de rede (*Network Address Translation* – NAT) e um proxy para oferecer autenticação do usuário e, possivelmente, realizar filtragem em nível de aplicação.

Em todos os livros de Segurança de Redes a abordagem das tecnologias relacionadas a Firewalls segue uma ordem específica. Geralmente, os filtros de pacotes são abordados primeiro, seguidos pelo NAT e proxy respectivamente. No entanto, este projeto é baseado na criação de uma interface que possibilite o gerenciamento do Firewall do sistema operacional Linux, em específico o Iptables, que é um modelo de firewall filtro de pacotes. Por isto, neste trabalho ficou mais pertinente a abordagem dos filtros de pacotes por último como forma de estabelecer uma ligação com o firewall cujo qual se escolheu para realizar este projeto. Como o firewall escolhido para desempenhar este trabalho foi o Iptables, a próxima seção trará as principais abordagens sobre esta ferramenta.

3.4 Iptables

Em primeiro lugar, antes de realizar as principais abordagens sobre o Iptables é interessante começar definindo o conceito de Netfilter. O Netfilter é um software de filtragem de pacotes localizado dentro do kernel do Sistema Operacional Linux. Caracteriza-se por um conjunto de funções encontradas dentro do Linux responsáveis por atuar como firewall, tradutor de endereços de rede (NAT), além de guardar em log todo o tráfego de pacotes que passa pela rede. (CORETEAM, 2009) (WIKIPÉDIA, 2009)

Segundo Rubem (FERREIRA, 2003)

> O filtro de pacotes do kernel do Linux 2.4.X funciona por meio de regras estabelecidas na inicialização do sistema operacional. Todos os pacotes entram no kernel para serem analisados. [...] O programa Iptables fornece uma interface para que o usuário possa manipular o filtro de pacotes do kernel. (FERREIRA, 2003, p. 215).

De acordo com Gregor (PURDY, 2005)

> O subsistema de processamento de pacote de rede kernel do Linux é denominado Netfilter, **iptables** é o comando utilizado para sua configuração. (PURDY, 2005, p. 5).

Portanto, com base nas definições acima citadas, pode-se perceber que o Netfilter é o software que realiza as funções de firewall no sistema operacional Linux em nível de kernel e o Iptables é a ferramenta responsável por configurar o Netfilter através da inserção de linhas de comando. Dessa forma, o Netfilter e o Iptables estão estreitamente associados e, assim sendo, este trabalho usará o termo Iptables para fazer referência a estas ferramentas.

O Iptables configura o Netfilter por meio de linhas de comando que utilizam certos parâmetros e realizam determinadas ações com pacotes de rede que são solicitadas pelo usuário. Para entender como o usuário solicita essas ações, por meio de linhas de comando, é preciso antes entender como se dá a aplicação dos parâmetros necessários para que esta linha de comando seja corretamente interpretada pelo Netfilter.

Portanto, as próximas seções apresentarão as principais abordagens sobre os parâmetros utilizados pelo Iptables.

3.4.1 Regras

De acordo com Gleydson, as regras são linhas de comando passadas ao Iptables para que, por meio delas, ele realize determinadas ações como permitir ou bloquear pacotes, de acordo com a análise da interface, endereço e porta de origem e destino. (SILVA, 2007)

Segundo Gregor (PURDY, 2005)

> Uma regra **iptables** consiste em um ou mais critérios de combinação (“matching-criteria”), que determinam quais pacotes de rede a regra atingirá (todas as opções de combinação devem ser satisfeitas para que a regra seja aplicada ao pacote) e a especificação do alvo, que determina como os pontos de rede serão afetados. (PURDY, 2005, p. 11).

Portanto, a abordagem das regras Iptables é bastante sucinta. Caracteriza-se por linhas de comando responsáveis por realizar algumas ações relativas à filtragem de pacotes de rede. Para isso, algumas informações são necessárias: endereço, porta e interface de origem e destino. Com base nessas informações cria-se a regra que irá especificar se determinado pacote tem ou não permissão de passar pela rede. Caso exista a regra que possibilite a passagem do pacote, ele trafega normalmente pela rede, no entanto, se não houver, ele é imediatamente descartado.

Rubem (FERREIRA, 2003) escreve a sintaxe da regra do Iptables da seguinte forma:

"iptables [-t tabela] <comando> <chains> [opção<parâmetro>] <destino>" (FERREIRA, 2003, p. 315).

Para entender melhor a sintaxe da regra, acima citada, deve-se ter o conceito de certos parâmetros: chains, tabelas, opções, etc. Desta forma, as próximas seções abordarão estes conceitos fundamentais.

3.4.2 Chains

Segundo Rubem (FERREIRA, 2003)

> As chains determinarão se a regra será aplicada quando um pacote tenta entrar, sair ou ser redirecionado pelo firewall. (FERREIRA, 2003, p. 316).

Para Gleydson, as chains são os locais onde as regras definidas pelo usuário serão armazenadas para operação do firewall. Classificam-se em dois tipos:

- Embutidas – *INPUT*, *OUTPUT*, *FORWARD*, *PREROUTING* e *POSTROUTING*
- Criadas pelo usuário. (SILVA, 2007)

De acordo com Rubem (FERREIRA, 2003)

Chain	Descrição
INPUT	Verifica todos os pacotes que tentam entrar na rede interna.
OUTPUT	Verifica todos os pacotes que tentam sair da rede interna.
FORWARD	Verifica todos os pacotes que atravessam a rede, tanto da rede externa para a interna, como da rede interna para a rede externa.
PREROUTING	Analisa todos os pacotes que estão entrando no firewall para sofrerem NAT. O PREROUTING pode fazer ações de NAT com o endereço de destino do pacote. Isso é chamado de DNAT (Destination NAT).
POSTROUTING	Analisa todos os pacotes que estão saindo do firewall para sofrerem NAT. O POSTROUTING pode realizar ações de NAT com o endereço de origem do pacote. Isso é chamado de SNAT (Source NAT).

(FERREIRA, 2003, p. 316).

Portanto, a diversidade de chains existentes está associada ao tipo de tráfego que cada uma delas é responsável por tratar. Como dito anteriormente, o Iptables é capaz de atuar como firewall, realizar NAT, além de guardar em log todo o tráfego passante da rede. Para fazer isto, é preciso que sejam criadas regras que são armazenadas dentro das chains as quais determinarão a execução destas regras de acordo com o tipo de tráfego: entrada, saída no firewall ou redirecionamento. No entanto, é preciso que estas chains sejam armazenadas em algum local responsável por diferenciar se a regra diz respeito à filtragem ou NAT, por exemplo. Para isso o Iptables possui algumas tabelas. A próxima seção trará as principais abordagens sobre as tabelas Iptables.

3.4.3 Tabelas

A escolha do nome Iptables deve-se ao fato desta ferramenta realizar sua finalidade com base em tabelas com funções específicas de tratamento de pacotes predefinidas. (ORNELLAS, 2009)

As tabelas correspondem aos locais responsáveis por armazenar o conjunto de chains e regras utilizadas pelo Firewall, que apresentam características em comum. Na sintaxe da regra

Iptables, anteriormente citada, as tabelas podem ser referenciadas através da opção –t *tabela* das quais as principais são: *filter*, *nat* e *mangle*. (SILVA, 2007)

3.4.3.1 Tabela *filter*

Segundo Gregor (PURDY, 2005)

> Utilizada para estabelecer políticas para o tipo de tráfego permitido para dentro, através e para fora do computador. A menos que você se refira explicitamente a uma tabela, iptables opera, por padrão, nas "chains" dentro desta tabela. Suas "chains" embutidas são: FORWARD, INPUT e OUTPUT. (PURDY, 2005, p. 9).

Para Rubem (FERREIRA, 2003)

> É a tabela-padrão, sendo usada quando nenhuma tabela for especificada. É usada quando há tráfego normal de dados, sem a ocorrência de NAT (Network Address Translation – Tradução de Endereço de Rede). Usa as chains INPUT, OUTPUT e FORWARD. (FERREIRA, 2003, p. 315).

Esta é, sem dúvida, a tabela mais utilizada pelos que fazem uso do Iptables. É nela que são armazenadas todas as regras responsáveis por realizar a filtragem dos pacotes. Esta filtragem, em geral, se dá por meio da abertura ou fechamento de portas, com base nos endereços de origem e destino, interfaces de origem e destino, assim como nos protocolos utilizados para cada serviço em específico.

No entanto, em alguns casos, o uso desta tabela apenas não é suficiente para garantir o tratamento total do que se pretende fazer com um determinado host da rede interna. Por exemplo, se o administrador da rede pretende liberar internet direta (Internet com acesso livre) para um host da rede interna, será necessário inserir uma regra na tabela filter utilizando a chain FORWARD que permita a passagem dos pacotes do determinado host, presente na interface de rede interna que deseja sair pela interface que esteja ligada a rede externa, a Internet. No entanto, somente essa regra não será suficiente para permitir que este host tenha

livre acesso a Internet, pois não haverá a volta dos pacotes que pediram conexão, a menos que exista uma rota estática dentro do modem que garanta este retorno.

Para que este host interno tenha livre acesso a Internet é necessário que se crie uma regra que se utilize a chain POSTROUTING no objetivo de se realizar um mascaramento no endereço de rede deste host. No entanto, a tabela filter não reconhece a chain POSTROUTING dentro de sua sintaxe e nem é capaz de realizar mascaramento de endereços de rede. Desta forma, tornou-se necessária a criação de outra tabela que pudesse realizar a tradução de endereços de rede, criou-se a tabela *nat*.

3.4.3.2 Tabela *nat*

Segundo Gregor (PURDY, 2005)

> Utilizada com o rastreamento de conexão para redirecionar conexões para tradução de endereços de rede, tipicamente baseadas nos endereços de origem e destino. Suas "chains" embutidas são: OUTPUT, POSTROUTING e PREROUTING. (PURDY, 2005, p. 9).

De acordo com Rubem (FERREIRA, 2003)

> É utilizada quando há NAT. Exemplo: passagem de dados de uma rede privada para a Internet. Usa as chains PREROUTING, POSTROUTING e OUTPUT. (FERREIRA, 2003, p. 315).

Como dito na citação acima, esta tabela é fundamental quando existe a passagem de pacotes de uma rede privada para uma rede pública. Isto ocorre, pois a tabela *nat* realiza alterações nos cabeçalhos dos pacotes de rede que permitem algumas funções como SNAT, DNAT, IP masquerade, proxy transparente, entre outros.

Além da tabela *nat*, existe outra tabela que permite realizar algumas alterações nos pacotes de rede. A próxima seção trará as principais abordagens sobre a tabela *mangle*.

3.4.3.3 Tabela *mangle*

Segundo Gregor (PURDY, 2005)

> Utilizada para alteração especializada de pacotes, como modificações nas opções IP (com a extensão alvo IPV4OPTSSTRIP). Suas "chains" embutidas são: FORWARD, INPUT, OUTPUT, POSTROUTING e PREROUTING. (PURDY, 2005, p. 9).

De acordo com Rubem (FERREIRA, 2003)

> É utilizada para efetuar alterações especiais em pacotes. Usa as chains PREROUTING e OUTPUT. (FERREIRA, 2003, p. 315).

Portanto, a tabela *mangle* realiza alterações consideradas especiais, em pacotes de rede, por estabelecerem-se em um nível mais complexo. Um exemplo disso deve-se a sua capacidade de realizar alterações na prioridade de entrada e saída de um pacote de acordo com o tipo de serviço (ToS) associado a este pacote.

É exatamente por isso, que na citação acima de Rubem (FERREIRA, 2003), são referenciadas apenas as chains PREROUTING e OUTPUT. Pois são exatamente as chains utilizadas para fazer especificação e alteração dos tipos de serviço (ToS).

O Iptables é uma ferramenta muito complexa dotada de inúmeros módulos e funcionalidades o que torna extremamente difícil, sua abordagem de forma completa. No entanto, por seu objetivo principal, este projeto não poderia deixar de trazer, ainda que de forma objetiva e sucinta, as principais abordagens inerentes ao uso desta ferramenta. Desta forma, com base nos conhecimentos previamente fornecidos durante todo o desenvolver deste documento, o próximo capítulo trará as questões referentes à implementação propriamente dita deste projeto, que consiste no desenvolvimento de uma interface responsável por realizar o supervisionamento das funções de Firewall do Iptables com foco em pequenas empresas de informática.

4 IMPLEMENTAÇÃO

Para a realização deste projeto foi utilizado um Sistema Operacional Linux, distribuição Fedora Core 5 com os módulos Iptables e os pacotes do programa dialog instalados.

Este projeto consiste na criação de uma interface de supervisionamento das funções de firewall do Iptables com foco em pequenas empresas de informática. Desta forma, a ferramenta criada não disponibiliza a configuração do Iptables para atuar como firewall pessoal.

A interface busca estabelecer um relacionamento entre o Iptables e o usuário (Administrador da Rede) de modo que as configurações de filtragem de pacotes sejam realizadas de forma simples e amigável. No entanto, apesar de facilitar bastante a configuração das regras do Iptables, a ferramenta desenvolvida necessita que o usuário tenha certos conhecimentos de redes, segurança, protocolos e os principais serviços.

Para a criação desta ferramenta foram utilizados e adquiridos conhecimentos relativos à programação, uma vez que se trata do desenvolvimento de uma interface. Portanto, caracteriza-se por um projeto de engenharia de software.

A próxima seção trará as principais abordagens da linguagem utilizada para o desenvolvimento da interface de supervisionamento do Iptables à qual este trabalho se destina.

4.1 Shell Script

A linguagem utilizada para desenvolver este projeto é conhecida como Shell Script. Mas antes de abordar o conceito de Shell Script é mais interessante separar estes dois termos e conceituá-los separadamente.

Retirando algumas definições relevantes de autores que trabalham neste meio e que possuem reconhecimento evidente, tem-se:

Para Julio Cezar,

> O *Shell* é simplesmente o programa que lê o comando que você teclou e converte-o em uma forma mais simplificada e legível para o Sistema Operacional UNIX, diminuindo o tempo gasto pelo UNIX (ou *kernel*) na execução deste comando. (NEVES, 2008).

Segundo Aurélio Jargas,

> O Shell é o "prompt" da linha de comando do Unix e Linux, é o servo que recebe os comandos digitados pelo usuário e os executa.[7]

Dentro do Sistema Operacional Linux existe inúmeros programas que são executados a partir de uma tela de *prompt*, denominada Shell. Como o Linux não é tão difundido quanto os sistemas operacionais Microsoft, uma forma didática de se imaginar como seria esta tela de *prompt* é lembrar-se do sistema MSDOS. Assemelham-se bastante pelo fato de realizarem manipulação de arquivos, diretórios, execução de serviços, entre outros. No entanto, o Shell é infinitamente mais poderoso, pois ele possui todos os componentes e comportamentos de uma linguagem de programação estruturada, tais como CASE, IF, WHILE, FOR, definição de variáveis, criação de funções, que podem ser desenvolvidas dentro de arquivos chamados scripts.

Para realizar o login no Sistema, deve-se fornecer o nome do usuário e a senha de acesso. Quando o login é estabelecido o usuário se depara apenas com uma tela preta que

[7] JARGAS, Aurélio Marinho – **Introdução ao Shell Script** / Texto retirado de Apostila disponível em: http://aurelio.net/shell/apostila-introducao-shell.pdf. Pag. 2 Acesso em: 13/05/2009.

espera pelos comandos que serão digitados e executados dentro de um terminal. A partir deste momento, o usuário encontra-se dentro do Shell.

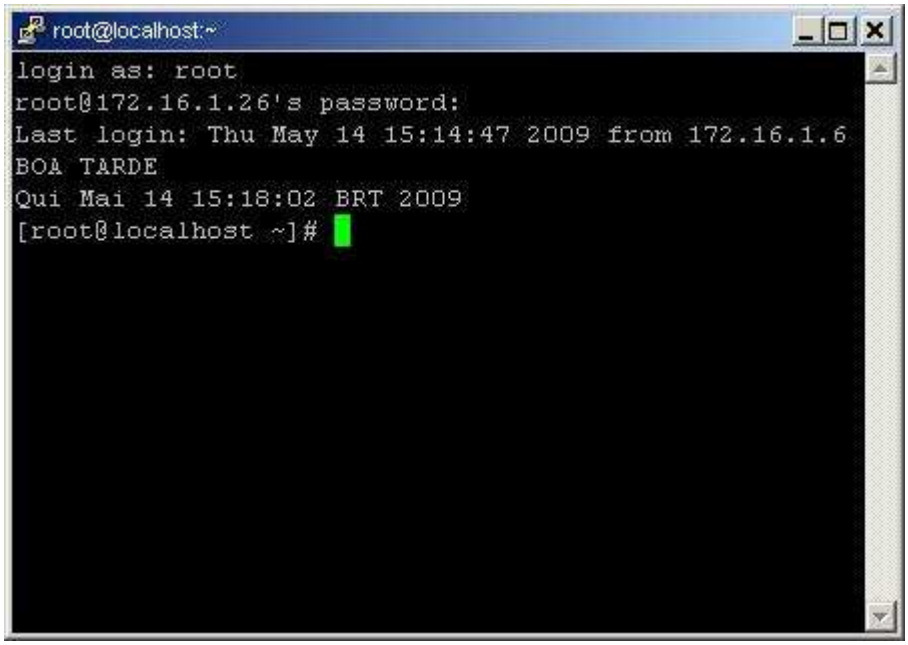

Figura 7: Ambiente Shell.

Foi criado um ambiente Shell mais amigável dentro do Linux para a execução das linhas de comando fornecidas pelo usuário. Encontra-se dentro da interface gráfica do Linux e pode ser acessado pelos nomes: Terminal ou Konsole.

Na verdade, é mais amigável pelo simples fato de não ser uma tela preta, o que assusta bastante os usuários que não estão acostumados a trabalhar com o Linux. Pode ser personalizada, acrescentando fundos de tela, no entanto, comporta-se da mesma forma como um *prompt* de comandos.

O Linux é um sistema desenvolvido em camadas com funções específicas. A primeira delas é o Shell, responsável por estabelecer o relacionamento entre o sistema e o usuário. Em seguida, tem-se o kernel ou núcleo que espera pelos comandos inseridos no Shell, e realiza o gerenciamento das funcionalidades da última camada chamada, Hardware (Dispositivos físicos).

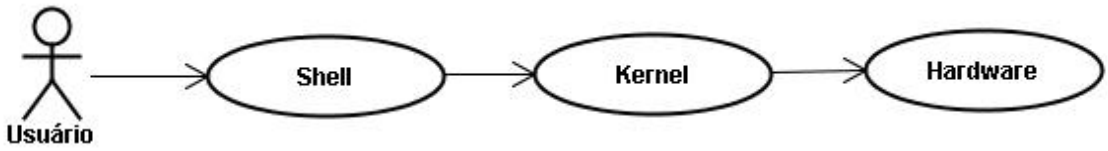

Figura 8: Relacionamento Usuário e Sistema Operacional Linux.

Agora, que já foi passado o conceito de Shell, restou dizer o que é um Script. O Script é um arquivo de texto que possui diversas linhas de comando que são utilizadas no Shell, que podem ser executadas em conjunto. Se o usuário deseja executar diversos comandos em seqüência, ao invés de ficar digitando e executando cada comando, um por um, ele os insere dentro de um arquivo, dá permissão de execução e pronto, foi criado um Script em Shell.

Foi justamente a idéia que se utilizou neste projeto. Como o que se estava querendo era desenvolver uma interface para supervisionar o Iptables e sabendo que esta ferramenta para ser implementada corretamente necessita da inserção de inúmeras linhas de comando que representam suas regras, foi criado um script onde todas estas regras seriam adicionadas para serem executadas em seqüência.

Assim, todas as vezes que o usuário criasse ou acrescentasse uma nova regra, após isto, o Script do Firewall seria executado, limpando todas as regras que foram estabelecidas anteriormente e implementando as novas mudanças.

Dentro deste ambiente, encontrou-se um pouco de dificuldade apenas na distribuição das regras dentro do Script, pois se uma regra fosse executada, mas ela dependesse de outra regra que deveria ter sido fornecida previamente, causaria conflito e não se obteria o resultado desejado.

Então foi preciso criar dentro do Script do Firewall, espécies de seções as quais iriam representar os locais certos, onde determinadas regras deveriam ser inseridas. Desta forma, as regras seriam distribuídas de forma coerente e as funcionalidades esperadas, oferecidas pelo Iptables, iriam ser bem atendidas.

O projeto foi todo desenvolvido em Shell Script. Além do Script do Firewall, toda a interface de relacionamento, com seus menus e funções, foi desenvolvida em Shell Script. Para a criação das telas de menu, foi utilizado o programa Dialog.

4.2 Dialog

Segundo Aurélio Jargas,

> O Dialog é um programa usado para desenhar interfaces amigáveis para o usuário, com botões e menus, a partir de um Shell *Script*.[8]

O Dialog, como foi dito, é um programa dentro do Linux que é executado a partir de uma linha de comando inserida dentro de um Shell. Quando é inserida a linha de comando referente a esta ferramenta, ela imprime na tela do usuário uma interface de relacionamento entre o usuário e o Shell, com botões, entradas para fornecimento de textos e senhas, manipulação de arquivos entre diretórios, entre outras funções, capazes de fazer com que esse relacionamento se estabeleça de forma mais amigável.

Por ser um programa executado a partir de linhas de comando, o Dialog é, geralmente, utilizado dentro de Shell Scripts. Todas as telas de menu feitas neste projeto foram criadas em Dialog e suas programações realizadas dentro de Shell Scripts.

Cada tela de menu criada, corresponde a um Shell Script único. Todas elas apresentam suas opções de acordo com suas funcionalidades. Quando o usuário seleciona uma opção, o Shell Script referente àquela aplicação é executado e, ao final de sua execução, o usuário é direcionado para outra tela de menu, que corresponde a outro Shell Script e assim por diante.

Dessa forma, no desenvolvimento desse projeto todas as telas de menu criadas correspondem a diversos Shell Scripts separados, que estabelecem pontes de ligação entre si, de acordo com linhas de código que chamam os próximos Scripts que correspondem às telas de menu seguintes. Por exemplo, se o usuário deseja adicionar uma rede ou máquina, ele deve selecionar a opção “Redes”, representada por uma tela de menu programada dentro de um Shell Script. Quando a opção é selecionada, o Script referente a essa opção é executado e chama, através de uma linha de código a próxima tela de menu programada em um outro Shell Script, que traz todas as opções que podem ser realizadas dentro de uma rede, inclusive adicionar uma nova.

---

[8] JARGAS, Aurélio Marinho – **Dialog --tudo** / Texto retirado de Apostila disponível em: http://aurelio.net/shell/dialog/. Acesso em: 15/05/2009.

Para entender melhor isto tudo, a próxima seção trará todo o desenvolvimento do projeto bem como a lógica utilizada para manipular as regras do Iptables e as funções do Firewall, a criação e a lógica de programação das telas de menu, as dificuldades encontradas, entre outros fatores que surgiram durante todo o processo de desenvolvimento desta ferramenta.

4.3 Desenvolvimento

As próximas seções irão apresentar as etapas do desenvolvimento deste projeto, que consiste na criação de uma interface de supervisionamento para as funções de Firewall do Iptables.

4.3.1 Construindo o Shell Script do Firewall

A construção do Shell Script principal, onde são inseridas todas as regras do Firewall necessitou de alguns cuidados, para garantir que todas estas regras seriam atendidas.

Todas as regras adicionadas pelo usuário são guardadas pelo Iptables até que a máquina seja desligada. Quando se liga a máquina novamente, todas as regras que haviam sido fornecidas pelo usuário não existem mais, pois foram descartadas no momento em que se desligou o sistema. Para isso, existe o iptables-save que salva todas as regras fornecidas pelo usuário, até o momento, em um arquivo que o usuário deverá fornecer como parâmetro. No entanto, esta opção pode ser substituída por um Shell Script, onde todas as regras criadas pelo usuário permanecem dentro do arquivo e, caso necessite-se reiniciar o sistema basta executar o Shell Script novamente e todas as regras entram em vigor.

Quando uma regra Iptables é inserida existe dentro da sintaxe um parâmetro, conhecido por Alvo ou Destino que irá especificar para a regra quais medidas tomar em relação a determinado pacote. Dentre esses alvos, os mais utilizados pela tabela de filtragem são: ACCEPT, REJECT e DROP.

O ACCEPT libera a entrada, saída ou redirecionamento de um determinado pacote. O REJECT rejeita todos os pacotes e se for um pacote ICMP retorna ao host solicitante a mensagem de máquina inalcançável. Por último, o DROP nega o tráfego de um pacote e não retorna mensagens à origem.

Um dos problemas na criação do Script do Firewall surgiu exatamente neste ponto. Quando o usuário liberava uma regra para determinado pacote, utilizando evidentemente o Destino ACCEPT, e posteriormente no intuito de bloquear esta regra reescrevesse-a utilizando o Destino DROP, o que acontecia é que o pacote continuava liberado. Isto ocorre, pois o Iptables guarda temporariamente as duas regras fornecidas pelo usuário e dá prioridade a regra que libera o tráfego do determinado pacote, representada pelo Destino ACCEPT.

Então, a idéia que se teve foi colocar no início do Script as linhas de código responsáveis por limpar todas as regras fornecidas pelo usuário, em seguida as linhas que definem a política padrão do Firewall e abaixo as seções onde seriam armazenadas todas as regras definidas pelo usuário novamente. O detalhe é que não se utilizou o Destino REJECT ou DROP. Utilizou-se apenas o Destino ACCEPT e, caso o usuário desejasse bloquear o tráfego de um pacote que havia sido liberado, a regra que permitia esta liberação seria excluída, ao invés de criar uma nova regra ineficaz tentando bloquear. É importante ressaltar que a política padrão adotada neste Firewall bloqueia toda e qualquer entrada ou passagem de pacotes pelo Firewall. Assim, essas entradas e passagens só serão liberadas à medida que o usuário for inserindo regras de permissão para estes fins. É exatamente isto que garante, que para bloquear o tráfego de um determinado pacote liberado basta excluir a regra com Destino ACCEPT, pois, após isto, o Script é rodado novamente limpando todas as regras inseridas, inserindo a política padrão bloqueando tudo e rodando novamente as regras contidas no Script.

Outra questão importante que deve-se tomar cuidado é colocar as linhas responsáveis por limpar as regras antes da política padrão e das regras que serão inseridas pelo usuário. Se as linhas que limpam as regras forem colocadas ao final, quando o Script do Firewall for executado ele insere a política padrão e todas as regras definidas pelo usuário e ao final as apaga por completo.

Esses são os procedimentos que devem ser realizados com cuidado para que o Shell Script principal que executa todas as regras do Firewall Iptables não possua inconsistências e corresponda de forma positiva no desenvolvimento de suas atribuições.

O Shell Script utilizado para inserir todas as regras do Firewall tratado nesta seção será incluído neste documento no índice referente aos anexos.

4.3.2 Desenvolvendo a Tela Principal

A interface de supervisionamento do Iptables desenvolvida neste projeto realiza a gestão das funções de Firewall desta ferramenta com foco específico em pequenas empresas de informática. Portanto, como foi dito anteriormente, não é possível a utilização desta ferramenta como Firewall Pessoal. Isto ocorre, pois a política padrão adotada neste Firewall bloqueia toda e qualquer entrada ou passagem de pacotes pelo Firewall e as regras inseridas pelo usuário na maioria dos casos são referentes à passagem de pacotes (chain FORWARD) entre redes internas ou de redes internas para internet. Desta forma, se o usuário desejasse utilizar este projeto como Firewall pessoal não seria possível, pois todas as entradas de pacotes (chain INPUT) no Firewall estão bloqueadas e as regras inseridas não tratam de pacotes vindos da Internet entrando no Firewall, e sim somente passando por ele.

A maioria das empresas de informática, principalmente escolas e centros universitários possuem inúmeras máquinas em suas redes internas. Corresponde a máquinas de laboratórios de informática, máquinas de departamentos internos, como administração, coordenação, secretarias, entre outros. Dependendo do departamento ou setor onde essas máquinas estão localizadas, elas podem possuir certos dados pessoais e de extrema valia para a empresa, que em hipótese alguma poderão ser obtidos por pessoas não autorizadas para aquela informação. Dessa forma, torna-se necessário a utilização de um Firewall para definir políticas de acessos entre as redes internas e das redes internas para Internet.

Para construir a interface de supervisionamento do Iptables necessitou-se do desenvolvimento de cinco itens importantes que deveriam estar presentes na Tela Principal da ferramenta criada neste projeto.

O primeiro deles é a opção de executar o Firewall, pois quando a máquina é desligada o Iptables descarta as regras fornecidas pelo usuário. Assim, quando a máquina é ligada novamente basta selecionar a opção “Rodar Firewall” que o Shell Script contendo todas as regras fornecidas pelo usuário, antes do desligamento do sistema, será executado e as regras entram em vigor novamente.

O segundo deles é a opção “Interfaces”, pois, como foi dito, para a criação das regras Iptables o usuário deve contar com alguns requisitos básicos que são endereço e interface de origem e destino e portas. Desta forma, foi necessário acrescentar ao menu principal a opção de criar e configurar Interfaces.

Em seguida, a próxima opção que o usuário deverá acessar corresponde ao item “Redes”. Nessa opção o usuário poderá adicionar e configurar as redes internas de acordo com a necessidade de sua empresa.

A quarta opção diz respeito aos “Serviços”, onde o usuário realizará a configuração dos serviços disponíveis pelo Firewall.

Por último, a opção “Regras” responsável por inserir as regras de filtragem de pacotes dentro do Shell Script do Firewall. A figura 9 é referente à Tela Principal da interface desenvolvida neste projeto:

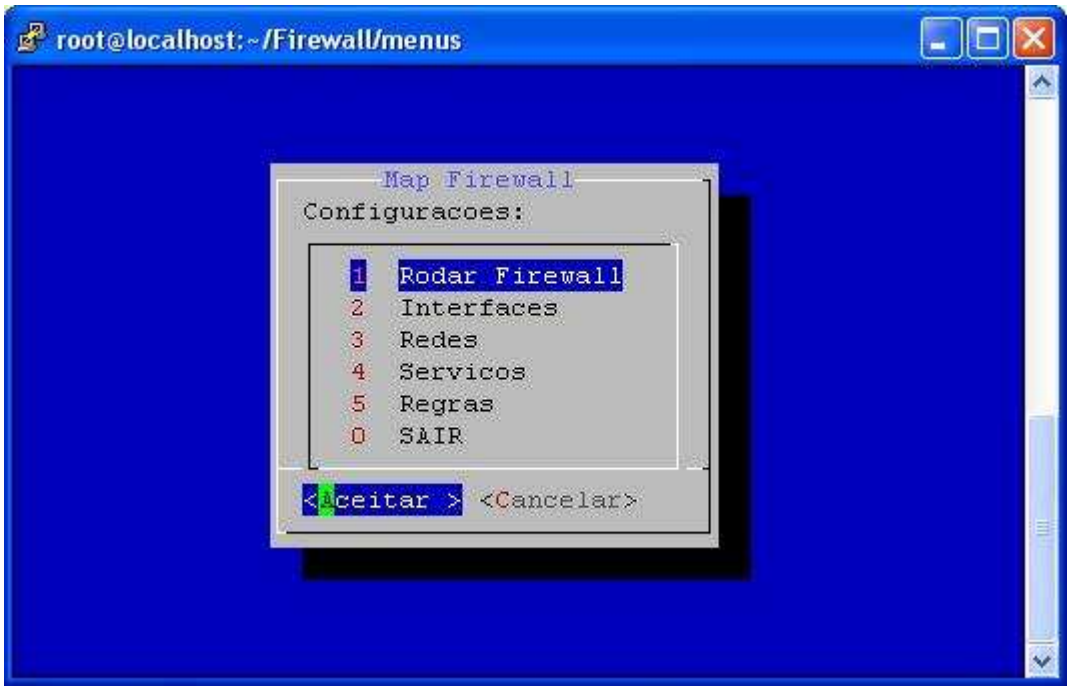

Figura 9: Tela Principal da Interface de Supervisionamento do Iptables.

4.3.3 Criando as variáveis

Esta seção aborda a criação das variáveis necessárias para a construção de uma regra de filtragem Iptables. Todas as variáveis criadas pelo usuário são inseridas no início do Shell Script do Firewall e encontram-se presentes em todas as regras inseridas pelo usuário.

4.3.3.1 Interfaces

As interfaces de rede estão presentes em todas as regras de filtragem de pacotes criadas neste projeto. É um fator fundamental para designar a origem ou o destino de um tráfego de dados. No Linux, as interfaces de rede são geralmente eth0, eth1, eth2, variando em alguns casos para ppp0 entre outras.

Quando o usuário acessa a opção “Interfaces” no menu principal, imediatamente se depara com o menu para adicionar interfaces. Nele o usuário adiciona tanto interfaces relacionadas à rede interna quanto a interface externa correspondente a Internet. O procedimento de adicionamento de Interfaces de rede é muito simples, o usuário digita um nome para a interface, por exemplo, “INTERNET” e, em seguida, digita a interface correspondente, por exemplo, eth0, eth1, eth2, etc. Após isto, a interface é imediatamente adicionada como variável dentro do Shell Script do Firewall e ao menu de adicionar Interfaces de rede, apresentando-se da seguinte forma:

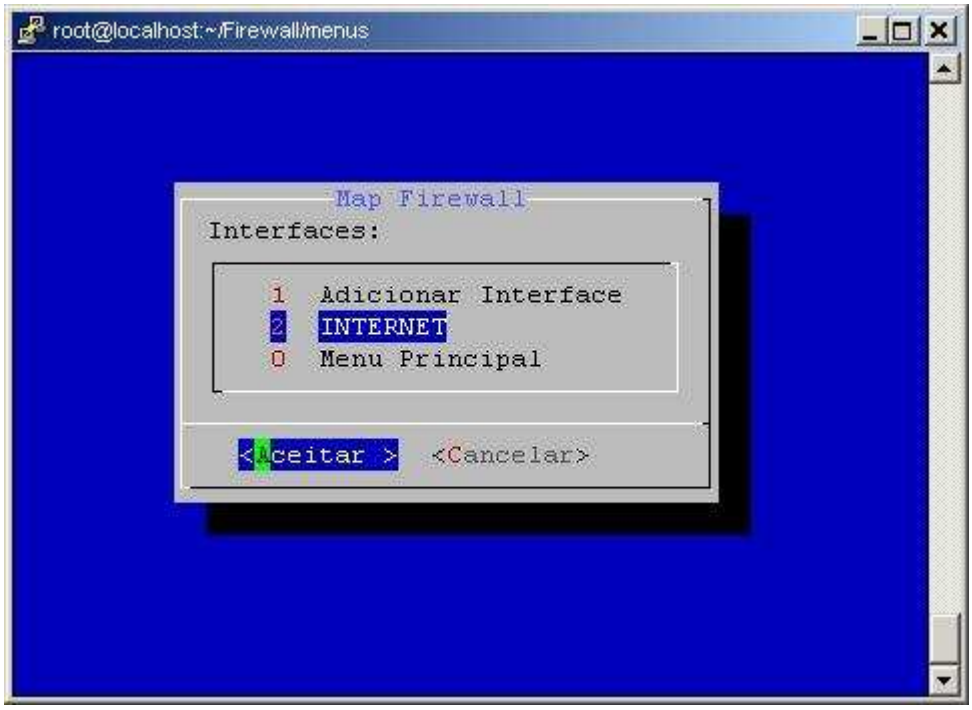

Figura 10: Menu para adicionar e acessar Interfaces de Rede.

Foi exatamente neste ponto que surgiu certa dificuldade. O menu que iria ser criado anteriormente era um menu estático. No menu estático, o usuário adicionava Interfaces que eram incluídas apenas no Shell Script do Firewall, e se o usuário deseja-se removê-la ou configurá-la era preciso digitar em uma inputbox (caixa de inserção de dados) a interface escolhida para realizar as alterações desejadas. O menu estático era bem mais simples, no entanto muito rústico e sem praticidade. Em algumas situações tornar-se-ia quase que impraticável, pois dependendo da demanda da empresa a qual fosse empregada a ferramenta criada neste projeto, dificultaria imensamente para o usuário ter conhecimento de todas as interfaces adicionadas, identificação, interface correspondente, etc.

Desta forma, foi orientado que deveriam ser construídos menus dinâmicos, onde a cada Interface criada, imediatamente ela seria adicionada ao Shell Script do Firewall e ao menu principal referente ao adicionamento de Interfaces, tal qual ilustrou a figura 10.

No entanto, para construir o menu dinâmico não foi uma tarefa tão simples, principalmente levando-se em conta que foi preciso adquirir muitos conhecimentos de programação e da linguagem Shell. As telas de menu do Firewall criadas neste projeto foram todas desenhadas pelo Dialog, que foi devidamente programado dentro de um Shell Script. Para cada interface de rede criada, devem ser adicionadas linhas de código dentro do Shell Script correspondente à determinada tela de menu a qual a interface de rede criada deverá

aparecer. Por exemplo, a tela de menu apresentada na figura 10 diz respeito a um Shell Script onde as opções como “Adicionar Interface”, “INTERNET” e “Menu Principal” correspondem a linhas de código inseridas dentro do mesmo. Desta forma, a cada nova Interface criada, o Shell Script representado pela figura 10 deve ser alterado, através da inclusão de linhas de código que representem a próxima interface adicionada pelo usuário, que pode ser “LAN_01”, por exemplo, e que será a opção 3 do menu.

Para ficar mais claro, vamos visualizar o Shell Script que traz as linhas de código que desenham a tela de menu da figura 10:

```
#!/bin/bash
# Implementando Menu Interfaces!
OP=$( dialog                    \
        --stdout                \
        --title “Map Firewall”  \
        --menu “Interfaces:”    \
        0 0 0                   \
        1 “Adicionar Interface” \
        2 “INTERNET”            \
        0 “Menu Principal”      )
#:INTERNET:#LINHA_FIM_MENU
case $OP in
        1)
                . /DIRETÓRIO/SHELL-SCRIPT/ADICIONAR/INTERFACES;;
        2) #:INTERNET:#INTERNET_LINHA
                . /DIRETÓRIO/SHELL-SCRIPT/CONFIGURAR/INTERNET;;
        *) #LINHA_DE_COMANDO
                . /DIRETÓRIO/SHELL-SCRIPT/ACESSO-MENU-PRINCIPAL;;
esac
```

Vamos supor que iremos adicionar uma nova interface de rede no Firewall chamada LAN_01. Assim que o usuário cria a interface LAN_01, a programação busca pela linha onde existe a expressão “#LINHA_FIM_MENU” localizada dentro do Shell Script do menu dinâmico, que corresponde a linha número 11. Como existe uma linha antes que corresponde

ao “Menu Principal” a programação pega a linha 11 e subtrai uma linha, apontando que a próxima interface de rede LAN_01 terá que ser incluída na linha número 10. Mas para incluir a expressão “LAN_01” na linha número 10 é preciso saber qual será o número da opção referente a esta nova interface. Sabe-se que o item “Adicionar Interface” está na linha número 8 e corresponde a opção número 1 que é parte integrante do Menu “Interfaces” e não pode ser removido. Se está na linha número 8 precisou-se utilizar o fator de subtração 7 para se ter esta opção como número 1. Da mesma forma acontece com as demais Interfaces adicionadas pelo usuário. Como a LAN_01 deverá ser incluída na linha número 10, se pegarmos sua linha correspondente 10 e subtrairmos pelo fator de subtração 7, a opção resultante referente a esta nova interface corresponde a número 3. Assim, na linha número 10 do menu dinâmico será incluída a seguinte expressão: 3 “LAN_01” \

No entanto, observe que falta adicionar a opção número 3) dentro da estrutura condicional “case” programada dentro do Shell Script. Para isso, a programação busca pela linha onde localiza-se a expressão: “#LINHA_DE_COMANDO”. A expressão localiza-se na linha 17, no entanto, como foi adicionada a linha “3 “LAN_01” \”, a expressão “#LINHA_DE_COMANDO” passa a localizar-se na linha de número 18. Desta forma, a linha 18 irá receber a seguinte expressão: “3) #:LAN_01:#LAN_01_LINHA” e a próxima linha número 19 irá receber a linha de comando que executa o Shell Script automaticamente criado para configurar a nova interface de rede criada “LAN_01”.

Todas as expressões iniciadas pelo símbolo “#” são comentários. Estes comentários foram utilizados como a lógica de programação principal deste projeto. Para cada linha de código criada é inserido um comentário responsável pela identificação da linha de código em questão. Por exemplo, se o usuário deseja remover a Interface de rede “INTERNET”, o Shell Script criado para realizar a remoção além de removê-la do Shell Script do Firewall deverá removê-la do Shell Script correspondente ao menu dinâmico de Interfaces. Para isso, dentre outras funcionalidades, a programação irá procurar pela linha onde contém expressão “#:INTERNET:#INTERNET_LINHA” apagando-a juntamente com a próxima linha que aponta o diretório onde localiza-se o Shell Script de Configurações desta Interface.

A programação dos menus dinâmicos foi ganhando bastante complexidade, pois as Interfaces e Redes criadas pelo usuário são utilizadas por outros Scripts e cada nova configuração, alteração, ou mesmo remoção deve-se aplicar a todos os Scripts que as utilizam.

Enfim, o menu “Interfaces” permite ao usuário o adicionamento, configuração e remoção de Interfaces de Rede. Em relação às configurações, o usuário pode alterar o nome

da interface de rede adicionada, por exemplo, alterar de “INTERNET” para “NET”, assim como alterar a interface corresponde, por exemplo, alterar de “eth0” para “eth1”. Além disso, o usuário deverá definir sua interface ligada à Internet para distinguir das demais interfaces que deverão corresponder as Redes Internas. Basta o usuário acessar o menu de configurações de Interfaces e escolher a opção “Definir INTERFACE WAN”.

A seguir, a próxima seção trará as abordagens sobre a variável Rede necessária para a construção de uma regra Iptables.

4.3.3.2 Redes

Para a criação de uma regra Iptables, assim como é necessário fornecer as interfaces de origem e destino para designar o sentido do tráfego de dados, também é necessário fornecer as redes ou máquinas de origem e destino para ser mais criterioso e específico quanto ao caminho que um pacote poderá percorrer dentro de uma rede interna. Isso ocorre, pois se designarmos somente as interfaces de origem e destino para o tráfego de dados, todas as máquinas e redes pertencentes às interfaces em questão estarão incluídas na autenticação dos pacotes que por entre as interfaces trafegam. Como em muitos dos casos não se deseja incluir todas as máquinas internas para determinado tráfego de pacotes, então é necessário fornecer as redes ou máquinas para as quais esse determinado tráfego será autorizado.

Portanto, foi necessário incluir na interface de supervisionamento do Iptables desenvolvida neste projeto, a opção de adicionar, configurar e remover redes que dentro de um ambiente organizacional corresponderá às máquinas internas.

Para tanto, assim como se utilizou um menu dinâmico para a criação de Interfaces de Rede, também foi criado um menu dinâmico para a criação de Redes Internas. O menu dinâmico utilizado para o adicionamento de Redes internas é exatamente igual ao criado para o adicionamento de Interfaces de Rede, apresentando-se da seguinte forma:

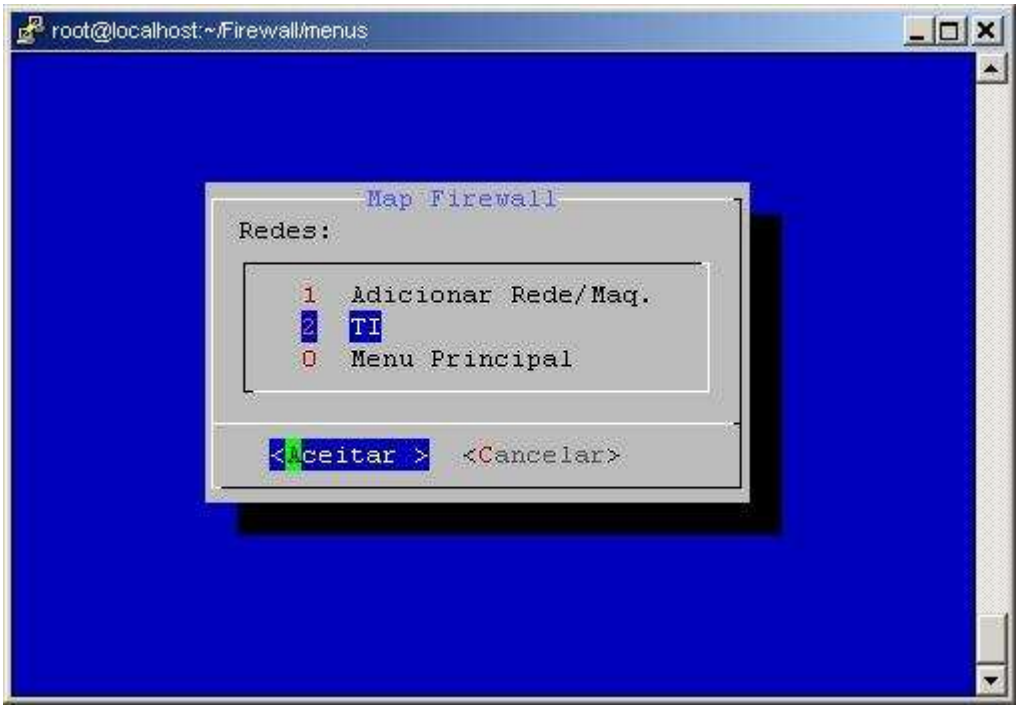

Figura 11: Menu para adicionar e acessar Redes.

O processo de adicionamento de Redes é bastante simples. O usuário acessa a opção "Adicionar Rede/Maq.", representada na figura 11 e, em seguida, deverá fornecer o nome da rede, que pode ser "TI", por exemplo, o endereço da rede e a máscara de rede, também conhecida como barramento de rede. Na inserção do barramento de rede, o usuário pode colocar 8,16,24, 32, assim como a máscara completa, por exemplo, 255.255.0.0.

O aspecto relativo à programação do menu dinâmico é exatamente igual ao explicado na seção anterior "Interfaces". Portanto, não é necessário ser explicado aqui, para não tornar-se repetitivo.

O que difere o menu "Interfaces" do menu "Redes" são os aspectos relativos às configurações. O menu "Redes" traz algumas funcionalidades na configuração de redes que não fazem parte do contexto de configuração de interfaces.

Quando o usuário cria uma rede ele tem a possibilidade de realizar alterações no nome da rede e no endereço da rede, que inclui a mudança da máscara de rede, também. Além disso, quando o usuário acessa a opção "Configurar Rede/Maq.", existe a opção para definir a Interface de Rede para a determinada rede criada. Para toda rede criada deverá ser atribuída uma interface de Rede correspondente, que será previamente criada pelo usuário. Por exemplo, o usuário cria a Interface de Rede "LAN_01", em seguida cria uma rede interna

chamada “TI”. Após isso, o usuário terá que acessar o menu de configuração de Redes e atribuir à Rede “TI” a interface de rede “LAN_01”. Isto é necessário para atrelar a rede “TI” a sua interface correspondente, pois quando o usuário for inserir alguma regra de filtragem de pacotes que inclua a rede TI, na regra deverá estar incluída, também, a interface de rede cuja qual a rede “TI” está conectada.

No entanto, para atribuir a Interface de Rede correspondente a uma determinada Rede, é criado outro menu dinâmico que fornece todas as interfaces de rede criadas pelo usuário até o momento. Este menu, conta com a mesma lógica de programação utilizada pelo menu dinâmico de adicionamento de interfaces e redes. Porém, a cada criação de um menu dinâmico surgiam certas dificuldades, pois a programação para o desenvolvimento da interface de supervisionamento desenvolvida neste projeto, ganhava maior complexidade.

No menu de configuração de Redes, além da opção de atribuir a interface de rede correspondente, o usuário pode adicionar uma máquina e definir como máquina proxy. O proxy é um dos serviços contemplados por este projeto. Se o proxy estiver configurado dentro da própria máquina Firewall, não é necessário definir nenhuma máquina como proxy. No entanto, se o proxy estiver configurado dentro de uma máquina da rede interna que não seja a máquina Firewall, é necessário adicionar esta máquina pela opção de “Adicionar Rede/Maq.”, e em seguida defini-la como máquina proxy dentro da opção de configurações de rede, para que sejam inseridas as regras Iptables que possibilitem a máquina em questão de trabalhar como proxy.

Estas são as principais funções oferecidas pelo menu “Redes”, necessárias para que o usuário se relacione com Iptables de forma amigável por meio da interface desenvolvida neste Projeto.

A próxima seção trará os Serviços contemplados pela interface de supervisionamento do Iptables.

4.3.4 Definindo Serviços

Toda rede de computadores precisa que alguns recursos estejam liberados para conseguir realizar determinadas ações, consideradas úteis para o ambiente organizacional. Acessar Web Sites, servidores FTP, e-mail, acesso remoto, entre outros, são os recursos que muitas empresas necessitam para desempenhar suas atividades, e que são chamados de Serviços.

A quantidade de Serviços existentes e possíveis de serem implementados dentro de um ambiente de redes de computadores é muito grande. Portanto, seria impraticável colocar neste Projeto todos os Serviços existentes ou mesmo a maioria deles. Posto isso, o que se buscou foi escolher os Serviços considerados elementares para as atividades desenvolvidas dentro de uma pequena empresa de informática:

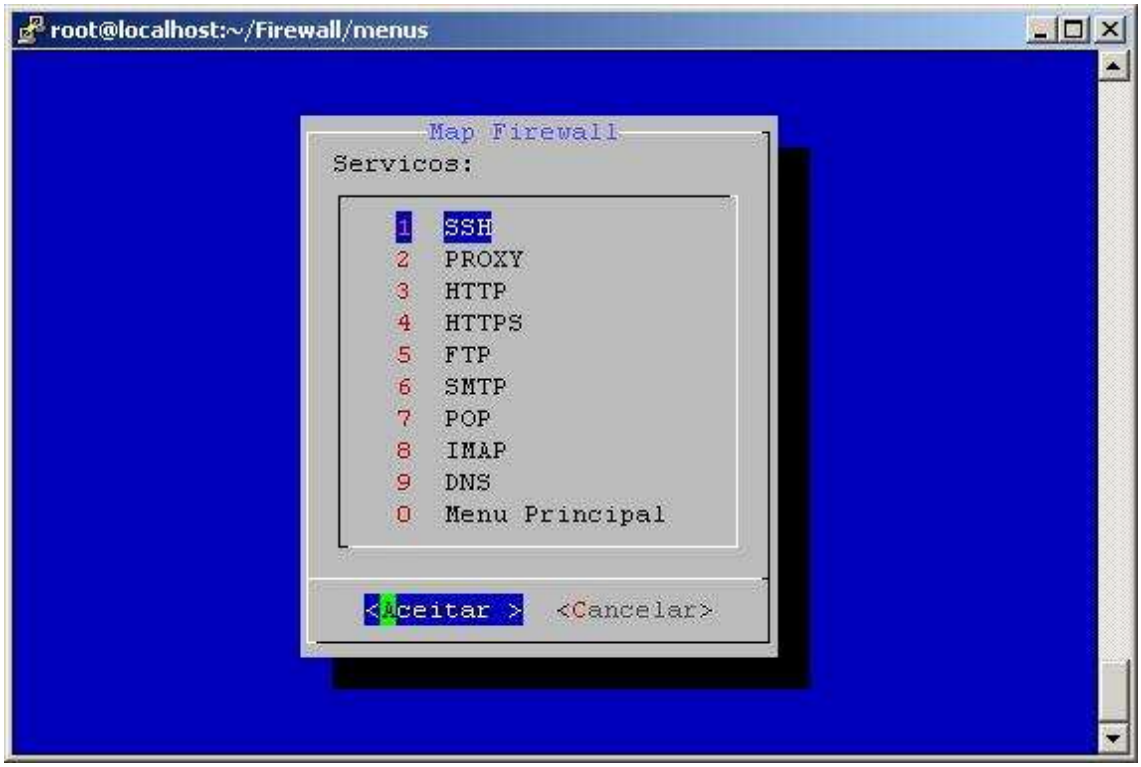

Figura 12: Menu para configuração dos Serviços.

Para o funcionamento dos Serviços é preciso que sejam liberadas as portas correspondentes a cada um deles. Portanto, para o Iptables, os Serviços são identificados através das portas que são atribuídas na sintaxe da regra, que poderão ser liberadas ou não.

No Menu Serviços, representado pela figura 12, o usuário faz a configuração das portas dos Serviços. Por exemplo, se o usuário deseja configurar o SSH dentro da sua rede para trabalhar em outra porta que não seja sua porta padrão 22, basta ele selecionar a opção "SSH" e alterar a porta de funcionamento desse Serviço. Vale ressaltar, que se por ventura o usuário deseja retornar à porta original de qualquer Serviço que ele havia alterado, ele não precisa ter o conhecimento desta porta, pois existe opção "Retornar Porta PADRÃO" dentro de cada Serviço, que realiza essa função para ele.

Outro Serviço que este Projeto contempla, porém, que não consta no Menu Serviços é o ICMP. A interface de supervisionamento desenvolvida estabelece a liberação do ICMP tanto entre redes internas quanto de redes internas com destino à máquina Firewall. Esse serviço não foi incluído no Menu Serviços, pois o Iptables dá suporte ao protocolo ICMP e, por isto, não o faz referência através de uma porta, e sim pela expressão "-p icmp".

O Serviço SSH é utilizado para o acesso remoto entre as máquinas e é muito útil para executar comandos remotamente e principalmente transferência de arquivos entre máquinas e servidores.

O PROXY neste projeto consiste apenas na liberação da porta 8080. O projeto não contempla a configuração de um servidor proxy de fato, faz apenas a liberação de máquinas em um servidor proxy caso o usuário (administrador da rede) disponha deste servidor. A principal importância da liberação de máquinas em um servidor proxy é estabelecer o filtro de conteúdo para os sites que poderão ou não serem acessados pelas máquinas da empresa.

O Serviço HTTP permite que os usuários acessem sites pela Word Wide Web (WWW). Muito útil dentro de uma empresa tanto para transferir dados através de um ambiente de intranet, quanto para acessar sites da Web.

O FTP permite a transferência de arquivos dentro de uma rede. É muito útil dentro de um ambiente empresarial, pois sua transferência de arquivos é bastante rápida além de proporcionar o armazenamento versátil de arquivos da empresa como o próprio site da mesma.

O Serviço SMTP caracteriza o protocolo padrão para envio de mensagens de correio eletrônico pela Internet. A interface de supervisionamento permite ao usuário utilizá-lo como

prioridade dentro de uma organização, assim como todos os serviços relacionados ao envio de e-mails disponibilizados por este Projeto. As mensagens de correio eletrônico se tornaram um dos principais meios de comunicação difundidos na Internet, e para algumas empresas se estabelecem como prioridade.

O POP3 é um serviço de configuração de correio eletrônico. Através dele é possível acessar uma caixa de correio eletrônico e transferir todos os e-mails contidos na caixa para dentro da máquina local do usuário. Isto permite o usuário manipular suas mensagens em modo *off-line*.

O Serviço IMAP, também, é um serviço de configuração de correio eletrônico, no entanto, é mais robusto que o POP3, pois possui alguns recursos superiores. Dentre algum deles, pode-se destacar a capacidade de compartilhar caixas postais para vários usuários pertencentes a um mesmo grupo de trabalho.

Por último, o DNS que é utilizado para tradução de nomes em endereços IP, assim como traduzir endereços IP em nomes, como meio de estabelecer a localização de hosts em um determinado domínio de rede.

Enfim, como foi dito, existem inúmeros outros Serviços que são liberados e utilizados dependendo da demanda de cada empresa. O que determina os serviços que deverão ser implementados dentro de um ambiente organizacional são as próprias atividades realizadas por cada empresa. Mais uma vez, deve-se deixar claro que neste Projeto buscou-se a implementação de Serviços considerados elementares para o bom funcionamento de um ambiente organizacional. Não que todos os Serviços contemplados por este Projeto sejam ferramentas obrigatórias dentro de uma Empresa, mas que de forma geral são utilizados pela grande maioria das Empresas de Informática.

4.3.5 Construindo as Regras

A Tela Principal da Interface de Supervisionamento do Iptables desenvolvida neste Projeto, enumera as opções de configuração do Firewall através de uma seqüência ordenada de implementação. Isto quer dizer, que antes do usuário criar as regras de filtragem, ele

deverá montar a topologia de sua rede criando as Interfaces, adicionando as Redes ou máquinas e, se necessário, configurar os serviços fornecidos pela ferramenta.

Quando o usuário acessa o menu “Regras” ele tem duas opções: “Inserir Regras” e “Listar Regras”.

No menu “Inserir Regras” o usuário dispõe da inserção e exclusão de regras referentes aos Serviços contemplados pela Interface de Supervisionamento, além de algumas outras opções que podem ser vistas na Figura 13 abaixo:

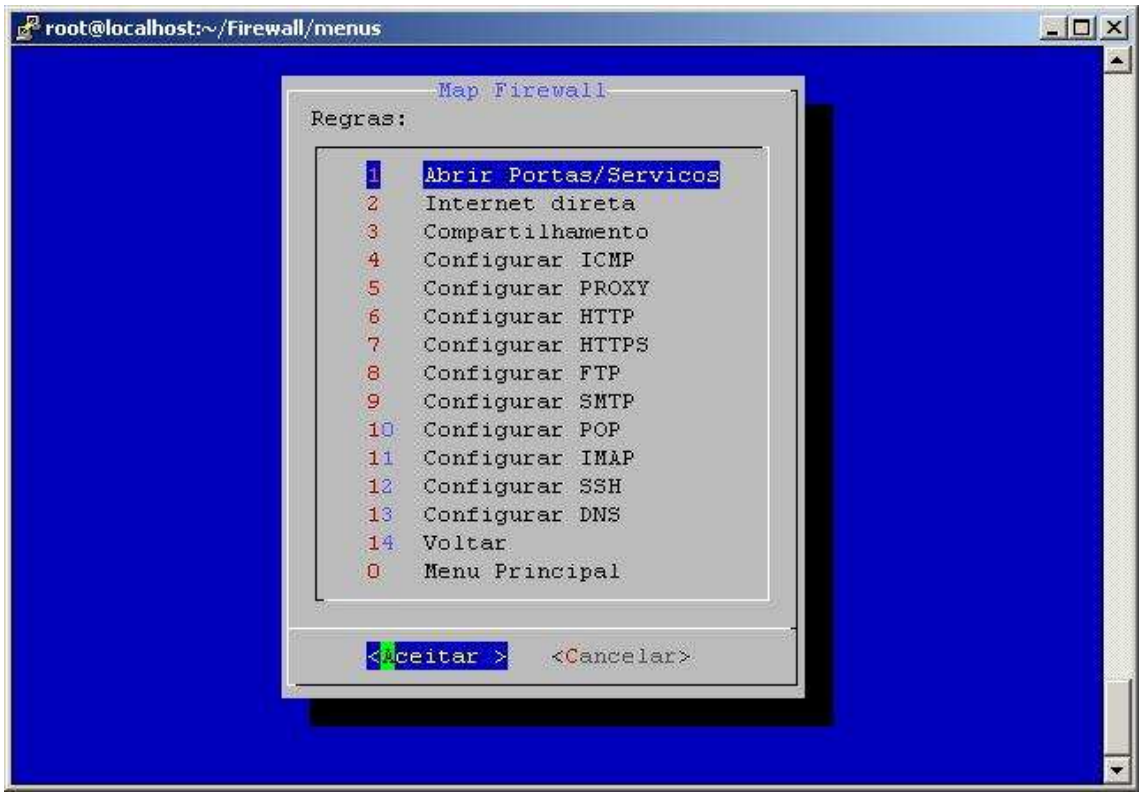

Figura 13: Tela do Menu de configuração de Regras.

A opção “Abrir Portas/Serviços” é utilizada pelo usuário para permitir a liberação de algum serviço para as máquinas da rede interna da empresa. Quando o usuário seleciona esta opção, ele fornece um nome para o serviço, seleciona o protocolo que o serviço utiliza como TCP ou UDP e, em seguida, a porta utilizada pelo serviço que será liberada. Por exemplo, se o usuário deseja liberar o Messenger, ele deverá fornecer o nome “MSN”, por exemplo, após isso selecionar o protocolo TCP e, em seguida, digitar a porta 1863. Após isto, o Messenger estará teoricamente liberado. Vale ressaltar que o fato do usuário liberar determinada porta

não garante que o serviço irá funcionar, pois em determinados casos e dependendo do serviço, exige-se um grau de configuração maior para tudo funcionar corretamente.

Um exemplo disso é o Skype, que trabalha utilizando o protocolo UDP e portas altas e dinâmicas. O fato de utilizar portas altas (acima de 1024) e dinâmicas (portas aleatórias) dificulta a liberação deste serviço por parte da interface de supervisionamento. Neste caso seria necessário liberar todas as portas altas e, conseqüentemente, isto traria certos riscos para a organização.

A opção “Internet direta” libera a Internet para as máquinas internas da rede sem estabelecer nenhum tipo de bloqueio. A máquina que estiver com esta opção liberada poderá acessar todos os sites, utilizar todos os programas instalados, baixar conteúdos, entre outros. Esta opção é útil caso precise-se liberar algum recurso para uma rede ou laboratório e a interface de supervisionamento não forneça suporte a este recurso.

A terceira opção “Compartilhamento” é utilizada para o compartilhamento de recursos entre máquinas da rede interna que se localizem em interfaces de rede distintas. Por exemplo, existe uma máquina interna A ligada à interface de rede eth1, que deseja acessar remotamente as pastas da máquina interna B ligada à interface eth2. O usuário seleciona a opção “Compartilhamento” e seleciona a máquina cliente A e a máquina servidora B. Posto isto, a máquina A obtêm livre acesso, independente de protocolos ou portas, para acessar os recursos contidos na máquina B, como pastas, arquivos, entre outros.

A opção “Configurar ICMP” estabelece a liberação do protocolo ICMP tanto entre máquinas internas, como de máquinas internas com destino à Máquina Firewall. A liberação do PING entre as máquinas internas foi criada no objetivo de realizar testes de conectividade, ou seja, testar se um host está respondendo as conexões estabelecidas dentro da rede.

Na opção “Configurar PROXY” o usuário seleciona todas as redes ou máquinas que serão liberadas no servidor proxy. O servidor proxy poderá ser tanto a Máquina Firewall, como outra máquina da rede interna que deverá ser definida pelo usuário como máquina proxy no Menu de configuração de Redes.

Nas demais opções como Configurar HTTP, FTP, SMTP, POP, IMAP, SSH e DNS o usuário estabelece a liberação de todos estes serviços para as redes ou máquinas internas previamente adicionadas. Em alguns deles como SMTP, POP e IMAP o usuário tem a opção de estabelecê-los como prioridade para rede da organização utilizando a opção ToS do Iptables.

Todas as opções fornecidas pelo menu “Inserir Regras” só podem ser estabelecidas se o usuário definir as interfaces de rede, as redes ou máquinas, atribuir as interfaces de rede para as redes ou máquinas internas, bem como definir a interface de rede que será utilizada como link para Internet. Do contrário, nenhuma regra poderá ser adicionada.

Para visualizar todas as Redes ou Máquinas que possuem os Serviços liberados pelo usuário foi criada a opção “Listar Regras”. Esta opção se baseia em um arquivo de texto que contem linhas com o nome de cada serviço disponibilizado pela Interface de Supervisionamento. Desta forma, se o usuário libera um serviço para uma rede, a programação busca a linha onde estiver referenciado este serviço e, após esta linha, adiciona a respectiva rede para a qual o serviço foi liberado. Assim, o usuário poderá se orientar que redes ou máquinas estão liberadas para os determinados serviços utilizados pela Interface de Supervisionamento.

Portanto, quando o usuário acessa a opção “Listar Regras” a programação chama pelo arquivo onde contém todas as regras adicionadas até o momento e, em seguida, o imprime para o usuário na tela da Interface de Supervisionamento utilizando caixa de diálogo textbox do Dialog:

Figura 14: Tela do Menu de Listagem de Regras.

4.3.6 Visualizando Variáveis e Regras incluídas no Shell Script do Firewall

As seções anteriores demonstraram a implementação dos requisitos necessários usados para o funcionamento da interface de supervisionamento do Iptables. Requisitos como adicionamento de interfaces de rede, adicionamento de redes, configuração de serviços, inserção de regras, entre outras opções.

No entanto, todas estas variáveis e regras precisam ser adicionadas de fato no Shell Script do Firewall, pois é através da execução deste, que todas estas regras entram em vigor estabelecendo a filtragem no tráfego de pacotes.

Utilizando alguns dos exemplos fornecidos nas seções anteriores, nesta seção veremos como as interfaces de rede, as redes e as regras são incluídas dentro do Shell Script do Firewall.

Imagine que o usuário cria, por exemplo, uma interface chamada “INTERNET” e outra chamada “LAN”, onde uma representa a placa de rede que possui o link para Internet e a outra representa a placa de rede onde as máquinas internas estarão ligadas respectivamente. Após isto, o usuário cria uma rede interna chamada “TI” e atribui a interface “LAN” para esta rede. Visualizando o Shell Script do Firewall tem-se:

Figura 15: Shell Script do Firewall com variáveis adicionadas.

Observe que a interface de rede “LAN” representa a placa de rede “eth1” e que a interface de rede “INTERNET” representa a placa de rede “eth0”. A rede “TI” possui o endereço “172.18.100.0/24”. A variável “INT_ATR_TI=$INT_LAN” identifica a interface de rede cuja qual a rede “TI” está conectada, que é igual à variável “INT_LAN” que representa a interface “eth1”. Portanto, a rede “TI” que representa um range de máquinas da rede interna está conectada a interface “LAN”.

Todos os serviços contemplados por este projeto correspondem também a variáveis dentro do Shell Script do Firewall e apresentam-se da seguinte forma:

Figura 16: Variáveis dos Serviços contemplados pelo Projeto.

Agora vamos visualizar como são inseridas as regras de filtragem. Por exemplo, o usuário deseja liberar o serviço HTTP para a rede “TI”. Baseado na figura 16 a variável que representa o serviço HTTP é “PRT_HTTP_PORT” que é igual a “80”. Portanto, a porta que deve ser liberada para o funcionamento do serviço HTTP é a porta 80.

Para que o serviço HTTP funcione, antes que seja liberada a porta 80, precisa-se liberar a volta dos pacotes da interface “eth1”, onde a rede “TI” encontra-se conectada, que pedirão conexão com a Internet. Só assim, o usuário conseguirá receber as respostas, que constituem o carregamento das páginas da Internet. Desta forma, quando o usuário libera o HTTP para a rede “TI”, a primeira regra inserida é a liberação da volta dos pacotes da Internet para a interface “eth1”:

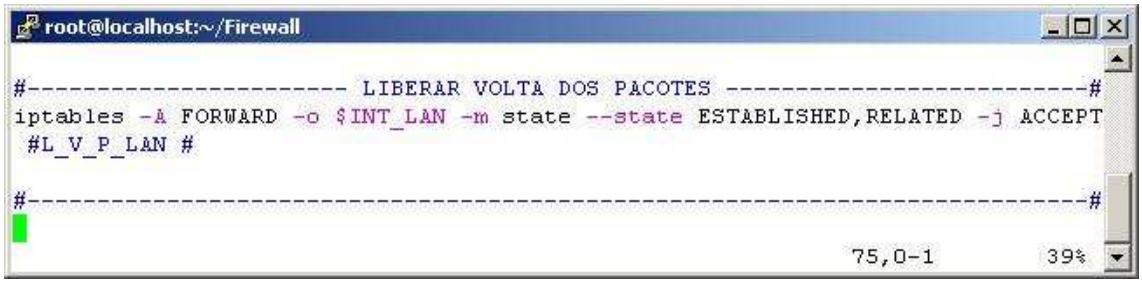

Figura 17: Regra para liberação da volta dos pacotes para eth1.

Após a liberação da volta dos pacotes, a programação insere a regra no Shell Script do Firewall que estabelece a liberação da porta 80 para o funcionamento do serviço HTTP:

Figura 18: Regra para liberação da porta 80 (HTTP).

Utilizando como referências as figura 15 e 16, pode-se observar que esta regra significa exatamente a seguinte expressão:

"iptables –A FORWARD –p tcp –i eth1 –s 172.18.100.0/24 –o eth0 --dport 80 –j ACCEPT"

Quando traduzimos a regra, temos que todos os pacotes vindos da interface "eth1" (Rede Interna), originados na rede "172.18.100.0/24" com destino a interface "eth0" (Rede Externa – Internet), utilizando a porta "80" terão acesso permitido.

Portanto, é desta forma que as regras de filtragem são executadas neste projeto. Os menus de configuração, por meio das programações desenvolvidas, armazenam todos os requisitos necessários dentro do Shell Script do Firewall, que a cada nova alteração ou configuração é executado e coloca todas as regras de filtragem estabelecidas pelo usuário em procedimento.

Para o desenvolvimento desse projeto foram criados inúmeros códigos. Não se pretende fornecer todos os códigos criados, até porque é inviável, devido à grande quantidade de códigos. No entanto, alguns códigos serão inseridos nos anexos deste documento para análise.

Posto todo o desenvolvimento desse projeto, o próximo capítulo irá abordar o procedimento de testes realizado com a Interface de Supervisionamento do Iptables em um ambiente de rede de computadores real.

5 TESTES E RESULTADOS

Para a realização dos testes com a Interface de Supervisionamento do Iptables, desenvolvida neste Projeto, foi necessária a realização de alguns procedimentos preliminares:

5.1 Configurando o ambiente de rede

A seguir serão enumerados os procedimentos para configuração do ambiente de rede:

1) Instalando o Linux e configurando o Modem;

2) Configurando a placa de Rede eth0;

3) Adicionando a rota default;

4) Configurando o DNS;

5) Configurando a placa de Rede eth1;

6) Configurando o protocolo TCP/IP para as máquinas internas;

7) Ativando o roteamento.

Com base na enumeração dos procedimentos de configuração do ambiente de rede, tem-se:

1) Instalando o Linux e configurando o Modem.

Em primeiro lugar, foram colocadas duas placas de rede Realtek na máquina que iria ser utilizada como Firewall. Em seguida, instalou-se o Linux, distribuição Fedora Core 9 na

máquina. Para o desenvolvimento do Projeto, foi utilizado o Linux Fedora Core 5, no entanto, para realizar os testes utilizou-se a distribuição Fedora Core 9.

Quando a instalação do Linux foi finalizada, deu-se início a instalação da Interface de Supervisionamento do Iptables, para a realização dos testes.

Os testes foram todos realizados em um ambiente de rede real. Pensou-se na possibilidade de utilizar máquinas virtuais, no entanto, devido a alguns problemas relacionados ao próprio tempo, tornou-se uma solução inviável.

Foram utilizadas no total 3 máquinas. A máquina Firewall utilizando o sistema operacional Linux e outras duas utilizando o Windows XP Professional. Foi utilizado um modem D-Link 2460 e um switch Encore ENH9116-NWY.

Antes de realizar os testes com a Interface de Supervisionamento, é necessário realizar algumas configurações no ambiente de rede criado. Primeiramente, realizou-se a configuração do modem. O modem foi ligado a uma máquina Windows por meio de um cabo de rede Ethernet RJ45 e acessado via web browser. Em seguida, atribuiu-se para o modem o endereço de rede 192.168.200.1 com a máscara 255.255.255.0.

Como foi dito, a máquina Firewall possui duas placas de rede. Em uma das placas seria ligado o modem para garantir o acesso à Internet. Na outra placa de rede, seria ligado o switch, onde as duas máquinas internas Windows seriam conectadas. Portanto, a rede a qual o modem faz parte é diferente da rede a qual as máquinas internas seriam ligadas, pois estão em placas de rede diferentes.

Posto isso, foi necessário adicionar dentro do modem uma rota para a rede na qual as máquinas internas estariam conectadas. Desta forma, adicionou-se uma rota para o endereço 10.0.0.10 com a máscara 255.0.0.0. Em seguida, foi feita a ligação física.

2) Configurando a placa de Rede eth0.

Ao concluir a ligação física, restou realizar algumas configurações dentro da máquina Firewall. A primeira configuração que deveria ser feita, era atribuir endereços de rede para as placas de rede contidas na máquina Firewall. Para atribuir os endereços para as placas é necessário descobrir qual placa corresponde à ligação com o modem e qual placa corresponde à ligação com o switch.

Então, primeiramente foi ligado o modem em uma das placas e utilizou-se o seguinte comando no Shell do Linux:

```
[root@localhost ~]# mii-tool
```

Esse comando faz a listagem das placas de rede contidas na máquina, e caso uma esteja com algum cabo de rede conectado, faz a identificação da placa em questão. Com a utilização desse comando, observou-se que a placa de rede a qual o modem estava conectado correspondia a “eth0”.

Em seguida, foi plugado o switch e usando o comando “mii-tool”, novamente, observou-se que a placa de rede a qual o switch estava conectado correspondia a “eth1”.

Para atribuir o endereço para a placa de rede eth0 utilizou-se o seguinte comando:

```
[root@localhost ~]# ifconfig eth0 192.168.200.2 netmask 255.255.255.0 up
```

Para realizar o teste de conectividade, como forma de saber se o IP para “eth0” foi atribuído corretamente, fez-se:

```
[root@localhost ~]# ping 192.168.200.1
```

Desta forma foi utilizado o PING no IP do modem, que respondeu corretamente. Portanto, a interface “eth0” foi configurada.

3) Adicionando a rota default.

Outro procedimento muito importante é o adicionamento de uma rota default, para garantir que as máquinas internas tenham acesso a Internet. Como se sabe, o modem é o equipamento que está ligado entre a rede interna e a rede externa. Portanto, é o endereço do

modem que deve ser utilizado para rota default, uma vez que é este equipamento que conhece a rede externa, a Internet. No entanto, antes era preciso saber se existia alguma rota default já adicionada, pois, caso houvesse, era preciso que esta rota fosse apagada. Para isto, utilizou-se o seguinte comando:

```
[root@localhost ~]# route –n
```

O comando não retornou nenhuma rota default, logo, era preciso adicionar a rota default apontando para o IP do modem, da seguinte forma:

```
[root@localhost ~]# route add default gw 192.168.200.1
```

4) Configurando o DNS.

Por ser o único equipamento que conhece a Internet, o modem será utilizado para resolver os nomes dos endereços correspondentes as máquinas externas. Por exemplo, deseja-se dar um ping pra fora no site “www.terra.com.br”, isto só será possível se for adicionada uma linha dentro do arquivo /etc/resolv.conf, possibilitando que o modem realize a resolução de nomes em endereços IP e de endereços IP em nomes. A linha que deve ser adicionada é a seguinte:

“nameserver 192.168.200.1”

5) Configurando a placa de Rede eth1.

Para a configuração da placa de rede “eth1”, foi utilizado o seguinte comando:

```
[root@localhost ~]# ifconfig eth1 10.0.0.1 netmask 255.0.0.0 up
```

6) Configurando o protocolo TCP/IP para as máquinas internas.

Conforme ilustra a figura 19, foram configuradas as máquinas internas, atribuindo os endereços IP internos, máscara de rede, direcionamento do gateway e servidor dns:

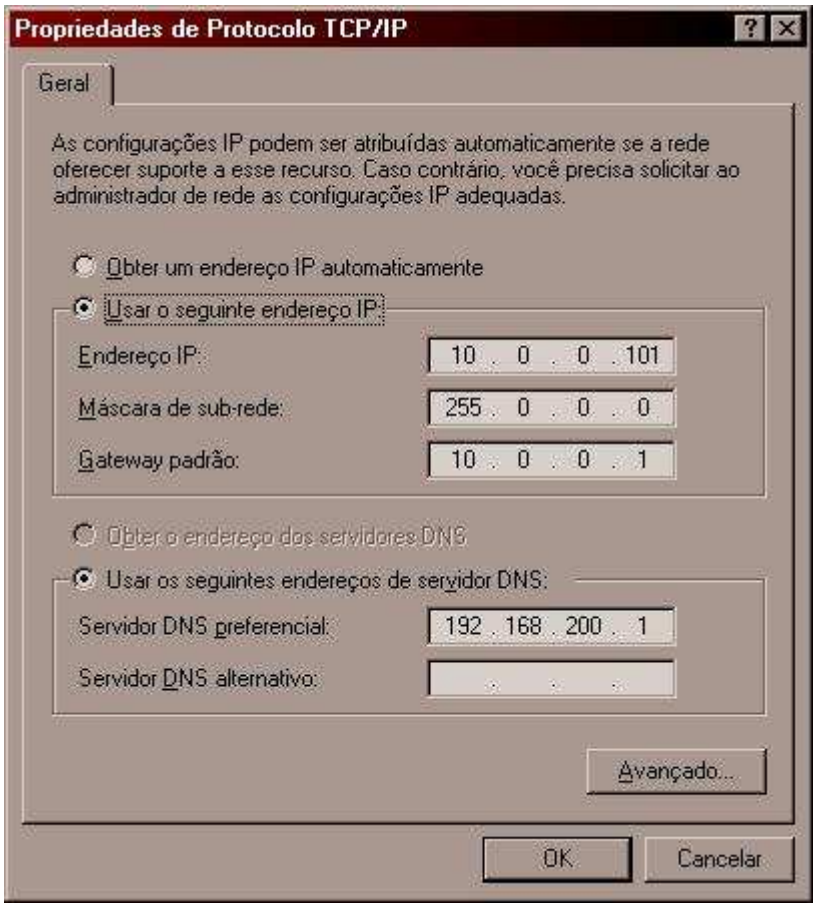

Figura 19: Configurando Protocolo TCP/IP das máquinas internas.

7) Ativando o roteamento.

Por último, o usuário ativa o roteamento fazendo uso do seguinte commando:

```
[root@localhost ~]# echo "1" > /proc/sys/net/ipv4/ip_forward
```

Posto isto, o ambiente de rede apresentou-se conforme a figura abaixo:

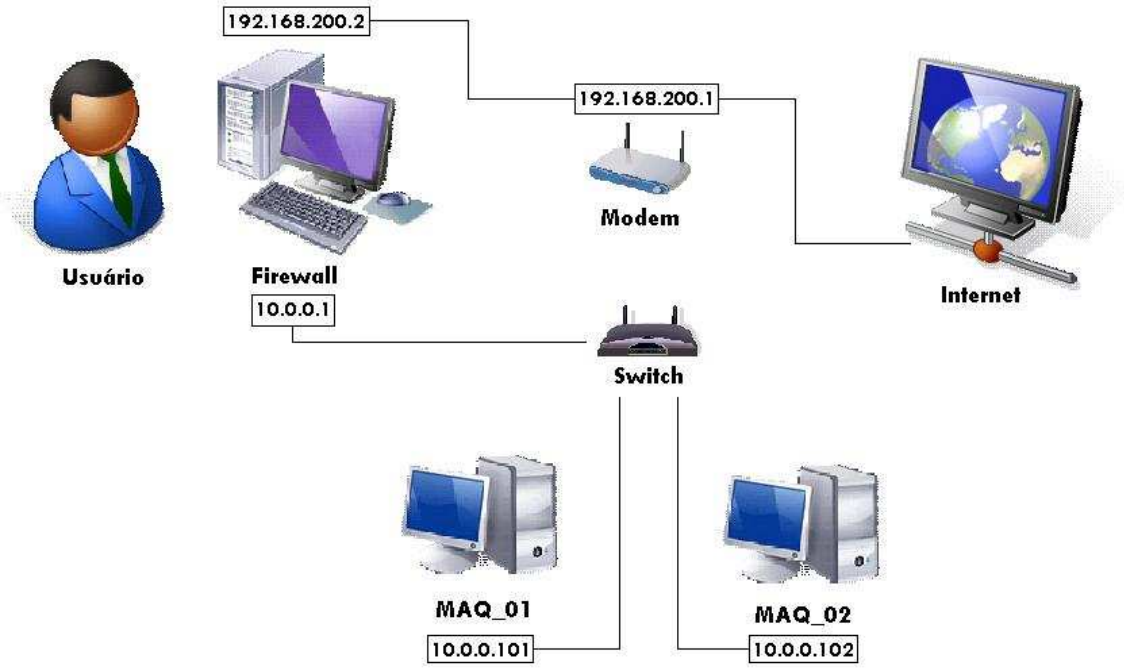

Figura 20: Topologia da Rede de Testes.

5.2 Configurações e testes na Interface de Supervisionamento

Após todas as configurações abordadas na seção anterior, realizou-se a configuração da Interface de Supervisionamento, para iniciar os testes:

1) **Adicionando variáveis (Interfaces e Redes/Máquinas);**
2) **Testando serviço ICMP e DNS;**
3) **Testando serviço HTTP e HTTPS;**
4) **Testando liberação de Internet direta;**
5) **Testando serviço FTP;**
6) **Testando serviço SSH;**

7) **Testando serviços SMTP e POP;**

8) **Testando liberação do Proxy;**

9) **Testando liberação de Portas/Serviços.**

A seguir serão apresentados os procedimentos de testes, conforme a enumeração fornecida acima:

1) **Adicionando variáveis (Interfaces e Redes/Máquinas).**

Para dar início a este procedimento, foi acessado o menu “Interfaces” e nele foram adicionadas as duas interfaces presentes no Firewall. Para a interface “eth0” atribuiu-se o nome “INTERNET”, uma vez que esta interface está ligada ao modem. Para a interface “eth1” atribuiu-se o nome “LAN”, já que é a interface onde as duas máquinas internas estão conectadas por meio de um switch.

Após ser criada, a interface “INTERNET” foi acessada e definida como “INTERFACE WAN”, para que a Interface de Supervisionamento a reconhecesse como a placa de rede conectada ao modem, ou seja, a placa de rede utilizada para o acesso à rede externa.

Após isso, foi acessado o menu “Redes” onde foram adicionadas as duas máquinas internas. As máquinas receberam os seguintes nomes: “MAQ_01” e “MAQ_02”. Após serem adicionadas as duas máquinas, definiu-se a placa de rede a qual elas estariam ligadas, “LAN”.

Após serem realizadas estas configurações, as variáveis foram armazenadas no Script do Firewall automaticamente:

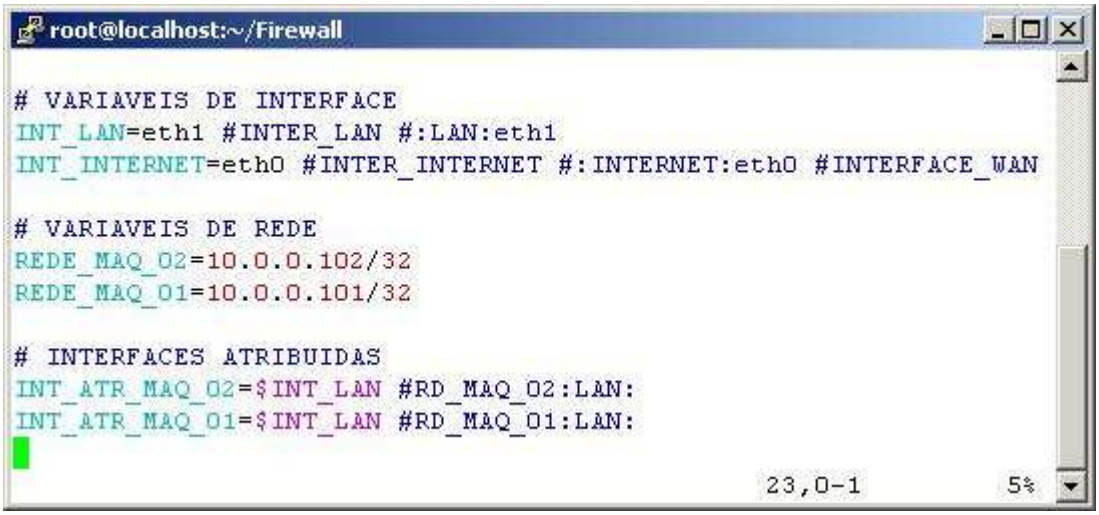

Figura 21: Variáveis adicionadas ao Script do Firewall.

É importante ressaltar que as variáveis foram adicionadas, no entanto, inicialmente não existia nenhuma regra definida para as redes criadas. Desta forma, a política padrão adotada pelo Firewall deste Projeto, bloqueia toda e qualquer entrada ou passagem de pacotes pela máquina Firewall. Esta política padrão é definida, por meio de linhas de código, inseridas dentro do Shell Script do Firewall, de modo que são executadas, a cada nova alteração ou configuração estabelecida pelo usuário na Interface de Supervisionamento. A política padrão dentro do Script do Firewall apresenta-se conforme a figura 22:

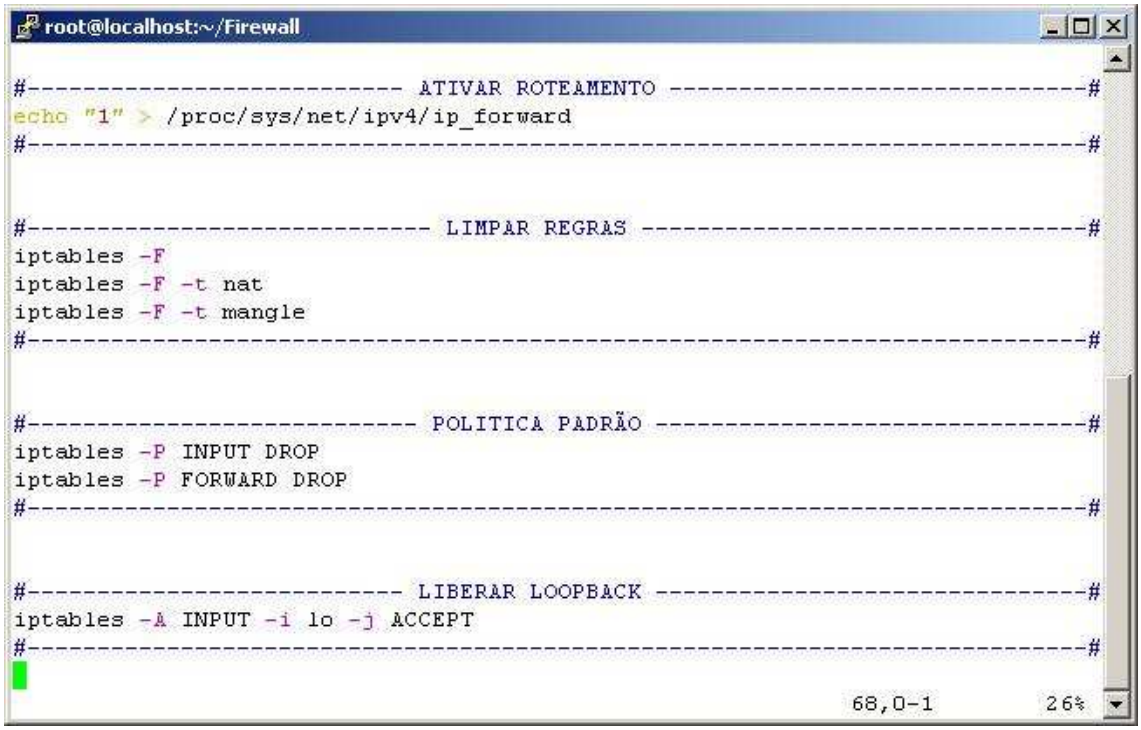

Figura 22: Ativação do roteamento e execução da política padrão.

2) Testando serviço ICMP e DNS.

Com base nos requisitos descritos no procedimento **1)**, deu-se inicio aos testes. O primeiro serviço testado foi o protocolo ICMP. Desta forma, habilitou-se o ICMP para permitir que a "MAQ_02" pudesse pingar na máquina Firewall. Deu-se esta permissão apenas para a "MAQ_02", no objetivo de testar se somente esta obteve o acesso ao PING, deixando, desta forma, a "MAQ_01" sem acesso. Ao manipular esta configuração de acesso na Interface de Supervisionamento, a programação adicionou a seguinte linha dentro do Script do Firewall:

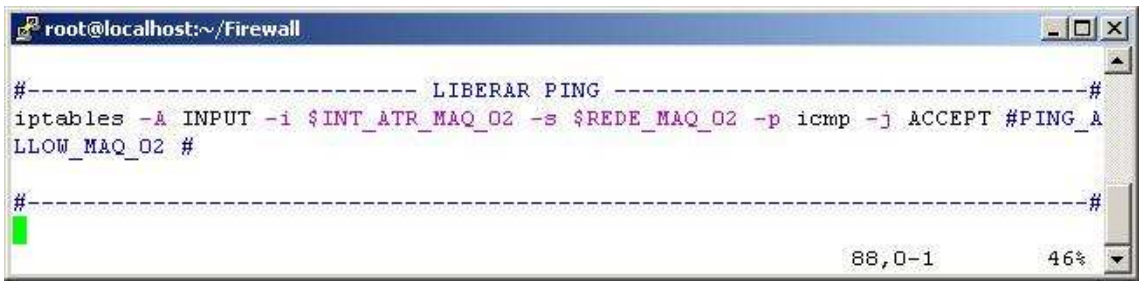

Figura 23: Regra para liberação do ICMP para a MAQ_02.

O resultado foi positivo. Apenas a “MAQ_02” obteve o acesso ao PING no Firewall. Tentou-se pingar no Firewall a partir da “MAQ_01”, mas não se obteve resposta, uma vez que esta máquina não tinha acesso para este comando.

O PING entre máquinas da rede interna estava funcionando perfeitamente. Então o segundo passo, foi testar se as máquinas internas estavam conseguindo pingar pra fora da rede interna. Então liberou-se dentro da Interface de Supervisionamento, o ICMP com origem na interface “LAN” com destino a interface “INTERNET”. Em seguida, tentou-se pingar no IP do portal Terra, que corresponde a 200.176.3.142, e obteve-se resposta. Portanto, o PING para fora da rede interna, também funcionou corretamente.

No entanto, quando tentou-se pingar no domínio “www.terra.com.br”, não obteve-se nenhuma resposta. Isto ocorreu, pois era preciso liberar o DNS para as máquinas internas “MAQ_01” e “MAQ_02”, respectivamente. Assim, quando o DNS foi liberado para as “MAQ_01” e “MAQ_02”, o PING para o domínio “www.terra.com.br” funcionou corretamente.

Após realizados os testes com os serviços ICMP e DNS, retornou-se a configuração inicial, bloqueando-se estes dois serviços. Tentou-se novamente utilizá-los, mas pelo fato de estarem bloqueados, não retornaram nenhuma resposta.

3) Testando serviço HTTP e HTTPS.

Após os testes com o ICMP e DNS, foi liberado o serviço HTTP para a “MAQ_01”. Quando utilizou-se o web browser para navegar nos sites da Internet, nenhum site conseguiu conectar. Porem, identificou-se que quando se utilizava o endereço da seguinte forma: “http://200.176.3.142”, o site do Terra abria normalmente. Portanto, mais uma vez era preciso liberar o DNS para a “MAQ_01”, pois só com a porta “53” liberada seria possível a resolução de nomes em endereço IP e vice-versa.

Assim, quando o DNS foi liberado para a “MAQ_01”, o site do Terra, assim como os demais sites abriram normalmente, quando inseridas suas URLs dentro no navegador de Internet.

Até então, para navegação na Internet, a Interface de Supervisionamento contemplava apenas o protocolo HTTP. No entanto, quando tentou-se acessar o site do G-mail, verificou-se

que era impossível, pois este utiliza o protocolo HTTPS. Então, foi incluído um novo serviço à Interface de Supervisionamento, o serviço HTTPS, que consiste na liberação da porta “443”. A liberação deste serviço tornou-se necessária, não apenas para o acesso ao G-mail, assim como a todos os demais sites de e-mails, que em grande maioria utilizam este protocolo de segurança.

4) Testando liberação de Internet direta.

Dando continuidade aos testes, foi liberada a opção “Internet direta”, para a “MAQ_01”. Esta opção funcionou corretamente. Após ser aplicada à “MAQ_01”, a mesma obteve livre acesso a Internet, tanto para baixar arquivos, quanto para utilizar todos os serviços contemplados pela Interface de Supervisionamento.

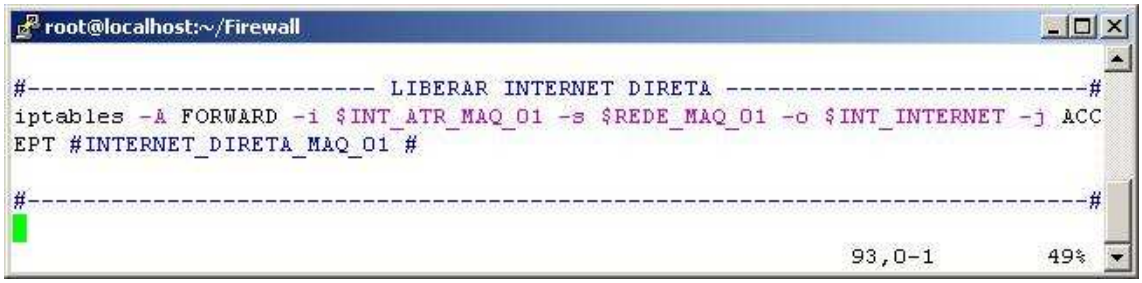

Figura 24: Regra para liberação de Internet direta para MAQ_01.

Após o teste de cada nova configuração, a configuração em questão era sempre desfeita, como forma de observar se foi corretamente bloqueada. Assim, quando desabilitou-se a opção “Internet direta” para a “MAQ_01”, a máquina perdeu o privilégio de acesso livre à Internet.

5) Testando serviço FTP.

Em seguida, habilitou-se o serviço de FTP passivo para a “MAQ_02”, que funcionou corretamente. Tentou-se acessar um servidor FTP, a partir de um web browser e a conexão foi

estabelecida corretamente. Dentro do Script do Firewall, a linha de código para a liberação do FTP passivo para a "MAQ_02" apresenta-se conforme a figura 25 abaixo:

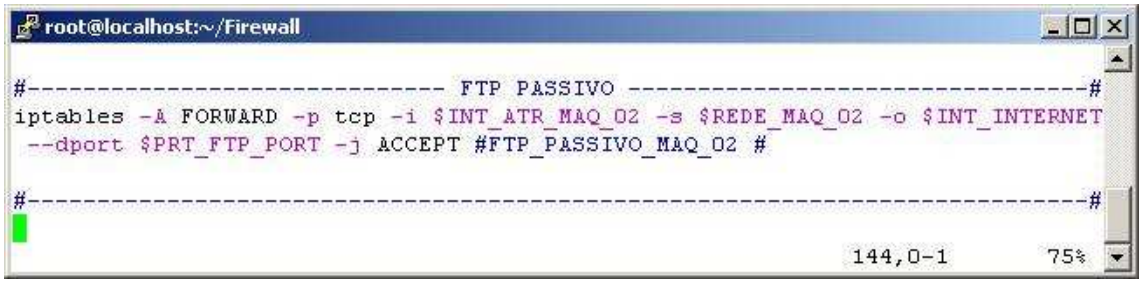

Figura 25: Regra para liberação do FTP passivo para MAQ_02.

Quando tentou-se acessar um servidor FTP a partir da "MAQ_02" que estava liberada, o resultado foi a apresentação da tela, ilustrada pela figura 26 abaixo:

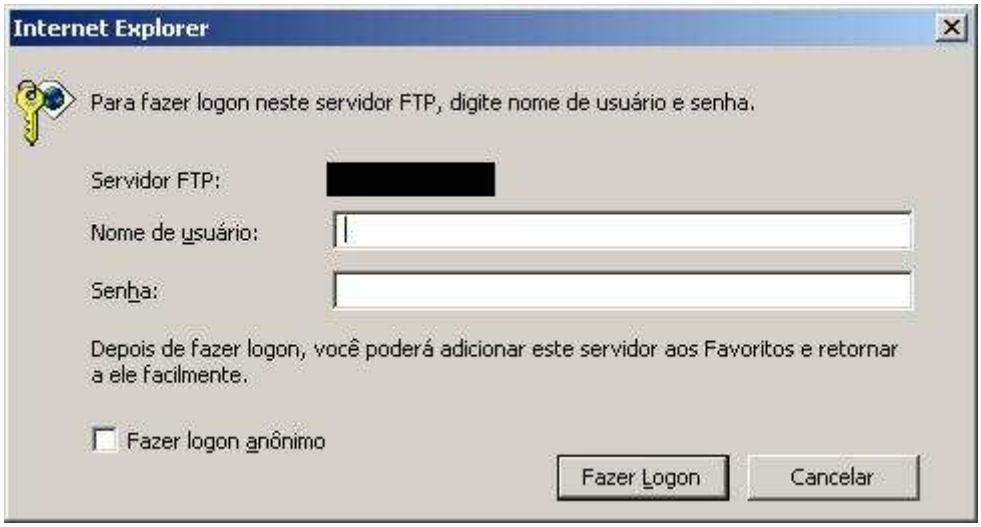

Figura 26: Acesso à um servidor FTP passivo.

O mesmo acesso foi tentado a partir da "MAQ_01", que não retornou nada, além da mensagem de que a página não pôde ser carregada.

Após isto, o próximo passo foi à liberação do serviço de FTP ativo para a "MAQ_01". Para realizar o teste do FTP ativo utilizou-se o software FileZile, que é um cliente para FTP que traz diversas funções dentro de sua interface, inclusive o suporte ao FTP ativo.

Um problema foi encontrado quando se tentou fazer acesso ao servidor FTP ativo. A "MAQ_01" estava com a opção "Internet direta" liberada, e na programação para liberar a Internet direta, existia uma linha que fazia NAT masquerading para toda e qualquer máquina que tivesse a opção de "Internet direta" liberada. Através de testes, observou-se que o problema com o FTP ativo, era devido o mascaramento do endereço IP que estava adicionado para a "MAQ_01". Então, foi removida a linha que realizava o masquerading dentro do Script que fazia a configuração da "Internet direta".

Após isto o FTP ativo, passou a funcionar normalmente, listando todos os diretórios de forma correta.

Para ilustrar a diferença entre as linhas dentro do Script do Firewall que liberam o FTP passivo e ativo, a figura 27 abaixo, trará as regras Iptables para a liberação do FTP ativo para a "MAQ_01" que foram inseridas no Script do Firewall, após ter sido feita a configuração deste serviço na Interface de Supervisionamento:

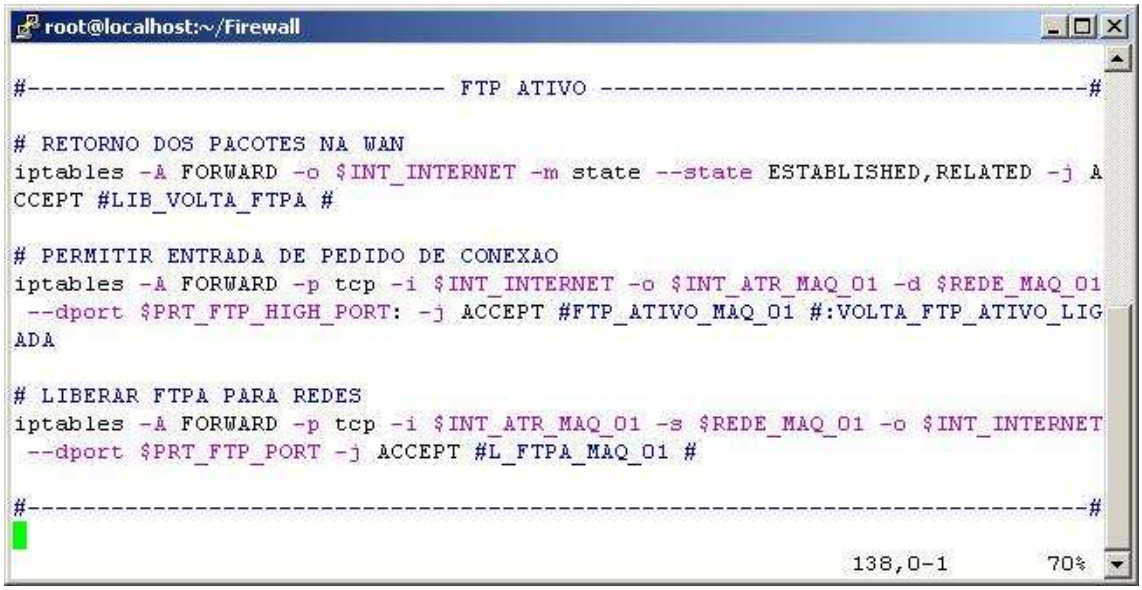

Figura 27: Regra para liberação do FTP ativo para MAQ_01.

6) Testando serviço SSH.

O Serviço SSH foi liberado para a "MAQ_01" e funcionou corretamente, conforme o esperado. Para realizar o teste, utilizou-se o programa PuTTY na "MAQ_01" e acessou-se a

máquina Firewall. O login na máquina Firewall se deu com êxito, assim, garantindo que a regra para liberação do SSH estava funcionando de forma correta.

7) Testando serviços SMTP e POP.

O próximo serviço testado foi o SMTP e POP. Foi configurada uma conta de e-mail no Outlook, e posteriormente liberado o SMTP e o POP para a "MAQ_01". O SMTP é o serviço utilizado para o envio de e-mail, e o POP é utilizado para o recebimento. Dependendo do servidor de e-mail, o serviço utilizado pode ser o IMAP, também contemplado por este projeto, que não foi testado por seu tratamento pela Interface de Supervisionamento ser exatamente igual ao POP.

A Interface de Supervisionamento dá a opção de configurar os serviços de e-mail como prioridade, conforme dito anteriormente.

Para ilustrar a liberação do SMTP dentro do Script do Firewall para a "MAQ_01", apresenta-se a figura 28 abaixo:

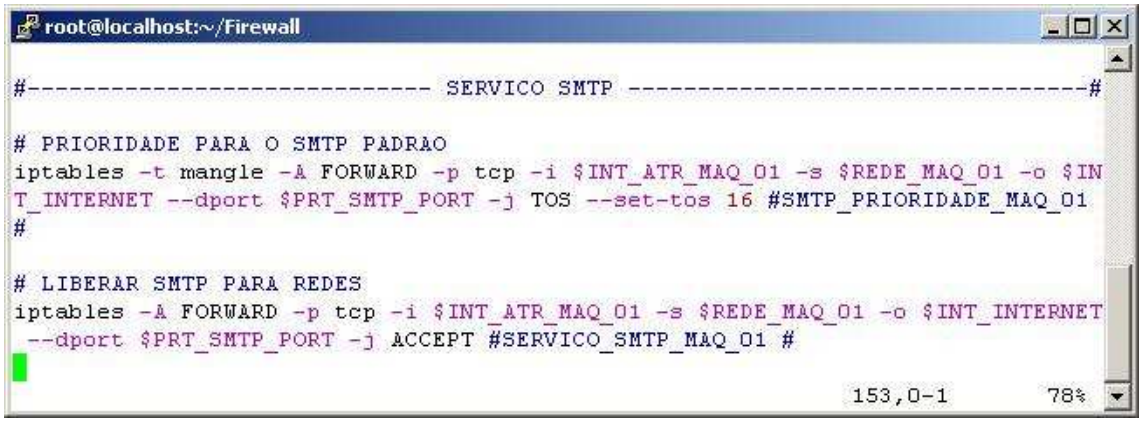

Figura 28: Regra para liberação do SMTP para MAQ_01.

8) Testando liberação do Proxy.

Em seguida, foi testado o serviço de liberação do proxy. Na própria máquina Firewall foi configurado o Squid que é um arquivo que atua como servidor proxy. Após a configuração

do Squid na máquina Firewall, acessou-se a “MAQ_01” e direcionou-se seu navegador de internet para o servidor proxy configurado:

Figura 29: Direcionamento da MAQ_01 para o servidor proxy.

Após o direcionamento da “MAQ_01” para o servidor proxy configurado, utilizou-se o navegador de Internet e a páginas carregaram corretamente. Portanto, o serviço de liberação do proxy fornecido pela Interface de Supervisionamento, também estava funcionando corretamente.

9) Testando liberação de Portas/Serviços.

Por último, foi testada a liberação do Messenger, que consiste em uma linha de código que libera a porta 1863 dentro do Script do Firewall, fornecida pelo usuário, na opção “Abrir Portas/Serviços”. A liberação do serviço se deu de forma correta, e o resultado foi à liberação do Software Messenger para as máquinas internas.

Houve algumas opções que não foram testadas, devido algumas indisponibilidades, inclusive em relação ao tempo disponível. A primeira delas foi à liberação do IMAP, por seu tratamento pela Interface de Supervisionamento ser tal qual ao do POP, que funcionou

corretamente. A outra opção, diz respeito ao teste da liberação do proxy que estaria configurado em uma máquina interna, mas que, no entanto, não seria a máquina Firewall. Houve indisponibilidade de mais uma máquina Linux para testar esta opção, uma vez que os testes foram em um ambiente de redes real. No entanto, teoricamente, funcionaria de forma correta, uma vez que o proxy a partir da máquina Firewall funcionou corretamente, e o tratamento para essa diferença é mínimo dentro do Script de regras do Firewall.

5.3 Considerações Finais

A partir dos testes realizados com a Interface de Supervisionamento do Iptables, objeto de estudo deste Projeto, a seguir serão apresentadas algumas considerações finais no que diz respeito às vantagens e desvantagens desta ferramenta, bem como sugestões para projetos futuros relacionados a este tema.

5.3.1 Vantagens

- Facilidade na adição, configuração e remoção de Redes/Máquinas e Interfaces de Rede;
- Facilidade na inserção de regras e configuração de serviços;
- Praticidade na manipulação e configuração das regras de filtragem do Iptables;
- Melhor organização do ambiente interno de rede;
- Solução de software livre, portanto, livre de custos com licenças.

5.3.2 Desvantagens

- Para a implementação da Interface de Supervisionamento é necessário ter conhecimentos de Redes de Computadores;
- Só roda em máquinas Linux.

5.3.3 Projetos Futuros

- Desenvolver um dispositivo Físico (Hardware) e ajustá-lo a Interface de Supervisionamento criada neste Projeto;
- Criar uma Interface de Supervisionamento do Squid.

6 CONCLUSÕES

Este Projeto objetivou a criação de uma Interface para realizar a supervisão e gestão das funções de firewall do Iptables para atuar como ferramenta de segurança em pequenas empresas de Informática.

Levando-se em conta, as complexidades inerentes as configurações dos módulos e regras do Iptables na busca pelo desenvolvimento de um ambiente de rede razoavelmente seguro, este Projeto contemplou o estudo de uma solução para estabelecer um relacionamento entre o usuário e o Iptables, de modo simples e amigável.

Esta solução foi implementada em um notebook com sistema operacional Linux, distribuição Fedora Core 5, e testada em um ambiente computacional de redes real, onde utilizou-se três máquinas, duas delas com sistema operacional Windows XP SP2, e a máquina Firewall com sistema operacional Linux, distribuição Fedora Core 9. Os equipamentos de rede utilizados foram um modem D-Link 2460, um switch Encore ENH9116-NWY e duas placas de rede Realtek.

Depois de realizada a fase de testes, a Interface de Supervisionamento do Iptables desenvolvida atendeu de forma bastante positiva, cumprindo com o objetivo para o qual destinou e motivou sua criação.

Como resultado, um usuário que não possui conhecimentos sobre a sintaxe das regras do Iptables, por meio da Interface de Supervisionamento, pode realizar a implementação de um Firewall Iptables em um ambiente organizacional de pequeno e médio porte, de modo simples, intuitivo e amigável.

Por fim, além de estabelecer de modo prático a supervisão dos módulos do Iptables, a Interface de Supervisionamento implementa uma boa política de segurança organizacional, caracterizada pela liberação de certos serviços elementares e bloqueio de demais outros que possam configurar um cenário de ameaça para a empresa.

Desta forma, com base nos resultados acima descritos, pode-se concluir que o objetivo para o qual motivou o desenvolvimento deste projeto, foi alcançado com êxito.

REFERÊNCIAS BIBLIOGRÁFICAS

ANÔNIMO. **Segurança Máxima:** o guia de um hacker para proteger seu site da internet e sua rede. Tradução [da 3.ed. original] de Edson Furmankiewicz. Rio de Janeiro: Campus, 2001.

BHERTOLDO, Leandro Márcio; TAROUCO, Liane M. R. **Uma Anásile do Software de Segurança SATAN – Security Administrator Tool for Analyzing Networks**. Disponível em: http://gtrh.tche.br/~berthold/work/satan.html. Acesso em: 2 abr. 2009.

CALETTI, Marcos. **IPS (INTRUSION PREVENTION SYSTEM) UM ESTUDO TEÓRICO E EXPERIMENTAL.** Novo Hamburgo: Feevale, 2006. Monografia (Bacharelado em Ciência da Computação), Instituto de Ciências Exatas e Tecnológicas, Centro Universitário Feevale, 2006, p. 32-33.

CERT.BR. **Incidentes Reportados ao CERT.Br – Janeiro a Dezembro de 2008**. Disponível em: http://www.cert.br/stats/incidentes/2008-jan-dec/total.html. Acesso: 16 mar. 2009.

_____. **Spams Reportados ao CERT.BR – Fevereiro de 2009**. Disponível em: http://www.cert.br/stats/spam/2009-feb/total.html. Acesso em: 16 mar. 2009.

_____. **Spams Reportados ao CERT.Br – Janeiro de 2009**. Disponível em: http://www.cert.br/stats/spam/2009-jan/total.html. Acesso em: 16 mar. 2009.

CHESWICK, William R; BELLOVIN, Steven M.; RUBIN, Aviel D. **Firewalls e Segurança na Internet: repelindo o hacker ardiloso**. Tradução de Edson Furmankiewicz. 2.ed. Porto Alegre: Bookman, 2005.

Comitê Gestor da Internet no Brasil – Antispam.br. **Tipos de spam** Disponível em: http://www.antispam.br/tipos/. Acesso em: 03.04.2009.

CORETEAM. **Project History**. Disponível em: http://www.netfilter.org/about.html#history. Acesso em: 27 abr. 2009.

DESAI, Neil. **Intrusion Prevention Systems: The Next Step in the Evolution of IDS.** SecurityFocus, 2003. Disponível em: http://www.securityfocus.com/print/infocus/1670 Acesso em: 3 abr. 2009.

FERREIRA, Rubem E. **Linux – Guia do Administrador do Sistema**. São Paulo: Novatec Editora Ltda, 2003.

FIALHO JR, Mozart. **Dicionário de Informática**. 2.ed. Goiânia: Editora Gráfica Terra Ltda, 2002.

FREIRE, Alexandre. **A Convergência das Tecnologias de Proteção de Perímetros**. Disponível em: http://blog.imasters.uol.com.br/alexandrefreire/2009/03/06/a-convergencia-das-tecnologias-de-protecao-de-perimetros/. Acesso em: 29 mar. 2009.

GEUS, Paulo Lício de; NAKAMURA, Emílio Tissato. **Segurança de Redes em ambientes cooperativos**. 2.ed. São Paulo: Futura, 2003.

JARGAS, Aurélio Marinho. **Dialog --tudo**. Texto retirado de apostila disponível em: http://aurelio.net/shell/dialog/. Acesso em: 15 mai. 2009.

_____. **Introdução ao Shell Script**. Texto retirado de apostila disponível em: http://aurelio.net/shell/apostila-introducao-shell.pdf. Acesso em: 13 mai. 2009.

JUCÁ, Humberto. **Técnicas avançadas de conectividade e Firewall em GNU/Linux**. Rio de Janeiro: Brasport, 2005.

NETO, Fernando Melis; GONÇALVES, Robério. Entenda melhor a segurança virtual. **Guia Fácil Informática: Segurança**. São Paulo: On Line Editora, n.04, p.12-19, 2005.

NEVES, Julio Cezar. **Programação SHELL LINUX**. 7. ed. Rio de Janeiro: Brasport, 2008.

ODIR. **IPTables – Desvendando o mistério**. Disponível em: http://www.vivaolinux.com.br/artigo/IPTables-Desvendando-o-misterio/. Acesso em: 27 abr. 2009.

ORNELLAS, Fabio Pugliese. **Firewall e roteamento avançado no Linux**. Disponível em: http://ornellas.apanela.com/dokuwiki/pub:pt-br:linuxfwrt. Acesso em: 07 mai. 2009.

PEREIRA, Marcio Machado. **Análise e estudo de segurança de corporações utilizando firewalls**. Espírito Santo: UFES, 2002. Monografia (Bacharelado em Ciência da Computação), Centro Tecnológico, UFES, 2002.

PURDY, Gregor N. **Linux iptables Guia de Bolso**. Tradução de Lilian Brandão. Rio de Janeiro: Alta Books, 2005.

Redação iMasters. **Spam custa anualmente às empresas mais de 180 mil dólares**. Disponível em: http://imasters.uol.com.br/noticia/12036/seguranca/spam_custa_anualmente_as_empresas_mais_de_180_mil_dolares/. Acesso em: 28 mar. 2009.

SILVA, Gleydson Mazioli da. **Guia Foca GNU/Linux, Capítulo 10 – Firewall iptables**, 2007. Disponível em: http://focalinux.cipsga.org.br/guia/avancado/ch-fw-iptables.htm. Acesso em: 02 mai. 2009.

SLOBODA, Vicente. **Conficker: O que muda depois do super-vírus**. Disponível em: http://imasters.uol.com.br/artigo/11805/seguranca/conficker_o_que_muda_depois_do_super-virus/. Acesso em: 28 mar. 2009.

STREBE, Matthew; PERKINS, Charles. **Firewalls 24 *seven***. Tradução de Lavio Pareschi; Revisão técnica de Alvaro Rodrigues Antunes. São Paulo: MAKRON Books, 2002.

WIKIPÉDIA, a enciclopédia livre. **Netfilter**. Disponível em: http://pt.wikipedia.org/wiki/Netfilter. Acesso em: 28 abr. 2009.

APÊNDICE A – CÓDIGOS E SCRIPTS

MapFirewall – Shell Script do Firewall.

```
#!/bin/bash
#+-----------------------------------------------------------------------------------------------------------+
#|                                                                                                           |
#| Map Firewall                                                                                              |
#| UniCEUB - Projeto Final de ENGENHARIA DA COMPUTACAO                                                       |
#| AUTOR: Marcelo de Souza Mendonca                                                                          |
#|                                                                                                           |
#+-----------------------------------------------------------------------------------------------------------+

#---------------------------------- VARIAVEIS DO FIREWALL ----------------------------------#

# VARIAVEIS DE INTERFACE

# VARIAVEIS DE REDE

# INTERFACES ATRIBUIDAS

# VARIAVEIS DE PROTOCOLOS

# VARIAVEIS DOS SERVICOS RAIZ
PRT_SSH_PORT="22"
PRTPROXY_PORT="8080"
PRT_HTTP_PORT="80"
PRT_HTTPS_PORT="443"
PRT_FTP_PORT="21"
PRT_FTP_HIGH_PORT="1024"
PRT_SMTP_PORT="25"
PRT_POP_PORT="110"
PRT_IMAP_PORT="995"
PRT_SMTP_GMAIL_PORT="465"
PRT_DNS_PORT="53"
PRT_ICMP_SERVICE="icmp"

# PROTOCOLOS ATRIBUIDOS

#-----------------------------------------------------------------------------------------------------------#


#--------------------------------------- ATIVAR ROTEAMENTO ----------------------------------#
echo "1" > /proc/sys/net/ipv4/ip_forward
#-----------------------------------------------------------------------------------------------------------#
```

```
#---------------------------------------- LIMPAR REGRAS ----------------------------------------#
iptables -F
iptables -F -t nat
iptables -F -t mangle
#-----------------------------------------------------------------------------------------------#

#---------------------------------------- POLITICA PADRÃO ----------------------------------------#
iptables -P INPUT DROP
iptables -P FORWARD DROP
#-----------------------------------------------------------------------------------------------#

#---------------------------------------- LIBERAR LOOPBACK ----------------------------------------#
iptables -A INPUT -i lo -j ACCEPT
#-----------------------------------------------------------------------------------------------#

#-------------------------------- LIBERAR FIREWALL NA INTERNET ----------------------------#

#-----------------------------------------------------------------------------------------------#

#-------------------------------- LIBERAR VOLTA DOS PACOTES ----------------------------#

#-----------------------------------------------------------------------------------------------#

#---------------------------------------- LIBERAR PORTAS ----------------------------------------#

#-----------------------------------------------------------------------------------------------#

#---------------------------------------- LIBERAR PING ----------------------------------------#

#-----------------------------------------------------------------------------------------------#

#---------------------------------- LIBERAR INTERNET DIRETA ----------------------------------#

#-----------------------------------------------------------------------------------------------#

#---------------------------------- ACESSO DIRETO INTERNET ----------------------------------#

#-----------------------------------------------------------------------------------------------#

#---------------------------- COMPARTILHAMENTO DE RECURSOS ----------------------------#
```

#----------#

#---------- PROXY INTERNO ----------#

#----------#

#---------- PROXY EXTERNO ----------#

#----------#

#---------- SERVICO HTTP ----------#

#----------#

#---------- SERVICO SECURE HTTP ----------#

#----------#

#---------- FTP ATIVO ----------#

RETORNO DOS PACOTES NA WAN

PERMITIR ENTRADA DE PEDIDO DE CONEXAO

LIBERAR FTPA PARA REDES

#----------#

#---------- FTP PASSIVO ----------#

#----------#

#---------- SERVICO SMTP ----------#

PRIORIDADE PARA O SMTP PADRAO

LIBERAR SMTP PARA REDES

PRIORIDADE PARA O SMTP DO GMAIL

LIBERAR SMTP DO GMAIL PARA REDES

```
#-------------------------------------------------------------------------------------------------------#

#---------------------------------------- SERVICO POP ----------------------------------------#
# PRIORIDADE PARA O POP
# LIBERAR POP PARA REDES
#-------------------------------------------------------------------------------------------------------#

#---------------------------------------- SERVICO IMAP ----------------------------------------#
# PRIORIDADE PARA O IMAP
# LIBERAR IMAP PARA REDES
#-------------------------------------------------------------------------------------------------------#

#---------------------------------------- LIBERAR SSH ----------------------------------------#
#-------------------------------------------------------------------------------------------------------#

#---------------------------------------- SERVICO DNS ----------------------------------------#
# LIBERAR DNS TCP
# LIBERAR DNS UDP
#-------------------------------------------------------------------------------------------------------#
```

Redes - Código para adicionar Redes/Máquinas

```
#!/bin/bash

# Implementando menu para adicionar rede!

prox=nome_rd

while : ; do

        case "$prox" in
                nome_rd)
                        prox=end_rd
                        nome_rd=$( dialog                       \
                                --stdout                        \
                                --title 'Map - Redes'           \
                                --inputbox 'Nome da rede:'      \
                                0 0                             )
                        LINHAEXS=`grep -n 'REDE_'$nome_rd'=' /root/Firewall/MapFirewall
| awk -F : '{print $1}'`
                        if [ $LINHAEXS -gt 0 ]
                                then
                                        . /root/Firewall/menus/REDES/f_rd_exs
                                        prox=0
                                        . /root/Firewall/menus/REDES/f_rd_inicio
                                        break
                                else
                                        prox=end_rd
                        fi
                        ;;
                end_rd)
                        prox=barr_rd
                        end_rd=$( dialog                        \
                                --stdout                        \
                                --title 'Map - Redes'           \
                                --inputbox 'Endereco da rede.
                                Ex: 172.16.2.0'                         \
                                0 0                             )
                        ;;
                barr_rd)
                        barr_rd=$( dialog                       \
                                --stdout                        \
                                --title 'Map - Redes'           \
                                --inputbox 'Barramento da rede.
                                Ex: 16, 24, 32.'                \
                                0 0                             )
                        VAR_END_BAR=$end_rd"/"$barr_rd
```

```
                        LINHAENDEXS=`grep -nw "$VAR_END_BAR"
/root/Firewall/MapFirewall | awk -F : '{print $1}'`
                        if [ $LINHAENDEXS -gt 0 ]
                                then
                                        . /root/Firewall/menus/REDES/f_rd_endexs
                                        . /root/Firewall/menus/REDES/f_rd_inicio
                                        break
                                else
                                        LINHADIN2=`grep -n '0 "Voltar"'
/root/Firewall/menus/REGRAS/f_rg_rd_criadas | awk -F : '{print $1}'`
                                        OPCAO2=`echo "$LINHADIN2-9" | bc`
                                        sed -i "$LINHADIN2's/^/       '$OPCAO2' "'$nome_rd"'
\\\n/' /root/Firewall/menus/REGRAS/f_rg_rd_criadas
                                        LINHAOPCAO2=`grep -n '#LINHA_DE_COMANDO'
/root/Firewall/menus/REGRAS/f_rg_rd_criadas | awk -F : '{print $1}'`
                                        sed -i "$LINHAOPCAO2's/^/       '$OPCAO2')
#:'$nome_rd':#'$nome_rd'_LINHA \n/' /root/Firewall/menus/REGRAS/f_rg_rd_criadas
                                        LINHAOPCAO2=`grep -n '#LINHA_DE_COMANDO'
/root/Firewall/menus/REGRAS/f_rg_rd_criadas | awk -F : '{print $1}'`
                                        sed -i "$LINHAOPCAO2's/^/
REDE_NOM="'$nome_rd"' # \n/' /root/Firewall/menus/REGRAS/f_rg_rd_criadas
                                        LINHAOPCAO2=`grep -n '#LINHA_DE_COMANDO'
/root/Firewall/menus/REGRAS/f_rg_rd_criadas | awk -F : '{print $1}'`
                                        sed -i "$LINHAOPCAO2's/^/
LINHA_REDE=6 \n/' /root/Firewall/menus/REGRAS/f_rg_rd_criadas
                                        LINHAOPCAO2=`grep -n '#LINHA_DE_COMANDO'
/root/Firewall/menus/REGRAS/f_rg_rd_criadas | awk -F : '{print $1}'`
                                        sed -i "$LINHAOPCAO2's/^/               cp
\/root\/Firewall\/menus\/REGRAS\/f_rg_PING_PADRAORG
\/root\/Firewall\/menus\/REGRAS\/f_rg_PING_"$REDE_NOM" # \n/'
/root/Firewall/menus/REGRAS/f_rg_rd_criadas
                                        LINHAOPCAO2=`grep -n '#LINHA_DE_COMANDO'
/root/Firewall/menus/REGRAS/f_rg_rd_criadas | awk -F : '{print $1}'`
                                        sed -i "$LINHAOPCAO2's/^/               \sed -i
"'"$LINHA_REDE"'s\/^\/REDE_NOM="'$REDE_NOM"' #\/"'
\/root\/Firewall\/menus\/REGRAS\/f_rg_PING_"$REDE_NOM" # \n/'
/root/Firewall/menus/REGRAS/f_rg_rd_criadas
                                        LINHAOPCAO2=`grep -n '#LINHA_DE_COMANDO'
/root/Firewall/menus/REGRAS/f_rg_rd_criadas | awk -F : '{print $1}'`
                                        sed -i "$LINHAOPCAO2's/^/               .
\/root\/Firewall\/menus\/REGRAS\/f_rg_PING_"$REDE_NOM";; \n/'
/root/Firewall/menus/REGRAS/f_rg_rd_criadas
                                        LINHAPROX=`grep -n "VARIAVEIS DE REDE"
/root/Firewall/MapFirewall | awk -F : '{ print $1+1 }'`
                                        LINHADIN=`grep -n '0 "Menu Principal"'
/root/Firewall/menus/REDES/f_rd_inicio | awk -F : '{print $1}'`
                                        LINHAOPCAO=`grep -n '#LINHA_DE_COMANDO'
/root/Firewall/menus/REDES/f_rd_inicio | awk -F : '{print $1+1}'`
                                        OPCAO=`echo "$LINHADIN-9" | bc`
```

```
                                        sed -i "$LINHADIN's/^/        '$OPCAO' "'$nome_rd'"
\\\n/' /root/Firewall/menus/REDES/f_rd_inicio
                                        sed -i "$LINHAOPCAO's/^/        '$OPCAO')
#:'$nome_rd':#'$nome_rd'_LINHA \n/' /root/Firewall/menus/REDES/f_rd_inicio
                                        LINHAOPCAO=`grep -n '#LINHA_DE_COMANDO'
/root/Firewall/menus/REDES/f_rd_inicio | awk -F : '{print $1}'`
                                        sed -i
""$LINHAPROX"s/^/REDE_"$nome_rd"="$end_rd"\/"$barr_rd"\n/"
/root/Firewall/MapFirewall
                                        sed -i "$LINHAOPCAO's/^/                .
\/root\/Firewall\/menus\/REDES\/f_rd_'$nome_rd';; \n/'
/root/Firewall/menus/REDES/f_rd_inicio
                                        cp /root/Firewall/menus/REDES/f_rd_PADRAORD
/root/Firewall/menus/REDES/f_rd_"$nome_rd"
                                        LINHANOM=`grep -n '#NOME_DA_REDE'
/root/Firewall/menus/REDES/f_rd_"$nome_rd" | awk -F : '{print $1+1}'`
                                        sed -i "$LINHANOM's/^/REDE_NOM="'$nome_rd'"/'
/root/Firewall/menus/REDES/f_rd_"$nome_rd"
                                        LINHAOP=`grep -n '#OPCAO_DA_REDE'
/root/Firewall/menus/REDES/f_rd_"$nome_rd" | awk -F : '{print $1+1}'`
                                        sed -i "$LINHAOP's/^/REDE_OP="'$OPCAO'"/'
/root/Firewall/menus/REDES/f_rd_"$nome_rd"
                                        LINHAEND=`grep -n '#ENDERECO_DA_REDE'
/root/Firewall/menus/REDES/f_rd_"$nome_rd" | awk -F : '{print $1+1}'`
                                        sed -i "$LINHAEND's/^/REDE_END='$end_rd'/'
/root/Firewall/menus/REDES/f_rd_"$nome_rd"
                                        LINHABARR=`grep -n '#BARRAMENTO_DA_REDE'
/root/Firewall/menus/REDES/f_rd_"$nome_rd" | awk -F : '{print $1+1}'`
                                        sed -i "$LINHABARR's/^/REDE_BARR='$barr_rd'/'
/root/Firewall/menus/REDES/f_rd_"$nome_rd"
                                        LINHAFIM2=`grep -n '#LINHA_FIM_MENU'
/root/Firewall/menus/REGRAS/f_rg_rd_criadas | awk -F : '{print $1}'`
                                        sed -i
"$LINHAFIM2'c\#:'$nome_rd':#LINHA_FIM_MENU'
/root/Firewall/menus/REGRAS/f_rg_rd_criadas
                                        LINHAFIM=`grep -n '#LINHA_FIM_MENU'
/root/Firewall/menus/REDES/f_rd_inicio | awk -F : '{print $1}'`
                                        sed -i
"$LINHAFIM'c\#:'$nome_rd':#LINHA_FIM_MENU'
/root/Firewall/menus/REDES/f_rd_inicio
                                        sed -i '1s/^/#:'$nome_rd':REDE_'$nome_rd'\n/'
/root/Firewall/menus/REDES/f_rd_REDESCRIADAS
                                        . /root/Firewall/MapFirewall
                                        . /root/Firewall/menus/REDES/f_rd_inicio
                        fi
                        break;;
                *)
                        . /root/Firewall/menus/REDES/f_rd_inicio;;
        esac
done
```

Regras – Script de liberação do SSH para Redes/Máquinas.

```
#!/bin/bash

# Implementando menu de liberacao do SSH entre Sub-redes!

#REDE_DE_ORIGEM

#REDE_DE_DESTINO



OP=$( dialog \
        --stdout \
        --title "Map Firewall" \
        --menu "Liberar SSH\nORIGEM: "$REDE_ORIGEM"\nDESTINO:
"$REDE_DESTINO"" \
        0 0 0 \
        1 "Sim" \
        2 "Nao" \
        3 "Voltar" \
        0 "Menu Principal" )
case $OP in
        1)
                rm -rf /root/Firewall/menus/REGRAS/f_rg_ORIGEM
/root/Firewall/menus/REGRAS/f_rg_DESTINO
                if [ $REDE_ORIGEM = $REDE_DESTINO ]
                        then
                                . /root/Firewall/menus/REGRAS/f_rg_RDIGUAIS
                                cp /root/Firewall/menus/REGRAS/f_rg_FOR_SSH_PADRAO
/root/Firewall/menus/REGRAS/f_rg_FOR_SSH
                                . /root/Firewall/menus/REGRAS/f_rg_config_SSH
                        else
                                L_ATR_OR=`grep -n "INT_ATR_"$REDE_ORIGEM"="
/root/Firewall/MapFirewall | awk -F : '{print $1}'`
                                if [ $L_ATR_OR -gt 0 ]
                                        then
                                                L_ATR_DE=`grep -n
"INT_ATR_"$REDE_DESTINO"=" /root/Firewall/MapFirewall | awk -F : '{print $1}'`
                                                if [ $L_ATR_DE -gt 0 ]
                                                        then
                                                                INTFANTASIAOR=`grep -n
"#RD_"$REDE_ORIGEM":" /root/Firewall/MapFirewall | awk -F : '{print $3}'`
                                                                INTREALOR=`grep -n
"INT_"$INTFANTASIAOR"=" /root/Firewall/MapFirewall | awk -F : '{print $4}'`
                                                                INTFANTASIADE=`grep -n
"#RD_"$REDE_DESTINO":" /root/Firewall/MapFirewall | awk -F : '{print $3}'`
```

```
                                                INTREALDE=`grep -n
"INT_"$INTFANTASIADE"=" /root/Firewall/MapFirewall | awk -F : '{print $4}'`
                                                if [ $INTFANTASIAOR =
$INTFANTASIADE ]
                                                        then
                                                                .
/root/Firewall/menus/REGRAS/f_rg_INTIGUAIS
                                                                cp
/root/Firewall/menus/REGRAS/f_rg_FOR_SSH_PADRAO
/root/Firewall/menus/REGRAS/f_rg_FOR_SSH
                                                                .
/root/Firewall/menus/REGRAS/f_rg_config_SSH
                                                        else
                                                                RGEXS=`grep -n
"#SSH_"$REDE_ORIGEM"_"$REDE_DESTINO" #" /root/Firewall/MapFirewall | awk -F :
'{print $1}'`
                                                                if [ $RGEXS -gt 0 ]
                                                                        then
                                                                                .
/root/Firewall/menus/REGRAS/f_rg_PING_ON
                                                                                cp
/root/Firewall/menus/REGRAS/f_rg_FOR_SSH_PADRAO
/root/Firewall/menus/REGRAS/f_rg_FOR_SSH
                                                                                .
/root/Firewall/menus/REGRAS/f_rg_config_SSH
                                                                        else

        REL_REG=`grep -n "# Liberar SSH entre REDES/MAQS:"
/root/Firewall/menus/RELATORIO_DE_REGRAS | awk -F : '{print $1+1}'`
                                                                                sed -i
"$REL_REG's/^/ORIGEM: '$REDE_ORIGEM' DESTINO: '$REDE_DESTINO' - SSH
OK\n/" /root/Firewall/menus/RELATORIO_DE_REGRAS

        LINHAPROX=`grep -n "LIBERAR SSH" /root/Firewall/MapFirewall | awk -F :
'{print $1+1}'`
                                                                                sed -i
"$LINHAPROX's/^/iptables -A FORWARD -p tcp -i $INT_ATR_'$REDE_ORIGEM' -s
$REDE_'$REDE_ORIGEM' -o $INT_ATR_'$REDE_DESTINO' -d
$REDE_'$REDE_DESTINO' --dport $PRT_SSH_PORT -j ACCEPT
#SSH_'$REDE_ORIGEM'_'$REDE_DESTINO' #\n/' /root/Firewall/MapFirewall

        L_VOLTA_PACOTES=`grep -n "#L_V_P_"$INTFANTASIAOR" #"
/root/Firewall/MapFirewall | awk -F : '{print $1}'`
                                                                                if [
$L_VOLTA_PACOTES -gt 0 ]

        then

                cp /root/Firewall/menus/REGRAS/f_rg_FOR_SSH_PADRAO
/root/Firewall/menus/REGRAS/f_rg_FOR_SSH
```

```
                . /root/Firewall/MapFirewall

                . /root/Firewall/menus/REGRAS/f_rg_config_SSH

        else

                LINHAPROX=`grep -n "LIBERAR VOLTA DOS PACOTES"
/root/Firewall/MapFirewall | awk -F : '{print $1+1}'`

                sed -i "$LINHAPROX's/^/iptables -A FORWARD -o
$INT_'$INTFANTASIAOR' -m state --state ESTABLISHED,RELATED -j ACCEPT
#L_V_P_'$INTFANTASIAOR' #\n/' /root/Firewall/MapFirewall

                cp /root/Firewall/menus/REGRAS/f_rg_FOR_SSH_PADRAO
/root/Firewall/menus/REGRAS/f_rg_FOR_SSH

                . /root/Firewall/MapFirewall

                . /root/Firewall/menus/REGRAS/f_rg_config_SSH
                                                                        fi
                                                                fi
                                                        fi
                                                else
                                                        .
/root/Firewall/menus/REGRAS/f_rg_RDATRINT_DE
                                                        cp
/root/Firewall/menus/REGRAS/f_rg_FOR_SSH_PADRAO
/root/Firewall/menus/REGRAS/f_rg_FOR_SSH
                                                        .
/root/Firewall/menus/REGRAS/f_rg_config_SSH
                                                fi
                                        else
                                                .
/root/Firewall/menus/REGRAS/f_rg_RDATRINT_OR
                                                cp
/root/Firewall/menus/REGRAS/f_rg_FOR_SSH_PADRAO
/root/Firewall/menus/REGRAS/f_rg_FOR_SSH
                                                .
/root/Firewall/menus/REGRAS/f_rg_config_SSH
                                        fi
                fi
                ;;
        2)
                rm -rf /root/Firewall/menus/REGRAS/f_rg_ORIGEM
/root/Firewall/menus/REGRAS/f_rg_DESTINO
                RGEXS=`grep -n "#SSH_"$REDE_ORIGEM"_"$REDE_DESTINO" #"
/root/Firewall/MapFirewall | awk -F : '{print $1}'`
                if [ $RGEXS -gt 0 ]
                        then
```

```
                                sed -i ""$RGEXS"d" /root/Firewall/MapFirewall
                                REL_REG=`grep -n "ORIGEM: "$REDE_ORIGEM"
DESTINO: "$REDE_DESTINO" - SSH OK"
/root/Firewall/menus/RELATORIO_DE_REGRAS | awk -F : '{print $1}'`
                                sed -i ""$REL_REG"d"
/root/Firewall/menus/RELATORIO_DE_REGRAS
                                cp /root/Firewall/menus/REGRAS/f_rg_FOR_SSH_PADRAO
/root/Firewall/menus/REGRAS/f_rg_FOR_SSH
                                . /root/Firewall/MapFirewall
                                . /root/Firewall/menus/REGRAS/f_rg_config_SSH
                        else
                                . /root/Firewall/menus/REGRAS/f_rg_PING_OFF
                                cp /root/Firewall/menus/REGRAS/f_rg_FOR_SSH_PADRAO
/root/Firewall/menus/REGRAS/f_rg_FOR_SSH
                                . /root/Firewall/menus/REGRAS/f_rg_config_SSH
                fi
                ;;
        3)
                rm -rf /root/Firewall/menus/REGRAS/f_rg_ORIGEM
/root/Firewall/menus/REGRAS/f_rg_DESTINO
                cp /root/Firewall/menus/REGRAS/f_rg_FOR_SSH_PADRAO
/root/Firewall/menus/REGRAS/f_rg_FOR_SSH
                . /root/Firewall/menus/REGRAS/f_rg_config_SSH
                ;;
        *)
                rm -rf /root/Firewall/menus/REGRAS/f_rg_ORIGEM
/root/Firewall/menus/REGRAS/f_rg_DESTINO
                cp /root/Firewall/menus/REGRAS/f_rg_FOR_SSH_PADRAO
/root/Firewall/menus/REGRAS/f_rg_FOR_SSH
                . /root/Firewall/menus/f_inicio
                ;;
esac
```