

**LIGA DE ENSINO DO RIO GRANDE DO NORTE
FACULDADE NATALENSE PARA O DESENVOLVIMENTO DO RN
ESPECIALIZAÇÃO EM REDES DE COMPUTADORES**

MARCELO FIGUEIREDO BELLAGUARDA

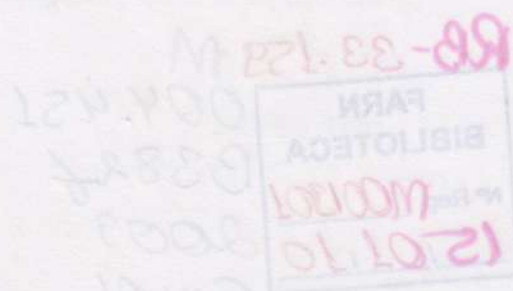
**FWBUILDER : UMA FERRAMENTA GRÁFICA DE ADMINISTRAÇÃO DE
FIREWALL NO LINUX**

**FWBUILDER : UMA FERRAMENTA GRÁFICA DE ADMINISTRAÇÃO DE
FIREWALL NO LINUX**

**ORIENTADOR: ProC MSc. Aluísio
Ferreira da Rocha Neto.**

NATAL-RN

2009



LIGA DE ENSINO DO RIO GRANDE DO NORTE
FACULDADE NATALENSE PARA O DESENVOLVIMENTO DO RN
ESPECIALIZAÇÃO EM REDES DE COMPUTADORES

MARCELO FIGUEIREDO BELLAGUARDA

belaguarda@pop.com.br

FWBUILDER : UMA FERRAMENTA GRÁFICA DE ADMINISTRAÇÃO DE
FIREWALL NO LINUX

RB-33.159 M

FARN	004.451
BIBLIOTECA	B382f
Nº Reg	2009
15.01.10	Ex:01

NATAL-RN

2009

MARCELO FIGUEIREDO BELLAGUARDA

**FWBUILDER : UMA FERRAMENTA GRÁFICA DE ADMINISTRAÇÃO DE
FIREWALL NO LINUX**

Monografia apresentada e aprovada em 11 de setembro de 2009, pela banca examinadora

**FWBUILDER : UMA FERRAMENTA GRÁFICA DE ADMINISTRAÇÃO DE
FIREWALL NO LINUX**

Prof. MSc. Aluizio Ferreira da Rocha Neto
(Orientador)

Monografia apresentada ao curso de Especialização em Redes de Computadores da Faculdade Natalense para o Desenvolvimento do Rio Grande do Norte como requisito parcial para a obtenção do título de Especialista em Redes de Computadores.

**ORIENTADOR: Prof. MSc. Aluizio
Ferreira da Rocha Neto.**

NATAL-RN

2009

Catálogo na Publicação – Biblioteca da FARN
Setor de Processos Técnicos

Bellaguarda, Marcelo Figueiredo

Fwbuilder: uma ferramenta gráfica de administração de firewall no linux/
Marcelo Figueiredo Bellaguarda. – Natal: FARN, 2009.
51f.

Orientador: Prof. MSc. Aluizio Ferreira da Rocha Neto
Monografia (Especialização em Redes de Computadores) – Faculdade
Natalense para o Desenvolvimento do Rio Grande do Norte.

1. Redes de Computadores – Monografia. 2. Administração de firewall –
Monografia. 3. Linux – Monografia. I. Título.

RN/FARN/BC

CDU 004.451

MARCELO FIGUEIREDO BELLAGUARDA

**FWBUILDER : UMA FERRAMENTA GRÁFICA DE ADMINISTRAÇÃO DE
FIREWALL NO LINUX**

Monografia apresentada e aprovada em 11 de setembro de 2009, pela banca examinadora

composta pelos seguintes membros

Prof. MSc. Aluizio Ferreira da Rocha Neto
(Orientador)

(Membro examinador)

(Membro examinador)

RESUMO

O propósito deste trabalho foi desenvolver um estudo sobre uma ferramenta de gerenciamento de firewall, visando compreender o FWBuilder, que é uma ferramenta de fácil gerenciamento e edição de regras e entender alguns protocolos de rede, onde foi explorado todas as funções da ferramenta como criação de um objeto firewall, placas de rede, serviços customizados, de grupos, ICMP, IP, TCP e UDP, objetos de endereços, faixas de endereços, grupo de objetos, hosts, redes, tempo em que as regras serão executadas, utilização de protocolos, como utilizar as abas de adições das políticas de firewall, NAT e roteamento, um exemplo prático em um ambiente simulado de uma rede corporativa, aplicando-se regras necessárias para um bom funcionamento e uma maior segurança do firewall, como permissões para algumas regras e negações para outras. Também foi utilizado traduções de endereços, para que, na saída do firewall, os pacotes saíssem com um endereço público sendo reconhecido na internet e os endereços vindos da internet sejam reconhecidos pela rede interna, controle de acesso via SSH ao firewall, redirecionamento de portas para o monitoramento de conteúdos acessado pelos usuários da rede e um pequeno script para que todas as vezes que o firewall for iniciado possa executar automaticamente todas as regras gravadas no firewall. A grande vantagem da ferramenta estudada é que ao compilar as regras que serão aplicadas no firewall, podem-se ver possíveis duplicações ou redundâncias nas regras que serão aplicadas.

Palavras-Chave: Gerenciamento. Firewall. Protocolos. Regras. Redirecionamentos. Monitoramento. FWBuilder.

ABSTRACT

The purpose of this study was to develop a study on a management tool firewall, seeking to understand the FWBuilder, which is a tool of easy management and publishing of the rules and understand some network protocols, where he explored all the functions of the tool as creating an object firewall, network cards, customized services, groups, ICMP, IP, TCP and UDP objects, addresses, address ranges, a group of objects, hosts and networks, at which time the rules will be implemented, use of protocols, how to use the tabs of items of firewall policies, NAT and routing, a practical example in a simulated environment of a corporate network, applying the rules necessary for the proper functioning and greater security of firewall, such as permissions to a few rules and disclaimers for others. It was also used address translations, so that the output of the firewall, the packets go out with a public address being recognized on the Internet and addresses from the Internet to be recognized by internal network access control via SSH to the firewall, port forwarding for monitoring of content accessed by Internet users and a small script so that every time the firewall is automatically started to run all rules stored in the firewall. The great advantage of the tool study is that to compile the rules to be applied on the firewall, you can see the possible duplication or redundancy in the rules that will apply.

Key-words: Management. Firewall. Protocols. Rules. Redirects. Monitoring. FWBuilder.

Figura 17	Tela de definição das regras de NAT	31
Figura 18	Tela de definição das regras de encaminhamento	35
Figura 19	Captura de tela de uso do FWBuilder	36
Figura 20	Janela do FWBuilder com a opção de abrir ou criar um arquivo de regras	38
Figura 21	Tela de definição das propriedades do Firewall	39
Figura 22	Tela de opções avançadas do Firewall	40
Figura 23	Tela com as configurações das interfaces de rede do Firewall	41
Figura 24	Tela com as regras de políticas de filtragem do Firewall	43
Figura 25	Tela com as regras de NAT e redirecionamento de portas do Firewall	46
Figura 26	Compilação das regras e scripts aplicados no Firewall	48
Figura 27	Script para iniciar o Firewall	49

LISTA DE ILUSTRAÇÕES

Figura 1	Interface do FWBuilder	17
Figura 2	Tela de definição do nome do Firewall.....	19
Figura 3	Tela de definição das interfaces do Firewall.....	20
Figura 4	Tela de definição das interfaces do Firewall.....	21
Figura 5	Tela de definição dos endereços de rede.....	22
Figura 6	Tela de definição dos endereços de Hosts	23
Figura 7	Tela de definição do intervalo de endereços de rede	23
Figura 8	Tela de definição do grupo de objetos	24
Figura 9	Tela de definição de redes.....	25
Figura 10	Tela de personalização dos serviços de rede.....	26
Figura 11	Tela de definição dos grupos de serviços	27
Figura 12	Tela de definição de um novo serviço ICMP.....	27
Figura 13	Tela de definição dos serviços IP.....	29
Figura 14	Tela de definição dos serviços TCP.....	30
Figura 15	Tela de definição dos serviços UDP	31
Figura 16	Tela de definição das políticas do Firewall.....	32
Figura 17	Tela de definição das regras de NAT.....	33
Figura 18	Tela de definição das regras de roteamento	35
Figura 19	Cenário do caso de uso do FWBuilder	36
Figura 20	Janela do FWBuilder com a opção de abrir ou criar um arquivo de regras do mesmo	38
Figura 21	Tela de definição das propriedades do Firewall	39
Figura 22	Tela de opções avançadas do iptables.....	40
Figura 23	Tela com as configurações das interfaces de rede do firewall.....	41
Figura 24	Tela com as regras de políticas de filtragem do Firewall	43
Figura 25	Tela com as regras de NAT e redirecionamento de portas do Firewall.....	46
Figura 26	Compilação das regras a serem aplicadas no Firewall.....	48
Figura 27	Script para iniciar o Firewall.....	49
28	APLICANDO AS REGRAS DE FIREWALL NO SERVIDOR	47
29	UM SCRIPT PARA INICIAR O FIREWALL AUTOMATICAMENTE.....	49
30	CONCLUSÃO	50
31	REFERÊNCIAS.....	51

1	INTRODUÇÃO.....	7
1.1	PROBLEMA DA PESQUISA.....	8
1.2	OBJETIVOS.....	9
1.2.1	Objetivos Específicos.....	9
1.3	JUSTIFICATIVA.....	9
2	REFERÊNCIAL TEÓRICO.....	10
2.1	REDES DE COMPUTADORES.....	10
2.2	<i>INTERNET</i>	11
2.3	<i>INTRANET</i>	11
2.4	PRINCÍPAIS PROTOCOLOS DA FAMÍLIA TCP/IP.....	12
2.4.1	IP (<i>Internet Protocol</i>).....	12
2.4.2	TCP (<i>Transmission Control Protocol</i>).....	12
2.4.3	UPD (<i>User Datagram Protocol</i>).....	13
2.5	<i>FIREWALL</i>	13
2.5.1	Tipos de <i>Firewall</i>.....	13
2.6	<i>IPTABLES</i>	14
2.6.1	Algumas diferenças entre <i>IPTABLES</i> E <i>IPCHAINS</i>.....	15
3	FWBUILDER.....	15
3.1	FUNÇÕES DO <i>FWBUILDER</i>	17
3.1.1	Categoria de objetos <i>USER</i>.....	18
3.1.2	Categoria de objetos <i>Standard</i>.....	31
3.1.3	Organização das regras nos painéis.....	31
4	EXEMPLO DE CASO DE USO DO FWBUILDER.....	36
4.1	DEFINIÇÃO DO DIRETÓRIO DE TRABALHO.....	38
4.2	CONFIGURAÇÃO DO <i>FWBUILDER</i>	38
4.3	CONFIGURANDO AS INTERFACES DO <i>FIREWALL</i>	41
4.4	DEFININDO AS REGRAS DE FILTRAGEM.....	43
4.5	DEFININDO AS REGRAS DE NAT.....	45
4.6	APLICANDO AS REGRAS DE FIREWALL NO SERVIDOR.....	47
4.7	UM <i>SCRIPT</i> PARA INICIAR O <i>FIREWALL</i> AUTOMATICAMENTE.....	49
5	CONCLUSÃO.....	50
	REFERÊNCIAS.....	51

1 INTRODUÇÃO

O surgimento das redes de computadores tem sua origem nos períodos áureos da Guerra Fria. Na década de 60, o governo dos Estados Unidos temia um ataque às suas bases militares pela URSS. Acontece que, em um caso de ataque, informações importantes e sigilosas poderiam ser perdidas, não oferecendo aos EUA condições de resistência e reação. Então foi idealizado um modelo de troca e compartilhamento de informações que permitisse a descentralização das mesmas. Foi preciso, portanto, criar uma rede, a ARPANET, criada pela ARPA, sigla para *Advanced Research Projects Agency*.

A ARPANET funcionava através de um sistema conhecido como chaveamento de pacotes, que era um esquema de transmissão de dados em rede de computadores no qual as informações eram divididas em pequenos "pacotes" que, por sua vez, continham trecho dos dados, o endereço do destinatário e informações que permitiam a remontagem da mensagem original.

Na década de 70, o governo dos EUA permitiu que pesquisadores desenvolvessem, nas suas respectivas universidades, estudos na área de defesa, para que pudessem também entrar na ARPANET. Dividiu-se então este sistema em dois grupos, a MILNET, que possuía as localidades militares e a nova ARPANET, que possuía as localidades não militares. O desenvolvimento da rede, nesse ambiente mais livre, pôde então acontecer.

A mesma lógica se deu com a Internet. Um esquema técnico denominado Protocolo de Internet (Internet Protocol) permitia que o tráfego de informações fosse encaminhado de uma rede para outra. Todas as redes conectadas pelo endereço IP na Internet comunicavam-se para que todas pudessem trocar mensagens.

Na década de 80, a rede vai se tornando mais desenvolvida. Tim Berners-Lee foi o responsável pela criação da *World Wide Web*, um sistema que inicialmente interligava sistemas de pesquisas científica e acadêmicas, interligando universidades. A rede coletiva ganhou uma maior divulgação pública a partir de 1990.

Vale destacar que, em 1992, o interesse mundial aliado ao interesse comercial observava o potencial financeiro e rentável daquela "novidade", e a popularização da internet na década de 90.

Com o "boom" da informática surgem os hackers que efetuam ataques através de softwares, *spyweres*, *worms* e etc. A cada geração que passa os firewalls vão ficando mais seguros, mas nunca totalmente imune a ataques.

Os primeiros firewalls de segurança de redes surgiram no início dos anos 90 e eram dispositivos que possuíam um pequeno conjunto de regras do tipo: Alguém da rede A pode acessar a rede B, ou alguém da rede C não pode acessar a rede B por exemplo. Esses firewalls eram efetivos, mas bastante limitados, pois era muito difícil configurar as regras corretamente.

A segunda geração de firewalls foi mais bem elaborada pois usavam filtros de pacotes e de aplicativos (*proxy*) além de trazer uma GUI (*Graphic User Interface* – Interface gráfica) para gerenciar as políticas de firewall. Estes dispositivos eram conhecidos como *Bastion Host*, que são Firewalls ou roteadores que provêm acesso de controle ao perímetro da rede.

Na terceira geração eles suportavam a tecnologia SMLI - *Stateful Multi-Layer Inspection*, ou seja, Inspeção Total de todas as Camadas do modelo OSI. Esta tecnologia permite que o firewall examine cada “pacote” em todas suas camadas do modelo OSI, desde a de transporte até a de aplicação, sem necessidade de processar a mensagem.

O IPTABLES, um sistema de controle de filtros para protocolos ipv4, surgiu para um melhor gerenciamento dos firewalls. É com ele que serão criadas as regras do firewall deste trabalho.

Este trabalho mostrará um estudo sobre uma dessas ferramentas de firewalls, o FWBuilder, onde será explorada a sua configuração e analisado um exemplo prático da ferramenta em um ambiente simulado de rede corporativa.

1.1 PROBLEMA DE PESQUISA

Diante dos perigos existentes na Internet, surgiram os firewalls e a cada dia surgem novas ferramentas para gerenciamento dos mesmos e com elas novas regras vêm sendo implantadas para que torne mais seguro a navegação pela web, e principalmente a integridade das redes corporativas.

Acompanhando o avanço da internet, onde a cada dia surge um novo vírus, os firewalls vêm acompanhando essa mudança e freqüentemente desenvolvendo novas tecnologias para acompanhá-las.

A importância dessa pesquisa é de mostrar alguns conceitos básicos de Redes de Computadores, firewall, IPTables, entre outros, e a utilização da ferramenta FWBuilder no gerenciamento do mesmo. Portanto foi necessário um estudo para entender e verificar as regras que poderão ser aplicadas. Além disso, será abordado o estudo e o entendimento dessa

ferramenta de gerenciamento de firewalls e a aplicação de regras de iptables e os principais protocolos TCP/IP.

2.1 REDES DE COMPUTADORES

1.2 OBJETIVOS

Esse projeto tem a finalidade de realizar um estudo sobre firewall e seus principais protocolos e um detalhamento sobre a utilização da ferramenta FWBuilder para administração de firewall Linux, suas vantagens e as principais funções existente na ferramenta.

1.2.1 Objetivos Específicos

Para atingir o objetivo geral do trabalho, as seguintes etapas serão realizadas:

- Pesquisar a respeito dos Firewalls, desde o surgimento até os dias de hoje.
- Apresentar os principais protocolos TCP/IP e seus conceitos.
- Apresentar alguns conceitos de redes de computadores, intranet e internet.
- Apresentar as vantagens da ferramenta FWBuilder e suas principais funções.
- Mostrar um exemplo prático do FWBuilder, para que haja um maior entendimento desta ferramenta.

1.3 JUSTIFICATIVA

A importância dessa pesquisa é entender os reais motivos de se ter um firewall e as ferramentas que podem ser utilizadas para o gerenciamento do mesmo. Hoje já existem diversos softwares que realizam esse gerenciamento. Aqui, Será aprofundado os estudos numa única ferramenta de gerenciamento de firewall chamada FWBuilder, que tem como principal objetivo criar um ambiente de administração gráfica das suas regras de Iptables e PIX-Firewall da CISCO. Sua interface gráfica torna a utilização ainda mais simples.

Além disso, o projeto irá mostrar, também, as funções do FWBuilder com suas principais características e como funciona cada função.

2 REFERENCIAL TEÓRICO

2.1 REDES DE COMPUTADORES

Segundo Tanenbaum (1997), uma Rede de Computadores consiste na conexão de dois ou mais computadores para permitir o compartilhamento de recursos e a troca de informações entre as máquinas.

As redes de computadores divide-se em 3(três) categorias, são elas:

- LAN: É uma rede de área local que cobre uma distância reduzida, como uma empresa, um escritório ou um conjunto de prédios. A LAN cobre uma distância de até 10 km no máximo. Quanto maior a distância de um nó da rede a outro, maior a ocorrência de taxas de erros.
- MAN: É uma rede de área metropolitana, que ocupam o perímetro de uma cidade. São mais rápidas e permitem que empresas com filiais em bairros diferentes se conectem entre si. A distância alcançada por uma MAN é a partir de 10 km.
- WAN: É uma rede de área alargada ou de longa distância, que abrange uma grande área geográfica como um país ou continente. Um exemplo das WAN'S é a internet, a rede mundial de computadores.

Nas redes de computadores, existem algumas topologias, para que ocorra a comunicação entre os equipamentos, as principais são:

- Topologia em estrela: Todas as conexões partem de um ponto central (concentrador), normalmente um hub ou switch. É o modelo mais utilizado atualmente.
- Topologia em anel: Todos os computadores são conectados em um anel. É a topologia das redes Token Ring, popularizadas pela IBM nos anos 80. Hoje, esse modelo é mais utilizado em sistemas de automação industrial. Existe uma opção na topologia em anel, para aumentar a confiabilidade e o desempenho da rede, usando anéis múltiplos.
- Topologia em barra: É uma topologia de rede em que todos os computadores são ligados em um mesmo barramento físico de dados. Essa topologia tem um grande problema, pois uma máquina apenas pode enviar um dado no barramento por vez.

2.2 INTERNET

Segundo Wikipédia (2009), Internet é um conglomerado de redes em escala mundial de milhões de computadores interligados pela família de protocolos de rede conhecida como TCP/IP, que permite o acesso a informações e todo tipo de transferência de dados. Ela carrega uma ampla variedade de recursos e serviços, incluindo os documentos interligados por meio de hiperligações da World Wide Web, e a infra-estrutura para suportar correio eletrônico e serviços como comunicação instantânea e compartilhamento de arquivos.

Existe uma diferença entre Internet e internet, a principal delas é que a Internet se refere à *internet* global e pública, disponibilizada pelo Protocolo de Internet e a *internet* significa um conjunto de redes de computadores interligadas.

2.3 INTRANET

Segundo Lawnton (2005), Intranet é uma rede de computadores privada, e só está disponível para uma organização interna.

As principais características de uma intranet são:

- Permite o compartilhamento de arquivos e impressoras;
- Permite a transmissão de vídeos;
- Unifica as informações para todos os membros de uma organização, não importando sua localização geográfica;
- Facilidade de instalação e administração;
- Permite a arquitetura aberta;
- Baixo custo de implementação com boa relação custo-benefício;
- Acesso rápido as informações, com melhora para tomada de decisão;
- Utiliza múltiplos protocolos.

A grande vantagem de uma intranet é que ela pode aumentar a produtividade em uma organização e ajuda a encontrar dados de forma rápida e fácil através de uma interface do *browser*.

2.4 PRINCIPAIS PROTOCOLOS DA FAMÍLIA TCP/IP

2.4.1 IP (*Internet Protocol*)

Tem sido utilizado juntamente com o TCP. A principal característica desse protocolo é que a transmissão dos pacotes é efetuada sem a necessidade de uma conexão entre máquina fonte e máquina destino, sendo baseada no envio de datagramas que podem passar por muitas redes intermediárias até chegar ao destino.

Esse protocolo oferece um serviço de datagramas não confiável (também chamado de melhor esforço); ou seja, o pacote vem quase sem garantias. O pacote pode chegar desordenado (comparado com outros pacotes enviados entre os mesmos hosts), ou podem ser perdidos por inteiro.

2.4.2 TCP (*Transmission Control Protocol*)

Segundo Wikipédia (2009) TCP é um protocolo do nível da camada de transporte (camada 4) do modelo OSI e é sobre o qual assentam a maioria das aplicações cibernéticas.

Algumas das principais características do TCP são:

- Orientado a conexão – A aplicação envia um pedido de conexão para o destino e usa a “conexão” para transferir dados.
- Confiabilidade – O TCP usa várias técnicas para proporcionar uma entrega confiável dos pacotes de dados, que é a grande vantagem que tem em relação ao UDP. Permite a recuperação de pacotes perdidos, a eliminação de pacotes duplicados, à recuperação de pacotes corrompidos e pode recuperar a ligação em caso de problemas no sistema e na rede.
- Entrega ordenada – A aplicação faz a entrega ao TCP de blocos de dados com um tamanho arbitrário num fluxo (ou *stream*) de dados, tipicamente em octetos.

2.4.3 UDP (User Datagram Protocol)

Segundo Wikipédia (2009) UDP é um protocolo simples da camada de transporte. Ele não é um protocolo confiável. Caso garantias sejam necessárias, é preciso implementar uma série de estruturas de controle, tais como *timeouts*, retransmissões, *acknowledgments*, controle de fluxo, etc.

Podemos dizer também que o UDP é um serviço sem conexão, pois não há necessidade de manter um relacionamento longo entre cliente e o servidor.

2.5 FIREWALL

Segundo Wikipédia (2009), Firewalls são dispositivos que atuam no perímetro da rede, controlando o tráfego entre duas redes distintas fazendo uso de políticas de segurança pré-definidas (ZWICKY, 2000). Sua função consiste em regular o tráfego de dados entre redes distintas e impedir a transmissão e/ou recepção de acessos nocivos ou não autorizados de uma rede para outra.

2.5.1 Tipos de Firewalls

Existem basicamente 2 tipos de firewalls:

- Nível de aplicação - Este tipo de firewall analisa o conteúdo do pacote para tomar suas decisões de filtragem. Firewalls deste tipo são mais intrusivos (pois analisam o conteúdo de tudo que passa por ele) e permitem um controle relacionado com o conteúdo do tráfego. Alguns firewalls em nível de aplicação combinam recursos básicos existentes em firewalls em nível de pacotes combinando as funcionalidade de controle de tráfego/controla de acesso em uma só ferramenta. Servidores proxy, como o squid, são um exemplo deste tipo de firewall.
- Nível de pacotes - Este tipo de firewall toma as decisões baseadas nos parâmetros do pacote, como porta/endereço de origem/destino, estado da conexão, e outros parâmetros do pacote. O firewall então pode negar o pacote

(DROP) ou deixar o pacote passar (ACCEPT). O iptables é um excelente firewall que se encaixa nesta categoria.

Os dois tipos de firewalls podem ser usados em conjunto para fornecer uma camada dupla de segurança no acesso as suas máquinas/máquinas clientes.

2.6.1 Algumas diferenças entre IPTABLES e IPCHAINS

2.6 IPTABLES

Segundo Wikipédia (2009), IPTABLES é um firewall em nível de pacotes e funciona baseado no endereço/porta de origem/destino do pacote, prioridade, etc. Ele funciona através da comparação de regras para saber se um pacote tem ou não permissão para passar. Em firewalls mais restritivos, o pacote é bloqueado e registrado para que o administrador do sistema tenha conhecimento sobre o que está acontecendo em seu sistema. Ele também pode ser usado para modificar e monitorar o tráfego da rede, fazer NAT, redirecionamento de pacotes, marcação de pacotes e etc. Ele é um firewall com estado, ou seja, um firewall *stateful*. Os anteriores eram *stateless*.

O tipo de filtragem *stateful* (IPTABLES) cria um poderoso sistema de firewall que se "lembra" das conexões entrantes, evitando ataques do tipo *Stealth Scans*, que trazem flags especiais para técnicas de port scanning, como o uso da flag ACK para enganar tais firewalls.

O IPTABLES ainda tem a vantagem de ser modularizável, funções podem ser adicionadas ao firewall ampliando as possibilidades oferecidas. Ele é um código de firewall das versões 2.4 do kernel, que substituiu o IPCHAINS (presente nas séries 2.2 do kernel). Ele foi incluído no kernel da série 2.4 em meados de Junho/Julho de 1999.

Algumas características do IPTABLES são:

- Especificação de portas/endereço de origem/destino;
- Suporte a protocolos TCP/UDP/ICMP;
- Permite um número ilimitado de regras por *chain* (Locais onde as regras do firewall definidas pelo usuário são armazenadas para operação do firewall);
- Suporte a detecção de fragmentos;
- *Masquerading*;
- Contagem de pacotes que atravessaram uma interface/regra;
- Redirecionamento de portas;

- Permite enviar alertas personalizados ao *syslog* sobre o tráfego aceito/bloqueado.

2.6.1 Algumas diferenças entre IPTABLES e IPCHAINS

Primeiramente, os nomes das *chains* padrão passarão a ser escritos com MAIÚSCULAS em vez de minúsculas, porque as chains INPUT e OUTPUT apenas recebem pacotes destinados localmente e gerados localmente. Antes, essas chains visam todos os pacotes entrando e saindo, respectivamente.

Portas TCP e UDP agora precisam ser descritas com as opções `--source-port` ou `-sport` (ou `--destination-port/--dport`), que devem se colocadas depois das opções `“-p tcp”` ou `“-p udp”`, já que essas carregam as extensões TCP ou UDP respectivamente.

MASQ agora é MASQUERADE e utiliza uma sintaxe diferente. REDIRECT, embora tenha mantido o nome, também sofreu uma mudança de sintaxe.

3 FWBUILDER

Este capítulo apresenta o software ferramenta foco deste trabalho, conhecido como FWBuilder.

O FWBuilder é um gerenciador de firewalls para múltiplos servidores. Isso quer dizer que, em uma única interface, é possível gerenciar diversos firewalls espalhados por vários locais do mundo, bastando para tal, ter uma simples conexão SSH entre uma máquina com Firewall Builder e os servidores.

Uma de suas vantagens é que ele possui versões gratuitas para Linux e Windows. Essa ferramenta é muito customizável e completa. A seguir, algumas funcionalidades:

- Permite comentários nas regras;
- Permite criar grupos de regras;
- Possui templates já prontos para os firewalls mais simples;
- Suporte a módulos;
- Multiplataforma.

- Algumas características do compilador Firewall Builder:
- Apóia grupos de objetos e serviços na GUI;
- Apóia ações “Aceitar”, “Negar”, “Rejeitar”, “Contabilidade”;
- Pode gerar código que responde com diferentes envia mensagens ICMP ou TCP RST para a ação Rejeitar;
- Pode processar regras com negação;
- suporta logging.

Algumas funções avançadas:

- O compilador pode detectar os erros comuns em muitos dos objetos, políticas e regras NAT;
- Pode detectar regra "sombra";
- Gerencia adequadamente as regras que correspondem endereços em broadcast e multicast.

O Firewall Builder pode ser compilado e funciona nos seguintes sistemas operacionais e distribuições Linux:

- Debian(Incluindo o Ubuntu)
- Mandrake
- RedHat
- Susi
- Gentoo
- FreeBSD
- OpenBSD
- Mac OS X
- Solaris

Para compilar a partir do código fonte, primeiramente é preciso baixar as dependencias de sua plataforma, que são elas:

- Automake
- Autoconf
- Libtoll
- Libxml2-devel
- Libxslt-devel
- Net-snmp-devel
- Qt

- Qt-devel
- Qt-x11

Para instalar a ferramenta gráfica do FWBuilder, no prompt de comando de um Linux com suporte a pacotes do Debian e uso da ferramenta de gerência de pacotes apt-get, deve-se digitar:

```
apt-get install fwbuilder
```

Após a instalação da ferramenta gráfica, deve-se instalar o serviço de SSH, pois o FWBuilder após compilar as regras usa o ssh para abrir uma conexão com o servidor (firewall) para aplicação destas regras.

```
apt-get install ssh
```

3.1 FUNÇÕES DO FWBUILDER

O FWBuilder é uma ferramenta poderosa de firewall, pois tem uma interface gráfica visual para das regras, facilitando muito a administração do firewall.

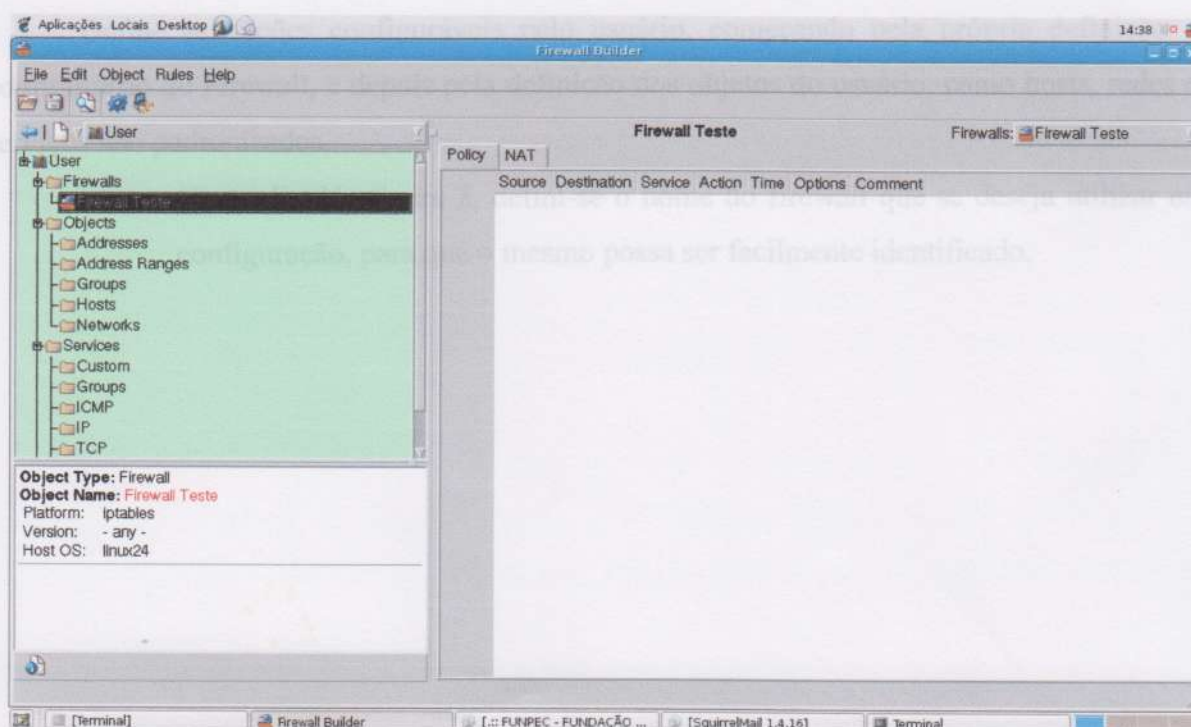


Figura 1: Interface do FWBuilder.

Fonte: Ferramenta FWBuilder(Captura da Tela)

Na barra de botões na figura 1, existem 5(cinco) opções para uma melhor navegação, são elas:

- Abrir: Abre uma caixa de diálogo, que permite selecionar um arquivo existente terminado com .FWB.
- Salvar: Salvar o arquivo atual.
- Localizar: Localiza objetos e substitui funções.
- Compilar: Pode-se escolher qual arquivo de firewall deseja compilar.
- Instalar: Permite instalar um firewall que já tenha sido compilado.

Ao executar o FWBuilder, a ferramenta é apresentada na Figura 1. Na área esquerda da figura estão as definições dos objetos que serão trabalhados nas regras do firewall, e na área da direita, são organizadas as regras do firewall. A organização dos objetos visuais que irão compor as regras são organizados em duas categorias, User e Standard, selecionáveis através do menu pull-down na esquerda abaixo da barra de botões.

A seguir nas sub-seções seguintes, breves descrições das opções disponibilizadas pela interface do FWBuilder.

3.1.1 Categoria de objetos *User*

Define as opções configuráveis pelo usuário, começando pela própria definição e configuração do Firewall, e depois pela definição dos objetos do usuário, como hosts, redes e serviços não padronizados.

- Firewalls: Na figura 2, defini-se o nome do firewall que se deseja utilizar na configuração, para que o mesmo possa ser facilmente identificado.

Figura 2: Tela de definição do nome do Firewall.

Fonte: Ferramenta FWBuilder(Captura da Tela)

- Nome do Objeto: Definir o nome do firewall.
- Programa do Firewall: Definir que plataforma será utilizada no firewall.
- Sistema Operacional: Tipo do sistema operacional utilizado.

No FWBuilder, pode-se adicionar varias interfaces na sua criação, como mostrado na figura 3. Caso esqueça alguma será necessário adicionar manualmente.

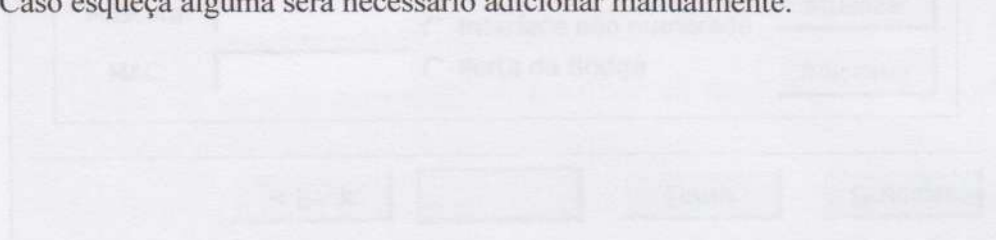


Figura 3: Tela de definição das interfaces do Firewall.

Fonte: Ferramenta FWBuilder(Captura da Tela)

Nome: Nome da placa de rede.

Endereço: Endereço definido para a placa de rede criada.

Máscara: Máscara de rede de acordo com o endereço ip da placa.

MAC: Não é necessário utilizá-la, mas pode ser usada para combater a clonagem de MAC.

- o Interfaces: um firewall pode ter varias interfaces de rede. Como mostrado na figura 4, para cada interface, deve-se definir algumas configurações como os endereços IP's e as máscaras para as placas de rede utilizadas no firewall, como a eth0, eth1, eth2 e etc.

Aqui você pode adicionar ou editar interfaces manualmente. 'Nome' corresponde ao nome da interface física, como 'eth0', 'fxp0', 'ethernet0' etc. 'Etiqueta' é usado para marcar a interface para refletir topologia de rede, por exemplo, 'fora' ou 'dentro'. Etiqueta é obrigatório para firewall PIX.

Clique 'Avançar' quando pronto.

Nome	Etiqueta	Endereço	Máscara	Dyn	M
------	----------	----------	---------	-----	---

Nome: Etiqueta:

Endereço: ☒ Interface normal

Máscara: ☐ Endereço Dinâmico

MAC: ☐ Interface não numerada

☐ Porta da Bridge

< Back Next > Finish Cancelar

Figura 3: Tela de definição das interfaces do Firewall.

Fonte: Ferramenta FWBuilder(Captura da Tela)

Nome: Nome da placa de rede.

Endereço: Endereço definido para a placa de rede criada.

Máscara: Mascara de rede de acordo com o endereço ip da placa.

MAC: Não é necessário utilizá-la, mas pode ser usada para combater a clonagem de MAC.

- Interfaces: um firewall pode ter várias interfaces de rede. Como mostrado na figura 4, para cada interface, deve-se definir algumas configurações como os endereços IP's e as máscaras para as placas de rede utilizadas no firewall, como a eth0, eth1, eth2 e etc.

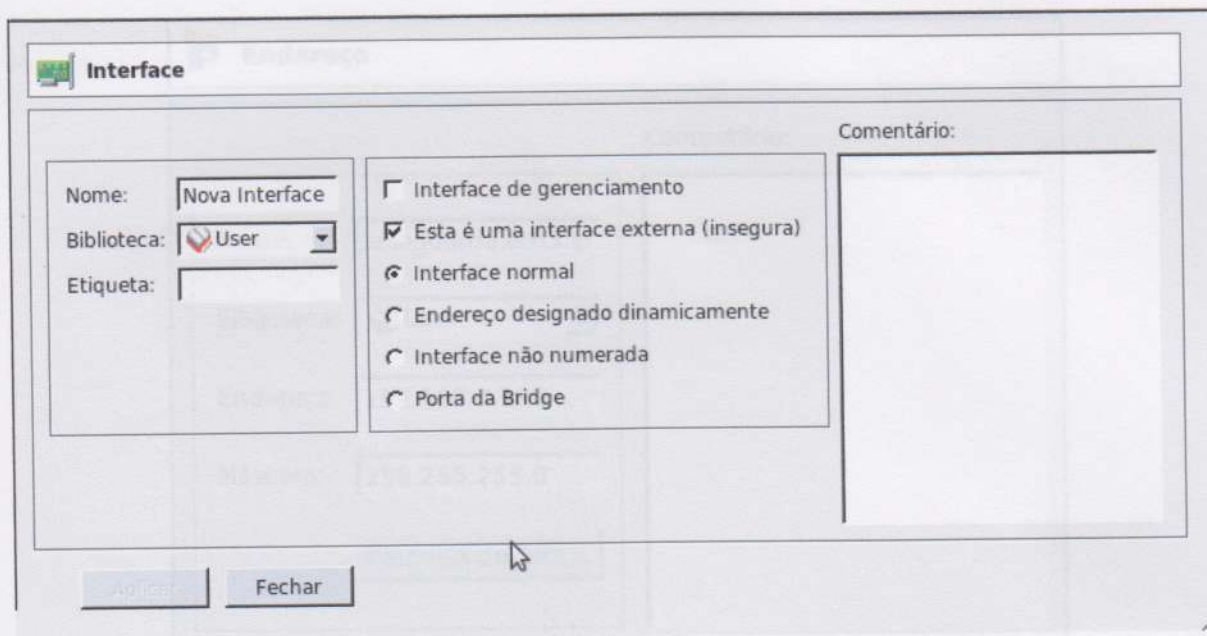


Figura 4: Tela de definição das interfaces do Firewall.
Fonte: Ferramenta FWBuilder(Captura da Tela)

- Nome: Nome definido para cada interface do firewall.
- Biblioteca: Biblioteca de usuário,
- Etiqueta: Não utilizado na maioria dos sistemas operacionais.
- Interface de Gerenciamento: A interface de rede definida com esta opção garante que o firewall será gerenciado por ela.
- Interface Externa: Interface que se conecta a internet ou a uma área que é fora da rede protegida pelo firewall.
 - Interface normal: Utilizado para um endereço ip atribuído manualmente.
 - Ao ser adicionado uma interface normal, tem que ser atribuído os respectivos endereços ip's, como mostrado na figura 5.

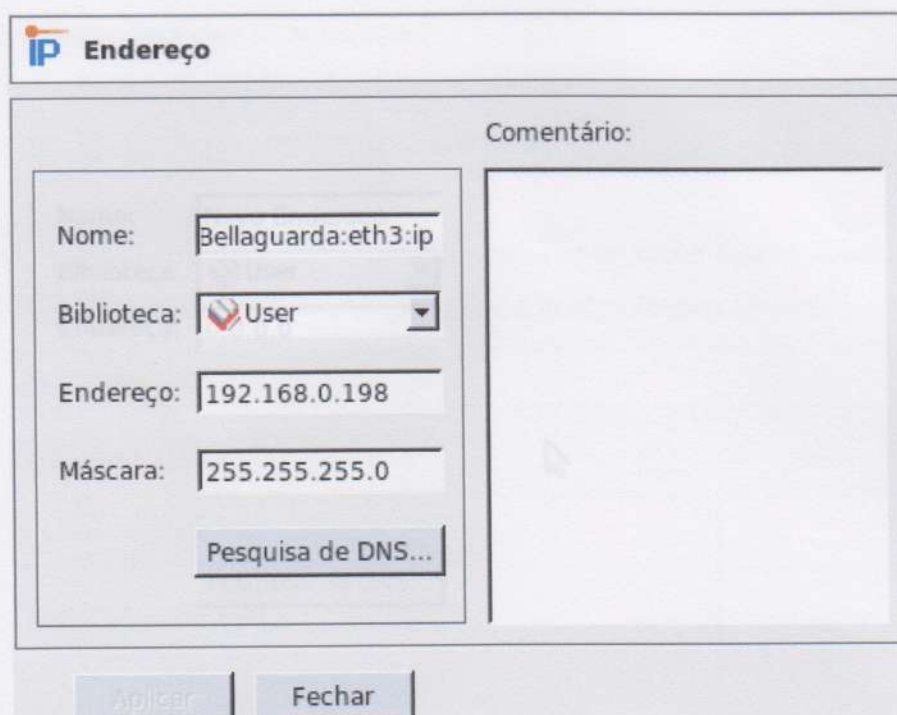


Figura. 5: Tela de definição dos endereços de rede.
Fonte: Ferramenta FWBuilder (Captura da Tela)

Nome: Nome definido para cada endereço de rede.

Endereço: Endereço ip atribuído para a placa de rede.

Máscara: Máscara de rede definida para o endereço ip.

Pesquisa de DNS: Traduz o nome de uma máquina para o endereço IP.

- Endereço Dinâmico: Endereço atribuído dinamicamente por um servidor de DHCP previamente instalado.
- Interface não numerada: Opção utilizada se a interface não pode nunca ter um endereço IP, como a interface ETHERNET usado na conexão PPPoE em algumas conexões ADSL.
- Objects: Objetos que podem ser usados para definir endereços, faixas de endereços, grupos, equipamentos e redes.
 - Addressess: Definir endereços específicos para equipamentos de uma rede, que sejam aplicadas as regras de configuração para o endereço desejado como mostrado na figura 6. Ex: Em uma rede empresarial, bloquear ou permitir acessos em toda rede de uma máquina específica.

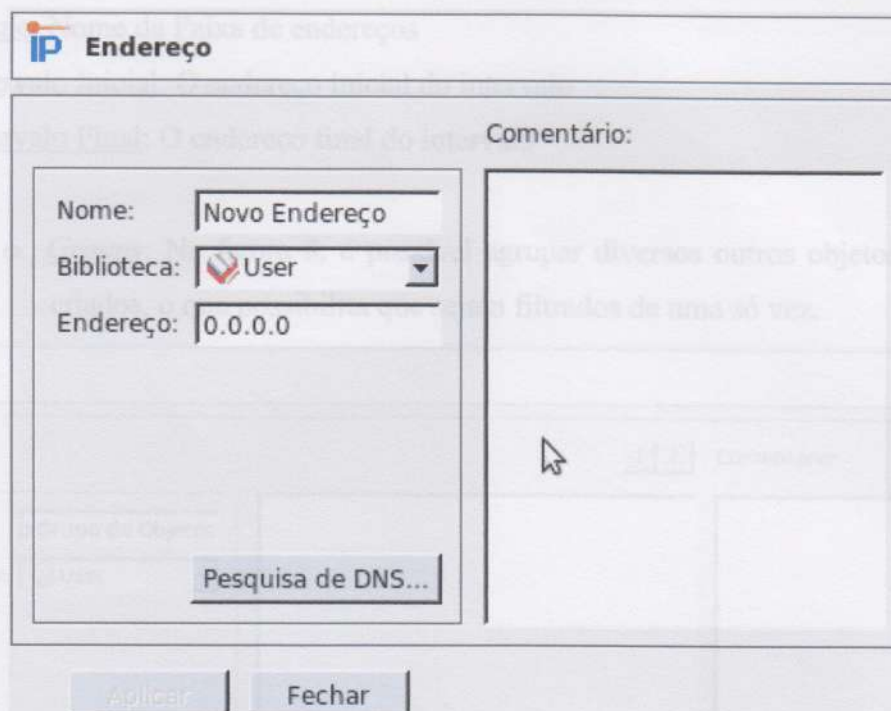


Figura. 6: Tela de definição dos endereços de Hosts.

Fonte: Ferramenta FWBuilder(Captura da Tela)

Nome: Nome do Objeto Endereço.

Endereço: Endereço de uma interface específica.

- Address Ranges: possibilita Filtrar faixas de endereços IP's (figura 7).

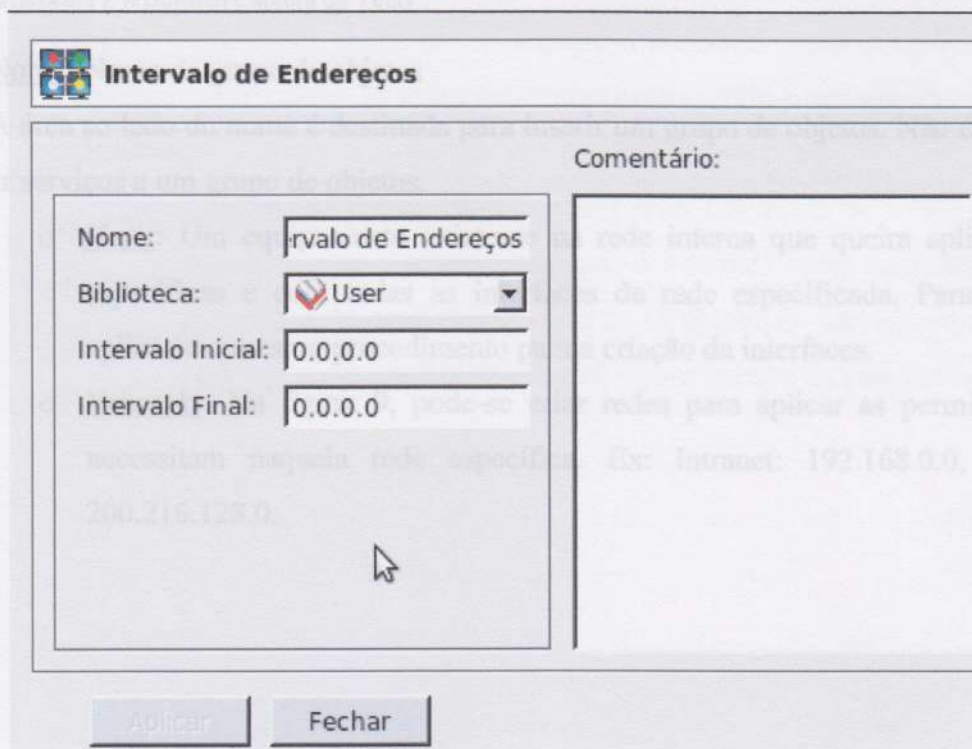


Figura 7: Tela de definição do intervalo de endereços de rede.

Fonte: Ferramenta FWBuilder(Captura da Tela)

Nome: Nome da Faixa de endereços

Intervalo Inicial: O endereço inicial do intervalo

Intervalo Final: O endereço final do intervalo

- Groups: Na figura 8, é possível agrupar diversos outros objetos previamente criados, o que possibilita que sejam filtrados de uma só vez.

Figura 8: Tela de definição do grupo de objetos.

Fonte: Ferramenta FWBuilder(Captura da Tela)

Nome: Nome do grupo de objetos

A área ao lado do nome é destinada para inserir um grupo de objetos. Não é permitido adicionar serviços a um grupo de objetos.

- Hosts: Um equipamento existente na rede interna que queira aplicar regras específicas e com todas as interfaces de rede especificada. Para utilizá-lo aplica-se o mesmo procedimento para a criação da interfaces.
- Networks: Na figura 9, pode-se criar redes para aplicar as permissões que necessitam naquela rede específica. Ex: Intranet: 192.168.0.0, Extranet: 200.216.128.0.

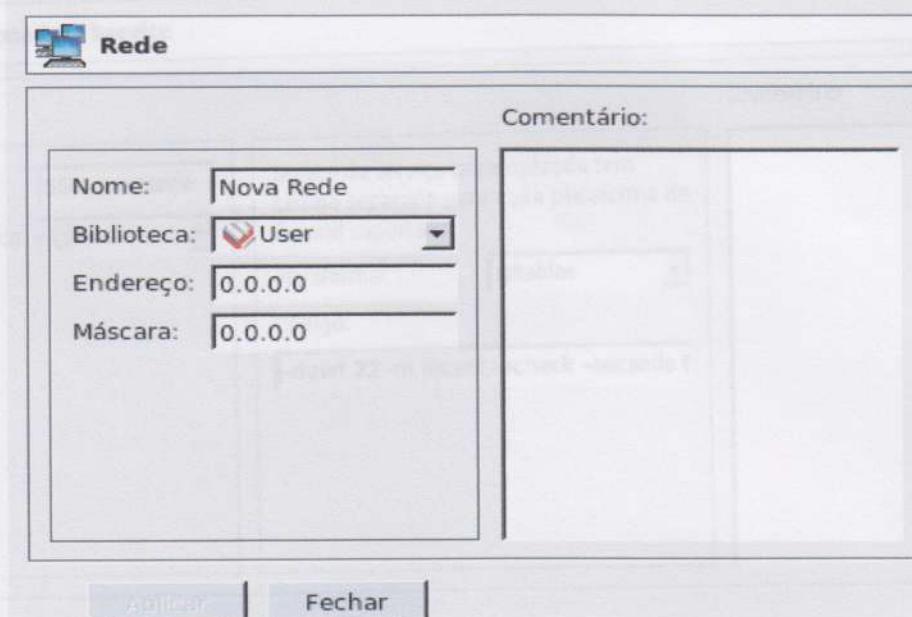


Figura 9: Tela de definição de redes.

Fonte: Ferramenta FWBuilder(Captura da Tela)

Nome: Nome da rede que deseja adicionar.

Endereço: Endereço da rede

Máscara: Mascara da rede

- Services: São os serviços customizados, que se pode criar para portas e protocolos diferentes. Os protocolos padrão (os bem conhecidos) da Internet já estão previamente definidos na categoria Standard. Assim, aqui se definem apenas os protocolos de serviços criados pelo usuário e que não são padrões da Internet.
 - Custom: Na figura 10, é possível criar Cadastros de serviços e serem definidos pelo usuário, para que o Firewall tome conhecimento dos mesmos e de suas regras de uso. O objeto de serviço personalizado pode ser usado para inserir um código arbitrário na geração do firewall.

Figura. 10: Tela de personalização dos serviços de rede.
Fonte: Ferramenta FWBuilder(Captura da Tela)

Nome: Nome do objeto

Plataforma: Menu que mostra todas as plataformas de firewall para o módulo que será instalado, que no caso é uma regra de iptables.

Código: Linha de código do firewall.

- Groups: Na figura 11, os grupos de serviços podem definir uma série de regras semelhantes para vários hosts ou redes. Por exemplo, pode haver uma necessidade de permitir o mesmo serviço para 10 diferentes máquinas na rede, enquanto continua a bloquear a todos os outros. A maneira mais simples de fazer isso é adicionar 10 regras com a mesma fonte e serviços e apenas destinos diferentes. O FWBuilder suporta os grupos de objetos e serviços, pode-se colocar "Host", "Rede" e "Firewall" em um grupo de objetos, mas não pode colocar serviços de objetos em um desses grupos. Da mesma forma, um grupo de serviços pode conter objetos "IP Service", "TCP Service", "UDP Service" e "ICMP Service", mas não podem conter hosts ou redes. Os grupos podem também conter outros grupos do mesmo tipo.

Figura. 11: Tela de definição de um novo serviço ICMP.
Fonte: Ferramenta FWBuilder(Captura da Tela)

Grupo

Nome do serviço de ICMP

Nome: Grupo de Serviços

Biblioteca: User

Comentário:

Aplicar Fechar

Figura. 11: Tela de definição dos grupos de serviços.
Fonte: Ferramenta FWBuilder(Captura da Tela)

Nome: Nome do grupo de serviços

A área ao lado do nome é destinada para inserir um grupo de serviços. Não é permitido adicionar objetos a um grupo de serviços.

- ICMP: O objeto de serviço ICMP é uma representação do protocolo ICMP e são utilizados para comunicar mensagens de erros como mostrado na figura 12, seja pela camada IP ou protocolos da camada superior(TCP e UDP), como também pode ser usado como um protocolo de consulta simples.

Serviço ICMP

Nome para o tipo de serviço e de rede

Nome: Novo Serviço ICMP

Biblioteca: User

Tipo de ICMP: qualquer

Código de ICMP: qualquer

Comentário:

Aplicar Fechar

Figura. 12: Tela de definição de um novo serviço ICMP.
Fonte: Ferramenta FWBuilder(Captura da Tela)

Nome: Nome do serviço de ICMP

Tipo de ICMP: Tipo da mensagem ICMP

Código de ICMP: Código da Mensagem ICMP

No protocolo ICMP existe uma tabela com todos os tipos de mensagens, são elas:

TIPO	CÓDIGO	DESCRIÇÃO	PERGUNTA	ERRO
0	0	Respondendo Echo	*	
3		Destino Inacessível		*
	0	Rede Inacessível		*
	1	Host Inacessível		*
	2	Protocolo Inacessível		*
	3	Porta Inacessível		*
	4	Fragmentação Necessária		*
	5	Origem da Rota falhou		*
	6	Rede de Destino desconhecido		*
	7	Host de Destino desconhecido		*
	8	Host de origem isolado		*
	9	Rede de destino administrativamente proibido		*
	10	Host de destino administrativamente proibido		*
	11	Rede inacessível para TOS		*
	12	Host inacessível para TOS		*
	13	comunicação proibida Administ. por filtragem		*
	14	Violação de procedência		*
	15	Atalho de precedência em vigor		*
4	0	controle de fluxos elementar		*
5		Redirecionar		*
	0	Redirecionar para a rede		*
	1	Redirecionar para o host		*
	2	redirecionar para o tipo de serviço e de rede		*
	3	redirecionar para o tipo de serviço e de host		*
8	0	echo request	*	
9	0	anúncio do roteador	*	
10	0	solicitação do roteador	*	
11		tempo excedido		*
	0	tempo de vida durante o transito		*
	1	tempo de vida durante a remontagem		*
12		problema de parâmetro		*
	0	Bad IP header		*
	1	Opção necessária em falta		*
13	0	timestamp request	*	
14	0	timestamp reply	*	
15	0	pedido de informação	*	
16	0	Resposta de informação	*	
17	0	address mask request	*	
18	0	Responder máscara de endereço	*	

- IP: Na figura 13, o objeto de serviço IP descreve os protocolos que não são ICMP, TCP ou UDP. Um protocolo IP é definido pelo campo de 8 bits no cabeçalho do pacote IP.

Figura. 13: Tela de definição dos serviços IP.
Fonte: Ferramenta FWBuilder(Captura da Tela)

Nome: Nome do serviço IP.

lsrr: O remetente pode especificar uma lista de roteadores que o pacote deve percorrer, ou seja, fica com a rota de origem livre.

ssrr: Trabalha da mesma maneira do Lsrr, porém o pacote terá que percorrer apenas através dos endereços especificados.

rr: Cada roteador controla o pacote sobre a forma de adicionar o seu endereço ip para uma lista no campo de opções.

timestamp: Opção raramente usada, mas pode ser explorada para recolher informações sobre as redes protegidas.

- TCP: Oferece um serviço orientado a conexão. O cabeçalho TCP contém campos especiais que são especificados a origem e o destino da porta e que são utilizados para identificar o envio e o recebimento dos pacotes como mostrado na figura 14.

Figura 14: Tela de definição dos serviços TCP.
Fonte: Ferramenta FWBuilder(Captura da Tela)

Nome: Nome do serviço TCP;

Intervalo de portas de origem: o início e o fim da porta de origem aceita valores de 0 a 65535.

Intervalo de portas de destino: o início e o fim da porta de destino aceita valores de 0 a 65535.

TCP Flags: Existem 6 flags no cabeçalho TCP, são eles:

U – O ponteiro é válido.

A – O numero de reconhecimento é válido.

P – O receptor deve passar os dados para a aplicação o mais rápido possível.

D – Redefine a conexão.

S – Sincronizar os números de sequência para iniciar uma conexão.

F – O remetente conclui o envio de dados.

- UDP: Na figura 15, pode criar cadastros de serviços baseados no protocolo UDP. É um transporte do protocolo de camada sem conexão. Algumas aplicações usam o protocolo UDP, como o DHCP, NTP e etc.

Figura 15: Tela de definição dos serviços UDP.
Fonte: Ferramenta FWBuilder(Captura da Tela)

Nome: Nome do serviço UDP.

Intervalo de portas de origem: o início e o fim da porta de origem aceita valores de 0 a 65535.

Intervalo de portas de destino: o início e o fim da porta de destino aceita valores de 0 a 65535.

3.1.2 Categoria de objetos *Standard*

Esta categoria agrupa todos os objetos de serviços *standards*, isto é, padrões da Internet. Desta forma, os objetos desta categoria não são editáveis. Há uma lista bastante extensa de serviços padrões da Internet, o que facilita a definição de regras para tais serviços por parte do administrador do firewall.

3.1.3 Organização das regras nos painéis

As seguintes opções estão disponibilizadas no painel da direita da interface do FWBuilder, separadas pelas seguintes abas:

- **Regras (Policy):** São as regras do firewall propriamente dito. Elas servem para restringir/liberar acessos a determinados hosts, redes e serviços. Para compor uma regra de firewall, são necessárias as seguintes informações, mostrado na figura 16:

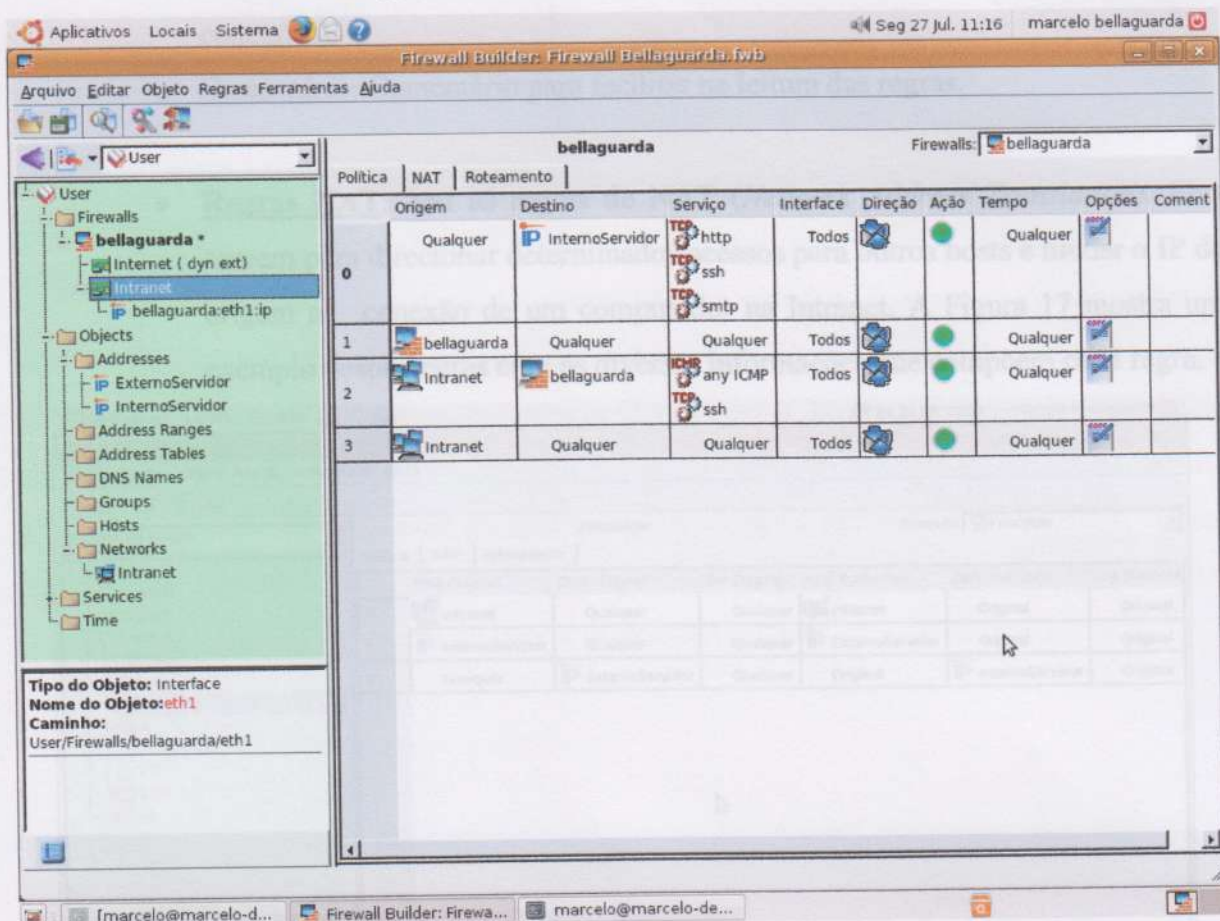


Figura 16: Tela de definição das políticas do Firewall.
Fonte: Ferramenta FWBuilder (Captura da Tela)

- **Origem:** Origem da conexão (uma estação interna, um servidor externo, uma rede...).
- **Destino:** Destino da conexão (uma estação interna, um servidor externo, uma rede...).
- **Serviço:** Porta e protocolo a ser aplicado na regra especificada.
- **Interface:** interfaces existentes no firewall.
- **Direção:** Direção para os pacotes que entram ou saem da interface do firewall.
- **Ação:** Ação a ser tomada, *Accept* (acesso liberado), *Deny* (acesso negado, porém o pacote continuará com o mesmo destino, ocorrendo assim *Time Out*), *Reject* (o pacote será negado pelo Firewall, ocorrendo assim acesso negado) ou *Accounting* (executa a regra com base na ação de outra regra, não utilizado).

- Tempo: Hora que a regra estará ativa (não utilizado, pois necessita de módulo externo para o Iptables).
- Opções: Opções da regra Rule Options (opções que raramente são utilizadas), Loggin On (habilitar o Log das conexões), Loggin Off (desabilitar o Log das conexões).
- Comentário: Comentário para facilitar na leitura das regras.
- **Regras NAT**: São as regras de NAT (*Network Address Translation*). Elas servem para direcionar determinados acessos para outros hosts e mudar o IP de origem na conexão de um computador na Intranet. A Figura 17 mostra um exemplo destas regras com as diversas informações que compõem cada regra.

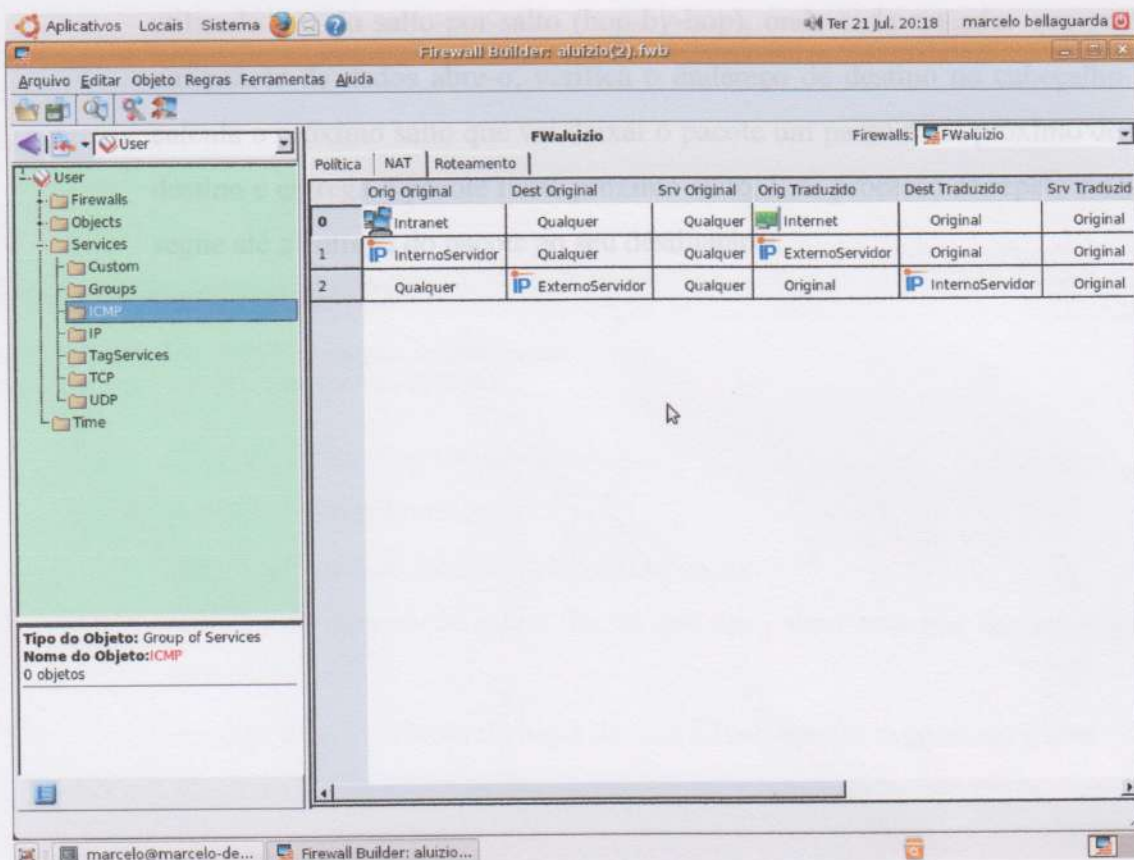


Figura 17: Tela de definição das regras de NAT.

Fonte: Ferramenta FWBuilder(Captura da Tela)

- Orig Original: Endereço original de origem da conexão (uma estação interna, um servidor externo, uma rede, etc..).
- Dest Original: Endereço original de destino da conexão (uma estação interna, um servidor externo, uma rede, que esteja em redes diferentes).

- Srv Original: Identificação original do serviço (porta) e protocolo da conexão que foi iniciada.
 - Orig Traduzido: Endereço IP traduzido da origem da conexão.
 - Dest Traduzido: Endereço IP traduzido do destino da conexão.
 - Srv Traduzido: Serviço (protocolo e porta) trocado (redirecionado) da conexão.
 - Comentário: Comentários para uma melhor leitura das regras.
- **Roteamento**: Como todo Firewall interliga várias redes, ele também funciona como um roteador. Nesta aba, é possível configurar o roteamento que o Firewall deve utilizar. O roteamento é a principal forma utilizada na internet para entrega de pacotes de dados entre hosts. O modelo de roteamento utilizado é o do salto-por-salto (hop-by-hop), onde cada roteador que recebe um pacote de dados abre-o, verifica o endereço de destino no cabeçalho IP, calcula o próximo salto que vai deixar o pacote um passo mais próximo de seu destino e entrega o pacote neste próximo salto. Este processo se repete e assim segue até a entrega do pacote ao seu destinatário.

Figura 18: Tela de Definição das regras de roteamento.
Fonte: Ferramenta FW3200(Captura de Tela)

- Destino: Destino do roteamento rede.
- Roteador: Roteador da rede.
- Interface: Por qual interface chegar os dados.
- Métrica: O número de saltos (hops) que um pacote tem que dar até chegar a esta rede.
- Opções: Se a instalação da regra de rota falhar, apenas seguirá em frente.

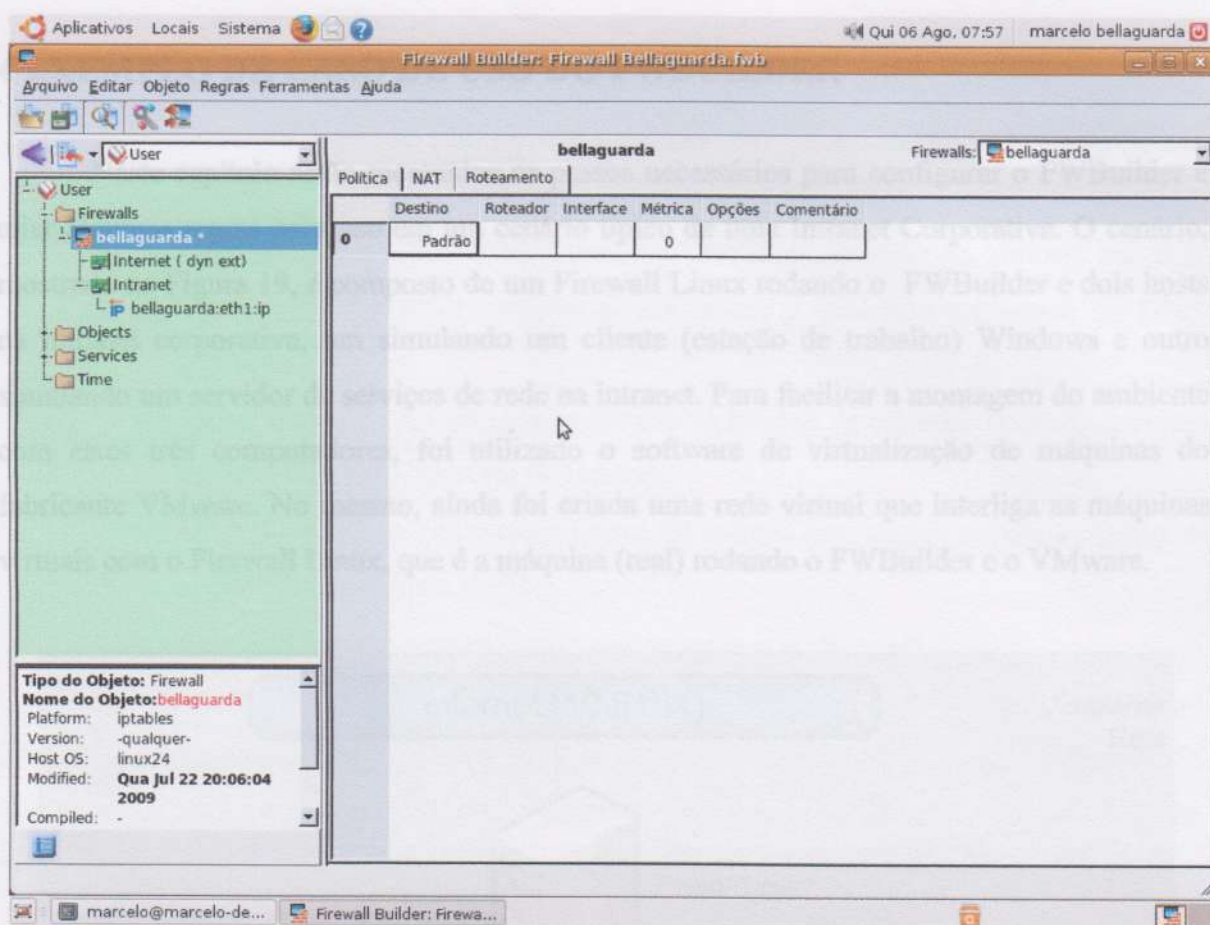


Figura 18: Tela de definição das regras de roteamento.

Fonte: Ferramenta FWBuilder(Captura da Tela)

- Destino: Destino do roteamento rede.
- Roteador: Roteador da rede.
- Interface: Por qual interface chegam os dados.
- Métrica: O número de saltos (hops) que um pacote tem que dar até chegar a esta rede
- Opções: Se a instalação da regra de rota falhar, apenas seguirá em frente.

Figura 19: Captura do caso de uso do FWBuilder.

Fonte: Material Pê-Constructo (Nota de Computadores(FARN))

Neste caso de uso da Figura 19, há uma intranet com faixas de IP's 172.16.x.y, um servidor com o Windows 2003 e uma estação cliente com o Windows 2000 e a Firewall com o Linux Ubuntu realizando as permissões dos serviços da intranet para a internet e vice-versa.

Para a montagem das regras, são considerados os seguintes aspectos:

- O Firewall deve mascarar (esconder) o endereçamento interno (rede da intranet), possibilitando que as máquinas internas acessem a internet com o IP do Firewall;

4 EXEMPLO DE CASO DE USO DO FWBUILDER

Neste capítulo serão mostrados os passos necessários para configurar o FWBuilder e criar algumas regras para uso em um cenário típico de uma Intranet Corporativa. O cenário, mostrado na Figura 19, é composto de um Firewall Linux rodando o FWBuilder e dois hosts na intranet corporativa, um simulando um cliente (estação de trabalho) Windows e outro simulando um servidor de serviços de rede na intranet. Para facilitar a montagem do ambiente com estes três computadores, foi utilizado o software de virtualização de máquinas do fabricante VMware. No mesmo, ainda foi criada uma rede virtual que interliga as máquinas virtuais com o Firewall Linux, que é a máquina (real) rodando o FWBuilder e o VMware.

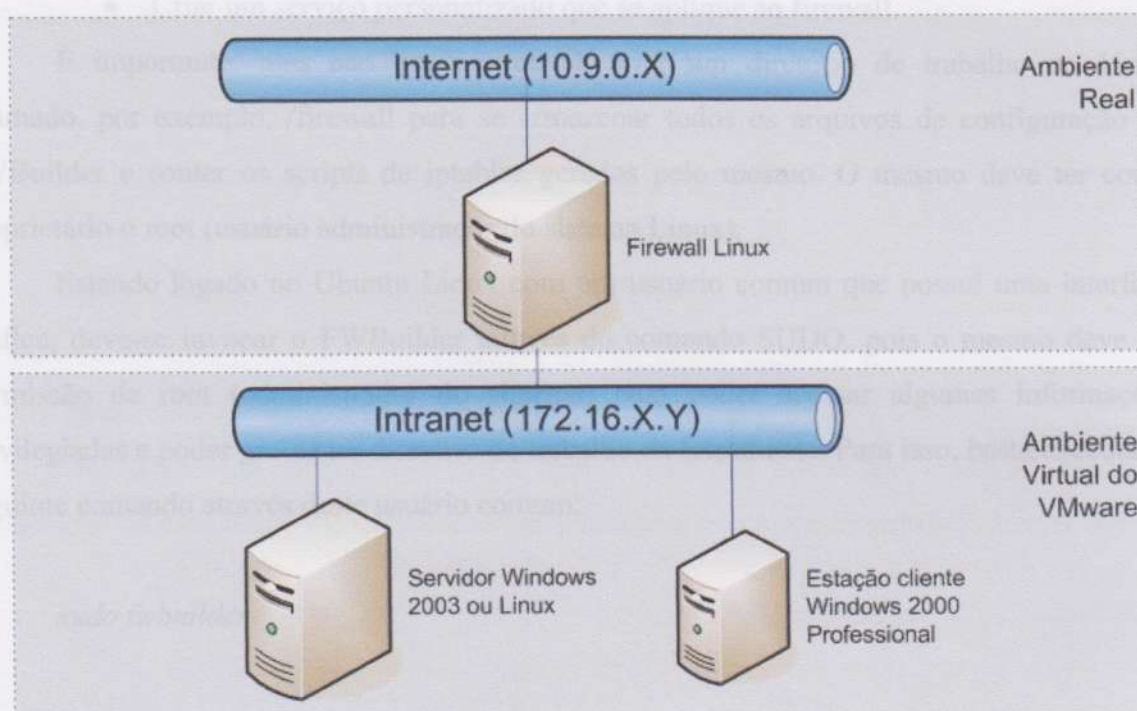


Figura 19: Cenário do caso de uso do FWBuilder.

Fonte: Material Pós-Graduação Redes de Computadores(FARN)

Neste caso de uso da Figura 19, há uma intranet com faixas de IP's 172.16.x.y, um servidor com o Windows 2003 e uma estação cliente com o Windows 2000 e o Firewall com o Linux Ubuntu realizando as permissões dos serviços da intranet para a internet e vice-versa.

Para a montagem das regras, são considerados os seguintes aspectos:

- O Firewall deve mascarar (esconder) o endereçamento interno (rede da intranet), possibilitando que as máquinas internas acessem a Internet com o IP do firewall;

- O Firewall deve ser o responsável pelo DNS externo, isto é, as consultas ao domínio vindas da Internet deverão ser respondidas pelo Firewall. As consultas de DNS internas (da Intranet) deverão ser respondidas pelo Servidor da Intranet.
- O Firewall deve fazer NAT 1 para 1 com o IP do Servidor da Intranet. Isto é, o servidor deve possuir um endereço externo, o qual será registrado no DNS externo.
- Os serviços de páginas (site) e correio eletrônico da empresa (e-mail) deverão ser providos pelo Servidor da Intranet.
- Deverá existir o redirecionamento de portas pro squid, existindo assim o controle de acessos a WEB.
- Criar um serviço personalizado que se aplique ao firewall.

É importante, mas não imprescindível, criar um diretório de trabalho no Linux chamado, por exemplo, /firewall para se armazenar todos os arquivos de configuração do FWBuilder e conter os scripts de iptables gerados pelo mesmo. O mesmo deve ter como proprietário o root (usuário administrador do sistema Linux).

Estando logado no Ubuntu Linux com um usuário comum que possui uma interface gráfica, deve-se invocar o FWBuilder através do comando SUDO, pois o mesmo deve ter permissão de root (administrador do sistema) para poder acessar algumas informações privilegiadas e poder gravar no diretório de trabalho da ferramenta. Para isso, basta executar o seguinte comando através deste usuário comum:

```
sudo fwbuilder
```

Ao abrir o fwbuilder pela primeira vez, aparecerá uma opção de abrir um arquivo existente já configurado, ou criar um novo, como mostrado na Figura 20.



Figura 20: Janela do FWBuilder com a opção de abrir ou criar um arquivo de regras do mesmo.

Fonte: Ferramenta FWBuilder(Captura da Tela)

Neste momento, foi criado um novo projeto de firewall salvando o arquivo deste no diretório /firewall. Após a definição do arquivo que guardará todas as informações do novo projeto, aparece a tela principal do FWBuilder, já vista na Figura 1.

Figura 21: Tela de definição das propriedades do Firewall.

4.1 DEFINIÇÃO DO DIRETÓRIO DE TRABALHO

Para configurar o diretório onde o fwbuilder irá salvar suas configurações, deve-se abrir o menu Editar, opção Preferências, e na aba Geral, existe a opção *Working directory*. Nesta opção deve-se informar o caminho onde será salvo toda a configuração.

Na opção *On startup*, escolher a opção *Load last edited file*, que toda vez que o fwbuilder for executado ele carregue automaticamente o arquivo editado pela ultima vez.

Sistema Operacional: Linux 2.4/2.6

Existem 3(tres) maneiras de ser criado um novo firewall no fwbuilder, são elas:

- Usar modelos pré-configurados de objetos do firewall;

4.2 CONFIGURAÇÃO DO FWBUILDER

Na Figura 21, pode-se observar a tela apresentada quando se cria um novo objeto do tipo *Firewalls*. Para isso, com o cursor posicionado em cima de *Firewalls* deve-se clicar com o botão direito do mouse e selecionar a opção *Novo Firewall*.

Nas opções do firewall, mostradas na figura 22, existem algumas configurações importantes para o funcionamento correto do firewall.

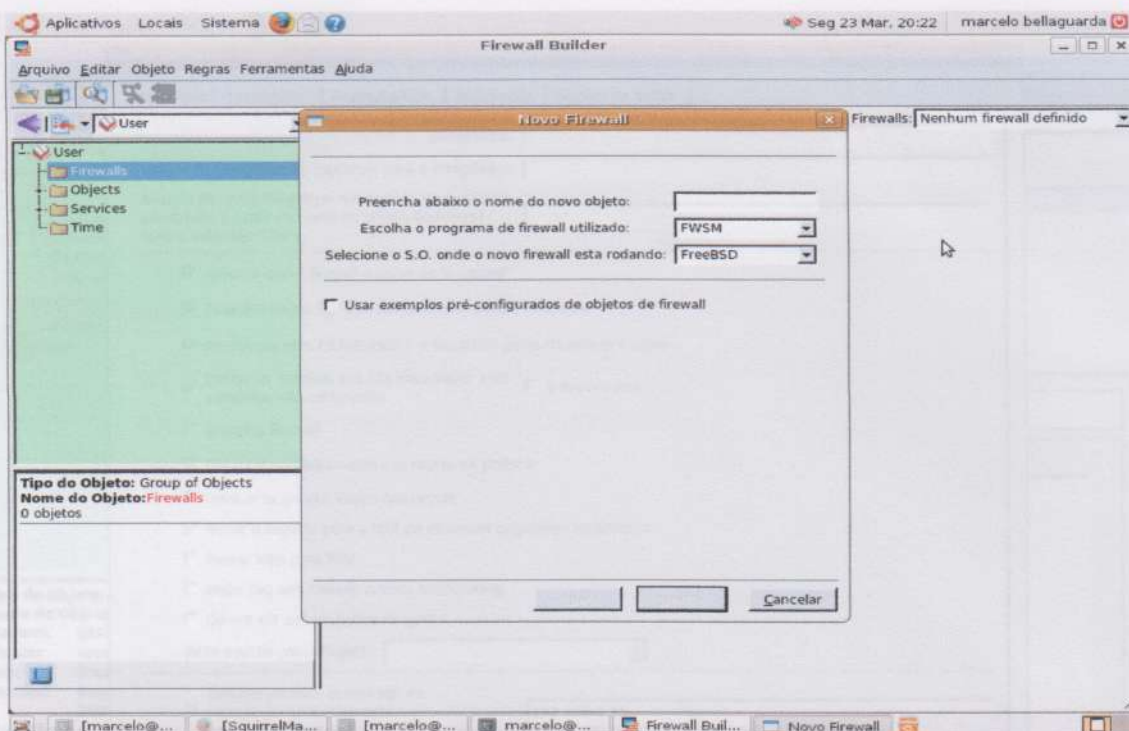


Figura 21: Tela de definição das propriedades do Firewall.
Fonte: Ferramenta FWBuilder (Captura da Tela)

Ao adicionar um novo firewall, irá aparecer a primeira tela de configuração do firewall como mostrado na figura 21, com o nome do firewall, o tipo de programa a ser utilizado e o sistema operacional que será utilizado.

Nome do firewall: bellaguarda

Plataforma: Iptables

Sistema Operacional: Linux 2.4/2.6.

Existem 3(três) maneiras de ser criado um novo firewall no fwbuilder, são elas:

- Usar modelos pré-configurados de objetos do firewall;
- Criar um firewall a partir do zero;
- Usar o SNMP para criar um objeto com interfaces do firewall, mas com uma política vazia.

Ao avançar para o próximo passo, será solicitada a adição das interfaces no firewall. Nas opções do firewall, mostradas na figura 22, existem algumas configurações importantes para o funcionamento correto do firewall.

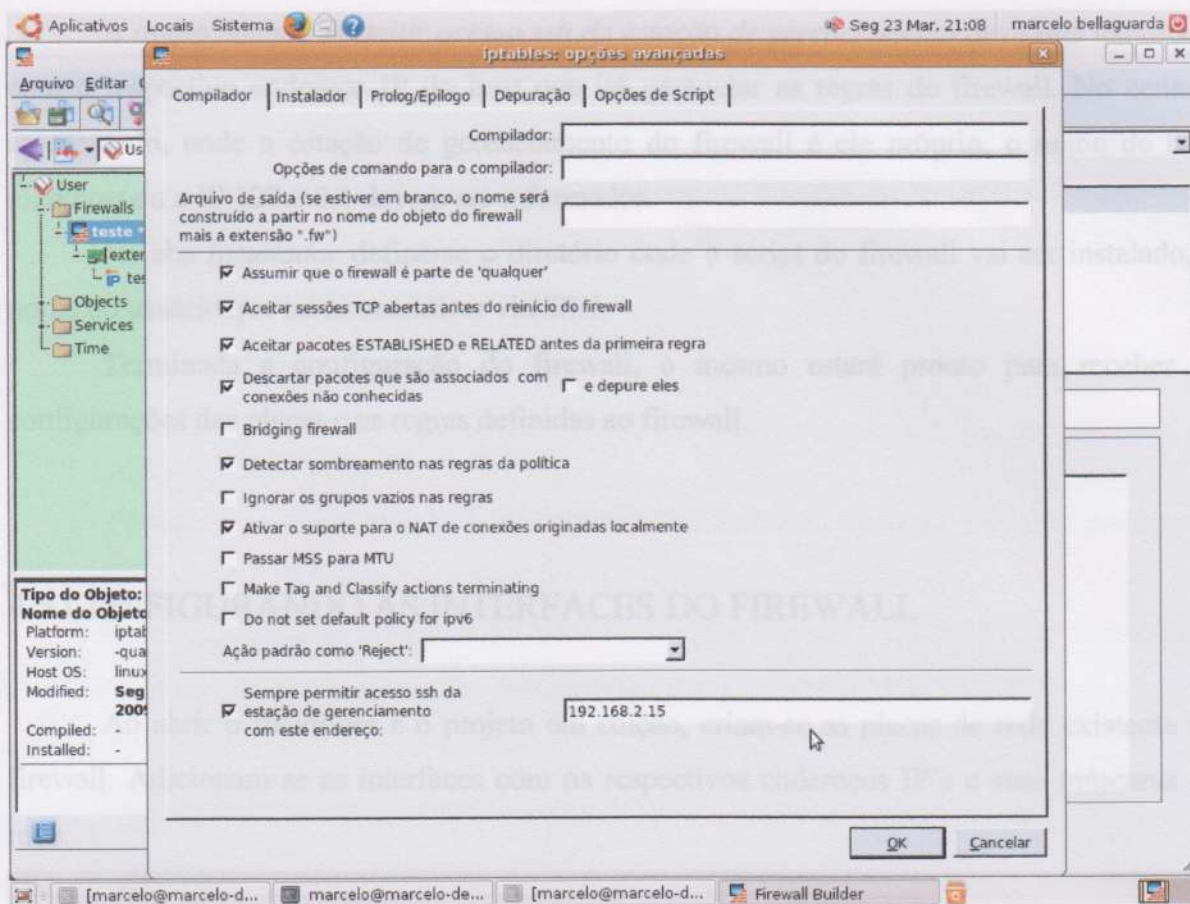


Figura 22: Tela de opções avançadas do iptables.
Fonte: Ferramenta FWBuilder(Captura da Tela)

As opções são as seguintes:

- Assumir que o firewall é parte de "qualquer": O firewall se inclui na categoria *qualquer* quando se estiver definindo o host de origem ou de destino na criação das regras de filtragem;
- Aceitar sessões TCP abertas antes do reinício do firewall: Ao reiniciar o firewall ele aceita as conexões que já estão abertas;
- Aceitar pacotes ESTABLISHED e RELATED antes da primeira regra: Aceita conexões estabelecidas antes mesmo de ativar a primeira regra da política;
- Descartar pacotes que são associados com conexões não conhecidas: Descartar pacotes que não estão associados a uma conexão.
- Detectar sobreposição nas regras da política: Detecta regras repetidas em suas políticas.
- Ativar o suporte para o NAT de conexões originadas localmente: Habilita suporte a regras NAT para conexões locais.

A opção *Sempre permitir acesso ssh da estação de gerenciamento* deve estar habilitada com o respectivo endereço IP do host que irá gerenciar as regras de firewall. No cenário apresentado, onde a estação de gerenciamento do firewall é ele próprio, o nome de host *localhost* ou o IP 127.0.0.1 devem ser informados.

Na aba *Instalador* define-se o diretório onde o script do firewall vai ser instalado, o nome do usuário que irá se autenticar via SSH.

Terminada a configuração do firewall, o mesmo estará pronto para receber as configurações das placas e as regras definidas ao firewall.

4.3 CONFIGURANDO AS INTERFACES DO FIREWALL

Ao abrir o fwbuilder e o projeto em edição, criam-se as placas de rede existente no firewall. Adicionam-se as interfaces com os respectivos endereços IP's e suas máscaras de rede.

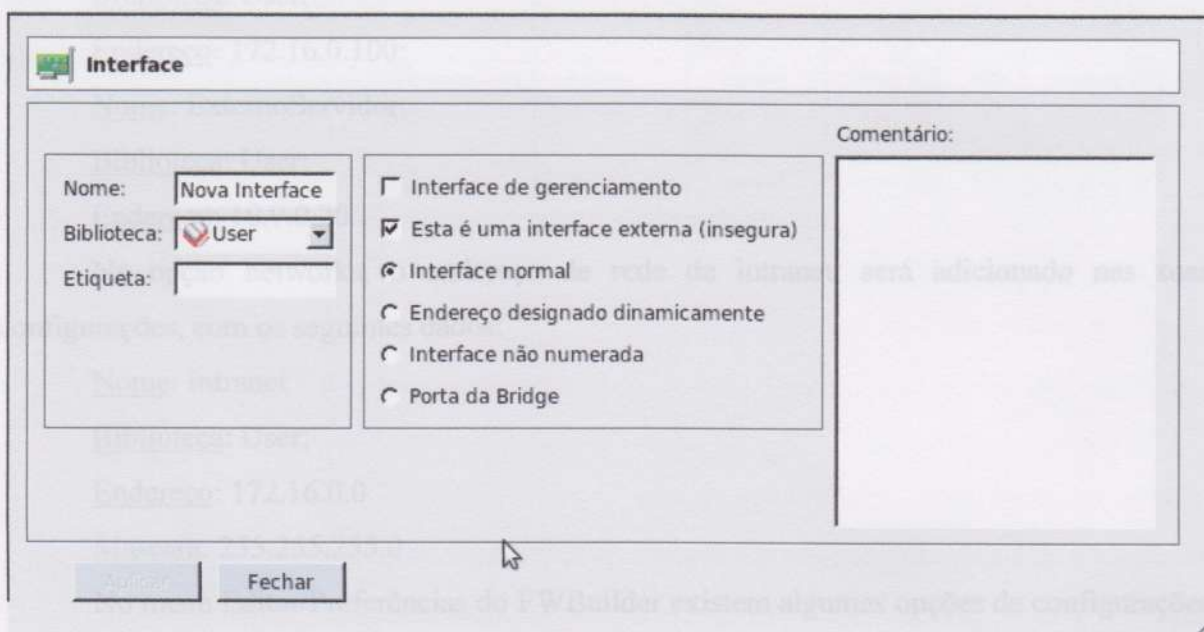


Figura 23: Tela com as configurações das interfaces de rede do firewall.

Fonte: Ferramenta FWBuilder(Captura da Tela)

A placa Internet é uma interface externa com o seu endereço de rede sendo atribuído dinamicamente, ou seja, receberá um IP da rede onde estiver sendo configurada por meio do serviço de DHCP, e sendo atribuído um IP como mostrado abaixo:

Nome: Internet;

Biblioteca: User;

Endereço: 10.9.0.x

Máscara: 255.255.255.0

A placa da intranet será responsável pelo gerenciamento do firewall e configurado como uma interface normal com um endereço de rede fixa.

Nome: Intranet;

Biblioteca: User;

Endereço: 172.16.0.1

Máscara: 255.255.255.0

O pacote enviado da rede 172.16.x.y para o firewall, será realizado o NAT e sairá para internet com o ip o 10.9.0.20.

Na pasta *Addresses* com as interfaces devidamente criadas, os endereços de rede do servidor interno e externo serão adicionados para a configuração do firewall. As configurações do servidor interno e externo são:

Nome: InternoServidor;

Biblioteca: User;

Endereço: 172.16.0.100;

Nome: ExternoServidor;

Biblioteca: User;

Endereço: 10.9.0.20

Na opção *networks*, o endereço de rede da intranet, será adicionado nas suas configurações, com os seguintes dados:

Nome: Intranet

Biblioteca: User;

Endereço: 172.16.0.0

Máscara: 255.255.255.0

No menu *Editar/Preferências* do FWBuilder existem algumas opções de configurações do software, são elas:

Diretório de Trabalho: Esta opção define onde se deve armazenar o arquivo de dados.

Verificar atualizações automaticamente: Se esta opção estiver marcada, toda vez ao iniciar o programa ele verificará a existencia de atualizações do programa.

Verificar agora: clicando nessa opção as atualizações serão verificadas naquele exato momento.

Usar o Proxy http para verificar atualizações(host:port): Se usar o método manual ou automático para verificar se há alguma atualização através do proxy. Para definir o proxy, será necessário separar o endereço IP do número da porta com dois pontos (:).

4.4 DEFININDO AS REGRAS DE FILTRAGEM

Na figura 24 serão apresentadas as regras de filtragem definidas no firewall, com as políticas de acesso e a de NAT, como uma demonstração de um firewall com suas regras específicas.

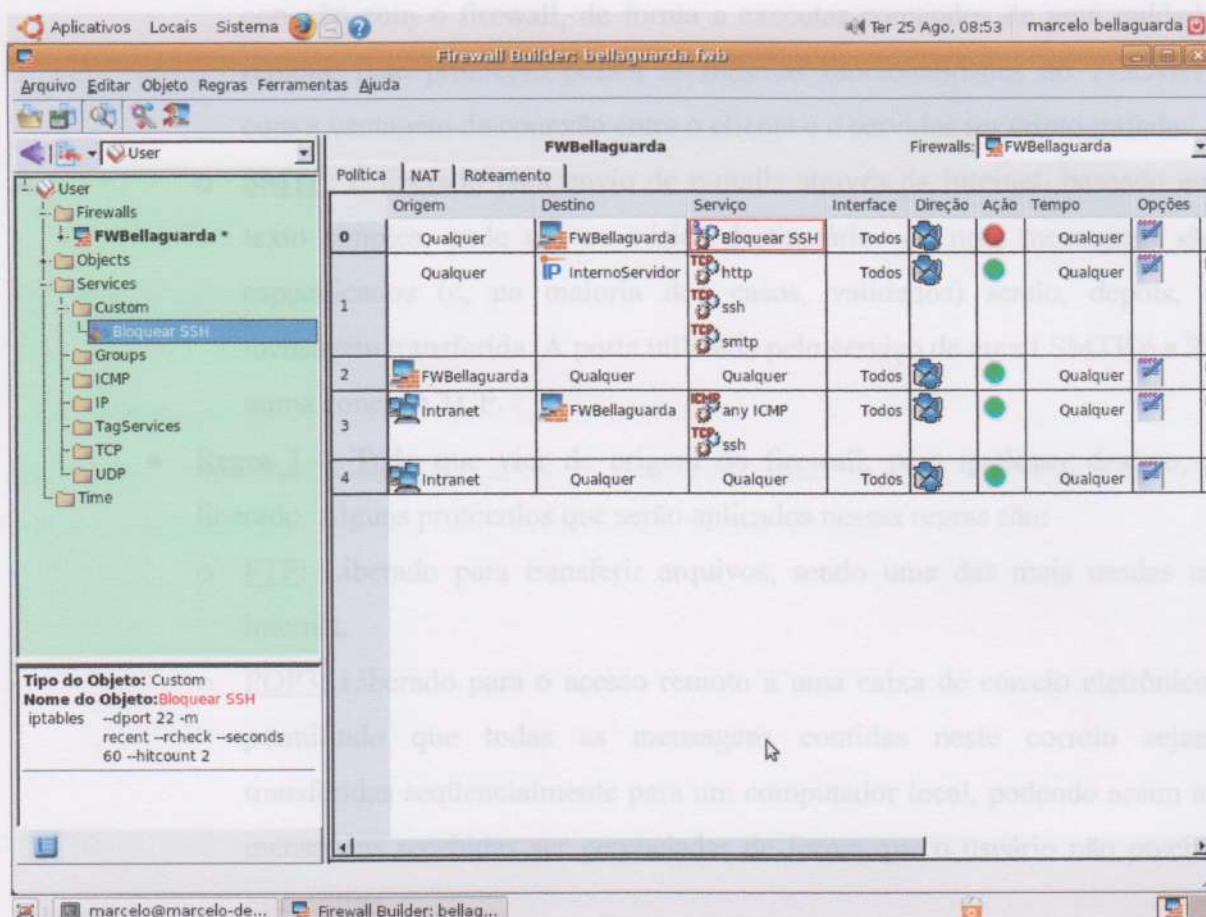


Figura 24: Tela com as regras de políticas de filtragem do Firewall.

Fonte: Ferramenta FWBuilder(Captura da Tela)

No FWBuilder, a leitura das regras são feitas de cima para baixo. No exemplo das políticas implementadas na figura 24, são definidas as seguintes regras de firewall:

- Regra 0 – O que vier de qualquer origem com destino ao firewall, realizando acessos via SSH na porta 22, caso exista 2 tentativas acesso sem sucesso em 1 minuto, a origem da conexão será negada.

- Regra 0 – Tudo que vier de qualquer origem, com destino ao servidor interno de IP 172.16.0.1, realizando os serviços de HTTP, SSH e SMTP, é liberado no servidor interno. Os serviços HTTP, SSH e SMTP são:
 - HTTP: Hiper Text Transfer Protocol, está sendo liberado na regra 0 para a transferência de Hipertexto da camada de aplicação do modelo OSI, utilizado para transferência de dados na rede mundial de computadores, a Word Wide Web (WWW). O mesmo transfere dados de hiper-mídia (Imagens, sons e textos)
 - SSH: Está sendo usado no firewall para o acesso remoto a ele, pois o fwbuilder utiliza o SSH para a aplicação das regras, permite assim a conexão com o firewall, de forma a executar comandos de uma unidade remota. Este protocolo possui as mesmas funcionalidades do TELNET, com a vantagem da conexão entre o cliente e o servidor ser criptografada.
 - SMTP: É liberado para envio de e-mails através da Internet, baseado em texto simples, onde um ou vários destinatários de uma mensagem são especificados (e, na maioria dos casos, validados) sendo, depois, a mensagem transferida. A porta utilizada pelo serviço de email SMTP é a 25 numa conexão TCP.
- Regra 1 – Tudo que vier de origem do firewall, para qualquer destino, é liberado. Alguns protocolos que serão aplicados nessas regras são:
 - FTP: Liberado para transferir arquivos, sendo uma das mais usadas na internet.
 - POP3: Liberado para o acesso remoto a uma caixa de correio eletrônico, permitindo que todas as mensagens contidas neste correio sejam transferidas seqüencialmente para um computador local, podendo assim as mensagens recebidas ser gerenciadas de forma que o usuário não precise estar online.
 - SQUID: é um servidor proxy que suporta HTTP, HTTPS, FTP e outros. Ele reduz a utilização da conexão e melhora os tempos de resposta fazendo cache de requisições freqüentes de páginas web numa rede de computadores. É utilizado também para gerenciamento das páginas da internet a serem acessadas.
 - TELNET: É um protocolo cliente-servidor usado para permitir a comunicação entre computadores ligados numa rede baseado em TCP.

- DOMAIN: É o protocolo utilizado para o DNS(Domain Name System), permitindo assim a resolução de nomes, ao consultar um site na web.
- Regra 2 – Tudo que vier de origem da intranet com destino ao firewall, permitir acesso aos protocolos any ICMP e o SSH.
 - ICMP: Utilizado no firewall para fornecer relatórios de erros à fonte original. Todos os computadores da intranet precisa aceitar as mensagens ICMP, e alterar o comportamento em resposta ao erro relatado. Os gateways devem estar programados para enviar mensagens ICMP quando receberem datagramas que provoquem algum erro.
- Regra 3 – Tudo que vier da intranet para qualquer destino e utilizando qualquer protocolo de rede permite tudo. Esta regra libera o acesso a qualquer destino utilizando qualquer protocolo a qualquer tempo.

4.5 DEFININDO AS REGRAS DE NAT

Na figura 25 algumas regras de tradução de endereços (NAT – *Network Address Translation*) foram definidas, assim como o redirecionamento da porta 80 (HTTP), para o SQUID, realizando assim o controle dos sites acessado pela Intranet.

Na figura 25 algumas regras de tradução de endereços (NAT – *Network Address Translation*) foram definidas, assim como o redirecionamento da porta 80 (HTTP), para o SQUID, realizando assim o controle dos sites acessado pela Intranet.

As regras de NAT no exemplo acima são:

- Regra 0: Na regra 0 todo acesso de origem da intranet com destino a Internet sairá com o IP externo (10.9.0.x) que o Firewall estiver disponibilizando naquele momento.
- Regra 1: Na regra 1 todo pacote que tiver como origem o Servidor Interno, traduzir o endereço de origem deste pacote com o IP externo do servidor, 10.9.0.20.

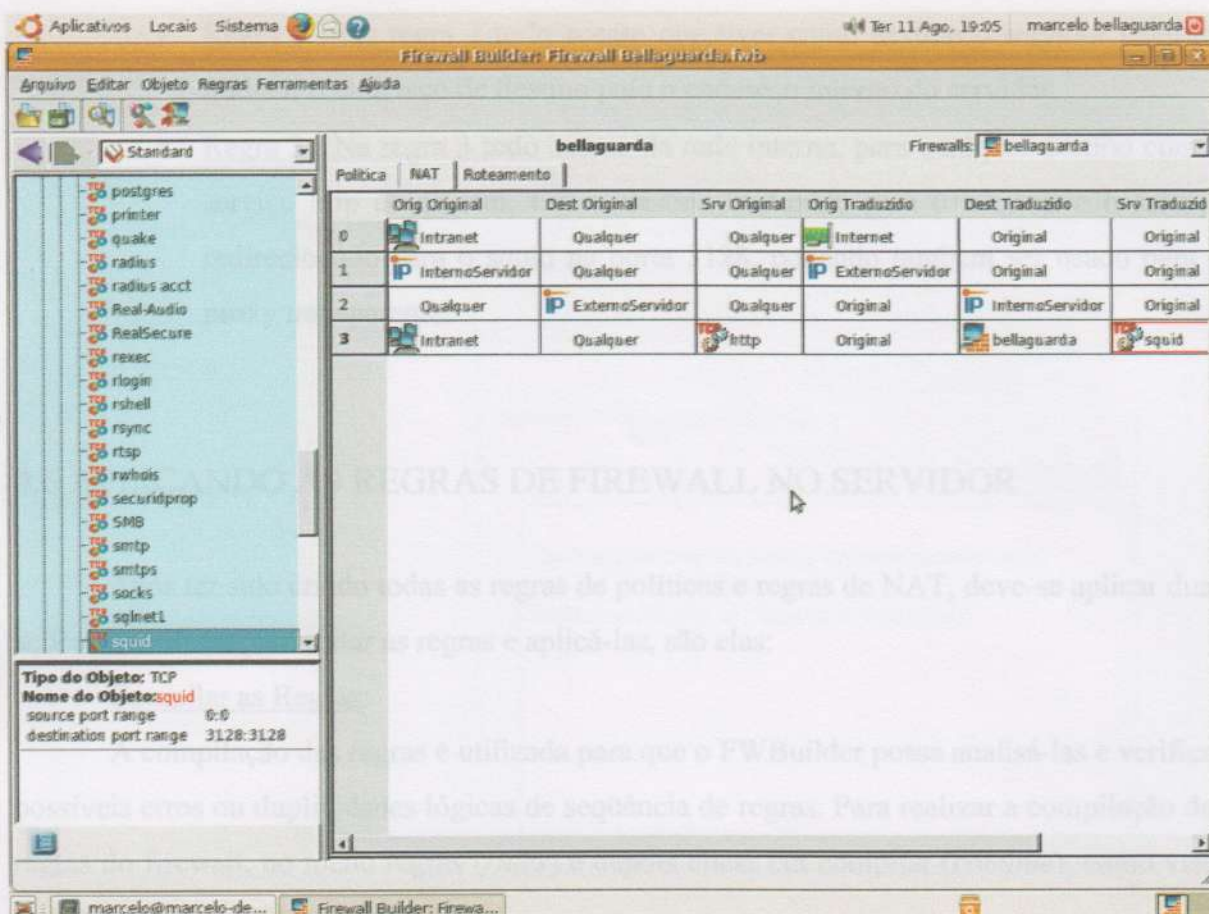


Figura 25: Tela com as regras de NAT e redirecionamento de portas do Firewall.

Fonte: Ferramenta FWBuilder (Captura da Tela)

NAT (*Network Address Translation*) é uma técnica que consiste em reescrever o endereço IP privado (da Intranet) de um pacote que passa por um *firewall* trocando este endereço privado por um público do firewall, permitindo que o computador da Intranet tenha acesso ao exterior (rede pública). No exemplo do estudo de caso, tudo que sair da rede 172.16.0.0 com destino a Internet, o endereço de origem do pacote será mascarado e sairá com o IP público do firewall 10.9.0.20, e no pacote de resposta acontecerá o processo inverso, traduzindo do IP público para o IP privado do host que gerou aquela conexão.

As regras de NAT no exemplo acima são:

- **Regra 0** : Na regra 0 todo acesso de origem da intranet com destino a internet sairá com o IP externo (10.9.0.x) que o Firewall estiver disponibilizando naquele momento.
- **Regra 1** : Na regra 1 todo pacote que tiver como origem o Servidor Interno, traduzir o endereço de origem deste pacote com o IP externo do servidor, 10.9.0.20.

- Regra 2 : Na regra 2 todo acesso que tiver como destino o servidor externo, traduzir o endereço de destino para o endereço interno do servidor.
- Regra 3 : Na regra 3 todo acesso da rede interna, para qualquer destino com o serviço http de origem, terá o destino traduzido para o firewall e o serviço redirecionado para o squid na porta 3128, podendo também ser usado para o proxy transparente.

4.6 APLICANDO AS REGRAS DE FIREWALL NO SERVIDOR

Após ter sido criado todas as regras de políticas e regras de NAT, deve-se aplicar duas ações específicas para testar as regras e aplicá-las, são elas:

Compilar as Regras:

A compilação das regras é utilizada para que o FWBuilder possa analisá-las e verificar possíveis erros ou duplicidades lógicas de sequência de regras. Para realizar a compilação das regras do firewall, no menu regras (*rules*) e depois clicar em compilar (*compile*), como visto na Figura 26.

Figura 26: Compilação das regras a serem aplicadas no Firewall.
Fonte: Ferramenta FWBuilder (Captura de Tela)

Aplicar as regras no servidor

Após ter realizado a compilação das regras, deve-se aplicá-las ao firewall. Para isso, deve-se clicar na mesma aba regras (*rules*) e depois em *install*, para que a interface aplique as regras no servidor do firewall, dentro da pasta *firewall* criada anteriormente.

Após clicar na opção *install* do firewall, será exibida uma tela para escolher qual ação executar, é aconselhável compilar primeiramente o arquivo e depois instalá-lo, pois assim evitam-se possíveis erros nas regras do firewall. Realizado o procedimento sem nenhuma erro, será solicitado o usuário que instale as regras e sua senha, para finalmente as regras serem aplicadas.

4.7 UM SCRIPT PARA INICIAR O FIREWALL AUTOMATICAMENTE

Ao aplicar as regras no firewall, pode-se criar um script para o firewall. Na figura 27 é mostrado um script de configuração do firewall, que será configurado da seguinte forma:

No arquivo /etc/rc.local, adiciona as seguintes linhas em negrito.

```
#!/bin/bash
# arquivo rc.local
...
# habilita roteamento
echo 1 > /proc/sys/net/ipv4/ip_forward
# carrega regras do firewall
/firewall/bellaguarda.fw
exit 0
```

Figura 27: Script para iniciar o Firewall.

Fonte: Criado no Word

No script da figura 27, o roteamento é habilitado e logo em seguida o arquivo do firewall é executado, sendo realizada a aplicação de todas as regras realizadas anteriormente.

5 CONCLUSÃO

A elaboração deste trabalho foi de suma importância para o aprendizado de forma prática da ferramenta FWBuilder.

Além dos conhecimentos da ferramenta, a elaboração do trabalho permitiu conhecer melhor algumas regras de firewall, o funcionamento da tradução de endereços(NAT), o redirecionamento de portas e os protocolos utilizados na Internet para um melhor gerenciamento.

Para o Administrador de Redes, a ferramenta de gerenciamento de firewall estudada vem a facilitar ainda mais o trabalho nas redes, pois as regras são de fácil entendimento e de serem editadas, podendo assim ter uma maior rapidez nas adições e remoções de regras do firewall.

WIKIPEDIA. *Internet*. Disponível em: <<http://pt.wikipedia.org/wiki/Internet>>. Acesso em: 26 jun. 2009.

VIVA O LINUX. *Apêndices*. Disponível em: <<http://www.vivailinux.com.br/algos/seguranca/seguranca-em-o-lp-tables>>. Acesso em: 22 jun. 2009.

ZWICKY, E. D.; COOPER, S. CHAPMAN, D. B. *Building Internet Firewalls*. 1. ed. Beijing: O'Reilly, 2000.

REFERÊNCIAS

TANENBAUM, A. S. **Redes de computadores**. 4. ed. Rio de Janeiro: Campus, 2003.

_____. **Redes de computadores**. 3. ed. Rio de Janeiro: Campus, 1997.

LAWTON, Stephen. *Intranets Fuel Growth of Internet Access Tools*. *Digital News & Review*, abr. , 1995.

TORRES, Gabriel. **Redes de Computadores: Curso Completo**. [S. l.]: Axel Books, 2001.

COMER, D. E. **Interligação de redes com TCP/IP**. Rio de Janeiro: Campus, 2006.

WIKIPÉDIA. *Internet*. Disponível em: <<http://pt.wikipedia.org/wiki/Internet>>. Acesso em: 26 jun. 2009.

VIVA O LINUX. *Iptables*. Disponível em: <<http://www.vivaolinux.com.br/artigo/Firewall-seguro-com-o-IPTables>>. Acesso em: 22 jun. 2009.

ZWICKY, E. D.; COOPER, S. CHAPMAN, D. B. *Building Internet Firewalls*. 2. ed. Beijing: O'Reilly, 2000.