PONTIFÍCIA UNIVERSIDADE CATÓLICA DE SÃO PAULO – PUC-SP

Dorival Moreira Machado Junior

Proposta de interface para ensino de funcionamento interno de um *Firewall*

MESTRADO EM TECNOLOGIAS DA INTELIGÊNCIA
E DESIGN DIGITAL

Dissertação apresentada à Banca Examinadora da Pontifícia Universidade Católica de São Paulo, como exigência parcial para obtenção do título de MESTRE em Tecnologias da Inteligência e Design Digital – Processos Cognitivos e Ambientes Digitais, sob a orientação do Prof. Doutor Alexandre Campos Silva.

São Paulo-SP

2011

MACHADO JR, DORIVAL MOREIRA, **Proposta de interface para ensino de funcionamento interno de um Firewall**, 2011, 106 f. Dissertação (Mestrado em Tecnologias da Inteligência e Design Digital) – Pontifícia Universidade Católica de São Paulo, São Paulo, 2011.

ERRATA

Folha	Linha	Onde se lê	Leia-se
1(capa)	**3**	**interface**	**simulador**
4(resumo)	**1**	**interface**	**simulador**
4(resumo)	**15**	**uma interface de software**	**um simulador**
4(resumo)	**24**	**Palavras chave: firewall, redes, interface, signos, design da informação**	**Palavras chave: firewall, redes, design da informação**
5(abstract)	**1**	**interface**	**simulator**
5(abstract)	**13**	**software interface**	**simulator**
5(abstract)	**21**	**Keywords: firewall, network, interface, signs, information design**	**Keywords: firewall, network, information design**
13	**18**	**interfaces**	**interfaces gráficas**
13	**34**	**interfaces**	**interfaces gráficas**
23	**16**	**conheciment**	**conhecimento**
26	**3**	**Interface tem por objetivo**	**interface gráfica tem por objetivo**
27	**18**	**como o Assembly[3]**	**como a Assembly (então compilada pelo Assembler[3])**
28	**5**	**interface**	**interface gráfica**
34	**10**	**melhoradas**	**melhoras**
45	**2**	**interface**	**interface gráfica**
69	**10**		**O Packet Tracer utiliza-se do recurso de simulação, o que permite ao aluno ver diversos ambientes sem precisar implementá-los no mundo real. Este recurso mostra-se útil no aprendizado, pois permite parecer real algum objeto, ambiente ou contexto a ser estudado. Desta forma, a simulação é uma alternativa para o objeto desta pesquisa, pois o ambiente de estudo, ou seja, o interior do *firewall* não é algo no qual o aluno possa "estar".**
71	**21**	**à interface de ensino e gerenciamento de um *firewall***	**à interface de um simulador para ensino de *firewall***
75	**25**	**interface**	**simulador**
100	**11**	**da interface**	**do simulador**
101	**23**	**Esta interface**	**Este simulador**

Banca examinadora

_____

_____

_____

Agradecimentos

Agradeço a Deus que me proveu mais uma oportunidade de aprendizado, bem como a inteligência necessária para adquirir tal conhecimento.

Agradeço aos meus pais, Dorival e Divina, pelo incentivo e apoio contínuo aos estudos, bem como pela atenção especial na condição de vovô e vovó.

Agradeço à minha esposa Márcia pela paciência e compreensão diante da minha ausência e noites reduzidas de sono durante o período de pesquisa. Agradeço pelo seu amor e companheirismo, em especial pelos sete anos de casamento completados recentemente no decorrer desta pesquisa.

Agradeço ao meu filho Giovanni pela alegria que ele me proporciona, pelos momentos inesquecíveis os quais não tem como serem descritos, mas só quem é pai conhece.

Agradeço aos meus irmãos Julio Cesar e Julio Henrique pela presença familiar.

Agradeço aos professores do TIDD que transmitiram grande conhecimentos na área estudada.

Agradeço ao amigo Davidson pelos lanches exóticos, bem como o companheirismo durante o curso e as viagens semanais até São Paulo-SP.

Agradeço ao professor Alexandre Campos Silva, que me conduziu fortemente no desenvolvimento desta dissertação, delineando e conduzindo a um resultado satisfatório.

RESUMO

MACHADO JR, DORIVAL MOREIRA, **Proposta de interface para ensino de funcionamento interno de um *Firewall***, 2011, 106 f. Dissertação (Mestrado em Tecnologias da Inteligência e Design Digital) – Pontifícia Universidade Católica de São Paulo, São Paulo, 2011.

A internet é um elemento de muita importância para a sociedade mundial nos dias de hoje, com tendência de cada vez mais se tornar algo indispensável para as pessoas. Um dos agentes responsáveis pelo equilíbrio e organização desta rede é o *firewall*. Embasando-me nos últimos quatro anos ministrando tal conteúdo em disciplinas de redes de computadores em curso de Sistemas de Informação, observei a dificuldade por parte de alunos em abstrair e visualizar os acontecimentos no interior do *firewall*. Esta dificuldade se refere ao entendimento do funcionamento interno do *firewall*, como ele se porta diante de uma lista de regras de controle, que ações devem ser tomadas perante cada pacote de dados que passa por ele. O objetivo deste trabalho é analisar as dificuldades de ensino de um *firewall* e propor a utilização de uma interface de *software* para melhoria no ensino do tema. Assim apresento uma revisão bibliográfica levantando conceitos sobre signos, semiótica, *design* e interface homem computador. Este estudo propiciou a eleição de uma lista de qualidades a serem caracterizadas na interface proposta neste trabalho. Em seguida, é apresentado o funcionamento básico de um *firewall*, descrevendo as principais habilidades que ele deve possuir, apresentando ainda uma análise de interfaces de gerenciamento de *firewall* mais utilizadas. Por fim, apresento a proposta de interface através de esboços de um ambiente didático pedagógico propício ao ensino do tema e levando em consideração as qualidades então identificadas.

Palavras chave: *firewall*, redes, interface, signos, *design* da informação

ABSTRACT

MACHADO JR, DORIVAL MOREIRA, **Proposed interface for teaching inner workings of a Firewall**, 2011, 106 f. Dissertação (Mestrado em Tecnologias da Inteligência e Design Digital) – Pontifícia Universidade Católica de São Paulo, São Paulo, 2011.

Internet is an element of great importance to society today, with a trend of increasingly become indispensable for our people. One of the agents responsible for balance and organization of this network is the firewall. Encouraged over the past four years ministering such content in the disciplines of computer networks in the course of Information Systems, noted the difficulty on the part of students to abstract and visualize the events inside the firewall. This difficulty comes to understanding the inner workings of the firewall, how he carries himself on a list of control rules, what actions should be taken before each data packet passing through it. The objective of this study is to analyze the difficulties of teaching a firewall and propose the use of a software interface to improve the teaching of the subject. So I present a literature review concepts about raising signs, semiotics, interface design and human computer. This study led to the election of a list of qualities to be featured on the interface proposed in this paper. Then we present the basic operation of a firewall, describing the key skills of it's own, presenting a further analysis of management interfaces most commonly used firewall. Finally, I present a proposal for a rough interface through a learning environment conducive to teaching and learning of the subject taking into account the qualities then identified.

Keywords: firewall, network, interface, signs, information design

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE SIGLAS

ABNT -Associação Brasileira de Normas Técnicas
ACK – Acknowledgement
AIGA – American Institute of Graphic Arts
DNAT – Destination Network Address Translate
DOS – Denial of Service
EUA – Estados Unidos da América
GNU – Acrônimo recursivo de “GNU's Not Unix”
GUI – Graphic User Interface
HTTP – Hypertext Transfer Protocol
ICMP – Internet Control Message Protocol
IEC – International Electrotechnical Commission
IP – Internet Protocol
ISO – International Organization for Standardization
NAT – Network Address Translate
NBR – Norma Brasileira
SNAT – Source Network Address Translate
SRI – Stanford Research Institute
SSH – Secure Shell
TCP – Transmission Control Protocol
UDP – User Datagram Protocol
VPN – Virtual Private Network
Xerox PARC – Paio Alto Research Center Xerox

Sumário

INTRODUÇÃO

O assunto redes de computadores é algo emergente na atualidade. A interligação mundial de computadores, antes artigo de filmes de ficção científica, torna-se real e tende cada vez mais interligar coisas e pessoas. Pode-se dizer que existe tecnologia antes e depois da internet. A grande maioria dos *softwares* desenvolvidos atualmente, são voltados para o funcionamento em rede. Dispositivos móveis através de tecnologia de terceira geração e similares, possibilitam cada vez mais a transmissão de dados em velocidades elevadas. Fatores como estes possibilitam a usuários em lados opostos do globo terrestre se comunicar e divulgar entre si, os mais diversos tipos de informações de forma quase instantânea. Empresas podem ter instalações geograficamente distantes, porém interligadas como se estivessem no mesmo local. Este avanço das redes é algo emergente, ainda mais quando se fala na tendência de interligação também de equipamentos eletrônicos como micro-ondas, geladeiras, entre outros dispositivos que cercam os seres humanos. A grande relevância neste assunto, torna essencial o estudo de redes em disciplinas de curso superior, extensão ou especialização. Praticamente é um conhecimento inevitável ao profissional de tecnologia da informação, e posteriormente quem sabe, às pessoas de uma forma geral, e neste último caso não necessariamente tão afundo.

O estudo de redes pode ser segmentado de forma a aprimorar o conhecimento em áreas específicas. Rede sem fio, comunicação via satélite, segurança da informação, *firewalls*, são alguns dos segmentos possíveis ao estudo de redes. Coloco em destaque o assunto *firewall*, por ser um elemento inevitável quando se fala de internet. Ele é a primeira linha de defesa de uma rede, controlando o que deve e o que não deve passar. Desta forma é de suma importância o conhecimento da correta configuração de regras de controle do *firewall*.

Atualmente ministro disciplinas de redes de computadores e segurança da informação. Nos últimos quatro anos ministrando tais disciplinas em curso superior de sistemas de informação, em especial o ensino de *firewall*, identifiquei a dificuldade por parte de alunos em compreender o funcionamento interno do mesmo. Dificuldade esta não limitada ao conceito, objetivo e contexto no qual está inserido, mas sim ao funcionamento interno, ao que ocorre com um pacote de dados (conhecido como datagrama IP) quando este entra no *firewall*. Percebi em minhas aulas, a dificuldade em abstrair e visualizar os acontecimentos dentro do mesmo. O que ocorre mediante as regras de controle então implementadas, como ocorre uma

proibição, liberação ou roteamento quando se tem varias regras as quais o pacote deve ser submetido. Este é o principal problema o qual esta dissertação busca resolver. Este processo poderia ser mais facilmente visualizado para estudo? A utilização de uma interface mais dinâmica possibilitaria um melhor entendimento do que se passa no *firewall* e ainda, melhorar o entendimento do que é um *firewall*? Atualmente existem diversas ferramentas livremente distribuídas, porém específicas para a configuração de regras e não para ensino.

Diante desta evidente relevância no estudo de redes de computadores e em especial o *firewall*, esta dissertação tem como objetivo: analisar as dificuldades de ensino de um *firewall* e propor a utilização de uma interface de *software* para melhoria no ensino do tema.

Para atender ao objetivo proposto, a metodologia de pesquisa foi dividida em três partes:

a) Leitura bibliográfica, a fim de levantar os conceitos fundamentais de signos, *design* e interface homem computador.
b) Apresentação do funcionamento básico de um *firewall*, conceituando os elementos que o envolvem, descrevendo a lógica de funcionamento e propondo uma estrutura didático pedagógica para ensino do mesmo.
c) pesquisa de interface de *software* para ensino de um *firewall*, fazendo uma análise das interfaces existentes, delineando uma melhor forma para prover o ensinamento ou análise de um *firewall*.

O esquema geral desta dissertação de forma a atender o objetivo proposto, é composto da seguinte forma:

a) Capítulo 1 - Os signos e o processo cognitivo: apresentará os conceitos de signos tais como qualidades e relação triádica, correlacionando-os ao conceito de consciência, dado e informação, descrevendo cada elemento envolvido. É discutido também o processo cognitivo de aprendizagem, apresentando a visualização de dados como um recurso de compreensão eficaz.
b) Capítulo 2 – Interface homem computador: objetiva estudar conceitos acerca de interface homem computador, considerando elementos como a artificialidade da comunicação humana e histórico de interfaces, afim de justificar conceitos, bem como uma definição clara de usabilidade que a interface deve possuir.
c) Capítulo 3 – Interfaces para ensino de *firewall*: tratará sobre a importância do *firewall* como agente de equilíbrio na internet, fazendo uma breve explanação do funcionamento interno do mesmo. Será feito uma análise de algumas interfaces existentes e por fim o levantamento de uma lista de qualidades ideais

para uma interface de ensino de *firewall*.

d) Capítulo 4 – Proposta de interface para visualização dinâmica: tratará sobre um esboço, uma proposta de interface que atenda a todas as qualidades identificadas no capítulo anterior.

e) Capítulo 5 – Considerações finais: é a conclusão do trabalho, indicando ainda os trabalhos futuros que esta pesquisa possibilitará.

1. OS SIGNOS E O PROCESSO COGNITIVO

Para o desenvolvimento deste estudo envolvendo a questão de interfaces, convém o levantamento de algumas informações acerca de signos e o processo cognitivo. A promoção da discussão bem como a resolução do problema envolvendo signos, requer uma pesquisa extensa e exclusivamente para este fim. Assim, este capítulo limita-se a fazer apenas uma abordagem inicial, uma introdução sobre signos e o processo cognitivo, alinhando alguns conceitos básicos ao estudo de interface.

Convém neste momento, tornar claro as primícias, o prelúdio do momento inicial de percepção da existência do signo por parte do indivíduo, justificando o signo como informação. São descritas as qualidades do signo: primeiridade, secundidade e terceiridade, correlacionando-as junto à consciência. Em seguida, são levantados os conceitos de signo-objeto-interpretante, elementos estes da relação triádica do signo, descrevendo cada um. Por fim, é abordado o processo cognitivo de aprendizagem, apresentando a visualização de dados como recurso de compreensão.

1.1. SIGNO: UMA INFORMAÇÃO AGUARDANDO POR SER INTERPRETADA

Conforme PETRY (2008, p.2) “Frequentemente nos deparamos diante de uma imagem que captura nossa atenção, tendo como efeito direto o nosso silencioso demorar-se sobre a sua consideração”. Através desta afirmação, dá-se a conhecer tal como é a primeira reação do indivíduo perante um signo em questão. Signo este que pode se apresentar de diversas maneiras: impresso, esculpido, sonoro, projetado mentalmente pelo próprio indivíduo, enfim nas possíveis formas em que ele é imediatamente percebido. Esta é a narração do momento crucial onde é possível perceber a relação triádica signo-objeto-interpretante, então objeto de estudo o qual este capítulo contempla.

Neste processo inicial de percepção, o signo é capaz de produzir um alerta ao indivíduo, objetivando representar algo, referir-se a um objeto, reduzir uma situação de estado de incerteza para um estado de certeza. Uma revisão dos conceitos de dado, informação e conhecimento, possibilitam uma melhor imersão nesta afirmação de certeza e incerteza, compreendendo seu real significado através de uma analogia. Tais conceitos estão suficientemente definidos da seguinte forma:

> A informação não é a extremidade no processo de construção da compreensão. Quando os dados, que por sua vez são meros registros, adquirem sentido interpretativo, eles se transformam em informação. Quando a informação é internalizada no indivíduo e compreendida a partir de experiências prévias, ela se transforma em conhecimento. Dessa forma, percebemos um fluxo crescente de interpretação entre dado, informação e conhecimento, nessa ordem. (RIBEIRO, 2009, p. 24)

Convém salientar que os conceitos de dado e informação também dependem do contexto no qual estão inseridos. Como exemplo, considere a mera sequência de caracteres “VHQWLPHQWRV” que em um primeiro momento transporta o indivíduo, então intérprete, a um estado de incerteza. Logo, esta sequência é por definição, um dado. Neste momento, isto não é um signo. Ao inserir no contexto o elemento criptografia, em especial o “Código de Cesar”[1], a sequência de caracteres adquire sentido interpretativo, transformando-se na palavra “SENTIMENTOS”. É transmitido a partir de agora, um estado de certeza, o que por definição torna-se uma informação. Agora pode-se dizer que este é um signo. Ele trás à mente novos signos, os quais também ocasionarão novos signos, entrando em um ciclo infinito de criação de signos. Esta palavra, mesmo que isolada, conduzirá o indivíduo a trazer à mente algum pensamento relacionado ao tema, uma lembrança, uma paisagem ou uma sensação. É sabido que a sequência de caracteres sempre foi uma informação levando-se em consideração um universo mais abrangente de potenciais intérpretes. Porém não perceptível ao intérprete em questão até que lhe seja inserido o fator criptografia. Em outras palavras, a organização dos dados mediante a utilização de um determinado processo (neste caso a criptografia), altera o conceito entre dado e informação (BAMBIRRA, 2009, p. 26) apud (TURBAN et al., 2004, p. 326).

Diante destas sustentações, observa-se que o signo tem por objetivo ser uma informação aguardando por ser interpretada, devendo sempre significar algo, representar um objeto e referir-se a ele. Se não significa algo, então não pode ser signo. Tal fundamento alinha-se ao conceito de Peirce, que diz:

> [...] se houver alguma coisa que veicule informação e, apesar disso, não tenha absolutamente relação nem faça referência a algo com o qual a pessoa a quem a informação é transmitida tenha a menor familiaridade, direta ou indireta, quando recebe a informação – informação que seria de uma espécie estranhíssima -, o veículo desse tipo de informação não será, neste contexto, denominado Signo. (SANTAELLA, 2008, p.35).

1 Algoritmo de criptografia de substituição simples, no qual cada letra do alfabeto é substituída pela próxima em três posições adiante. Um exemplo online de teste deste algoritmo pode ser encontrado no endereço: http://www.numaboa.com/criptografia/124-substituicao-simples/165-codigo-de-cesar

Conforme PETRY (2008, p.2), no momento de encontro, o indivíduo se depara com a possibilidade de deixar com que algo fale entre este e o signo. Acontece um diálogo silencioso entre ambos, afim de se internalizar tal informação no indivíduo e assim ser compreendida a partir de experiências prévias, transformando-se em conhecimento. Este conhecimento por si, são novos signos gerados, e que vão também gerar novos signos. Segundo SANTAELLA (2008, p.4),

> [...] não há, de modo algum, comunicação, interação, projeção, previsão, compreensão, etc sem signos. [...] Tudo é relativo, porque tudo depende dos signos de modo absoluto. No limite, signo é sinônimo de vida. Onde houver vida, haverá signos. A ação do signo, que é a ação de ser interpretado, apresenta com perfeição o movimento autogerativo, pois ser interpretado é gerar um outro signo que gerará outro e assim infinitamente, num movimento similar ao das coisas vivas.

Ao ser interpretado, o signo gera um outro signo em um ciclo infinito. Esse processo pode ser percebido na mente do intérprete, pois todo pensamento se processa por meio de signos. Tome-se por base qualquer pensamento que venha à mente. Um pensamento é a continuação de outro, dando origem a um novo. Conforme ainda a mesma autora SANTAELLA (2008, p.9), “Pensamento é diálogo. Semiose ou autogeração é, assim, também sinônimo de pensamento, inteligência, mente, crescimento, aprendizagem e vida”.

Conclui-se diante deste embasamento, que os signos estão presentes em todas as coisas e que mesmo involuntariamente, os seres intérpretes (sejam humanos ou não, pois deve-se considerar a possibilidade de intérpretes cibernéticos, entre outras tecnologias de reconhecimento de signos) geram novos signos a cada pensamento.

1.2. A CONSCIÊNCIA E AS QUALIDADES DO SIGNO

Qualquer coisa que esteja de algum modo presente à mente, seja um fator externo (um som, o cheiro de uma pizza, etc.), interno ou visceral (lembrança, dor no estômago ou uma recordação vaga e quase apagada da mente), ou ainda uma ideia geral abstrata, é um fenômeno. Logo, o signo também o pode ser considerado. A consciência é o ambiente onde aparecem os fenômenos, sendo estes, modos de operação do pensamento-signo que se processa na mente (SANTAELLA, 1983, p.1, p.7).

O termo “consciência” é um pouco diverso no seu significado perante algumas

ciências. Conforme PEREIRA (2003), trata-se de um problema clássico esta definição, pois o termo é utilizado livremente para delimitar vários significados diferentes, ou diferentes aspectos da função cerebral. Pelo conceito clássico, "consciência é aquele estado em que a pessoa está ciente de suas ações físicas e mentais. O que só ocorreria, se ela estiver acordada e alerta. Não, se dormindo, em coma, ou sob anestesia geral" (OLIVEIRA, 1998). Isto não quer dizer que um fenômeno externo não se englobe em tal situação. A pessoa no estado de consciência, está ciente de suas ações físicas perante um evento externo, como por exemplo a vibração do tímpano diante da audição de uma orquestra de câmara. Também está ciente de suas ações mentais, diante de uma lembrança trazida à mente logo ao interpretar um signo. Para esta dissertação foi observado a obra de Charles Sanders Peirce(1839-1914)[2], mais especificamente a parte sobre semiótica, ou seja, a ciência dos signos. Existe uma certa conformidade com a definição clássica e com o que Peirce menciona como consciência:

> Consciência não se confunde com razão. Consciência é como um lago sem fundo no qual as idéias (partículas materiais da consciência estão localizadas em diferentes profundidades e em permanente mobilidade. A razão (pensamento deliberado) é apenas a camada mais superficial da consciência. Aquela que está próxima da superfície. Sobre essa camada, porque superficial, podemos exercer autocontrole e também, porque superficial, é a ela que nossa autoconsciência está atada. Daí tendermos a confundir consciência com razão. No entanto, se bem que a razão seja parte da consciência, ela não compõe, nem de longe, o todo da consciência. [...] consciência não é tomada como uma espécie de alma ou espírito etéreo, mas como lugar onde interagem formas de pensamento. (SANTAELLA, 1983, p. 9)

Ou seja, a consciência é o local onde interagem as formas de pensamento, aos quais a pessoa mesmo involuntariamente tem ciência de suas ações físicas e mentais. Conforme SANTAELLA (1983), estas formas de pensamento, ou fenômenos como já mencionado anteriormente, aparecem à consciência de três modos: primeiridade, secundidade e terceiridade, também conhecidos como qualidades do signo (Figura 1).

2 Considerado o fundador da moderna Semiótica, tendo como uma das marcas do seu pensamento, a ampliação da noção de signo. Mais informações sobre Peirce estão disponíveis em http://www.pucsp.br/pos/cos/cepe/peirce/peirce.htm

FIGURA 1: qualidades do signo

A primeiridade refere-se ao momento da consciência imediata, é o momento da pura qualidade de ser e sentir. É uma forma livre e não pode ser manipulada. É o objetivo, fundamento, aspecto ou caráter percebido logo ao ver o signo.

A secundidade compreende o fato de existir, é a ação e reação. Compreende o ambiente ao redor do objeto, determinando a que o signo se aplica.

Por fim, a terceiridade, que é o pensamento em signos, através da qual o usuário representa e interpreta todas as coisas, o mundo em si. Enfim, são as interpretações possíveis para o signo. Uma pequena frase da autora (SANTAELLA, 1983) de muito peso e significado convém ser destacada em tempo: “[...] o simples ato de olhar já está carregado de interpretação [...]”, atando-se assim à definição de que tudo depende dos signos de modo absoluto. O mundo é tido como um universo material, mas sobretudo simbólico (ROYO, 2008, p.48).

1.3. O SIGNO E A SUA RELAÇÃO TRIÁDICA

Uma vez dada a conhecer a reação de um intérprete diante de um signo, alinhá-lo aos conceitos de dado, informação e conhecimento, e por fim apresentar e justificar a existência de signos em todas as coisas, convém uma definição clássica de o que é signo. SANTAELLA (2008), faz menção que existem muitas variações das definições de signo, algumas muito generalizadas. Desta forma, foi selecionada a seguinte definição nas próprias palavras de Peirce:

> Defino um signo como qualquer coisa que, de um lado, é assim determinada por um Objeto e, de outro, assim determina uma idéia na mente de uma pessoa, esta última determinação, que denomino o Interpretante do signo, é, desse modo, mediatamente determinada por aquele Objeto. Um signo, assim, tem uma relação triádica com seu Objeto e com seu Interpretante. (SANTAELLA, 2008, p. 12)

A utilização do termo “coisa” pode referenciar tanto uma entidade física, quanto uma entidade imaginária, mítica, fictícia, entre outros. Todos estes são capazes de ser signo. Peirce não define apenas as palavras “signo”, “objeto” e “interpretante”, mas “[...] a relação de representação como forma ordenada de um processo lógico.” (SANTAELLA, 2008, p. 17). A formulação da tríade não se resume simplesmente à nomenclatura signo-objeto-interpretante, mas também à relação entre estes, à forma como um está para o outro, como estes interagem e se completam mutuamente tornando-se uma semiose. Todos os membros da tríade (Figura 2) são signos, tendo como diferença apenas o papel lógico desempenhado por cada um. Não é possível organizá-los de forma linear, os três membros são correlatos e engendram-se de tal forma que não se pode ver a divisão exata onde um começa e outro termina (SANTAELLA, 2008, p.15, p.17) apud RANSDELL (1966).

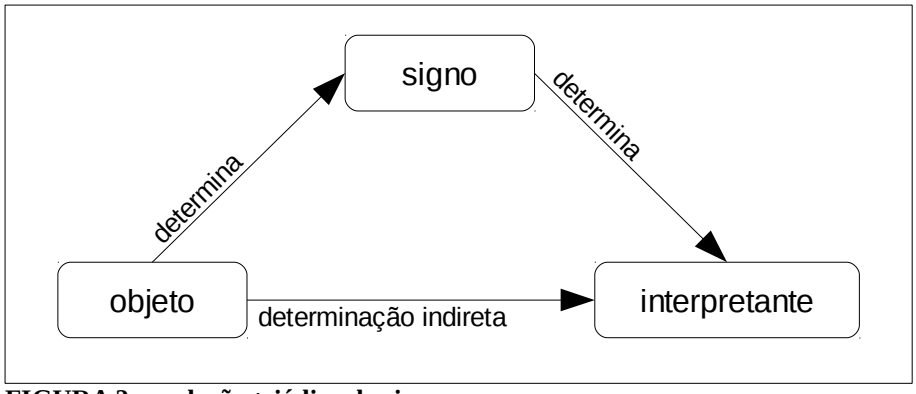

FIGURA 2: a relação triádica do signo

Para que o signo seja completo, ou seja, signo por excelência, os três elementos devem existir, e não apenas dois. O signo deve existir para justificar a determinação de um objeto, e por outro lado, sem o interpretante, isto é, sem a determinação de uma ideia na mente do intérprete, nenhum significado foi passado, o que descaracterizaria tal relação como signo por excelência. A influência entre os três elementos é tri-relativa, envolvendo a colaboração entre os elementos que buscam se completar um através dos outros.

Conforme SANTAELLA (2008, p.29), um signo é por natureza inevitavelmente incompleto, no sentido de que por sua própria constituição, está fadado a desenvolver-se num interpretante, o qual se desenvolverá em outro signo, assim indefinidamente. Neste momento, o intérprete procede a interpretação, ao mesmo tempo herdando do signo, o vínculo de representação. Justifica-se então o ciclo infinito, um processo de crescimento, onde o interpretante gerará um outro signo, mantendo a corrente sem fim.

Na relação triádica, o elemento denominado objeto, é caracterizado por Peirce como "[...] qualquer coisa que chega à mente em qualquer sentido [...]" (SANTAELLA, 2008, p.33), conduzindo à ideia de que trata-se então de qualquer coisa que é mencionada ou sobre a qual se pensa. Objeto é aquilo que provoca o signo, porém o objeto não é o signo. A ligação de ambos se dá sob algum aspecto ou qualidade e não em virtude de todos estes, pois desta forma o objeto poderia ser o signo. Daí a qualidade do signo ser incompleto, não podendo ser o objeto. O signo tende então a desenvolver-se no interpretante buscando se completar. Contudo, o interpretante então elemento da relação triádica, também é de natureza sígnica, o que o torna também incompleto, mantendo-se em compromisso para com o objeto.

Ainda como parte constitutiva do signo, a relação triádica é integrada por mais um elemento denominado interpretante. Afirmando-se que o signo representa um objeto, que o signo é o resultado provocado por um objeto, isto implica que o signo afeta uma mente, determinando nesta, algo mediatamente devido ao objeto. Esta determinação é o interpretante. É justamente devido ao fato de que o signo representa o objeto, que ele dispõe da qualidade de gerar um interpretante (SANTAELLA, 2008, p.62). Segundo Peirce (SANTAELLA, 2008, p.64), "[...] o interpretante não é outra coisa senão uma outra representação.", ou seja, todo interpretante é um signo, bem como um signo é um interpretante. Convém salientar que interpretante, intérprete e interpretação não são a mesma coisa. O signo afeta uma mente criando algo nesta. Este algo é o interpretante. Intérprete é o ato interpretativo, elemento perceptor do signo, podendo ser humano ou não. Por fim a interpretação que é o resultado do ato interpretativo.

Concluindo, fica claro que os elementos signo-objeto-interpretante, são de natureza

sígnica, sendo incompletos e necessitando um dos outros para se completarem. O signo representa o objeto, o objeto determina o signo, e o interpretante é determinado imediatamente pelo signo e indiretamente pelo objeto.

1.4. O PROCESSO DE SEMIOSE DOS SIGNOS

Durante o processo de abstração, o intérprete, seja ele humano ou não, busca imaginar, ou seja, interpretar a informação que o signo objetiva transmitir, o que ele quer conduzir do mundo exterior à mente ou área de processamento quando não humano. Involuntariamente acontece o processo de semiose dos signos: estética, ética e semiótica(lógica) (SANTAELLA, 1983). Assim como na qualidade dos signos, os componentes desta semiose são juntos, como o próprio nome sugere. A estética, é o ato da percepção, o momento em que o intérprete percebe a existência do signo. A ética, é o relacionamento do signo aos valores e crenças já estabelecidos na vida do indivíduo. Por fim, a semiótica (ou lógica): é a utilização dos valores anteriormente definidos involuntariamente e aplicados ao conhecimento.

Considerando estas definições de SANTAELLA (1983), é possível fazer uma visualização e perceber uma certa afinidade entre os três componentes do processo de semiose dos signos, as três formas de qualidade do signo, bem como a definição de dado, informação e conhecimento. A Tabela 1 demonstra visualmente esta comparação e diante desta, pode-se observar que:

a) No “momento” inicial, onde é identificada a qualidade de primeiridade, bem como a característica da semiose denominada estética, mesmo que pela menor fração de tempo conhecida, ou o tempo necessário para a imagem ser detectada pelos olhos do intérprete e levada à mente através de impulsos elétrico, durante este momento, o signo é tido como um dado, ou seja, no primeiro momento de percepção, tudo é dado, sem significado algum. A interpretação será contemplada pelas etapas seguintes.
b) Em um segundo momento, identificado pela qualidade de secundidade, bem como pela característica de semiose denominada ética, o signo adquire sentido interpretativo, através de informações do ambiente contexto ao qual o signo se aplica, bem como através da associação aos valores previamente estabelecidos na vida do indivíduo, mesmo que de forma involuntária. Neste momento, o signo é tido como uma informação, mas ainda não está completo, requerendo uma

próxima etapa.

c) Em um terceiro momento, identificado pela qualidade de terceiridade, bem como pela característica de semiose denominada semiótica, ou aplicação da lógica, o ciclo se completa. Ocorre neste momento a interpretação do signo, utilizando-se para isso os valores associados na etapa anterior, aplicando-os e adquirindo assim o conhecimento. Neste ponto, o signo alcança a sua plenitude, atendendo todas as qualidades e mantendo o processo de semiose.

Qualidades do Signo	Semióse dos Signos	Conceito	Características alinhadas
Primeiridade	Estética	Dado	– Consciência imediata, ato de percepção do signo
Secundidade	Ética	Informação	– o ambiente ao redor do objeto, determinando a que o signo se aplica; – associação aos valores já estabelecidos na vida do indivíduo – adquire sentido interpretativo
Terceiridade	Semiótica (lógica)	Conhecimento	– interpretações possíveis para o signo – utilização dos valores anteriores e aplicados ao conhecimento

Tabela 1: visualização de conceitos alinhados

1.5. PROCESSO COGNITIVO NA VISUALIZAÇÃO DE DADOS

Segundo ESLINGER (2004), a propriedade básica do córtex cerebral é armazenar informação. Este armazenamento ocorre em múltiplas áreas corticais devotadas a diferentes tipos de memória: linguística, motoras, visuo-espaciais, experiências emocionais, entre outros. Aprendizado e memória, não estão portanto limitados a um único sistema neural. Existem múltiplos sistemas de memória, sistemas estes espalhados por todo o cérebro e que podem ser interconectados. O aprendizado não precisa ser reduzido a uma forma linear, mas deve-se explorar esta capacidade cerebral, através das diversas memórias, buscando benefícios deste processo integrado e complexo que é a cognição humana (CRUZ, 2008, p. 25). Este é o conceito de sistema múltiplo de memória.

Geralmente as habilidades de aprendizado e memória em todas as áreas, não estão desenvolvidas por completo ou encontram-se em estágio drasticamente diverso. É comum que cada indivíduo tenha uma determinada habilidade mais desenvolvida em relação a outras. Um aluno pode se destacar em matemática, mas não em português. Conforme o mesmo autor (ESLINGER, 2004), a utilização do conceito de sistema múltiplo de memória no meio

educacional, pode promover um aprendizado eficaz, com entendimento melhorado e maior retenção da informação. Este aprendizado por meio de sistema múltiplo de memória se dá pela utilização de materiais didáticos que utilizam analogias visuais, esquemas visuais que possam mostrar conceitos verbais.

Hoje em dia, existem diversas ferramentas na internet que possibilitam e incentivam a produção e publicação por parte dos usuários de uma forma geral; seja para simplesmente se expressar ou divulgar material de cunho científico. Ferramentas deste tipo, impulsionam de forma considerável, ao que é chamado de sociedade da informação (RIBEIRO, 2009, p.19-20) apud (LEAO, 2003). A informação em rede, então provida pela sociedade da informação, ganha velocidade e fluidez, chegando aos mais diversos locais do mundo em tempo praticamente real, além ainda de se tornar colaborativa. Este excesso de dados e informações, muitas vezes não é interpretado ou compreendido pelo indivíduo. Desta forma, também neste contexto convém a utilização de aprendizado por meio de sistema múltiplo de memória. Conforme RIBEIRO (2009, p.20) “[...] uma das possíveis soluções para lidar com o excesso de conteúdo, está na pesquisa de novas cartografias para interação e representação visual dos dados do ciberespaço”. Ou seja, ideias complexas podem ser mais facilmente compreendidas ao se fazer uso de uma linguagem visual, uma representação metafórica ou não dos dados no ciberespaço. Em um sentido geral pode-se acolher o conceito de que a visualização “[...] é o processo de tornar visível o invisível, ou de falar ao indivíduo 'diretamente no olho'.” RIBEIRO (2009, p.72) apud (QUIGLEY, 2006).

As pessoas não são exatamente iguais, e assim, alguns indivíduos tem maior dificuldade no processo de abstração de uma informação passada verbalmente pelo professor ou mesmo na assimilação de grande quantidade de informação percebida ao acessar um *site* de notícias com diversas ligações, fazendo-o não manter o foco. Isso pode ocorrer por diversos fatores, como por exemplo a falta de experiência com o lúdico nos primeiros anos de vida, entre outros fatores, psicológicos ou fisiológicos.

Conclui-se então, que a utilização de recursos visuais pode promover a interpretação esperada, bem como prover um aprendizado eficaz e não eficiente.

1.6. CONCLUSÃO

Conclui-se por hora, que o signo é uma informação, e que ao ser interpretada, gera novos signos em um processo infinito de criação de signos. São revistos os conceitos de

qualidade do signo, na sua primeiridade (momento da consciência imediata), secundidade (ação e reação), e terceiridade (pensamento em signos, através do qual os seres humanos representam e interpretam todas as coisas). Dando continuidade, são levantados ainda os conceitos de signo-objeto-interpretante como relação triádica do signo, e concluindo que todos estes elementos são incompletos e que co-existindo, buscam se completar um ao outro, formando uma semiose. Finalizando, uma discussão sobre o processo cognitivo de aprendizagem justifica a utilização de recursos de visualização como promotor de uma compreensão não eficiente, mas eficaz no ensino.

2. INTERFACE HOMEM COMPUTADOR

A utilização de recursos visuais pode promover a interpretação esperada. É justamente esta interpretação que toda interface tem por objetivo. De nada adianta uma interface homem computador que não possibilita o entendimento um do outro, muito pelo contrário, ela não existiria. Assim, convém um estudo acerca de interfaces, considerando peculiaridades pertinentes a um signo, então informação aguardando por ser interpretada. Também é oportuno um breve levantamento sobre a artificialidade da comunicação humana, histórico de interfaces, bem como uma definição clara de usabilidade que a interface deve possuir.

2.1. ARTIFICIALIDADE DA COMUNICAÇÃO HUMANA

A comunicação humana é uma forma de ligação entre duas ou mais pessoas, na qual o objetivo é armazenar conhecimentos adquiridos. Esta prática é considerada por FLUSSER (2007, p.93) como inatural, conceituando-a como um processo artificial. Toda a comunicação humana baseia-se em descobertas, instrumentos, símbolos organizados em códigos, o que justifica a teoria da comunicação como uma ciência não natural. A escrita não é natural como a “dança das abelhas”. A habilidade de tocar um instrumento musical, não é natural como uma sequência de notas musicais cantadas pelo uirapuru. A fala é uma maneira “não natural”, onde não se produz sons naturais como o dos pássaros. Ao contrário, é necessário buscar o aprendizado de uma ou mais línguas, aprender e aprimorar pronúncias.

Um bebê aos primeiros meses de vida é estimulado pelos pais a se comunicar, seja por gestos, sons, entre outros. Os pais neste contexto procuram comunicar-se com a criança a fim de transmitir-lhe conhecimentos, estimulando-o a descobrir o mundo. Os primeiros gestos do bebê, os primeiros sons, são conhecimentos adquiridos os quais ele procura imitar, praticando a comunicação e consequentemente a transmissão da informação, que neste caso começa por sentimento de alegria, tristeza, fome, etc.

Obviamente existem também algumas relações naturais entre seres humanos como entre a lactante e um bebê, ou ainda a relação sexual (FLUSSER, 2007, p.89).

SANTAELLA (2008, p.4) cita que tudo depende dos signos de modo absoluto, sendo o signo sinônimo de vida. Este mundo codificado, cheio de signos, torna-se um tipo de “segunda natureza”, um mundo que de certa forma faz o ser humano esquecer-se da “primeira

natureza”(FLUSSER, 2008, p.90), do mundo totalmente natural sem nenhuma artificialidade existente. Tem-se aí uma conclusão que é dada pelo fato de que “[...] a artificialidade da comunicação humana nem sempre é totalmente consciente [...]” (FLUSSER, 2008, p.90). Após aprender um código, o ser humano tende a esquecer sua artificialidade. O simples acenar da cabeça significando “sim”, ou o ato de cantarolar ou assobiar uma melodia conhecida, são exemplos de artificialidade esquecidas inconscientemente, sendo processos “naturais” para o indivíduo.

Um aspecto essencial da comunicação humana é o fato da transmissão de informações adquiridas de geração em geração, o que caracteriza o homem como um animal que encontrou meios para armazenar informações adquiridas (FLUSSER, 2007, p.93). Obviamente o homem buscou meios de melhorar a forma de transmissão da informação, tendo a representação visual como recurso de destaque expressivo(RIBEIRO, 2009). A representação visual, ou *design é* um modificador da linguagem que busca otimizar, tornando a informação acessível e imediata (ROYO, 2008, p.41).

2.2. O QUE É INTERFACE

O ser humano e o computador, são por natureza elementos incompatíveis, pois falam linguagens diferentes. A interface deve existir, seja em um nível mais baixo, próximo à linguagem de máquina como o Assembly[3], até as interfaces metafóricas encontradas nos sistemas atuais. Quando se fala em interface homem computador, deve-se deixar claro o que é interface. A descrição encontrada no Dicionário Online de Português (DICIO, 2011) exprime uma definição satisfatória:

> s.f. Limite comum a dois corpos, sistemas, fases ou espaços, que permite sua ação mútua ou intercomunicação ou trocas entre eles [...]. Informática Meio físico ou lógico através do qual um ou mais dispositivos ou sistemas incompatíveis conseguem comunicar-se entre si.

Alguns autores da área de *design*, partilham desta definição, havendo uma harmonia dos conceitos e objetivos que a interface deve possuir. ROYO (2008, p.41) explica que “[...] O design desenvolve ferramentas conceituais para facilitar o uso da tecnologia”. Este uso nada mais é que a interação entre o homem e o computador, ou seja a interface que ocorre entre os

3 Programa de computador que converte instruções escritas em código simbólico(notação legível por humanos) no equivalente código de máquina (http://www.dicio.com.br/assembler/)

dois elementos incompatíveis. JOHNSON (2001, p.21), também dá sua definição de interface justificando que os seres humanos pensam através de palavras, conceitos, imagens, sons, entre outros, ao passo que o computador simplesmente manipula zeros e uns. Desta forma é necessário que o computador deva representar-se a si mesmo de uma forma que o usuário o compreenda. Esta representação é então provida pela interface. Por fim, RIBEIRO (2009, p. 41) apud HORN (1999) dá sua definição, também em harmonia com os demais: "[...]define o design da informação como a arte e a ciência de preparar a informação de forma a ser usada por seres humanos com eficiência.". Esta última talvez seja a definição mais objetiva e que justifica o *design* da informação como um recurso especial de trabalho que auxilia na concepção de interfaces. Em outras palavras, o *design* de informação também é um *design* de interface, que busca a melhor forma de traduzir a conversa entre homem e computador. Visto desta forma, conclui-se que a interface, bem como o *design* da informação são elementos de extrema importância na interação homem computador.

2.3. HISTÓRIA DO *DESIGN* DA INFORMAÇÃO

Antes de discutir os conceitos de interface e o *design* em si, convém integrar a esta dissertação, um pouco da história do *design* da informação, descrevendo eventos e fatores marcantes que delinearam o caminho das interfaces atuais.

O primeiro evento, é citado por RIBEIRO (2009, p. 37) apud (JOHNSON, 2008) intitulado "o mapa fantasma", o qual pode ter influenciado decisivamente o nascimento do *design* da informação.

No ano de 1854, uma epidemia de cólera consternou a cidade de Londres, tendo como resultado mais de 500 vítimas fatais em um período de 10 dias. O bairro denominado Soho era populado por uma quantidade excessiva de moradores, além de condições sanitárias e água potável inadequadas. O principal foco posteriormente descoberto, era uma bomba d'agua localizada na Broad Street. Dentre os envolvidos na investigação da causa, o Dr. John Snow defendia a ideia do contágio pela água, teoria até então não sustentada pela classe médica da época, a qual conservava a ideia de contágio pelo ar, teoria respeitada desde séculos anteriores.

Como suas opiniões não surtiam efeito, Dr. Snow utilizou um recurso bastante esclarecedor e que posteriormente (não obteve aceitação imediata) se tornaria muito significativo para a compreensão daquele fenômeno. Com a ajuda de pessoas daquela comunidade, contabilizou

as vítimas; utilizando-se de um mapa visual simplificado do bairro (Figura 3)[4], onde foram retirados os excessos de detalhes, representou cada morte com um grosso traço preto, objetivando demonstrar padrões ao redor das bombas d'agua. O mapa tinha um grande impacto visual, sendo possível perceber sem maiores esclarecimentos, a grande concentração de mortes ao redor da bomba d'agua da Broad Street, justificando assim a sua teoria.

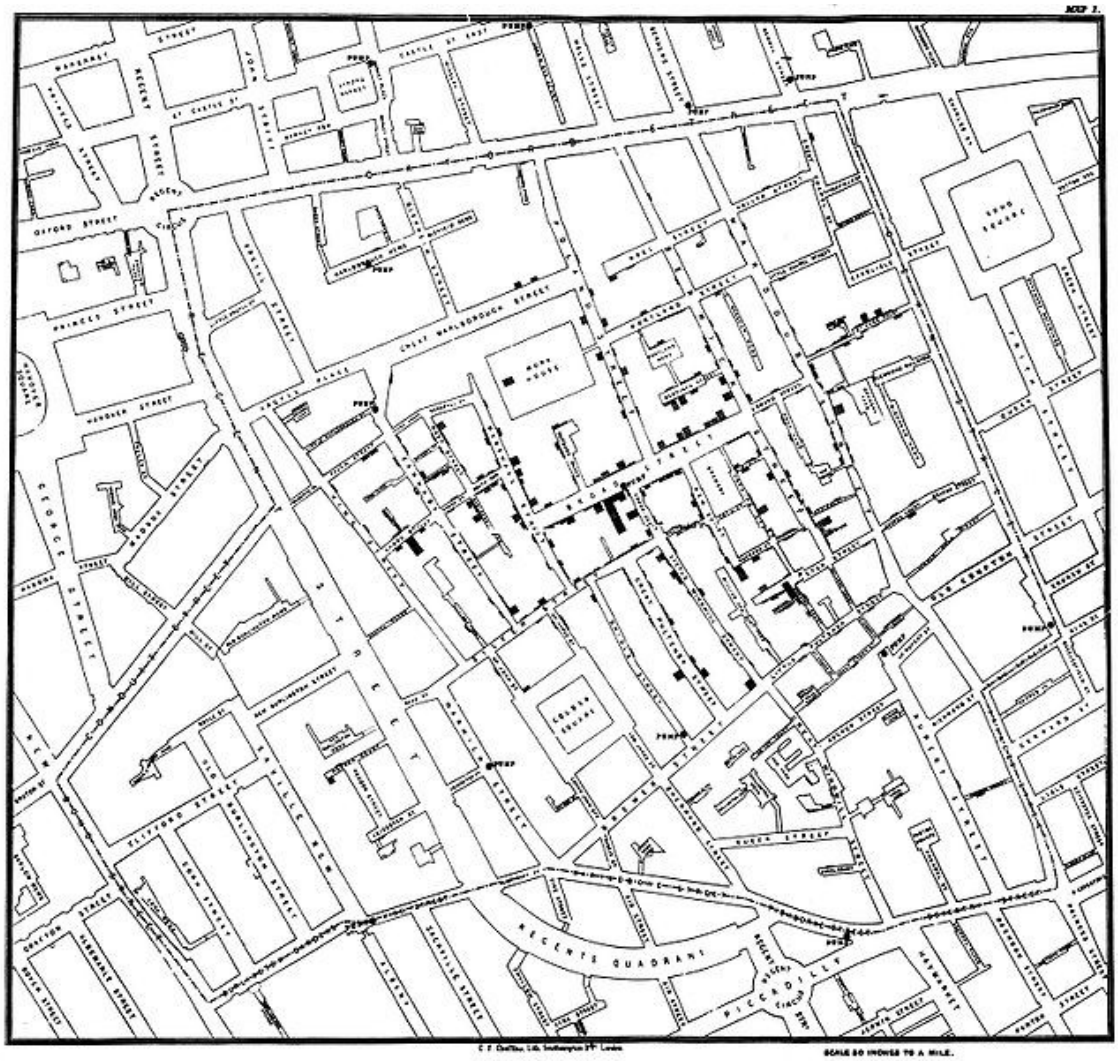

FIGURA 3: Mapa elaborado pelo Dr. John Snow, demonstrando as mortes registradas no bairro Soho em Londres

Conforme RIBEIRO (2009, p.40), o que fortaleceu esse modelo de visualização foi a "[...] ciência por trás da representação, ou seja, a intenção explícita de amplificar a capacidade de cognição do observador". Dr. Snow utilizou o que posteriormente viria a ser chamado sistema múltiplo de memória, então conceituado no capítulo sobre os signos e o processo cognitivo. Não eram necessários maiores esclarecimentos ao visualizar o mapa. Levando em

4 Figura disponível em http://johnsnow.matrix.msu.edu/images/online_companion/chapter_images/fig12-5.jpg

consideração as informações de morte contabilizadas, bem como as informações de tempo de locomoção das demais vítimas residentes mais longe da bomba contaminada, o mapa foi um recurso crucial para justificar o pensamento proposto da forma de contaminação.

Outro acontecimento interessante descrito em ROYO (2008, p.51), coincidentemente também ocorre na cidade de Londres. Trata-se da conclusão do *design* do metrô daquela cidade em 1933, no qual um desenhista chamado Harry C. Beck norteou os traçados dos planos de metrô do resto do mundo a partir deste evento. Beck propôs um *design* (Figura 4)[5] que substituía a geografia fiel da cidade, por uma interpretação diagramática, utilizando escalas diferentes para representar zonas centrais de maior complexidade, utilizando também cores distintas para cada linha. Este conjunto de soluções, facilitou a visualização do ambiente do metrô que antes tinha em seu mapa a exemplo da versão de 1927 (Figura 5)[6], as características geográficas da cidade. Informação talvez desnecessária a quem procura saber apenas as conexões com outras linhas, as estações existentes, bem como a relação de localização entre uma estação e outra. Como é possível notar, já estava sendo utilizado uma forma de representação visual. Porém diante das circunstâncias, considerando as informações pertinentes àquela representação e levando em consideração o tipo real de informação que deveria ser transmitida, Becker fez uma trabalho de *design* de informação, tornando a informação bem mais imediata aos passageiros do metrô.

FIGURA 4: mapa do metrô de Londres em 1933 (desenhado por Harry C. Becker)

5 Figura disponível em http://www.flickr.com/photos/36844288@N00/sets/72157625700026208/detail
6 Figura disponível em http://www.flickr.com/photos/36844288@N00/sets/72157625700026208/detail

FIGURA 5: mapa do metrô de Londres em 1927

Um fato interessante e também tema central de JOHNSON (2001, p.11-15), é a fusão entre tecnologia e arte, resultando no chamado *design* de interface, o que apesar de não ser uma novidade, alguns assim o consideram. Tem-se do lado da tecnologia, o técnico, onde o engenheiro busca por exemplo o algoritmo ideal para localizar determinada informação. Em contraposição, tem-se o lado cultural, onde o artista, tem o intuito de dar forma visual à informação obtida. JOHNSON (2001) justifica que tecnologia e arte sempre caminharam juntas desde sempre. Vários exemplos de artistas engenheiros são citados, dentre os quais está Simônides, um poeta grego nascido seis séculos antes de Cristo.

Simônides era famoso por sua capacidade de construir “palácios de memória”. Sua estratégia “[...] baseava-se numa peculiaridade da mente humana: nossa memória visual é muito mais duradoura que a memória textual.”(JOHNSON, 2001, p.19), o que justifica o fato de que é mais fácil esquecer um nome do que um rosto.

> Imaginando suas histórias como edificações, Simônides aplicou esse potencial à mnemônica espacial. Cada aposento desencadeava mais um episódio da história, mais uma reviravolta no argumento. Era capaz de mobiliar as salas para acrescentar mais detalhes, se precisasse de uma provisão de adjetivos ou de ornamentação estilística. O ato propriamente dito de contar a história era uma mera questão de perambular pelos aposentos do

palácio. (JOHNSON, 2001, p.19)

Assim como Simónides, os responsáveis pela edificação de catedrais em um tempo em que a alfabetização em massa era inimaginável, projetaram e levantaram edificações que serviam como “[...] uma espécie de texto popular feito de vitrais e gárgulas. Esse sistema de signos funcionava em diferentes escalas. Podia-se, é claro, ler a história de Cristo nas pedras cinzeladas em impossível detalhe [...]” JOHNSON (2001, p.42). Verdadeiras “bíblias de pedra”, são belas edificações que exemplificam a fusão entre obras de arte e engenharia, fusão esta que viria a ser consumada a partir de posteriores eventos na década de 60 e que deram um impulso definitivo ao conceito de *design* e interface.

Em 1963 Ivan Sutherland utilizando-se de um terminal TX-2[7], apresentou o sistema Sketchpad (Figura 6). Este sistema considerado precursor de aplicações gráficas de renome atuais, procurava resolver o problema de como fazer desenhos na tela do computador, fazer algo além da exibição de caracteres. O Sketchpad permitiu que o computador fosse utilizado como instrumento de expressão artística. Ele utilizava uma caneta de luz para guiar a criação objetos na tela, bem como manipulá-los. Porém ainda não atendia a questão de transformar a informação digital em uma linguagem visual (JOHNSON, 2001, p. 20). É justamente nesta época que Doug Engelbart, um cientista do Stanford Research Institute (SRI), dá continuidade a história.

FIGURA 6: Ivan Sutherland demonstrando o Sketchpad em um console do TX-2

7 TX-2 é um terminal de computador da década de 50 o qual funcionava baseado em transístores.

Engelbart inventou o conceito de espaço informação (JOHNSON, 2001, p.25) o qual envolvia vários componentes chaves dos quais está a ideia do mapeamento de bits(tecnicamente melhorada nos anos posteriores) e a aliança de cartografia e código binário.

> [...] Cada pixel na tela do computador era referido a um pequeno naco da memória do computador: numa tela simples, preto-e-branco, esse naco seria um único bit, um O ou um 1; se o pixel fosse iluminado, o valor do bit seria 1; se ficasse escuro, seu valor era 0. Em outras palavras, o computador imaginava a tela como uma grade de pixels, um espaço bidimensional. Os dados, pela primeira vez, teriam uma localização física — ou melhor, uma localização física e uma localização virtual: os elétrons em vaivém pelo processador e sua imagem espelhada na tela. (JOHNSON, 2001, p.25)

Contudo, o espaço informação, também conhecido como infosfera (JOHNSON, 2001), não era algo palpável. Mesmo caracterizada a localização de um dado virtual em um ambiente bidimensional, fácil de se ver e compreender, não era possível ao usuário tocá-lo. Era necessário um recurso adicional para facilitar a interação entre o homem e o computador. Para facilitar esta interação entre o usuário e o espaço informação na máquina, possibilitando a manipulação e seleção de objetos na tela, Engelbart criou um dispositivo chamado *mouse* (Figura 7)[8]. O dispositivo permitia repetir na tela os movimentos exatos realizados com o mesmo em uma superfície plana, tal como hoje ele funciona. Desta forma o usuário podia se mover na tela entre uma janela e outra, selecionar objetos, manipulá-los, enfim. Apesar de criados em 1963, a primeira demonstração pública do sistema operacional com janelas veio a ocorrer em 1968 (ROYO, 2008, p.61).

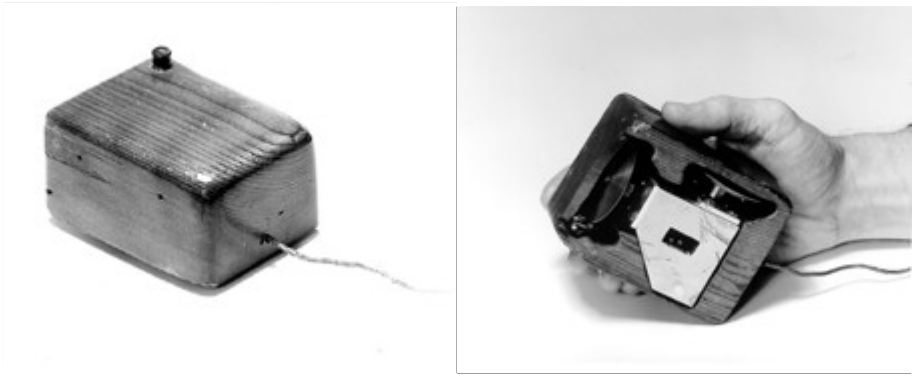

FIGURA 7: mouse projetado por Doug Engelbart em 1963

A invenção do conceito de espaço informação e junto com ele o invento do *mouse*(como dispositivo de manipulação), inferiu o conceito da manipulação direta. O próprio

8 Figura disponível em http://sloan.stanford.edu/MouseSite/Archive/patent/Mouse.html

usuário parecia fazer ele mesmo determinada tarefa ao invés de “dizer” ao computador para executá-la. ROYO (2008, p.61) apud JOHNSON (2001). A manipulação direta tinha uma qualidade de certa forma contraditória pois, uma nova camada havia sido colocada entre o usuário e a máquina. O fato da ilusão do tátil imediato, fazia parecer que a informação estivesse mais próxima. Seria uma falsa impressão de objetos palpáveis, onde o usuário utilizaria as próprias mãos para “pegar” (selecionar) um objeto. Ainda assim, a partir da manipulação direta juntamente com outras pesquisas realizadas por Engelbart, o conceito de interface viria a ser instituído.

O invento de Engelbart, assim como qualquer outro, era inicialmente limitado e com possíveis melhoradas a serem realizadas no decorrer de processos de aperfeiçoamento. O sistema de Engelbart possuía janelas, porém estas não eram totalmente funcionais pelo fato de não sobreporem-se, e como as telas da época tinha uma área de exibição extremamente limitada, não era funcional o uso de muitas janelas. Vários cientistas do Paio Alto Research Center Xerox (Xerox PARC), veteranos do SRI, utilizando-se de conceitos e ideias de Engelbart, trabalhavam na melhoria das janelas. Dentre estes, um pesquisador chamado Alan Kay concebeu a tela do computador como um *desktop*, uma mesa de trabalho, e cada projeto ou parte dele, ficava como papéis sobre a mesma. Esta metáfora era simplesmente para explicar o motivo de algumas janelas ficarem bloqueadas por outras. Como no ambiente real, quando o papel que se está utilizando no momento fica por cima, assim as janelas eram organizadas, onde a janela ativa sobrepunha as demais. Apesar das janelas de Kay não terem nenhuma metáfora visual, o que as tornavam pouco convincentes como a ideia de uma escrivaninha, surge a partir daí a metáfora de *desktop* até então utilizada em peso (JOHNSON, 2001, p.45-46). O *design* de interface busca trabalhar em dois sentidos: a simulação do mundo real bem como a metáfora. Ser capaz de simular objetos e ações do mundo real e é claro projetar coisas sem qualquer equivalência no mesmo.

Engelbart, Sutherland e Kay atuaram como um tripé que sustenta a interação homem máquina atual. Engelbart e Sutherland dotaram o computador digital de espaço. Kay adicionou a profundidade através de suas janelas sobrepostas.

> [...] Podíamos entrar e sair da paisagem da tela, puxar coisas na nossa direção ou afastá-las. A revolução do mapeamento de bits nos dera uma linguagem visual para a informação, mas as pilhas de papel de Kay sugeriam uma abordagem mais tridimensional, um espaço-tela em que era possível entrar. Toda a idéia do computador como um ambiente, um mundo virtual, tem origem nessa inovação aparentemente modesta, embora fossem ser necessários muitos anos para que esse legado se tornasse visível. (JOHNSON, 2001, p.46)

Nesta mesma época, mais especificamente no ano de 1974, o Departamento de Transporte dos EUA encomendou ao American Institute of Graphic Arts (AIGA) a organização do sistema de símbolos destinados aos usuários de transporte (Figura 8)[9]. Tal sistema composto por uma série de trinta e quatro símbolos harmoniosos, com linhas, figuras, volumes e formas que simplificavam as mensagens básicas nos meios de transporte, nacionais e internacionais. Este evento teve grande importância por ser um passo decisivo na unificação global de significados na comunicação gráfica, transcendendo barreiras culturais e idiomáticas. (ROYO, 2008, p.53) apud (MEGGS, 1983, p.489). Uma imagem simplificava expressões como “vire a esquerda” ou “é proibido fumar”, independente do idioma conhecido pelo usuário. Uma série de ícones nos novos sistemas de interface homem computador que viriam a surgir e que se tem até hoje, foram herdados destes sinais viários. Em um navegador de internet, o ícone com uma seta para a esquerda indica voltar. Este sistema criado pelo AIGA não era o primeiro.

Conforme ROYO (2008, p. 54-55), o pioneiro na realização de sistemas de signos foi Otto Neurath que desenvolveu em 1920 um sistema chamado Isotype. O objetivo deste sistema era criar objetos que permitisse o maior acerto possível na interpretação do signo, considerando os conceitos já existentes no modelo mental, isto é , experiência de vida dos mais variados tipos de indivíduos. Não é possível que todas as pessoas sejam iguais, mas é certo que a grande maioria das pessoas conhece por exemplo a imagem de um telefone analógico dos anos 80 e ao ver um símbolo com tal dispositivo, interpretará que aquele local possui um “telefone”. ROYO (2008, p.56) *apud (*AICHER e KRAMPEN, 1979, p.99) explica que um dos assistentes de Neurath era Rudolf Modley. Em 1964 Modley criou uma empresa que buscava a coordenação de uma comunicação mundial não alfabética. Um dos frutos deste trabalho foi a criação do glyph, definido pelo próprio Modley como um signo visual convencional (assimilado pelos próprios receptores baseando-se no modelo mental existente). Signo este não associado a nenhum sistema fonológico e conhecido internacionalmente.

9 Figura disponível em http://pt.scribd.com/doc/57395573/Otto-Neurath-e-o-Legado-do-ISOTYPE

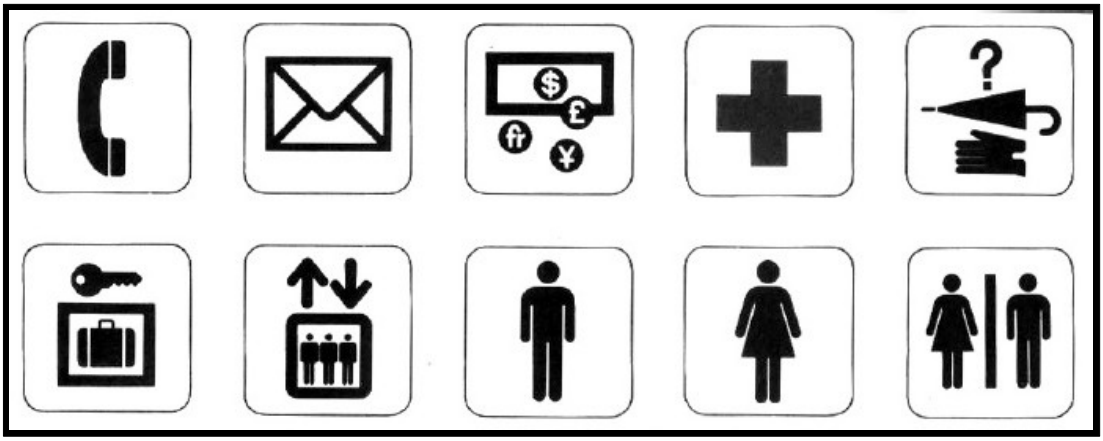

FIGURA 8: exemplo de pictogramas do Departamento de Transporte dos EUA

Observa-se assim que o glyph bem como o sistema de sinais viários, tinham um objetivo em comum: utilizar-se de uma figura para trazer um signo à mente das pessoas, facilitando o entendimento de uma informação independente da sua cultura, conceitos ou língua.

Nos anos seguintes, o Xerox PARC criou e aprimorou o seu primeiro protótipo de interface homem máquina utilizando-se de ícones característicos dos sinais viários então recém-criados, bem como da metáfora da escrivaninha. A utilização desta metáfora, se dava pela ideia de utilizar as aptidões que o usuário já possuía no mundo real, trazendo-as para o mundo virtual. A utilização de coisas do mundo real, como os sinais viários, possibilitaria ao usuário se situar. Este sistema, denominado Smalltalk (Figura 9)[10] foi integrado ao pacote de sistema computacional chamado Xerox Alto, então substituído em 1981 pelo seu sucessor, o Xerox Star(Figura 10)[11], então o primeiro computador comercial com mouse. Porém não foi o Smalltalk nem o Xerox Star que tornaram o *desktop* popular. O responsável por essa difusão, foi Steve Jobs após conhecer tal sistema em uma visita às dependências do Xerox PARC. Jobs e sua equipe recriaram essa Interface Gráfica do Usuário (GUI) para o LISA(Figura 11)[12], então primeiro produto da Apple. Um diferencial interessante do LISA em relação aos produtos Xerox, era a ideia de que um ícone poderia representar todos os arquivos no sistema de arquivo. Seria o início da hierarquia de diretórios ou pastas como é conhecida hoje. Ao clicar em um ícone de diretório, uma nova janela se abriria exibindo demais arquivos dentro do novo nível (REIMER, 2005). O LISA era um equipamento muito caro, sendo então um dos

10 Figura disponível em http://arstechnica.com/old/content/2005/05/gui.ars/3
11 Figura disponível em http://arstechnica.com/old/content/2005/05/gui.ars/3
12 Figura disponível em http://arstechnica.com/old/content/2005/05/gui.ars/4

motivos relevantes que deram origem ao Macintosh(Figura 12)[13], lançado em 1984 e verdadeiro responsável pela popularização do *desktop* (JOHNSON, 2001, p. 22 e 47).

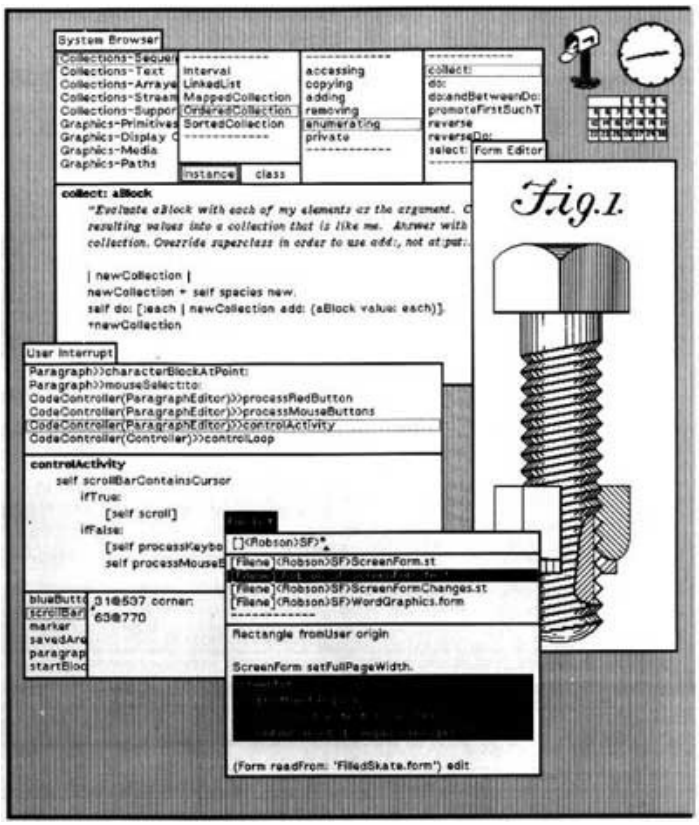

FIGURA 9: sistema Smalltalk - a primeira interface com a metáfora *desktop*

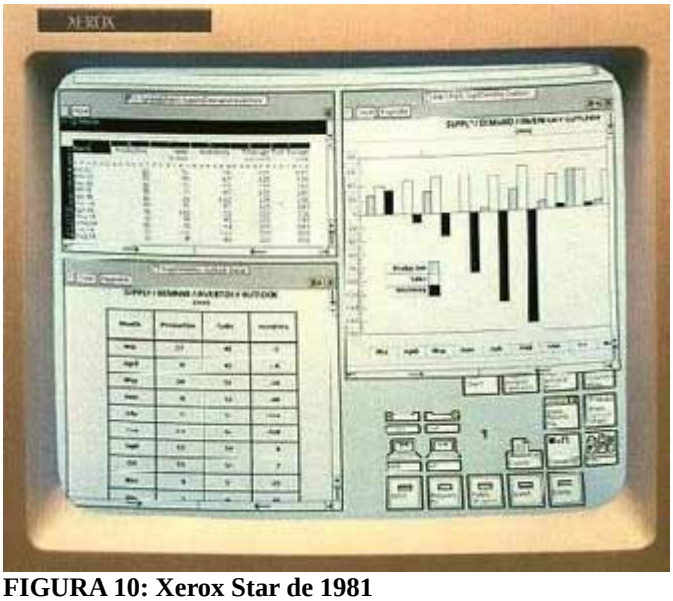

FIGURA 10: Xerox Star de 1981

13 Figura disponível em http://arstechnica.com/old/content/2005/05/gui.ars/4

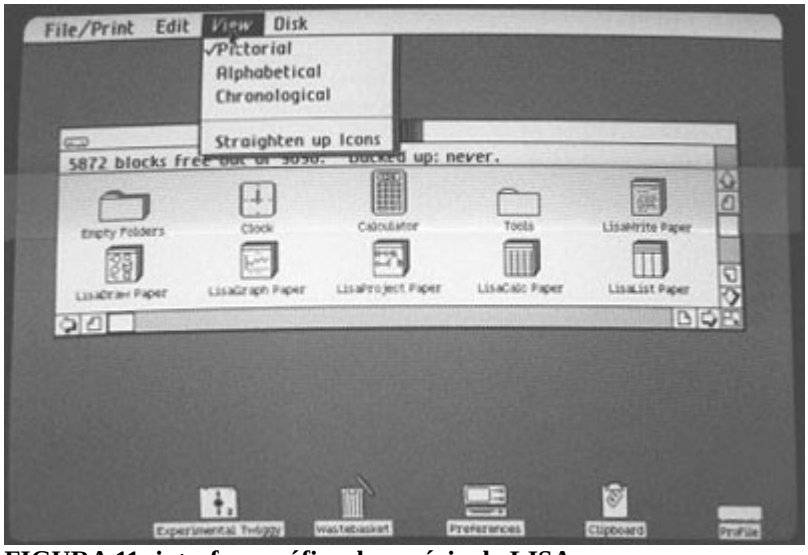

FIGURA 11: interface gráfica de usuário do LISA

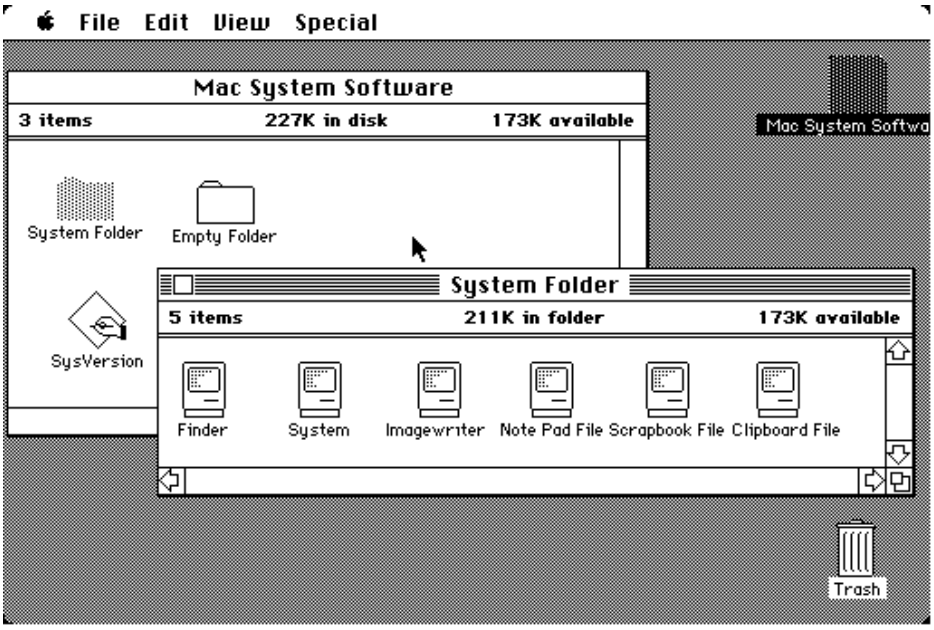

FIGURA 12: interface gráfica de usuário do Macintosh

A concepção e popularização da GUI mudou drasticamente a forma de interação entre homem e computador. A GUI como um resultado dos inventos de Engelbart, Sutherland e Kay, pode ser considerado um dos eventos mais importantes do século XX, pois alterou drasticamente a concepção de espaço de dados e ambientes do mundo real. As pessoas de uma forma geral, vivem em torno do *desktop* do computador, em torno de eventos produzidos no ambiente virtual, local este ainda fora da percepção humana.

2.4. MEMÓRIA ESPACIAL

O conceito de *desktop* foi adotado largamente por sistemas desde os mais antigos como o Macintosh até os sistemas atuais. Um fator interessante citado por JOHNSON (2001, p. 68-69) diz respeito à memória espacial. A memória espacial é a capacidade do ser humano em memorizar objetos através de coordenadas espaciais visualmente conhecidas. A princípio o uso de janelas dá a falsa impressão de utilização da memória espacial. Isto se dá pelo fato de que as janelas são recursos maleáveis, podendo mudar de tamanho e localização na tela, além ainda da possibilidade de reordenação de arquivos por uma determinada ordem, seja por data, lexicograficamente, tamanho de arquivo, entre outros. A dimensão espacial neste caso é uma ilusão, onde o usuário finge lembrar para ele mesmo onde colocou um arquivo, mas o que realmente vem à mente, é o nome do diretório que contém o arquivo em questão. Para se ter uma ideia do quão pouco este recurso é utilizado faz-se necessário a utilização de uma interface espacial como o TDFSB (TDFSB, 2011), um *browser* tridimensional de sistemas de arquivos para GNU/Linux. Este *software* produz o ambiente do sistema de arquivos como um plano tridimensional (Figura 13), onde é possível flutuar entre os arquivos, entrar em diretórios, abrindo assim um novo plano com os arquivos ali pertencentes. Também é possível ver as figuras armazenadas, arquivos de áudio, além ainda do fato de que o tamanho do arquivo também é representado através de tamanho diferenciado de objetos no plano. Ao entrar no ambiente, o usuário reconhece que um determinado arquivo está no canto direito, ao lado de um arquivo de vídeo com tamanho X. O usuário tem uma noção espacial da localização do arquivo, como se estivesse andando em uma cidade, a procura de um imóvel.

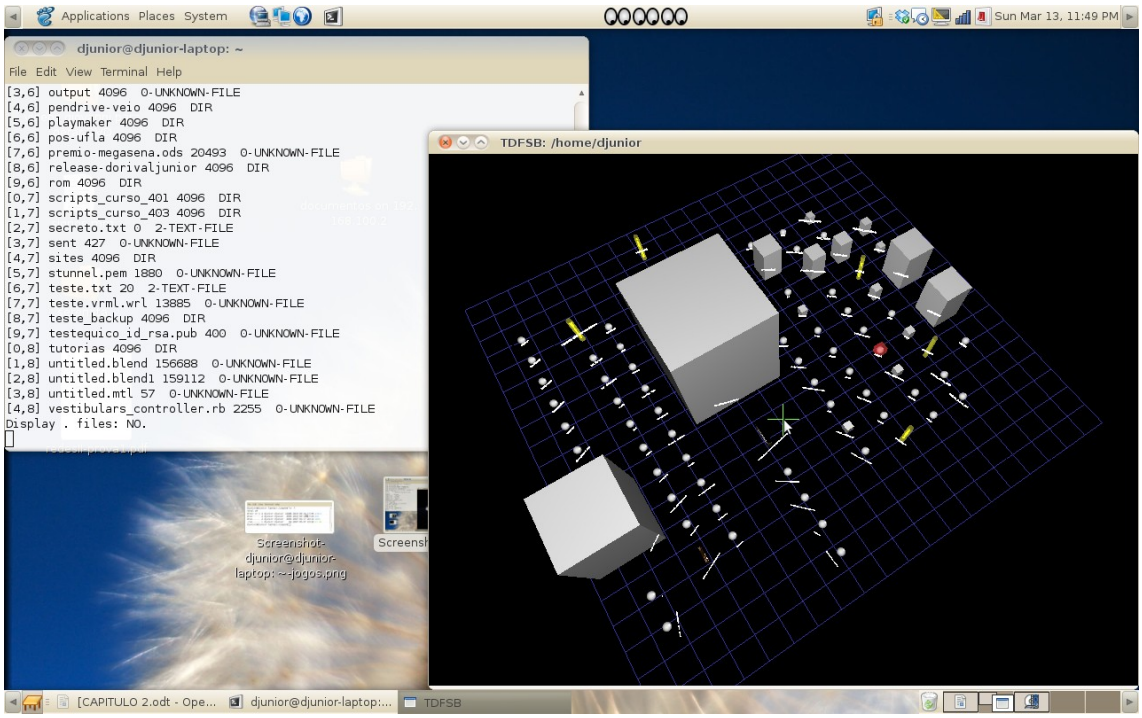

FIGURA 13: Interface do TDFSB exibindo uma visão geral de um diretório

Afim de se fazer uma comparação mais afinada, convém uma visualização de um mesmo ambiente, porém utilizando três interfaces diferentes. A primeira interface é a mais tradicional, sendo parte integrante da metáfora de *desktop*. A visualização realizada através do Nautilus(Figura 14), um *browser* tradicional de navegação bidimensional encontrado em sistemas GNU/Linux, exibe o conteúdo do diretório então denominado "/home/djunior/jogos". A segunda forma de visualização é interface conhecida como linha de comando(Figura 15), através de um comando específico para listar os arquivos ali existentes. Por fim, é exemplificado uma visualização utilizando memoria espacial (Figura 16).

Por estas comparações, fica claro a praticidade em encontrar um arquivo utilizando memória espacial. Em um ambiente com quantidade excessiva de informações, é um recurso muito eficiente e ainda pouco explorado.

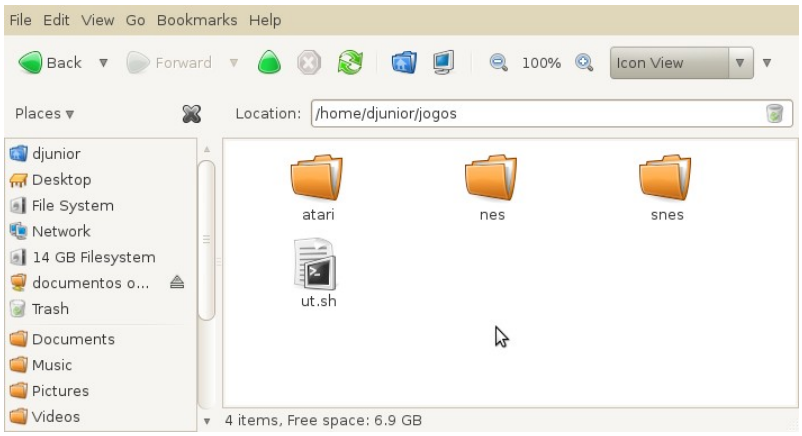

FIGURA 14: visualização bidimensional tradicional

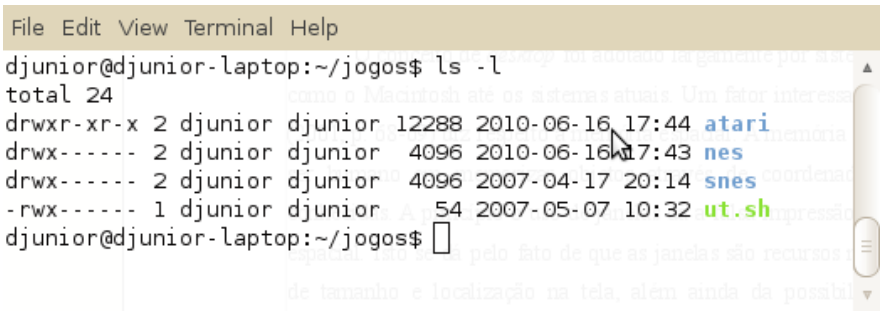

FIGURA 15: visualização através de linha de comando

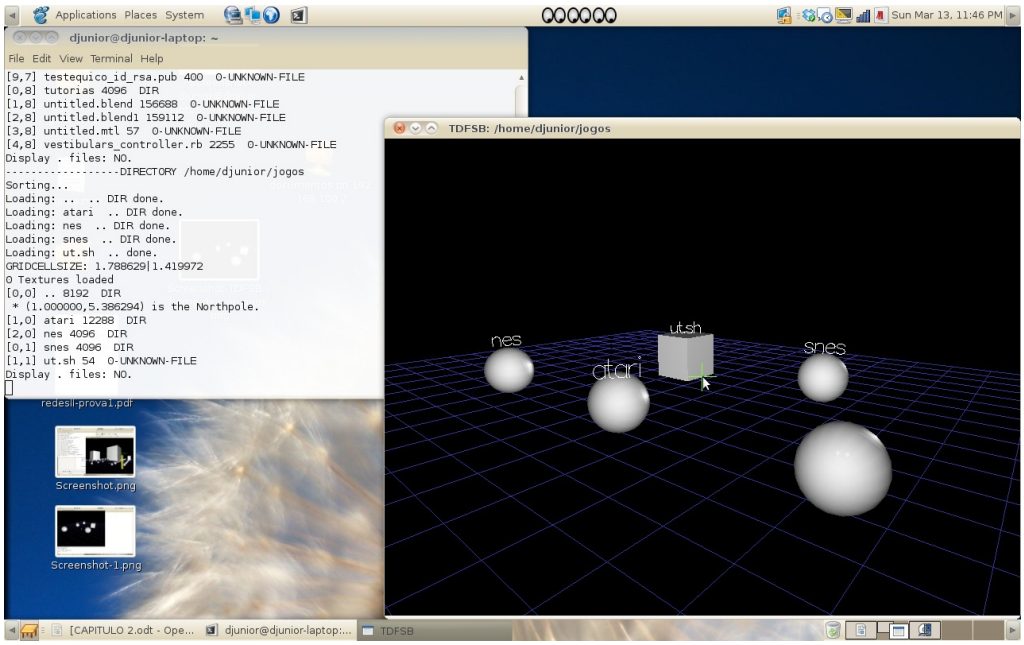

FIGURA 16: visualização que possibilita o uso de memória espacial

2.5. O CIBERESPAÇO E SUAS CARACTERÍSTICAS

Para se chegar à definição de ciberespaço, ROYO (2008, p. 23) apud ECHEVERRIA(1999, p. 29, p. 41) faz três classificações referentes ao usuário e o meio, as quais possibilitam uma melhor compreensão da palavra. Inicialmente tem-se o primeiro meio, que é o ambiente natural, compreendendo o corpo humano em si. Corpo este que é limitado mas que utiliza-se de cinco sentidos para ampliar o seu campo de ação. É o nível onde o sujeito se adapta ao meio. Em seguida, caracteriza-se o segundo meio, que referencia o ambiente social e cultural. Ele envolve a escrita, a família, grupos ou comunidades, costumes, ferramentas, enfim, recursos que possibilitem uma melhora na qualidade de vida e evolução sob algum aspecto. Trata-se de uma adaptação do meio ao sujeito. Por fim tem-se o terceiro meio que nas palavras de ROYO (2008, p.25) é definido da seguinte forma: "[...] é um espaço gerado pelas novas tecnologias, com a organização de uma grande cidade onde a humanidade vai se desenvolver.". Este terceiro meio é o ciberespaço. Um ambiente novo, não contemplado no primeiro e segundo meios. Talvez uma espécie de extensão do segundo meio, uma nova forma de melhora na qualidade de vida.

Uma segunda definição para o termo ciberespaço é encontrada da seguinte forma:

> Eu defino o ciberespaço como o espaço de comunicação aberto pela interconexão mundial dos computadores e das memórias dos computadores. Essa definição inclui o conjunto de sistemas de comunicação eletrônicos [...] (LEVY, 2000, p. 92)

Percebe-se que ambas as definições estão em harmonia, e de certa forma, também alinham-se ao pensamento de Willian Gibson, ao inventar e utilizar esta palavra em um romance de ficção chamado *Neuromante*, de 1984. No livro, o termo ciberespaço refere-se ao ambiente das redes digitais (LEVY, 2000, p.92).

Desta forma, pode-se considerar que o ciberespaço envolve qualquer ambiente computacional, desde o *desktop* dos computadores pessoais até sistemas de comunicação cabeada, roteadores, *firewall*, fibras, ondas de rádio, enfim todos os aparatos e recursos tecnológicos que mantém a interligação da rede mundial de computadores.

O autor (ROYO, 2008, p. 27-32) da primeira definição elucidada, define características (Figura 17) para o ciberespaço as quais são: características intrínsecas, espaciais e temporais.

As características intrínsecas, são relativas à própria estrutura e natureza do

ciberespaço. A artificialidade em relação à naturalidade é uma delas, pois o ciberespaço é totalmente artificial. São necessárias muitas máquinas para que ele exista, ao passo que na naturalidade, o espaço é por si próprio. O usuário pode experimentá-lo sem nenhum intermediário. Pode-se considerar ainda uma característica intrínseca, a representação, a simulação. O ciberespaço é uma construção feita à imagem e semelhança do mundo físico.

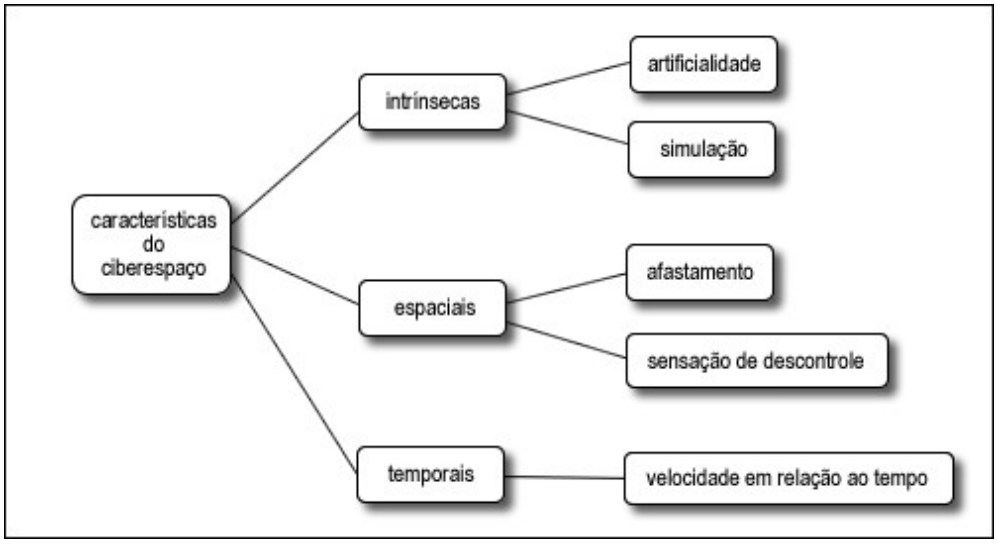

FIGURA 17: características do ciberespaço

Como característica espacial, tem-se o aumento da distância, o afastamento. No contexto da naturalidade, ou seja, no espaço do primeiro e segundo meios, o usuário mantém uma proximidade, uma distância curta ou contato com o objeto. Para sentir gosto de uma fruta, a distância é zero. Para escutar uma música a distância existe, variando de centímetros a vários metros. Em se falando do ciberespaço, ocorre um afastamento, a relação com os objetos é mais distante. O usuário interage com computadores que estão longe, em local não sabido como um portal de internet qualquer. Mesmo que as informações estejam na tela em frente ao usuário, acontece um uma sensação de perda de controle. Em suma, não existe uma localização física.

Características temporais englobam o incremento da velocidade em relação ao espaço. Esta característica merece destaque no contexto de *design* da informação pois, é necessário uma adequação contínua ao ritmo de produção e processamento de informações. Deve-se levar em consideração o usuário e sua velocidade humana de leitura e compreensão, adequando o ritmo ao usuário.

2.6. O PROCESSO DE CRIAÇÃO DE VISUALIZAÇÕES

Todo o ambiente do ciberespaço, as imagens, simulações, são visualizações resultantes de cálculos numéricos. Qualquer imagem produzida pelo computador é resultante de um cálculo. Mesmo o tráfego de dados que viaja pelo emaranhado de conexões da internet é resultado e produto de um cálculo numérico. Do ponto de vista do usuário, é um resultado quando se obtém uma resposta e produto quando se envia uma solicitação ou resposta para um terceiro. Mas olhando de uma ótica um pouco mais distante, existe o processo que envolve a criação da visualização já considerando que o computador faça bem a sua parte de cálculos.

RIBEIRO(2009, p. 79) cita um trabalho realizado por FREITAS et al. (2001), o qual trata-se de uma revisão das propostas de classificação de visualizações realizadas por autores especialistas em interface homem computador. Tal estudo promoveu a identificação de três necessidades inerentes ao processo de criação de visualizações e que são: definição de uma representação visual, escolha dos mecanismos de interação necessários para manipular os dados, e implementação dos algoritmos. Tais necessidades devidamente contempladas, permitirão uma visualização estruturada, rica e objetiva em seus signos.

> Os artistas da visualização de dados transformam o caos informacional de pacotes de dados que se locomovem através da rede em formas claras e ordenadas. (...) A visualização de dados nos permite enxergar padrões e estruturas por detrás do vasto e aparente fortuito conjunto de dados. (...) Os dados quantitativos são reduzidos a seus padrões e estruturas, os quais, a seguir, explodem em inúmeras imagens visuais ricas e concretas. (RIBEIRO, 2009, p. 72) apud (MANOVICH, 2004, p. 157)

Esta definição de MANOVICH (2004, p. 157) expressa a excelência quando atendidas as três necessidades identificadas (Figura 18) ao processo de visualização. A definição da representação visual é a arte em si. É o como fazer um determinado signo acontecer quando o usuário se depara com a informação. A escolha do mecanismo de manipulação de dados é a arte e a engenharia em conjunto. Não é possível fazer a escolha da melhor solução técnica sem conhecer as possibilidades de entrada e saída de informações para o usuário. A simples disposição de uma tela para busca de conteúdo a um banco de dados envolve ambos. Por fim a implementação do algoritmo que é puramente engenharia, envolvendo lógica de programação em si. A visualização de dados é uma interação metafórica. Sendo assim, cabe ao artista engenheiro, prover a estética ao processo que media entre usuário e máquina.

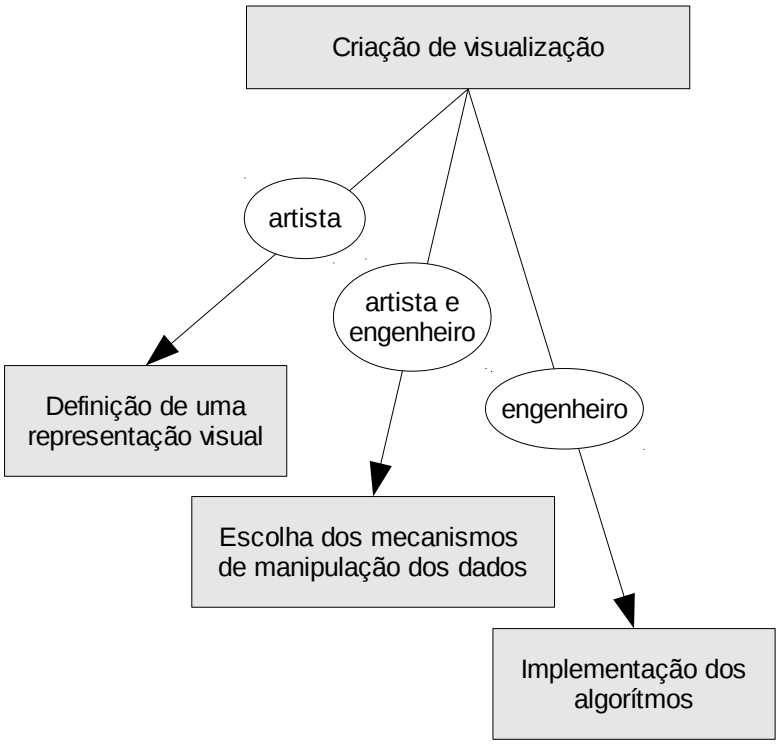

FIGURA 18: necessidades inerentes ao processo de criação de visualizações e característica do responsável por sua execução

2.7. USABILIDADE DE INTERFACE

A interface, é indiretamente uma melhoria da forma de comunicação artificial das pessoas. Considerando-se como exemplo as redes sociais, o computador é a ferramenta de comunicação com o mundo exterior e a interface é o recurso para que o usuário possa aumentar a sua forma de comunicação com mais pessoas. Em qualquer tipo de interface que envolva eletrônica e pessoa, desde computadores em si, a qualquer aparelho eletrônico, um fator interessante a considerar é a usabilidade.

Usabilidade é facilidade com a qual um equipamento ou programa pode ser usado (DICIO, 2011). Esta definição de dicionário expressa corretamente o significado da palavra, porém vários fatores implicam para que a facilidade exista. Afim de colocar esta definição em alinhamento com uma definição mais técnica, convém verificar uma definição no contexto de interface, então proposta pela International Organization for Standardization (ISO)[14]. A norma ABNT NBR ISO/IEC 9126 (ABNT, 2003) trata sobre modelo de qualidade de

14 Um dos membros fundadores da ISO é a Associação Brasileira de Normas Técnicas (ABNT), único Foro nacional de normalização (ABNT, 2011). Logo a ABNT é a representante oficial da ISO no Brasil.

software, o que envolve também a questão de interfaces. Segundo a ABNT (2003, p.9), usabilidade é a “Capacidade do produto de *software* de ser compreendido, aprendido, operado e atraente ao usuário […] Alguns aspectos como funcionalidade, confiabilidade e eficiência também afetarão a usabilidade [...]”.

Esta definição enfatiza fortemente a importância dos signos para se ter usabilidade: compreensão e aprendizado são os objetivos do uso de signos. Experiências prévias são transformadas em conhecimento e este gera novos signos. Obviamente a questão do ser atraente é também fator crucial para deleite do usuário e também diz respeito a qualidade de primeiridade do signo. Por fim, espera-se que a interface seja funcional, ou seja, sem complicações, apresentar resultados confiáveis e ser eficiente no seu objetivo de prover o conhecimento.

2.8. CONCLUSÃO

Neste capítulo, foram levantados aspectos importantes sobre a comunicação humana, além de fazer um breve histórico sobre interfaces, elegendo elementos chave que norteiam todo tipo de interface existente atualmente. Também foi abordado o conceito de usabilidade, fator intrínseco quando se fala em interface.

3. INTERFACES PARA ENSINO DE *FIREWALL*

Considerando a abordagem sobre signos e interface realizadas até então, é momento de introduzir especificamente sobre interface para ensino de *firewall*. Espera-se que esta seja funcional e sem complicações, ou seja, que a usabilidade esteja presente, bem como a estética, ética e lógica de cada elemento envolvido, afim de prover o conhecimento necessário ao perceber o funcionamento do *firewall*. Também é de suma importância realizar uma fundamentação da importância do *firewall* na internet como um todo, entender o seu funcionamento básico, conhecer o ambiente ao qual ele se relaciona, realizar uma breve análise de interfaces existentes. Por fim estabelecer algumas qualidades essenciais para que a interface seja eficaz no ensino.

3.1. A IMPORTÂNCIA DE UM *FIREWALL* COMO AGENTE DE EQUILÍBRIO NA INTERNET

A internet é sem dúvida um marco, um ponto culminante no mundo tecnológico. Pode-se afirmar que existe tecnologia antes e depois da internet. A interligação global de computadores inicialmente pleiteada por militares e acadêmicos, possibilitou um aumento exponencial na quantidade de informações disponíveis, bem como na velocidade de divulgação e difusão destas informações entre as pessoas. Pode-se dizer que esses benefícios favoreceram as mais diversas áreas, dentre elas: pesquisa, educacional, militar, governamental, filantrópica, comércio, artes e entretenimento. Tornou-se possível com isso a disponibilização de conteúdos de qualquer cunho, algumas vezes impróprios ou não condizentes com os interesses de uma empresa, grupo ou país. Tratam-se de conteúdos que não são vistos com bons olhos de uma forma geral. Outro fator a considerar é que na atualidade o interesse pelo fator informação aumentou exponencialmente. O principal motivo que levou a esse aumento, é a conscientização do ser humano de que informação é poder. O ciberespaço é um ambiente com grande excesso de informações disponíveis e o ser humano necessita possuí-las. Ameaças virtuais possibilitam cada vez mais o roubo ou extravio de informações, seja partindo de um ataque externo ou interno a uma organização. O fato é que possivelmente as informações da organização, sendo então um dos principais ativos, estarão vulneráveis. Diante destas afirmações, evidencia-se a importância do *firewall* como agente de equilíbrio na internet.

O *firewall* é a primeira linha de defesa de uma rede ou um computador. Conforme PALU (2005, p.51) apud PERKINS(2002), o *firewall* funciona como um ponto de controle(Figura 19) de segurança na fronteira entre duas redes. Estas redes normalmente são denominadas rede interna e rede externa, e o controle permite inspecionar o tráfego entre ambas, bloqueando ou aceitando os pacotes de dados de acordo com regras previamente definidas. PASTORE e DULANEY (2006, p.109) estabelecem uma definição mais simples e objetiva, porém em harmonia com a anterior, dizendo que o propósito básico do *firewall* é isolar uma rede de outra.

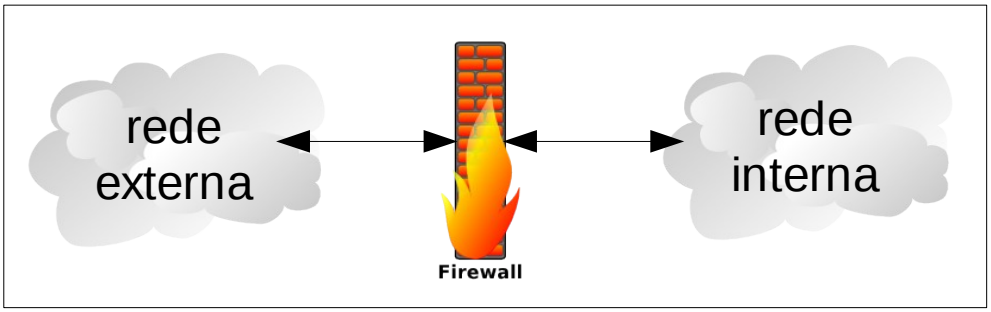

FIGURA 19: localização do *firewall* entre duas redes

Apesar destas definições serem claras, elas não fazem menção a uma situação na qual o *firewall* deve controlar o acesso a apenas uma máquina. Assim, uma descrição mais abrangente, que define o *firewall* em qualquer ambiente no qual está inserido, é a descrita por NOONAN e DUBRAWSKY(2006): *firewall* é um ponto de aplicação de política de controle de acesso, o qual busca fornecer métodos de reforço para este controle. Observa-se que esta definição é aplicável tanto em ambiente envolvendo redes (Figura 19), bem como o ambiente que envolva um *host* específico e qualquer localidade que comunique-se com ele. Neste caso ele é conhecido com *personal firewall* (Figura 20).

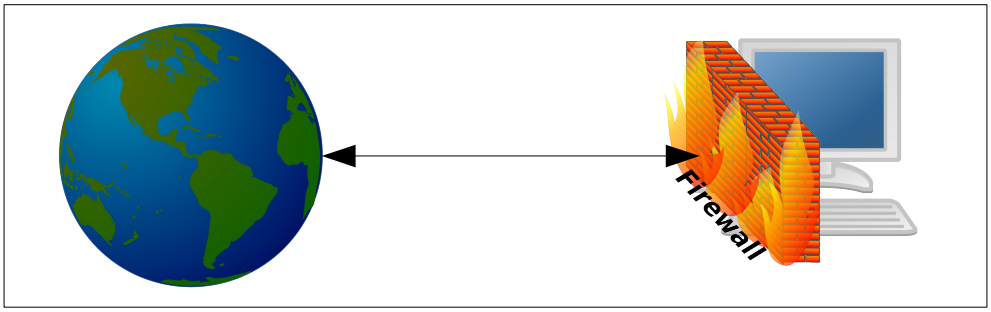

FIGURA 20: *firewall* específico para um host

3.2. AMBIENTE DE USO DO *FIREWALL*

Basicamente são três contextos nos quais o *firewall* está inserido.

No primeiro contexto (Figura 21), o ambiente é constituído pela rede interna(rede particular pertencente a uma empresa) e pela rede externa(que neste caso pode ser a internet). O ponto de controle entre as duas redes é conhecido como *firewall* de borda ou *bastion host*. Este nome é justamente pelo fato de que a máquina fica na borda, isto é, na extremidade de uma rede, local onde a mesma se encontra com outra rede qualquer. Pode-se dizer que ele é de suma importância para a organização pois todas as comunicações entre as duas redes, passarão obrigatoriamente por esta máquina. Ela é a primeira linha de defesa conforme já citado, devendo manter-se em harmonia com todas as tecnologias utilizadas pela empresa, como por exemplo voz sobre IP, VPN[15], conectividade com órgãos governamentais (Receita Federal[16], entre outros), e acesso remoto (ssh[17], terminal remoto, etc.).

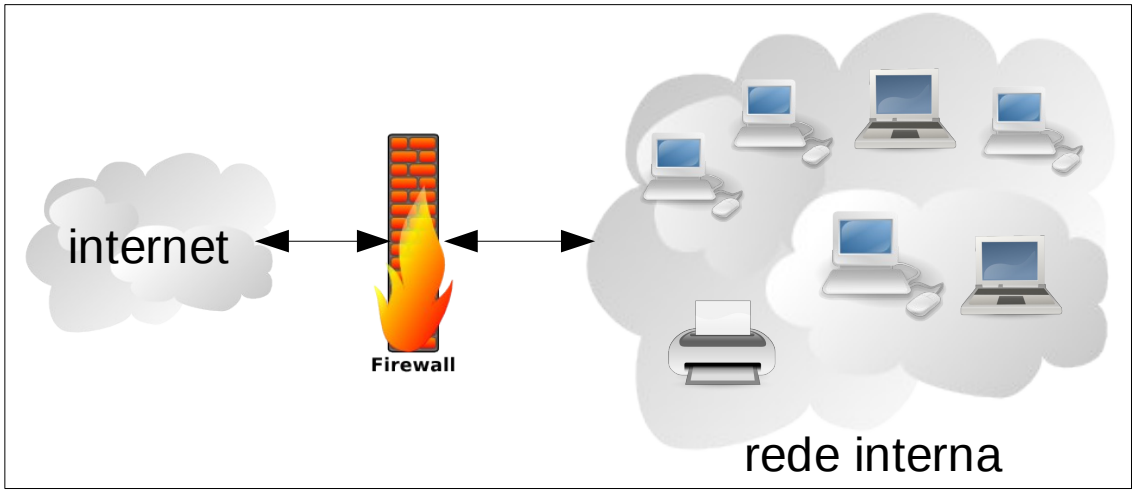

FIGURA 21: ambiente constituído por uma rede particular(rede interna) e a internet (rede externa)

15 *Virtual Private Network* – é uma conexão de rede privada que ocorre através de uma rede pública. VPNs podem ser usadas para conectada redes LAN em locais distantes, usando a internet ou outra rede pública qualquer. Uma VPN normalmente é utilizada criando-se um túnel encriptado que interliga o *firewall* de borda das redes envolvidas. (PASTORE, DULANEY, 2006, p.122).

16 A Receita Federal do Brasil disponibiliza um software chamado Receitanet, responsável por transmitir todas as informações que uma pessoa física ou jurídica precisa fazê-lo ao órgão. O *firewall* de borda é o responsável por permitir ou negar a conexão inciada por este aplicativo. (Disponível em http://www.receita.fazenda.gov.br/Pessoafisica/receitanet/default.htm)

17 O SSH ou Secure Shell, é um software que permite fazer acesso remoto ao console de uma máquina à distância, como se estivesse na frente da mesma. O firewall de borda é o responsável por permitir, negar ou redirecionar tal tipo de conexão. (SILVA, 2007)

No segundo contexto (Figura 22), o ambiente é constituído apenas da rede interna da própria empresa, podendo esta ser segregada, isto é, dividida em sub-redes menores, inclusive integrando alguma VPN. *Firewall* interno é o nome dado aos pontos de controle entre essas sub-redes internas. Neste caso as regras serão focadas apenas na comunicação entre as máquinas da rede interna. Deve-se considerar que as regras de bloqueio quanto a ameaças de uma rede externa, já foram implementadas no *firewall* de borda, eximindo a responsabilidade desta máquina.

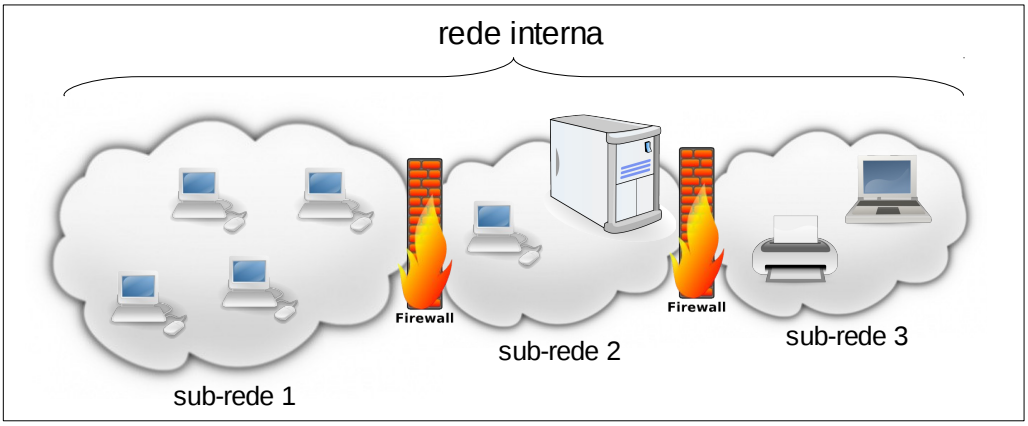

FIGURA 22: ambiente constituído por uma rede interna dividida em sub-redes menores

No terceiro contexto (Figura 20), o ambiente pode ser constituído de uma rede qualquer (seja ela externa ou interna, enfim qualquer origem) e a própria máquina *firewall* sozinha, que neste caso pode implementar regras de controle para acesso a ela mesma. Enquadra-se neste contexto a própria máquina de um usuário final bem como um servidor de aplicação de banco de dados, web, arquivos, entre outros.

A Figura 23 apresenta uma demonstração de ambiente que integra os três contextos em coexistência. Nela é apresentado uma rede externa (que neste caso é a internet) e uma rede interna, a qual é subdividida em três sub-redes menores. Observa-se que na borda da rede interna, no ponto em que ela se torna adjacente à rede externa, existe um *firewall* então responsável pelo controle de comunicação entre a rede interna e externa. Outro detalhe interessante a se observar é que o *firewall* de borda é um *host* pertencente à rede interna, como se identifica visualmente pela posição da linha que define a borda desta rede.

Ainda na mesma Figura 23, observa-se que entre as três sub-redes menores, existem *firewalls* internos, responsáveis pelos controles de comunicação entre estas. No exemplo em questão, para que um *host* da sub-rede um comunique-se com um *host* da sub-rede 3, esta conexão deverá passar obrigatoriamente pelos dois *firewalls* internos. Caso um *host* da sub-

rede 3 queira se comunicar com a internet, esta conexão deverá passar obrigatoriamente pelos dois *firewalls* internos e posteriormente pelo *firewall* de borda.

Por fim, observa-se um *host* na sub-rede 1, o qual possui um *firewall* pessoal, que controla todas as conexões que chegam a este *host* em especial. Qualquer requisição de conexão que chegue da internet ou de qualquer *host* dentre as sub-redes da rede interna, esta conexão estará sujeita ao controle deste *firewall* pessoal.

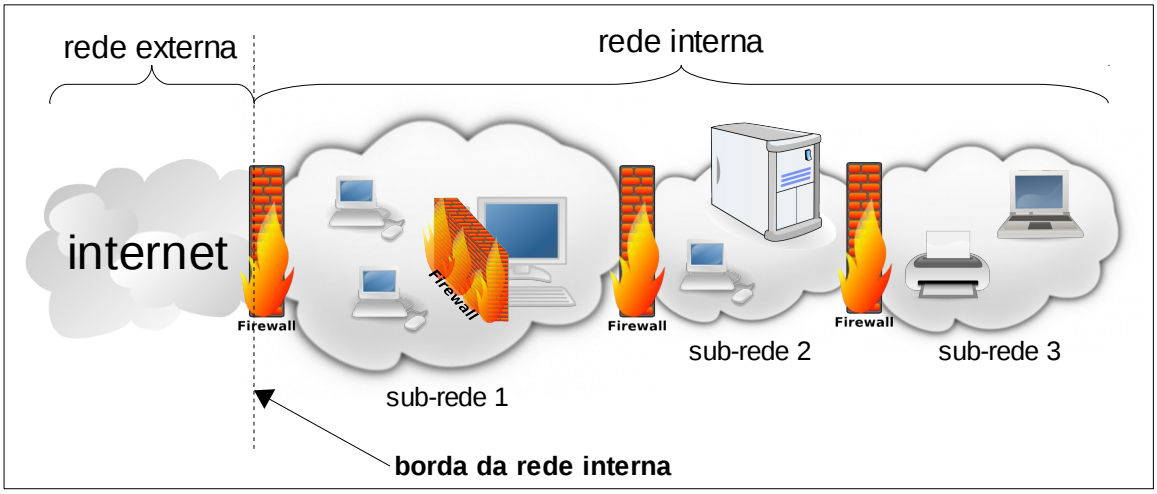

FIGURA 23: demonstração de ambiente contendo os três tipos de *firewalls* diferentes

3.3. O QUE FAZ UM *FIREWALL* ?

NOONAN e DUBRAWSKY(2006) citam algumas habilidades que o *firewall* deve possuir. Dentre elas, estão: gerenciamento e controle de tráfego de rede, intermediação de conexões, proteção de recursos, registro e reportagem de eventos. Uma outra habilidade descrita em BARBOSA (2006, p. 25), é o recurso de *network address translate* (NAT). Este recurso pode ser englobado no gerenciamento e controle de tráfego de rede, porém merece uma explicação mais detalhada. Segue a descrição de cada uma destas habilidades.

3.3.1. Gerenciamento e controle de tráfego de rede

Esta é a primeira e fundamental funcionalidade de um *firewall*. Ele deve gerenciar e controlar todo o tráfego que passa por este ponto de controle, permitindo a passagem para a

rede ou computador protegido. Este controle é feito através da inspeção de pacotes e inspeção de estados de conexão.

Inspeção de pacotes é o processo de interceptar e processar um pacote de dados, determinando se este pode ou não continuar o seu caminho, tendo como base a política de acesso definida. Esta inspeção pode ser realizada verificando alguns ou vários elementos do pacote em questão.

São objetos de verificação o endereço IP e porta origem, endereço IP e porta destino, protocolo utilizado, bem como outras informações do cabeçalho do pacote.

Um fator interessante a considerar é a possibilidade do *firewall* inspecionar cada pacote em cada sentido que ele trafega e para todas as relações, devendo as regras de controle de acesso existirem para cada situação destas. Para isso existem os conceitos de verificação *stateful* (estado de conexão) e *stateless* (sem estado de conexão).

Para que aconteça a comunicação entre dois *hosts* TCP/IP, é necessário estabelecer conexões primordiais que normalmente servem para dois propósitos.

No primeiro, ambas as máquinas usam a conexão para se identificarem. Este processo tem finalidade de impedir que os dados deste fluxo não sejam entregues a um *host* que não pertença a esta comunicação. As informações deste tipo de conexão podem ser utilizadas pelo *firewall* para determinar quais conexões entre ambos são permitidas pela política de controle, bloqueando ou negando o fluxo de dados.

Uma vez identificado a origem e destino, tem-se o segundo propósito, que é o momento de definir a forma de transmissão entre os dois *hosts.* Esta transmissão pode ser através de uma sessão orientada a conexão, isto é, para cada pacote do fluxo a ser enviado, um pacote de retorno (também chamado ACK) deve ser enviado de volta confirmando o seu recebimento pelo destinatário. Este é o caso de uma conexão que utiliza *transmission control protocol* (TCP). Também pode ser uma sessão sem conexão, isto é, para cada pacote do fluxo a ser enviado, não é necessário nenhuma confirmação do recebimento. Este é o caso de uma conexão que utiliza *user datagram protocol* (UDP) ou *internet control message protocol* (ICMP).

A combinação da inspeção de pacotes e a inspeção de estado de conexão é chamada de *stateful packet inspection*. Através desta técnica, é possível verificar não somente a estrutura de pacotes, mas também o estado da conversa entre origem e destino. Tal recurso permite geralmente que não sejam necessárias regras de controle para permitir o retorno de respostas e confirmações de uma conexão, pois o *firewall* reconhece a sessão já liberada previamente.

3.3.1.1. NAT

Este recurso está de certa forma inserido no gerenciamento e controle de tráfego de rede já descrito, porém merece uma descrição um pouco mais detalhada. Constitui-se da capacidade do *firewall* em traduzir endereços IP e manipular uma rota padrão de pacotes. Também possibilita a alteração do IP ou porta de origem, recurso este conhecido como *source network address translate* (SNAT), bem como alteração do IP ou porta e destino, recurso conhecido como *destination network address translate* (DNAT). Tais funcionalidades são muito úteis e um exemplo que ocorre normalmente em *firewall* de borda, é quando computadores de uma rede particular precisam acessar a internet. Para isso, utilizam-se do IP externo do *firewall* para que o pacote viaje, pois os IPs da rede interna são tidos como falsos na internet (Figura 24).

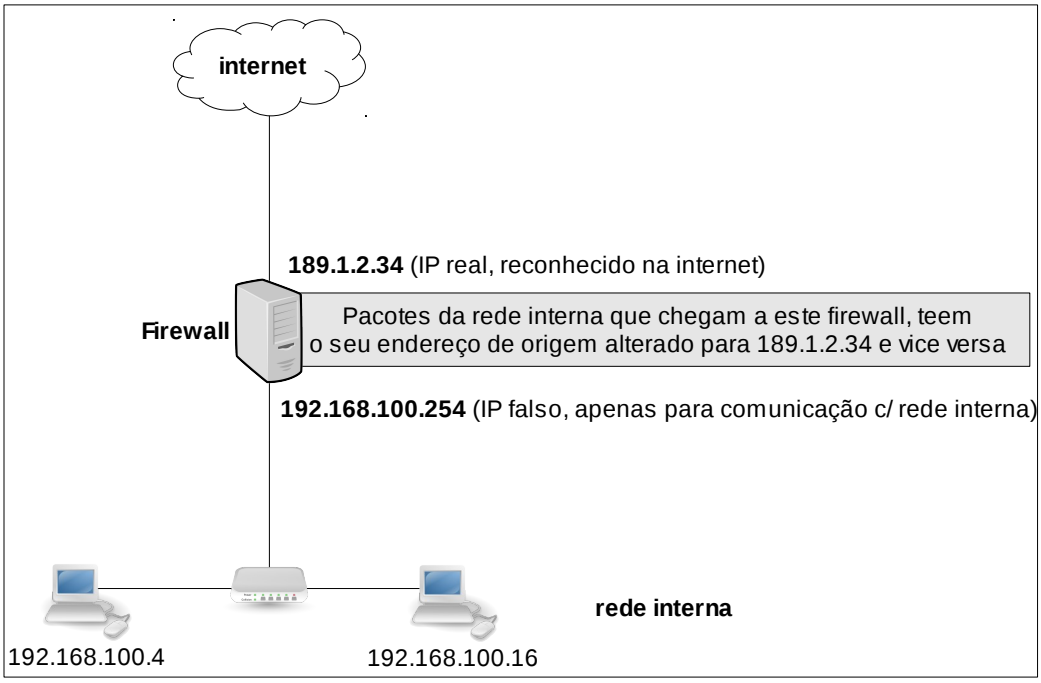

FIGURA 24: *firewall* com função de NAT

3.3.2. Intermediação de conexões

Também conhecido como *proxy*, é um recurso que atua na camada de aplicação. O *firewall* como intermediário de conexões funciona primeiramente como uma forma e proteger

contra possíveis riscos na interação direta com um *host* externo. Origem e destino não se comunicam diretamente. Um pacote com destino a um *host* da rede interna, ao chegar é recebido pelo *proxy*, o qual seleciona as informações relevantes do pacote, reconstruindo-o e enviando finalmente ao *host* destino.

Este tipo de tarefa normalmente é utilizado para cache de sessões HTTP, fazendo com que as páginas mais acessadas por um grupo de *hosts*, fique armazenado, diminuindo drasticamente a quantidade de dados que saem por um *link* externo.

3.3.3. Proteção de recursos

O *firewall* não é um anti-virus. Poderiam até serem implementadas regras de política de controle usando a combinação de várias inspeções no pacote, porém além de comprometer talvez a velocidade de conexão do usuário final, não é o intuito do *firewall*. Porém é possível o bloqueio a algumas ameaças comuns em se falando de redes. Ataques do tipo DoS[18] , IP Spoofing[19], entre outros podem ser interceptados de acordo com a política de controle definida.

3.3.4. Registro e reportagem de eventos

É o popularmente conhecido arquivo de log. Trata-se da habilidade de poder registrar pacotes e eventos que ocorram na linha de comunicação em questão. O registro pode ser feito de todo o tráfego ocorrido, o que seria indicado em uma época de auditoria ou em ambientes que requerem um nível de monitoramento elevado. Também pode ser realizado apenas o registro de situações que chamem a atenção mediante a política de controle implementada. Um exemplo seria o excesso de conexões destinadas a uma porta SSH sem sucesso, o que poderia poderia indicar um potencial ataque de força bruta.

18 *Denial of Service* – técnica utilizada para interromper um serviço em um servidor. Este ataque é constituído pelo envio por um determinado tempo, de um tráfego maior que o suportado pelo alvo, desencadeando a parada do serviço ou sistema. (FILHO, 2006, p. 28).

19 Técnica na qual o atacante utiliza-se de um IP falso (da própria rede) para receber pacotes desta (FILHO, 2006, p. 26).

3.4. O FUNCIONAMENTO BÁSICO DE UM *FIREWALL*

Atualmente existem diversas ferramentas para a definição das regras de um *firewall*. Para esta dissertação, foi adotada a ferramenta Netfilter pelo fato de ser um *software* de *firewall* nativo em distribuições Linux (NETO, 2004, p. 32), então utilizado por este pesquisador nas disciplinas de redes de computadores.

O Netfilter é acessível através de uma interface via linha de comando chamada Iptables (Figura 25), através da qual o usuário faz o gerenciamento das tabelas de regras (IPTABLES, 2011).

```
Chain INPUT (policy ACCEPT 98 packets, 6508 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     0    --  *      *       0.0.0.0/0            127.0.0.1

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
  276 13248 ACCEPT     0    --  *      *       192.168.100.0/24     0.0.0.0/0
    8   368 ACCEPT     0    --  *      *       0.0.0.0/0            192.168.100.0/24

Chain OUTPUT (policy ACCEPT 69 packets, 9508 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     0    --  *      *       0.0.0.0/0            127.0.0.1
```

FIGURA 25: interface Iptables

As funções gerenciamento e controle de tráfego de redes são contempladas pelo Netfilter. Ele é capaz de analisar o cabeçalho de cada pacote de dados que chega à máquina. Baseando-se no endereço IP de origem e/ou destino, bem como na porta de origem e/ou destino, ele faz uma extensa comparação às regras previamente definidas e então decide se o pacote deve ou não continuar seu caminho. Obviamente esta análise também é aplicada aos pacotes de dados destinados ao próprio *firewall*, bem como pacotes que saem do mesmo.

Uma vez justificada e descrita a ferramenta usada para gerenciamento do *firewall*, convém entender de forma resumida o funcionamento interno do mesmo. Para isso, utilizando-se do próprio conceito de visualização dinâmica para promover uma cognição mais apurada, foi elaborado para esta dissertação, um diagrama de fluxo (Figura 26) que exprime os possíveis caminhos que um pacote pode tomar ao chegar no *firewall*. Cada retângulo representa uma tabela a ser preenchida por regras. A tabela (se possuir regras), é aplicada em um determinado momento seguindo a ordem demonstrada no diagrama.

Basicamente o *firewall* faz a interligação entre dois pontos. Mas isso não quer dizer que fisicamente o mesmo acontece. É possível ao *host firewall* estar conectado diretamente a

mais que dois locais. Mesmo desta forma o fluxo de dados será idêntico, pois deve-se considerar apenas uma origem e um destino. Sempre haverá o lado com uma rede que originou o pacote e o lado com a rede ou *host* contendo o destino do mesmo. Tanto a rede interna quanto a rede externa (internet) podem ser origem ou destino. Ao digitar um endereço de *website* no *browser* requisitando assim o acesso ao mesmo, o pacote parte do lado da rede interna, ou seja, da máquina do usuário, sendo neste contexto a rede interna a originária do pacote. Quando uma solicitação de acesso por terminal remoto vindo de outra localidade chega ao *firewall*, neste contexto o lado da rede originária é a rede externa(internet) e o destino é o próprio *firewall* ou a rede interna caso hajam regras de redirecionamento para esta.

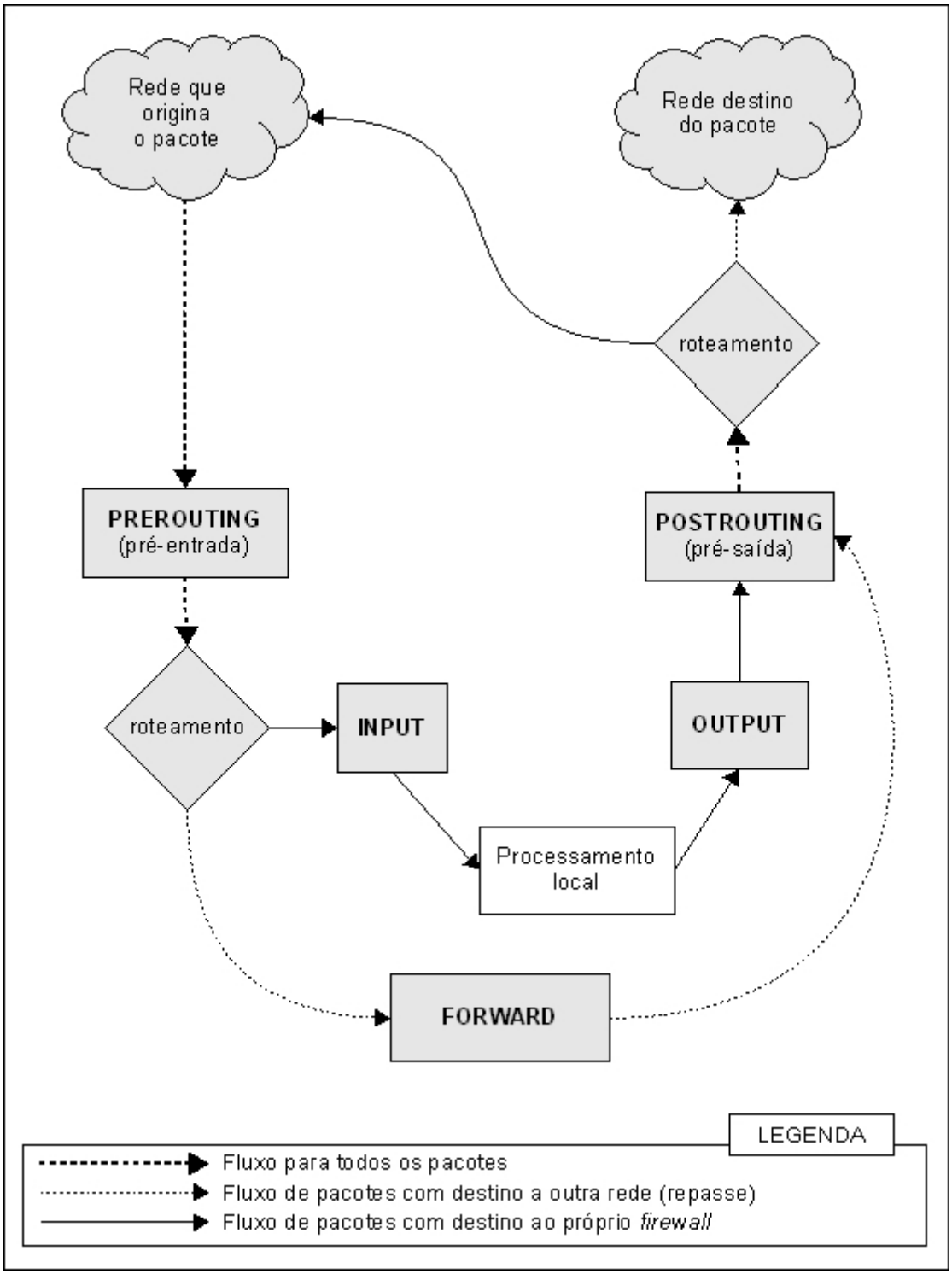

FIGURA 26: diagrama de fluxo do Iptables

São duas as possibilidades de pacotes que chegam ao *firewall*: pacotes com destino a uma segunda rede e pacotes com destino ao próprio *firewall.*

Considerando primeiramente um pacote com destino à próxima rede, o caminho tomado será da seguinte forma: o pacote passa pelas regras de PREROUTING, o que inclui por exemplo o redirecionamento de porta e IP destinos. Este recurso pode ser utilizado ainda

como exemplo, para redirecionar todo o tráfego que chega na porta 3389 (destinado a terminal remoto), para uma máquina da rede interna. Em seguida são aplicadas as regras de FORWARD (repasse), as quais simplesmente permitem ou não a passagem do pacote de acordo com as políticas estabelecidas. Considerando que o pacote foi liberado, são aplicadas as regras de POSTROUTING, o que inclui por exemplo a substituição do IP de origem (ação conhecida como mascaramento) pelo IP do *firewall*. Isto se faz necessário para o pacote seguir viagem com um endereço de origem válido, reconhecido na internet, possibilitando a sua volta quando necessário. Após isto, o pacote sai pelo dispositivo que liga o *firewall* à próxima rede.

O pacote com destino ao *firewall*, inicia seu caminho passando pelas regras de PREROUTING como descrito no caso anterior. Em seguida, o pacote será filtrado pelas regras de INPUT (entrada), as quais vão permitir ou não a continuação do caminho. Caso seja permitido, o pacote chega à máquina *firewall* e retorna à mesma rede de origem, mas passando antes pelas regras de OUTPUT(saída) que vão definir se um pacote pode ou não sair, bem como pelas regras de POSTROUTING já descritas.

Como se pode ver pela Figura 25, a interface Iptables não dispõe de recursos visuais que favoreçam suficientemente o processo cognitivo. É uma ferramenta eficiente para o usuário experiente, porém mesmo para este em um ambiente real com centenas de regras carregadas (Figura 27), torna-se um processo muito árduo a análise das regras. Algumas interfaces provém alguns recursos visuais para tentar melhorar este processo de cognição, porém na maioria das vezes, não apresentam diferenciais significativos.

Uma vez demonstrado o funcionamento básico do *firewall* através do uso do Netfilter, é demonstrando a seguir a execução das habilidades inerentes ao *firewall*.

Para a proteção de recursos, ele possui módulos específicos para bloquear ameaças de rede mais comuns. A Figura 28 demonstra o trecho de um *script* de *firewall* no qual é feita a ativação de módulo para proteção contra DoS e IP Spoofing. Outros tipos de ameaças podem ser inibidos mediante a configuração de regras personalizadas.

```
Chain INPUT (policy DROP)
target     prot opt source               destination
DROP       0    --  0.0.0.0/0            0.0.0.0/0           state INVALID
ACCEPT     0    --  0.0.0.0/0            0.0.0.0/0 state RELATED,ESTABLISHED
DROP       0    --  192.168.100.2        0.0.0.0/0
ACCEPT     0    --  0.0.0.0/0            127.0.0.1
ACCEPT     0    --  192.168.100.0/24     0.0.0.0/0
ACCEPT     icmp --  0.0.0.0/0            189.12.128.186      icmp type 0
ACCEPT     icmp --  0.0.0.0/0            189.12.128.186      icmp type 3
ACCEPT     icmp --  0.0.0.0/0            189.12.128.186      icmp type 8
ACCEPT     icmp --  0.0.0.0/0            189.12.128.186      icmp type 11

Chain FORWARD (policy DROP)
target     prot opt source               destination
DROP       0    --  0.0.0.0/0            0.0.0.0/0           state INVALID
DROP       0    --  192.168.100.2        0.0.0.0/0
DROP       0    --  0.0.0.0/0            192.168.100.2
ACCEPT     tcp  --  192.168.100.4        0.0.0.0/0           tcp dpt:1863
ACCEPT     tcp  --  192.168.100.0/24     0.0.0.0/0           tcp dpt:3389
ACCEPT     udp  --  192.168.100.0/24     0.0.0.0/0           udp dpt:3389
ACCEPT     tcp  --  192.168.100.0/24     0.0.0.0/0           tcp dpt:8181
ACCEPT     udp  --  192.168.100.0/24     0.0.0.0/0           udp dpt:8181
ACCEPT     tcp  --  192.168.100.0/24     0.0.0.0/0           tcp dpt:8017
ACCEPT     udp  --  192.168.100.0/24     0.0.0.0/0           udp dpt:8017
DROP       tcp  --  192.168.100.0/24     0.0.0.0/0           tcp dpt:1863
DROP       udp  --  192.168.100.0/24     0.0.0.0/0           udp dpt:1863
DROP       tcp  --  192.168.100.0/24     0.0.0.0/0           tcp dpt:445
DROP       udp  --  192.168.100.0/24     0.0.0.0/0           udp dpt:445
DROP       tcp  --  192.168.100.0/24     0.0.0.0/0           tcp spt:445
DROP       tcp  --  192.168.100.0/24     0.0.0.0/0           tcp dpt:1863
ACCEPT     tcp  --  192.168.100.0/24     200.201.174.207     tcp dpt:80
ACCEPT     tcp  --  192.168.100.0/24     200.201.174.204     tcp dpt:80
ACCEPT     tcp  --  192.168.100.0/24     200.201.174.204     tcp dpt:2631
ACCEPT     tcp  --  0.0.0.0/0            200.201.0.0/16
ACCEPT     tcp  --  192.168.100.0/24     200.255.42.71       tcp dpt:80
ACCEPT     tcp  --  192.168.100.0/24     200.255.42.71       tcp dpt:21
ACCEPT     tcp  --  192.168.100.0/24     189.21.233.19       tcp dpt:80
ACCEPT     tcp  --  192.168.100.0/24     189.21.233.19       tcp dpt:21
ACCEPT     tcp  --  192.168.100.0/24     189.21.233.19       tcp dpt:8181

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     0    --  0.0.0.0/0            127.0.0.1
ACCEPT     icmp --  189.12.128.186       0.0.0.0/0           icmp type 0
ACCEPT     icmp --  189.12.128.186       0.0.0.0/0           icmp type 3
ACCEPT     icmp --  189.12.128.186       0.0.0.0/0           icmp type 8
ACCEPT     icmp --  189.12.128.186       0.0.0.0/0           icmp type 11
```

FIGURA 27: interface Iptables com várias regras carregadas

```
echo “ativando modulo de protecao contra DOS”
echo "1" > /proc/sys/net/ipv4/tcp_syncookies

echo “ativando modulo de protecao contra IP Spoofing”
echo "1" > /proc/sys/net/ipv4/conf/all/rp_filter
echo "1" > /proc/sys/net/ipv4/conf/default/rp_filter
```

FIGURA 28: ativação de módulo de proteção contra ameaças mais comuns

Também o registro de eventos pode ser realizado pelo Netfilter. A Figura 29

exemplifica o trecho de um *script* de *firewall* no qual é feito o registro de todas as conexões TCP destinadas à porta 80 do próprio *firewall*.

```
echo “Registrando a entrada de conexão TCP na porta 80”
iptables -A INPUT -p tcp --dport 80 -j LOG --log-level debug
       --log-prefix “PORTA 80 ACESSADA”

echo “Permitindo a entrada de conexões na porta 80”
iptables -A INPUT -p tcp --dport 80 -j ACCEPT
```

FIGURA 29: registro de conexões

Por fim, o NAT é um recurso também possível ao Netfilter. A Figura 30 exemplifica o uso de regras de NAT para o ambiente demonstrado na Figura 24. Neste exemplo, todos os pacotes originários da rede 192.168.100.0/24 e que vão sair pela placa de rede externa (a que se comunica com a rede externa), deverão ter o seu IP de origem mascarado com o IP do próprio *firewall* que neste exemplo é 189.1.2.34.

```
echo “fazendo mascaramento entre a rede interna e a rede externa”
iptables -t nat -A POSTROUTING -s 192.168.100.0/24 -o $IFACE_EXTERNA -j MASQUERADE
```

FIGURA 30: exemplo de regra Iptables para fazer NAT

O recurso de SNAT também pode ser feito para atender o mesmo ambiente da Figura 24. Porém neste é necessário informar manualmente(ou no *script*), qual é o IP que se deseja definir como origem a cada pacote que saia da rede interna com destino a rede externa (Figura 31).

```
echo “fazendo SNAT entre a rede interna e a rede externa”
iptables -t nat -A POSTROUTING -s 192.168.100.0/24 -o $IFACE_EXTERNA -j
       SNAT --to 189.1.2.34
```

FIGURA 31: exemplo de regra IPTABLES para fazer SNAT

A Figura 32, exemplifica o uso de regras para fazer DNAT, onde todas as requisições de conexão que chegarem ao *firewall* na porta 22, sejam redirecionadas, ou sejam, tenham seu endereço de destino alterados para o IP192.168.100.16 (*host* da rede interna).

```
echo “Redirecionando porta de entrada 22 para 192.168.100.16”
iptables -t nat -A PREROUTING -p tcp --dport 22 -j DNAT --to 192.168.100.16:22
```

FIGURA 32: exemplo de regra IPTABLES para fazer DNAT

3.5. ANÁLISE DE INTERFACES PARA ENSINO DE *FIREWALL*

Não foi encontrado neste período de pesquisa, uma interface específica para o ensino do funcionamento interno do *firewall*. Dentre *softwares* didáticos, bem como *softwares* de gerenciamento, estes trabalham a simulação de redes, roteamento, mas nenhum provê o funcionamento interno do *firewall*.

Das interfaces selecionadas, algumas são utilizadas por este pesquisador no processo de ensino de redes no curso de sistemas de informação, bem como em ambiente de produção. Outras foram objeto de pesquisa de utilização junto a outros professores e profissionais da área de redes.

A análise a seguir busca observar conceitos e informações levantados nesta dissertação. Também merece uma análise, o *software* didático Packet Tracer[20] da CISCO, por ser uma referência, um recurso de renome entre especialistas em redes de computadores.

3.5.1. Iptables

A primeira interface a ser analisada é o próprio Iptables (Figura 33). Esta interface não apresenta nenhuma informação desnecessária, tornando-a uma interface bem limpa e objetiva. Ao contrário, o usuário precisa especificar quando precisa de mais informações utilizando-se de opções no momento da chamada do programa na linha de comando. Observa-se que mesmo em modo texto, são utilizados alguns recursos de sistema múltiplo de memória como o uso de tabelas por exemplo, mas não são explorados recurso de espaço e profundidade bem como qualquer representação metafórica, o que muitas vezes torna a interface pouco atraente ao usuário nos dias atuais. O Iptables não possui também uma adequação da velocidade ciberespacial à percepção humana. Para se observar um pacote submetido ao *firewall* e suas regras, o máximo que se consegue visualizar é a quantidade de regras processadas. Para isso,

20 Disponível em <http://www.cisco.com/web/learning/netacad/course_catalog/PacketTracer.html>

o usuário exibe a tabela de regras habilitando uma opção de contador de regras processadas. Conforme demonstrado na Figura 33, o comando executado faz com que o Iptables exiba as regras de *input* existentes e através da opção específica de visualização (-v) exibe a quantidade de pacotes (campo pkts) e a quantidade de *bytes* (campo *bytes*) que chegou a cada regra.

Em relação às regras de *firewall*, estas são compostas basicamente de três itens referente aos pacotes a serem processados: origem, destino e ação perante o pacote. Na composição das regras pelo Iptables, adiciona-se ainda mais dois elementos: a tabela desejada para se trabalhar, bem como o objetivo perante aquela tabela, ou seja: incluir ou excluir uma regra. A Figura 34 exemplifica um comando do Iptables para inserção de regras. Neste, é adicionada uma regra à tabela FORWARD (de repasse à outra rede) que diz o seguinte: bloqueie todos os pacotes TCP originados da rede 192.168.100.0/24 e que tenham como destino a porta 53 de qualquer outra rede. Conclui-se portanto que o Iptables é uma interface muito objetiva nos seus resultados bem como na forma de composição das regras, o que fomenta a sua utilização quase unânime por usuários experientes. Porém não propicia nenhuma ambiente para entendimento das regras, principalmente quando utilizado para o ensino e compreensão do funcionamento de um *firewall*.

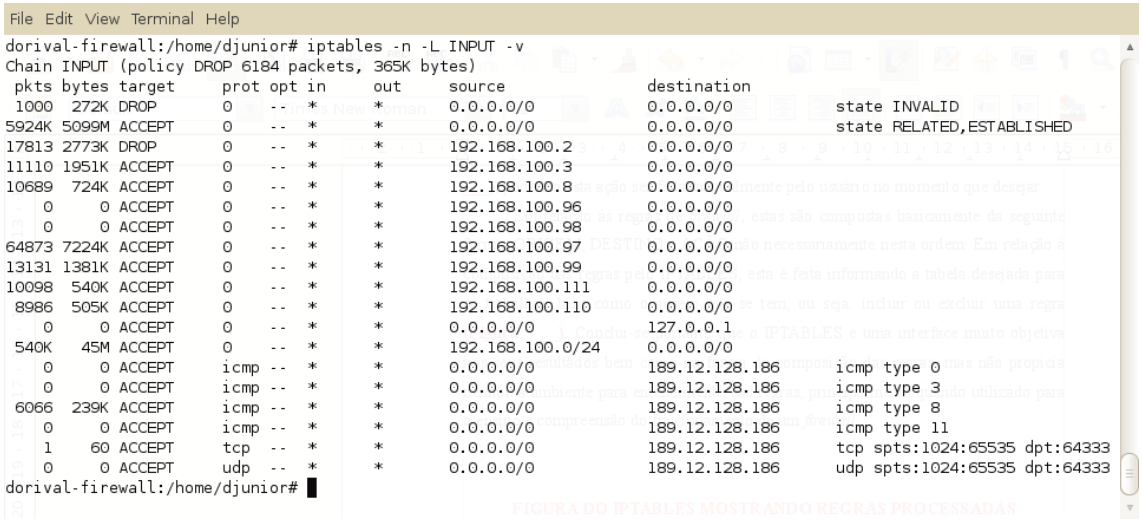

FIGURA 33: visualização de regras pelo IPTABLES

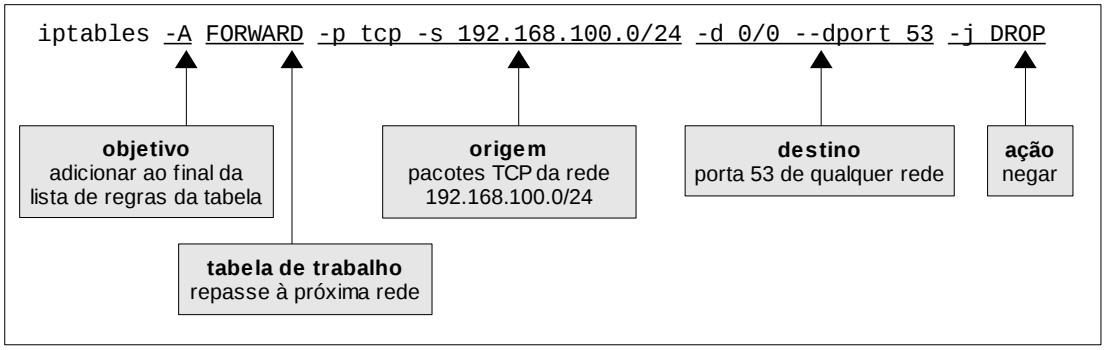

FIGURA 34: manipulação de regras usando Iptables

3.5.2. Firewall Builder

A próxima interface a ser analisada é o Firewall Builder, também conhecido como Fwbuilder (Figura 35). Com uma interface bem mais amigável que o Iptables, é notório à primeira vista que não se trata de uma interface tão limpa. Outro fator diz respeito ao uso de combinação de cores para expressar proibição e permissão. É evidente a presença forte da arte e engenharia trabalhando em conjunto. A arte no que diz respeito a disponibilização de representações visuais metafóricas e artificiais ao mesmo tempo. Metafóricas por utilizar imagens relacionadas a um castelo, como o muro vermelho. Artificial por utilizar figuras que representam placas de rede e computadores. Também está presente o uso de espaço e profundidade na disposição de *layout* da interface, porém não é apresentado nenhuma característica para uso de memória espacial bem como adequação da velocidade ciberespacial à percepção humana. Entretanto, esta interface tem um diferencial que é a geração das regras de *firewall* para execução por outras ferramentas de *firewall*, inclusive de sistemas operacionais diferentes. Dentre as possíveis, tem-se o ipfw e pf, utilizadas em sistema operacional FreeBSD.

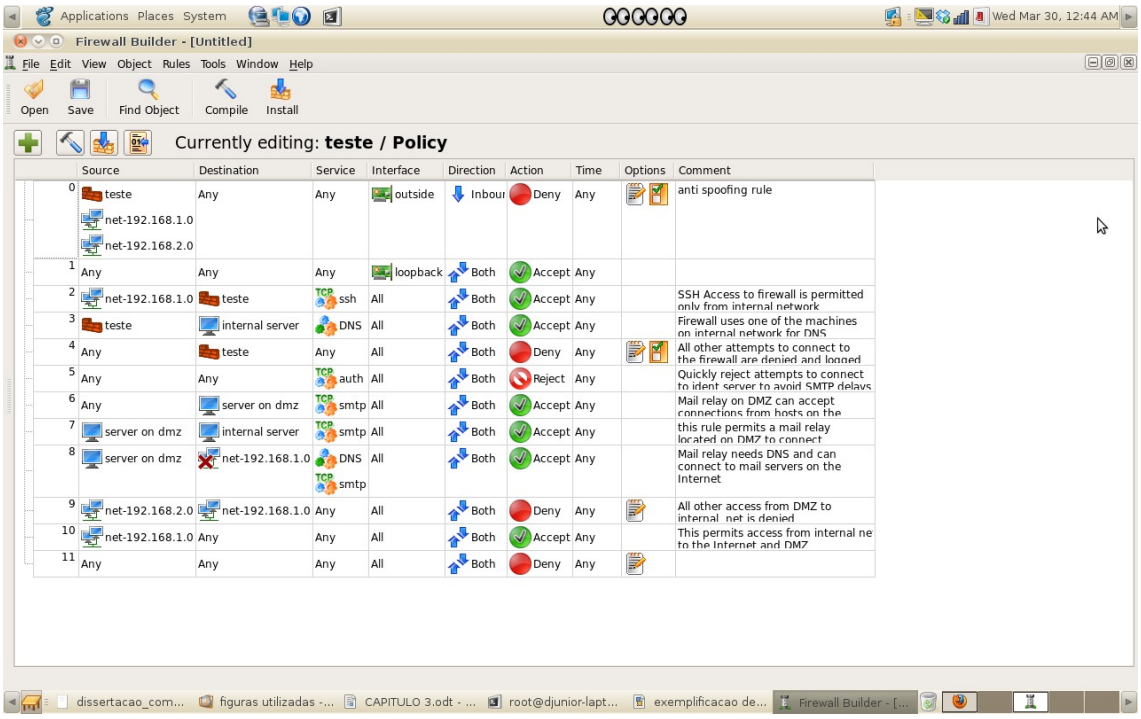

FIGURA 35: interface do Fwbuilder

3.5.3. Endian Firewall

Uma outra interface denominada Endian Firewall (Figura 36) também é analisada. Para este teste, foi utilizada uma versão de demonstração disponibilizada no próprio *website* do projeto[21]. Esta ferramenta possibilita diversas configurações, porém foi observado apenas a área referente ao *firewall*. Assim como Fwbuilder, é evidente o uso de sistema múltiplo de memória no que se refere a tabelas, cores e gráficos. São mantidas as informações necessárias e uma leve combinação de arte e engenharia é apresentada, com uma arte um pouco mais suave em relação ao Fwbuilder. O próprio layout da tabela de regras, bem como as cores utilizadas, são mais suavizados, possibilitando o reconhecimento de espaço e profundidade. Contudo, não é utilizado nenhuma representação visual metafórica ou artificial na composição e execução das regras e por nenhum indício que possibilite o uso de memória espacial. A composição das regras é feita como um cadastro de produto em uma sequência de opções similar à do Iptables via linha de comando.

21 Acessível através do endereço: http://www.endian.com/us/products/demo/

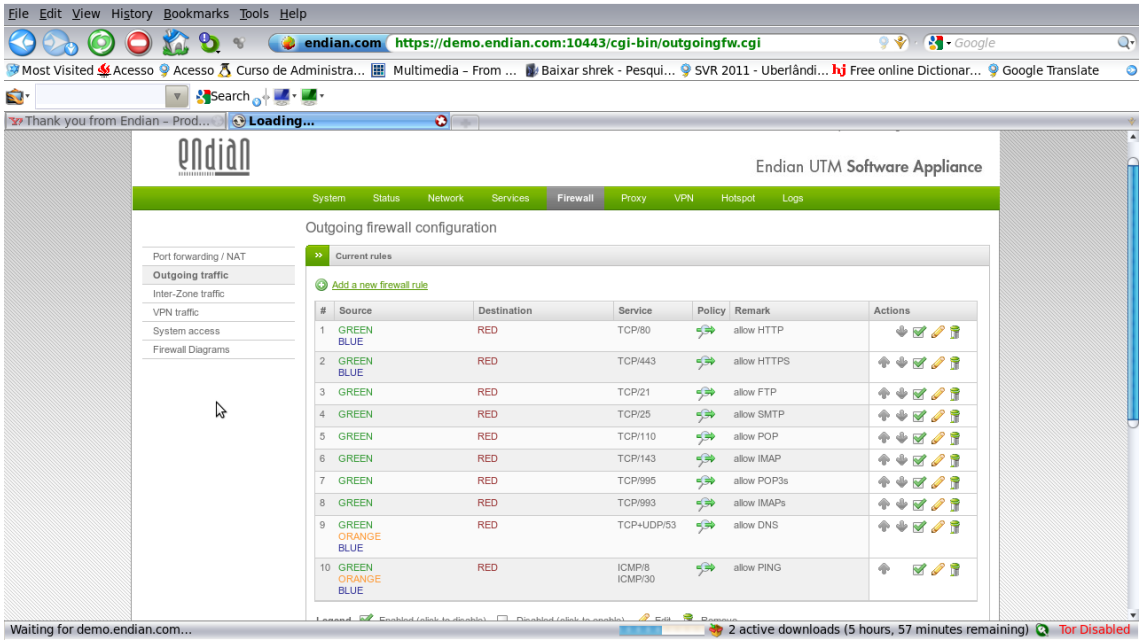

FIGURA 36: interface do Endian Firewall

3.5.4. IPCOP

Existem várias distribuições Linux especialmente montadas para atuar como *firewall*, sendo uma delas o IPCOP[22]. A interface IPCOP (Figura 37) possibilita administrar e visualizar diversas informações de sistema, rede, serviços, porém esta análise tem como foco o gerenciamento de *firewall*, sendo então avaliado apenas esta parte. A interface conta com recursos de cores suaves, bem como uma disposição de *layout* bem agradável ao usuário com tabelas bem colocadas, tornando claro a disponibilização de espaço e profundidade. Existe uma combinação eficiente entre arte e engenharia, uma vez que a forma de criação de regras é a mais simples possível, e com a forma de disposição da tabela de regras existente acontece o mesmo. É evidente o uso de uma representação visual metafórica de um *desktop*, através da simulação de pastas dispostas na tela, sendo bem dividido a área de inserção de regras da área de listagem das regras existentes. Assim como as demais interfaces analisadas, o IPCOP não disponibiliza recurso para visualização do *firewall* bem como o fluxo dos dados dentro dele. Conclui-se assim que esta é uma interface de fácil utilização, porém não permite a visualização ou compreensão do funcionamento do *firewall*.

22 Website oficial do IPCOP: http://www.ipcop.org

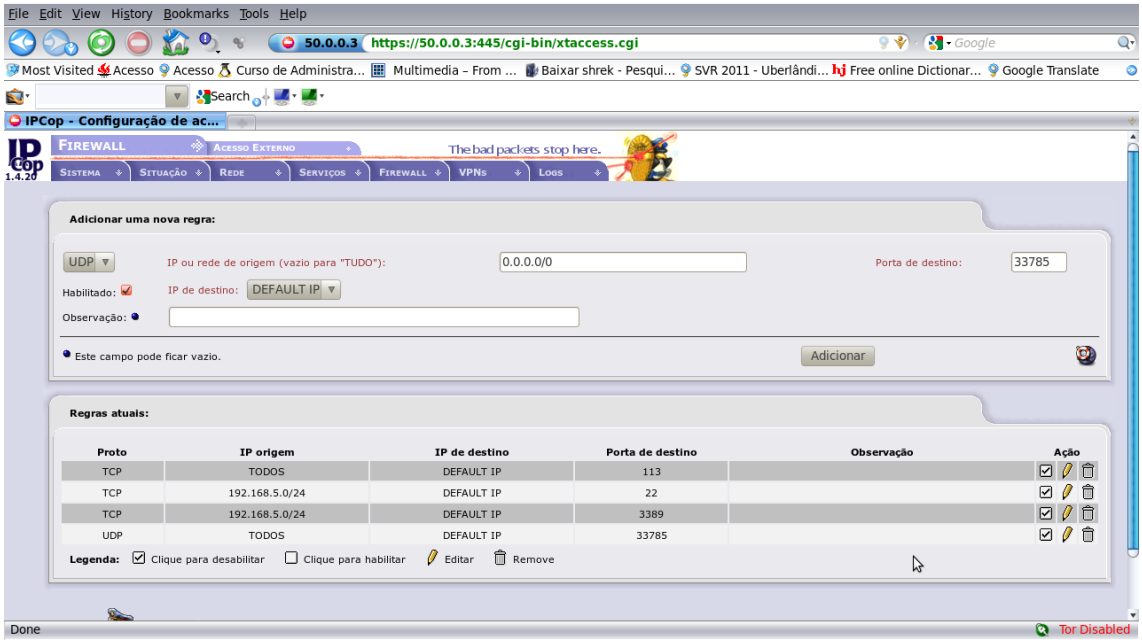

FIGURA 37: interface IPCOP

Concluí-se por esta análise que de uma forma geral, as interface de gerenciamento de *firewall* não permitem o uso de memória espacial e não possibilitam uma adequação de velocidade à percepção humana, recursos que conforme visto, possibilitariam uma melhor compreensão por parte do usuário de todo o processo dentro de um *firewall*.

Existem *softwares* auxiliares que demonstram o fluxo de dados, podendo estes serem usados em conjunto para entender o funcionamento do *firewall*. Alguns destes softwares são o TCPDump, IPTState e SS.

3.5.5. TCPDump

O TCPDump propicia um resultado puramente em modo texto, sem qualquer possibilidade de uso de cores, tabelas e arte em geral. As informações de cada pacote são jogadas linha a linha na tela, culminando em um resultado com muita informação e pouquíssimo atraente ao usuário. Obviamente um usuário mais experiente poderá ler os dados sem o uso de uma outra interface. Normalmente esta ferramenta é utilizada em um terminal a parte afim de se perceber a movimentação de pacotes e assim verificar se as regras do *firewall* estão em funcionamento. No exemplo da Figura 38, o TCPDump está capturando e exibindo todos os pacotes com destino a porta 80.

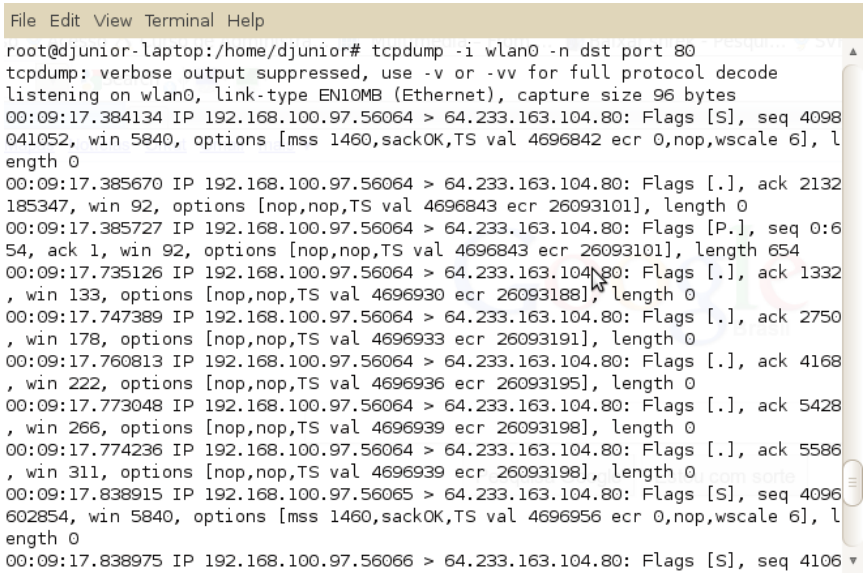

FIGURA 38: tcpdump exibindo os pacotes com destino a porta 80

3.5.6. IPTState

Outro *software* de visualização de fluxos é o IPTState (Figura 39), que mesmo em modo texto, já se apresenta com uma leve combinação de arte e engenharia, bem como a utilização de cores e tabelas. Este software exibe cada nova conexão aberta entre origem e destino, o que permite ao usuário então saber se uma regra funcionou ou não. Observa-se que o usuário precisa de utilizar dois *softwares*: um para confecção das regras e outro para visualização das conexões existentes. Assimilando ambas as informações, o usuário abstrai o que ocorreu dentro do *firewall*.

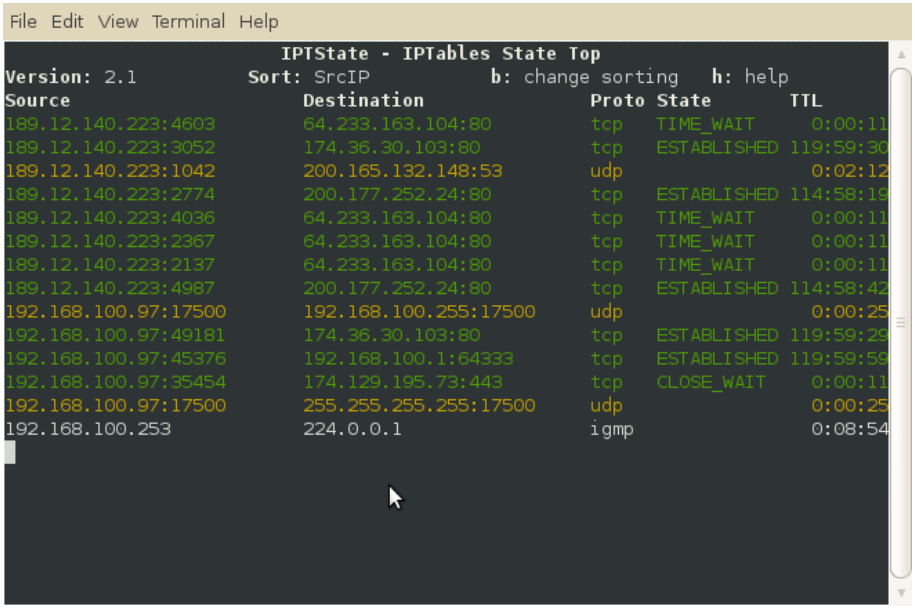

FIGURA 39: interface IPTState

3.5.7. SS

Como última ferramenta de auxílio na visualização de fluxos então analisada, tem-se o SS. Assim como o IPTState, ele exibe as conexões estabelecidas, porém o diferencial é a exibição das portas abertas no *firewall*, conforme se vê pela Figura 40. Com esta informação, o usuário sabe se uma regra para abrir ou fechar determinada porta foi efetivada ou não.

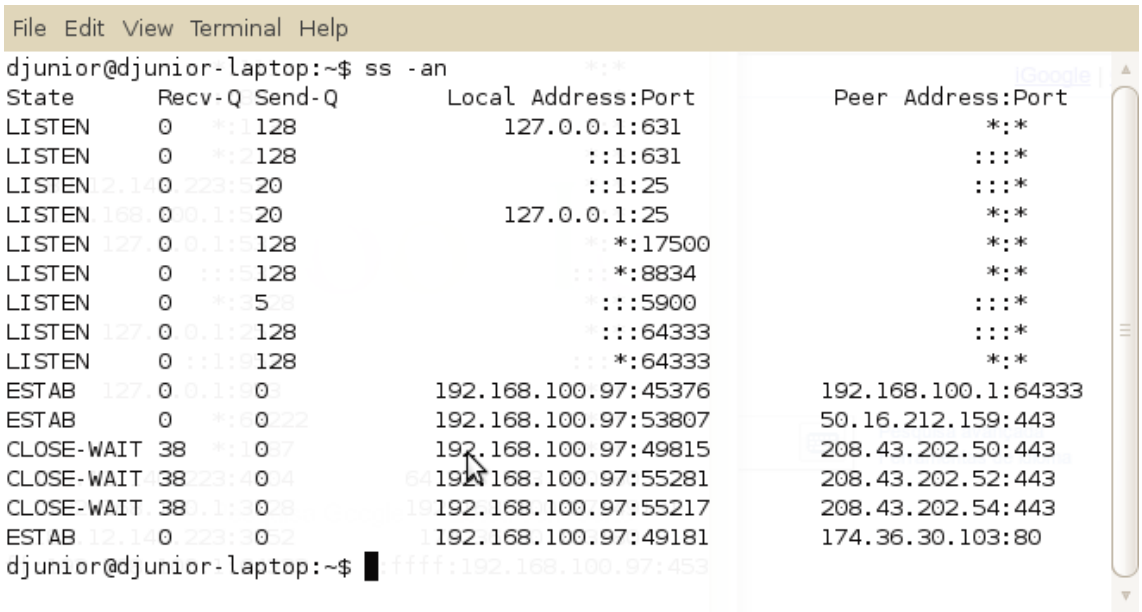

FIGURA 40: interface do SS

3.5.8. Packet Tracer

O próximo software não é especificamente para auxiliar na visualização de fluxo de dados, e sim um *software* didático, ou seja, para fins exclusivamente de ensino em redes de computadores. O Packet Tracer (Figura 41)[23], como ele é chamado, é desenvolvido pela CISCO, sendo utilizado em cursos preparatórios para certificações em redes. Trata-se de um *software* muito conceituado entre especialistas da área, pois permite a simulação dos mais diversos ambientes de rede possíveis, simulando inclusive a montagem e configuração de roteadores e outros equipamentos de *hardware*. Porém, nem mesmo este apresenta um conteúdo referente ao funcionamento interno do *firewall*.

23 Disponível em http://www.cisco.com/web/learning/netacad/course_catalog/docs/Cisco_PacketTracer_DS.pdf

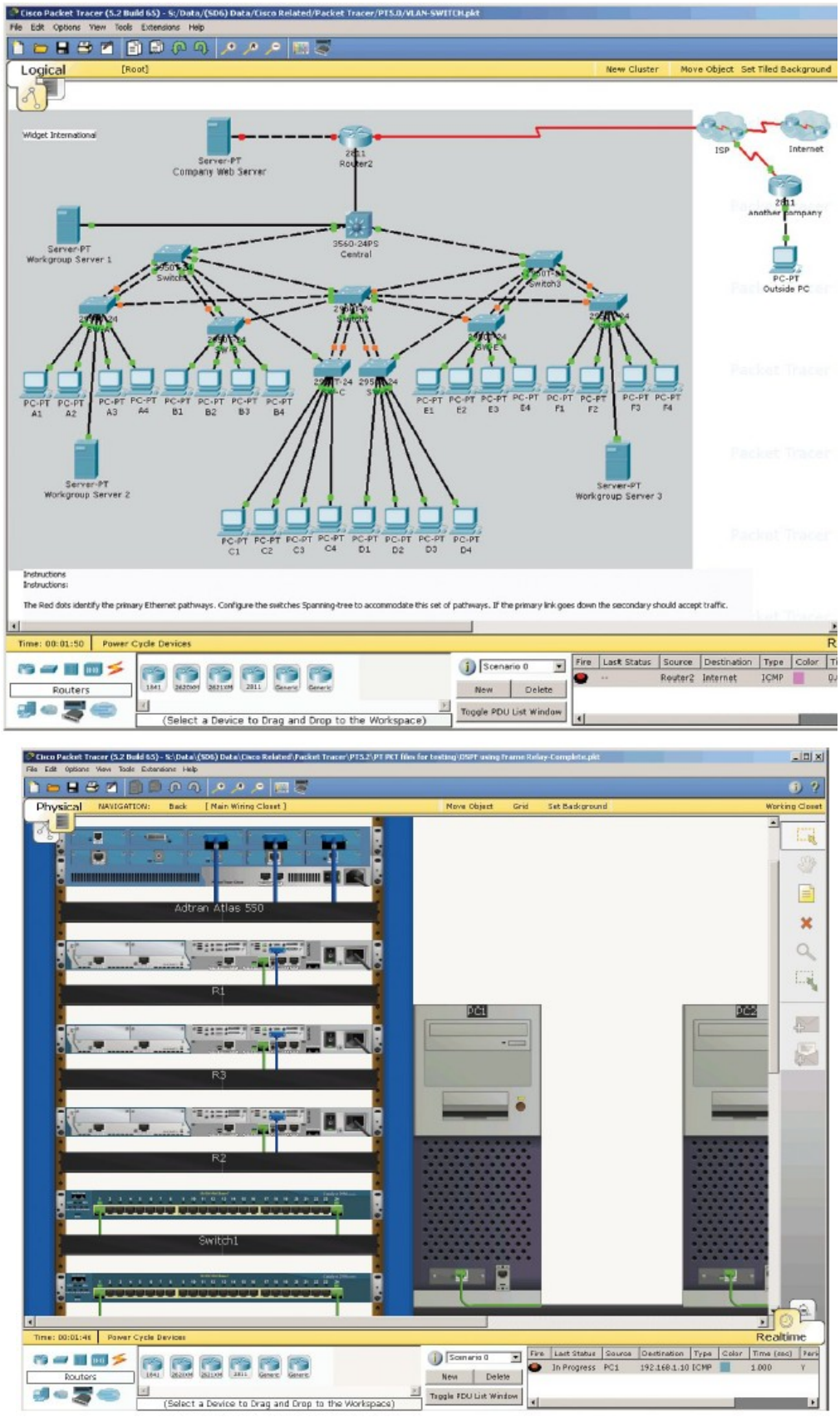

FIGURA 41: interface do Packet Tracer (configuração de ambiente de rede e configuração do hardware)

3.6. PROPOSTA DE QUALIDADES IDEAIS PARA UMA INTERFACE DE ENSINO DE *FIREWALL*

A arte de ensinar o funcionamento interno de um *firewall* é parte essencial que integra estudos de redes de computadores em disciplinas de curso de graduação bem como cursos de especialização que envolvam redes de computadores. Trata-se de um processo minucioso, fazendo o aluno conhecer cada opção e caminhos possíveis a um pacote de dados. São pequenas particularidades através das quais o conjunto de regras do *firewall* permite um resultado final esperado. Este conjunto de regras, nunca está definitivamente pronto, ele apenas alcança momentos de equilíbrio, de estabilidade, podendo por influência de fatores diretos ou indiretos, sempre receber melhorias e alterações de seu autor ou terceiros. Neste processo de melhoria o uso de recursos visuais amparados pelos conceitos de semiótica e interface, pode ser de fundamental importância para fins acadêmicos. A utilização de tais recursos, pode permitir a visualização do funcionamento de um *firewall* de modo que o usuário veja de uma forma reconhecível pelo seu modelo mental, o caminho e ações tomadas para cada pacote de dados que chega. O processo de criação bem como o de melhoria das regras, torna-se mais atraente ao usuário e consequentemente torna-se eficiente. É promovido aqui uma melhor interação homem-máquina, criando a tríade signo-objeto-interpretante, elementos que no modo tradicional de definição das regras, bem como do ensino desta técnica, são bem mais abstratos e menos compreensíveis.

Embasando-se nas informações levantadas acerca de signos e interfaces, é identificado e proposto aqui uma seleção de seis qualidades inerentes à interface de ensino e gerenciamento de *firewall* (Figura 42). Esta afirmação não implica que as demais interfaces não sejam eficientes, pois trata-se de outra forma de apresentação de informações. Tais qualidades em conjunto, poderão propiciar que esta interface culmine em uma qualidade estética eficiente, permitindo uma associação de valores coerentes, onde os objetos determinem signos eficazes no interpretante. Isto permitirá ao usuário utilizando-se de seu modelo mental, a interpretação correta objetivada pela interface. Em outras palavras, uma interface compreendível, aprendível, operável e atraente ao usuário.

As qualidades então levantadas são: exclusão de informações desnecessárias, adequação da velocidade à percepção humana e a utilização de sistema múltiplo de memória. Esta última contempla quatro características: definição de uma representação visual artificial ou metafórica, combinação de arte e engenharia, utilização de espaço e profundidade e por último, utilização de memória espacial. Todas estas qualidades são descritas a seguir.

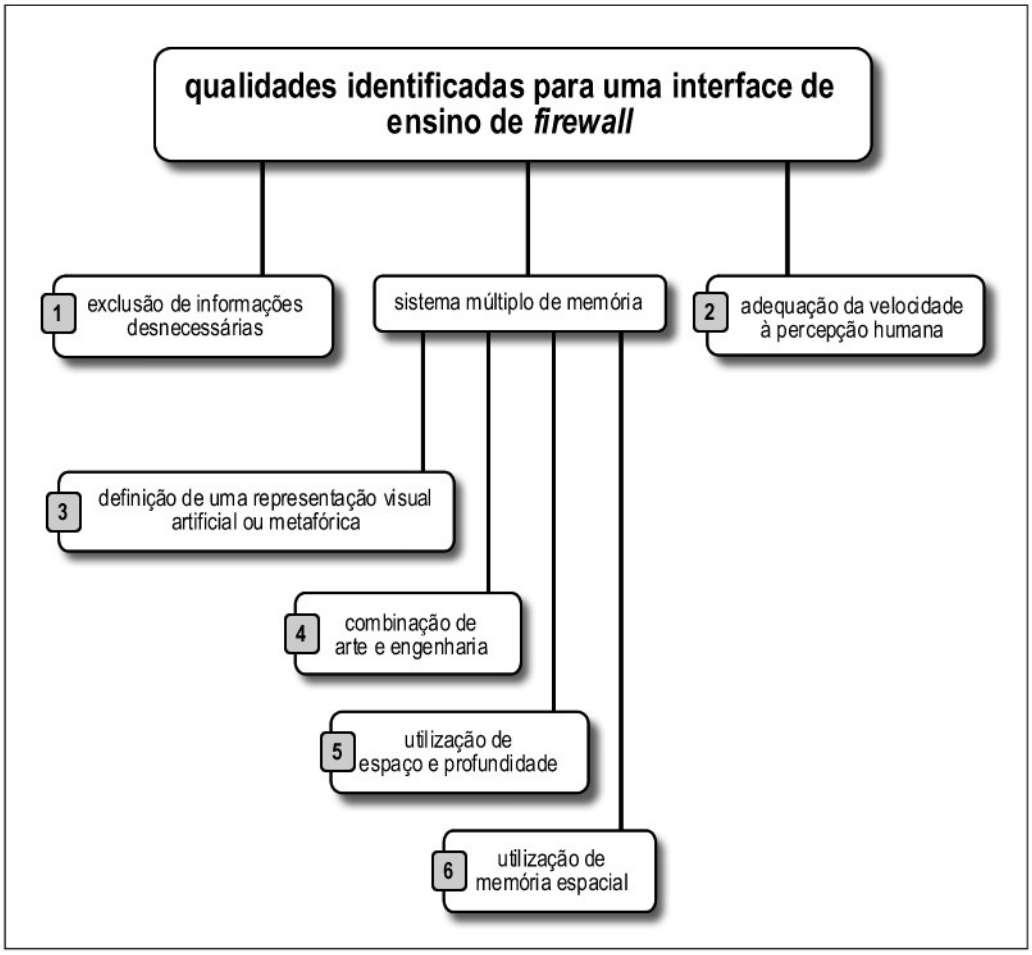

FIGURA 42: organograma das qualidades propostas à interface de ensino de firewall

3.6.1. Exclusão de informações desnecessárias

É uma característica de objetividade da interface. Assim como o desenho proposto por Becker referente ao metrô de Londres, constitui-se de manter apenas as informações necessárias, neste caso ao momento do aprendizado e visualização do funcionamento do *firewall*. Quando da criação de uma regra qualquer, o usuário quer visualizar apenas o trajeto do pacote dentro do *firewall* e não vê-lo passar de um *host* de uma rede para um *host* em outra rede, tendo o *firewall* apenas como um ponto de passagem. O objetivo é visualizar justamente dentro do *firewall*, e não o caminho completo do pacote.

3.6.2. Adequação da velocidade à percepção humana

Esta é uma característica temporal do ciberespaço e que se faz uma qualidade indispensável para a concretização do processo de ensino de funcionamento do *firewall* ou simplesmente análise do seu funcionamento. Considerando um *firewall* com regras já carregadas, é através desta qualidade que o usuário poderá ter consciência dos caminhos e ações sobre os pacotes de dados no interior do *firewall*.

3.6.3. Definição de uma representação visual artificial ou metafórica

Esta qualidade refere-se à composição artística de todo o ambiente. A utilização de metáforas de *desktop* ou a utilização de objetos artificiais especialmente desenhados para a interface, enfim a forma de demonstrar os caminhos existentes dentro do *firewall* utilizando-se de arte. Esta qualidade é essencial para o momento da secundidade, da ética, da informação que chega ao indivíduo. É esta qualidade que ditará o ambiente a que se refere a interface e permitirá a associação de valores com o modelo mental do usuário. A interface passa a ter sentido interpretativo.

3.6.4. Combinação de arte e engenharia

Esta qualidade complementa a representação visual, objetivando tornar os resultados atraentes ao usuário. Considerando que se tenha uma visualização metafórica, os resultados apresentados, sejam simples linhas com regras, ou a forma de propagação do pacote pelo ambiente, estes devem ser condizentes com o todo. Esta qualidade é essencial para o momento da primeiridade, da estética, do dado que chega à mente do usuário intérprete, afim de associá-lo ao ambiente.

3.6.5. Utilização de espaço e profundidade

Qualidade de utilização de janelas e mapeamento de bits, o que mais popularmente é conhecido como interface gráfica. Talvez seja uma das qualidades que em um primeiro

momento prenda a atenção do usuário, instigando a conhecer mais um pouco do que se está vendo, seja por curiosidade, repulsa ou interesse pela imagem do ambiente visualizado.

3.6.6. Utilização de memória espacial

Refere-se à possibilidade de “flutuar” dentro do ambiente composto de localizações espaciais, como a maquete de uma cidade, uma cidade virtual e no caso do *firewall*, a flutuação em um ambiente de metafórico como o de um *game*.

3.7. CONCLUSÃO

Conforme RIBEIRO (2009, p.117) apud MANOVICH (2007), novas relações de percepção com a tecnologia são incorporadas nas interfaces atuais, onde o usuário passa a exigir interfaces amigáveis, interativas, divertidas, satisfatórias, enfim atraentes e eficazes. Esta dissertação não objetiva desmerecer qualquer uma das interfaces citadas, mas sim propor uma nova relação de percepção, propondo uma interface atraente e eficaz. Todas as qualidades aqui eleitas, em conjunto são um potencial propiciador de tais qualidades. Assim é proposto em seguida, uma interface para visualização do funcionamento interno do *firewall* utilizando-se de tais qualidades.

4. PROPOSTA DE INTERFACE PARA VISUALIZAÇÃO DINÂMICA

Tendo com respaldo os últimos quatro anos ministrando disciplinas ligadas a redes de computadores em curso superior de sistemas de informação, este pesquisador identificou a dificuldade por parte dos alunos em compreender o funcionamento interno de um *firewall*. Esta dificuldade não se refere ao conceito, ao objetivo do mesmo, mas sim ao funcionamento interno do *firewall* mediante as mais diversas configurações através de regras de controle então definidas. Foi percebida uma certa dificuldade em abstrair e visualizar os acontecimentos neste interior, o tráfego de pacotes, as situações de verificações de proibição, permissão, roteamento. Enfim, o funcionamento em condições reais e como o *software* se porta diante de um pacote de dados.

O ensino de redes de computadores neste referido período, foi auxiliado por algumas das ferramentas as quais tiveram suas interfaces aqui analisadas. Como se pôde ver pelos resultados das análises, tais ferramentas são eficientes para se compreender a rede como um todo, mas inexiste recursos específicos para o interior do *firewall*, ou seja, suas ações diante de pacotes que chegam.

Um outro motivador desta proposta de interface é o filme *Warrios of the Net*[24]. O filme tem aproximadamente dez anos, o que pode ser considerado como obsoleto quando se fala em tecnologia. Mas apesar da idade, ele demonstra de forma atraente, a vida útil de um pacote de dados. Simulando uma requisição de acesso a um serviço *web* qualquer, é demonstrado desde a saída do *host* do usuário, a passagem pela rede interna, *firewalls*, até a chegada ao servidor *web* onde se localiza o destino do pacote. Durante o trajeto, o *firewall* é apresentado de forma muito resumida, porém atraente ao usuário, demonstrando as decisões do mesmo mediante as regras de controle. Pode-se dizer sem dúvidas que este vídeo é um bom auxílio para aulas de redes, porém é um recurso estático e sem qualquer interatividade.

A seguir são apresentados através de esboços, uma proposta de interface para visualização dinâmica do funcionamento interno do *firewall*, interface esta inicialmente exclusiva para fins didáticos em estudo de redes de computadores, seja em cursos de nível superior, especializações, bem como cursos de extensão. Em um primeiro momento foi cogitado a utilização desta interface também para o gerenciamento de um *firewall*, porém normalmente administradores experientes na sua grande maioria, realizam a configuração manualmente, escrevendo cada regra de controle que precisa.

---

24 Disponível em http://www.warriorsofthe.net

A representação da lógica interna do *firewall* é aqui baseada no fluxograma(Figura 25) criado nesta dissertação para representar o funcionamento do Netfilter.

4.1. ESBOÇO E FUNCIONAMENTO DO AMBIENTE

A Figura 43 apresenta um esboço geral, uma proposta de visão inicial materializada do *firewall* e o contexto no qual será inserido.

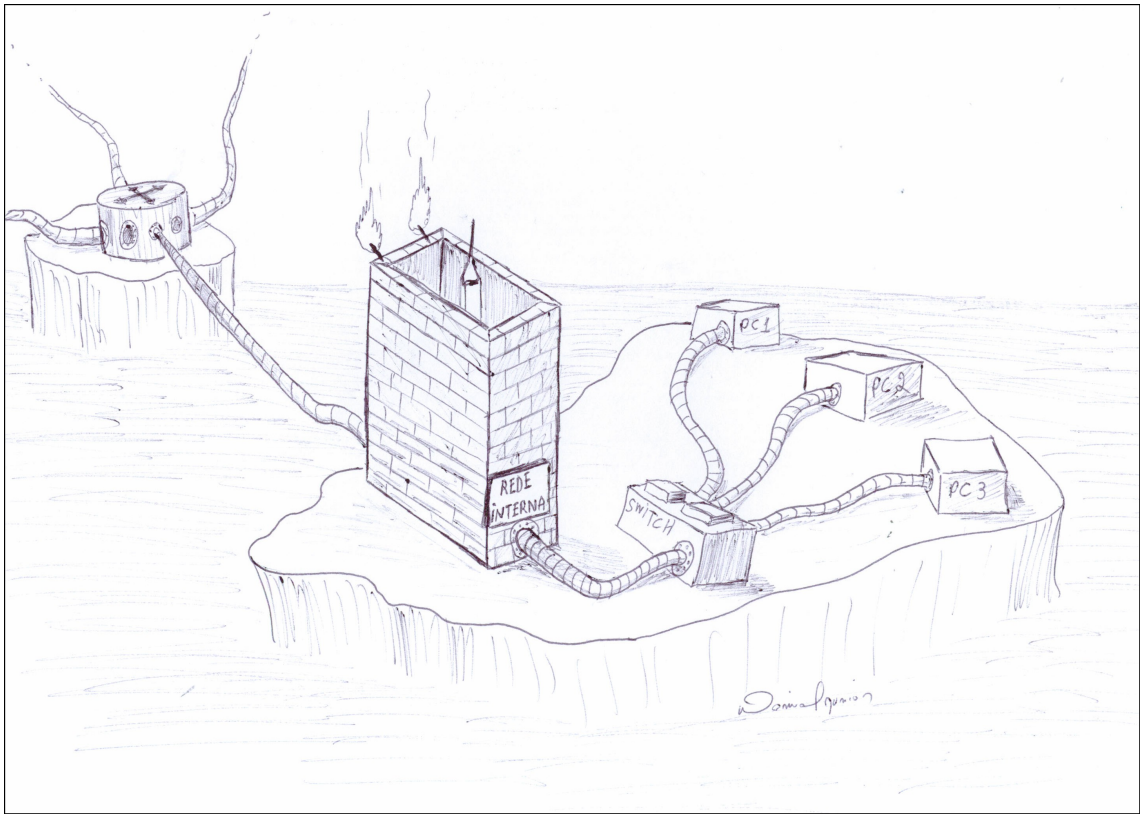

FIGURA 43: visão geral do contexto no qual o firewall está inserido

O *firewall* bem como cada equipamento envolvido no qual deva passar um pacote, são representados por edificações, as quais são interconectadas por tubulações, estas como único modo de viagem de um pacote. Observa-se ainda que o *firewall* fica localizado na borda da rede interna, então representada por uma ilha. Inicialmente esta interface é focada em *firewall* de borda, mas isso não impede de testar regras para outros contextos de funcionamento, como *personal firewall* por exemplo. A Figura 44 apresenta uma visão em destaque do *firewall* localizado na borda da rede.

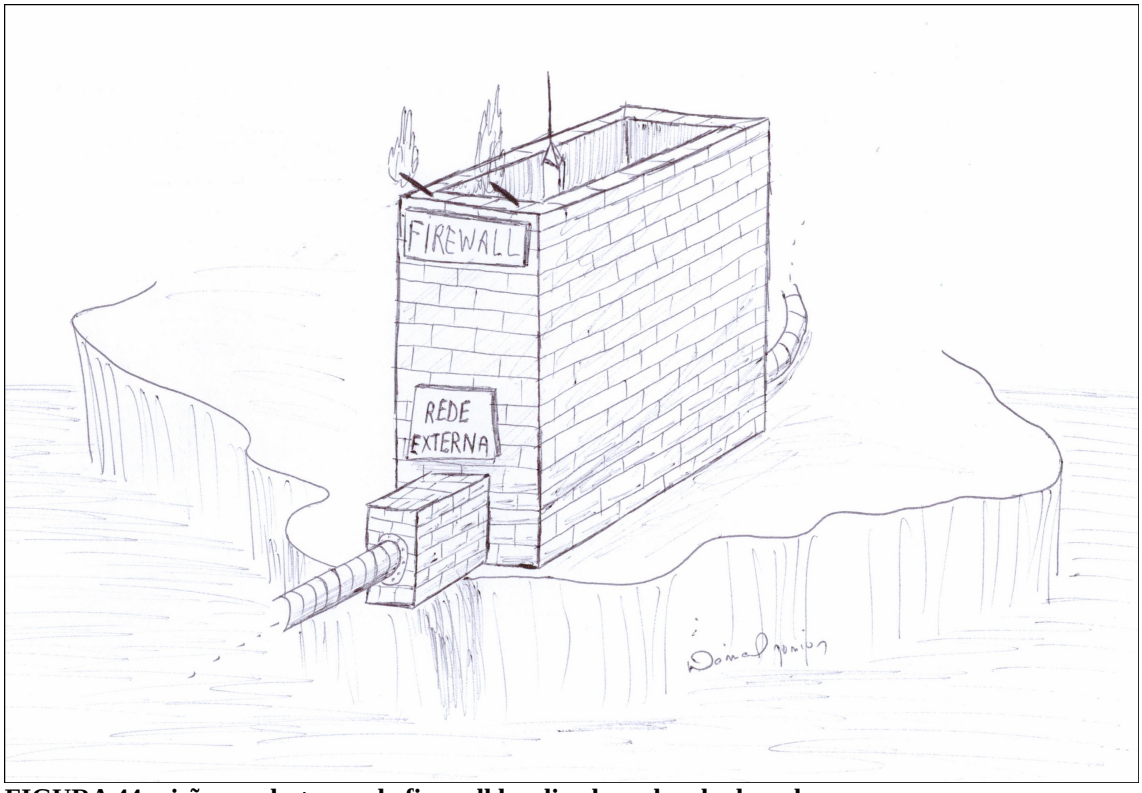

FIGURA 44: visão em destaque do firewall localizado na borda da rede

Olhando mais especificamente para o interior, para dentro dos muros do *firewall*, então proposto na Figura 45, observa-se uma visão geral dos componentes do mesmo, bem como os caminhos tomados pelos pacotes mediante a configuração das regras de controle. Porém um fator importante deve ser levado em consideração: no lado esquerdo da figura deve estar a rede que originou o pacote, ou seja, pode ser a rede interna quanto a internet. Logo, o lado direito fica a rede destino. Assim, observa-se na Figura, que deve ser considerado o sentido de entrada do pacote, isto é, estar atendo a quem é rede origem e rede destino.

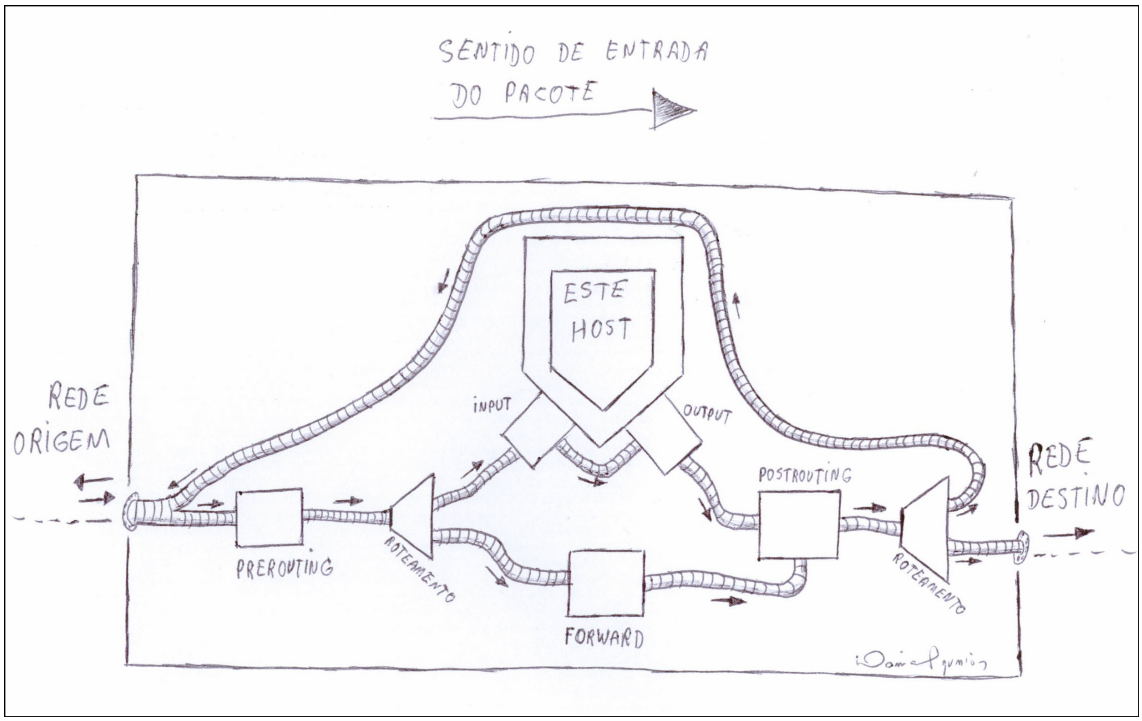

FIGURA 45: visão superior do ambiente interno do firewall

Neste ambiente de proposta de interface, são quatro os possíveis fluxos existentes:

a) O fluxo de um pacote originado de uma rede qualquer e com destino a uma próxima rede, será definido da seguinte forma: PREROUTING, roteamento, FORWARD, POSTROUTING, roteamento e enfim sai para a rede destino.

b) O fluxo de um pacote originado de qualquer lugar e com destino ao próprio *host firewall*, será definido como: PREROUTING, roteamento, INPUT, entra no *host* ou vai direto para OUTPUT em caso de rejeição.

c) O fluxo que sai do *host* pode ser uma resposta ao fluxo anterior, e neste caso será: OUTPUT, POSTROUTING, roteamento e então retorna à rede origem.

d) A última situação é onde o *host* origina um pacote com destino a qualquer lugar. Neste caso o fluxo será: OUTPUT, POSTROUTING, roteamento e sai para a rede destino.

Os elementos componentes deste ambiente interior são descritos a seguir.

4.1.1. PREROUTING

PREROUTING é a primeira checagem feita em todos os pacotes que chegam. A Figura 46 demonstra a materialização do local deste momento inicial. Observa-se em detalhe uma placa de identificação com o IP da placa de rede que está recebendo o pacote.

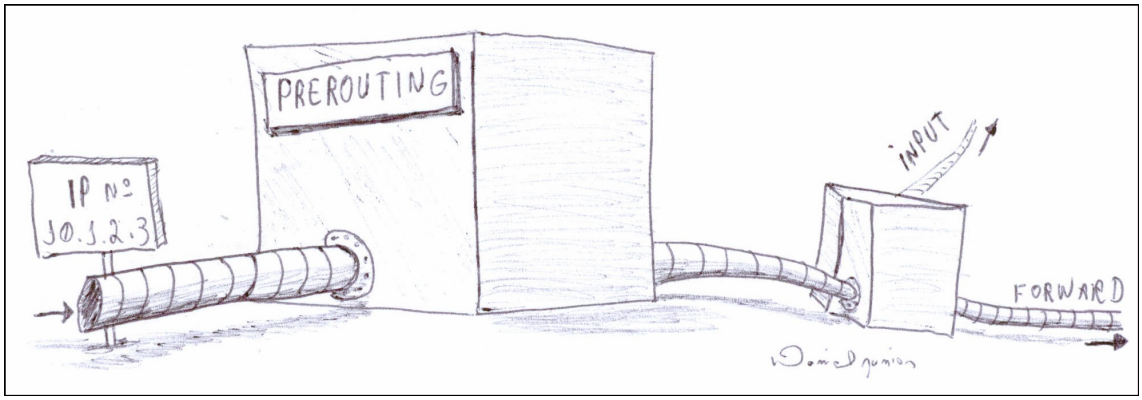

FIGURA 46: materialização do PREROUTING na interface

O funcionamento do PREROUTING é demonstrado na Figura 47. Ao chegar o pacote é colocado em uma esteira, a qual o conduzirá pelas checagens feitas por máquinas de raio-X. As verificações feitas são:

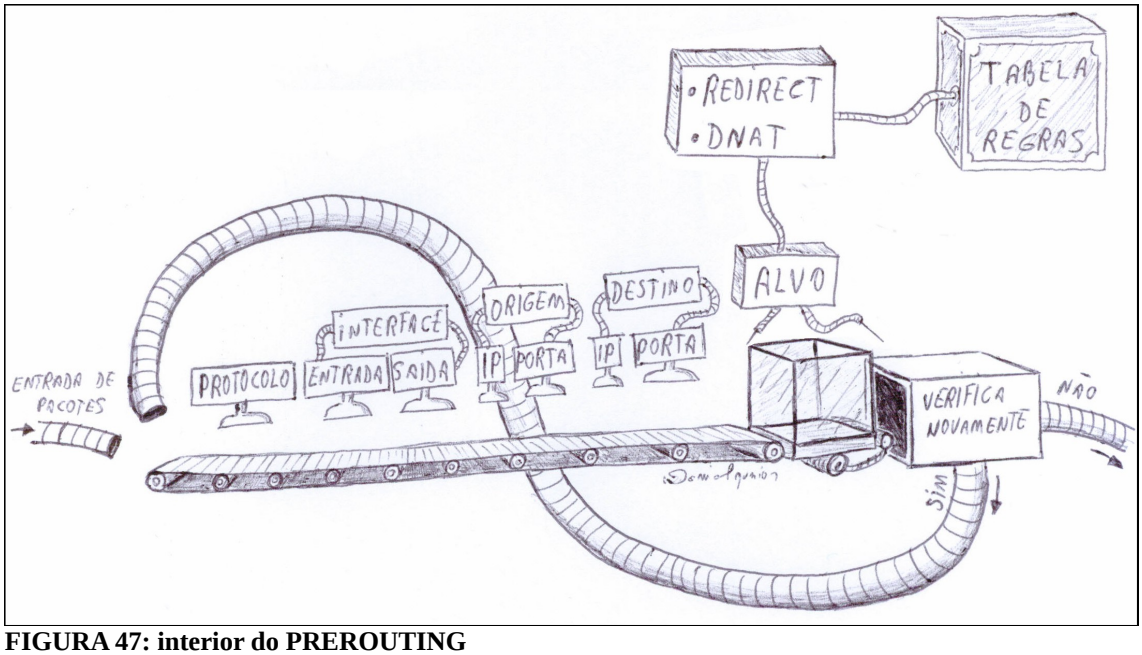

FIGURA 47: interior do PREROUTING

a) protocolo: tipo de protocolo, podendo ser (nesta interface) TCP ou UDP

b) interface de entrada e de saída: esta informação não vem com o pacote IP, mas será identificada a placa de rede afim de facilitar a localização na tabela de regras. A interface de saída será sempre com valor em branco, pois o pacote ainda não sabe o caminho de saída.

c) origem IP e porta: o número IP e o número da porta que originaram o pacote.

d) destino IP e porta: o número IP e o número da porta aos quais o pacote é destinado.

Feitas estas verificações, tem-se o alvo, isto é, a ação que o PREROUTING deverá realizar diante deste pacote. As suas opções são REDIRECT e DNAT, ações estas que serão realizadas mediante consulta à tabela de regras específicas de PREROUTING.

A tabela de regras do PREROUTING é demonstrada na Tabela 2 contendo três regras a título de exemplo. A descrição das regras é como segue:

- Regra 1: faz com que todo o tráfego originado da placa eth1 com destino a porta 80 seja redirecionado para a porta 3128. Esta é uma ação de REDIRECT.
- Regra 2: faz com que pacotes TCP destinados a 10.1.2.3:20100, sejam direcionados para 192.168.100.100:5900. Esta é uma ação de DNAT.
- Regra 3: faz com que pacotes UDP da rede 192.168.100.0/24 originados pela placa eth2 e com destino a 10.1.2.3:22, sejam direcionados para 192.168.100.50:22. Esta também é uma ação de DNAT.

Nº da regra	Prot.	Placa de Rede		Origem		Destino		Ação
		IN	OUT	IP	Porta	IP	Porta	
1	*	eth1	*	0/0	*	*	80	REDIRECT - Redirecionar a porta destino para para a porta 3128
2	TCP	*	*	0/0	*	10.1.2.3	20100	DNAT - Alterar o IP destino para 192.168.100.100 e a porta destino para 5900
3	UDP	eth2	*	192.168.100.0/24	*	10.1.2.3	22	DNAT – Alterar o IP destino para 192.168.100.50 e porta destino 22

Tabela 2: regras de PREROUTING

Suponha-se a chegada de um pacote originado do IP 51.4.4.4 e com destino ao IP 10.1.2.3 e porta 20100. Este pacote terá o endereço de destino do pacote alterado para 192.168.100.100 e porta destino alterada para 5900. Na interface proposta, esta alteração é feita através de cabos conectores ao estilo “matrix” que se inserem no pacote IP e executam a modificação. Feito isto, o pacote segue para as próximas verificações do *firewall*.

Após definido o alvo, isto é, realizado a ação necessária no pacote, o pacote deverá ser submetido à verificação pelas demais regras do *firewall*, isto caso não tenha atendido todos os requisitos da regra atual recém utilizada.

Ainda no mesmo exemplo, suponha-se a chegada de um pacote originado do mesmo IP 51.4.4.4 e com destino ao IP 10.1.2.3 e porta 34000. Este pacote não será atendido por

nenhuma regra, passando adiante, pois o PREROUTING não tem como função fazer bloqueios de pacotes, encaminhando-o adiante.

4.1.2. Primeiro roteamento

Conforme visualizado na Figura 46, o próximo passo após o PREROUTING, é um roteamento. Este é o primeiro roteamento que acontece dentro do *firewall*. Nele, o pacote se depara com uma bifurcação conforme apresentado na Figura 48. Caso o pacote tenha como destino o próprio *host firewall*, ele toma o caminho à esquerda(INPUT), caso contrário, ele é repassado(FORWARD). Esta identificação é feita através de uma máquina de raio-X localizada no meio da bifurcação. A Figura 49 apresenta uma visão superior para melhor identificação dos componentes, dentre eles a plataforma de identificação, local onde o pacote aguarda ser analisado e que depois rotaciona direcionando o pacote para o caminho correto.

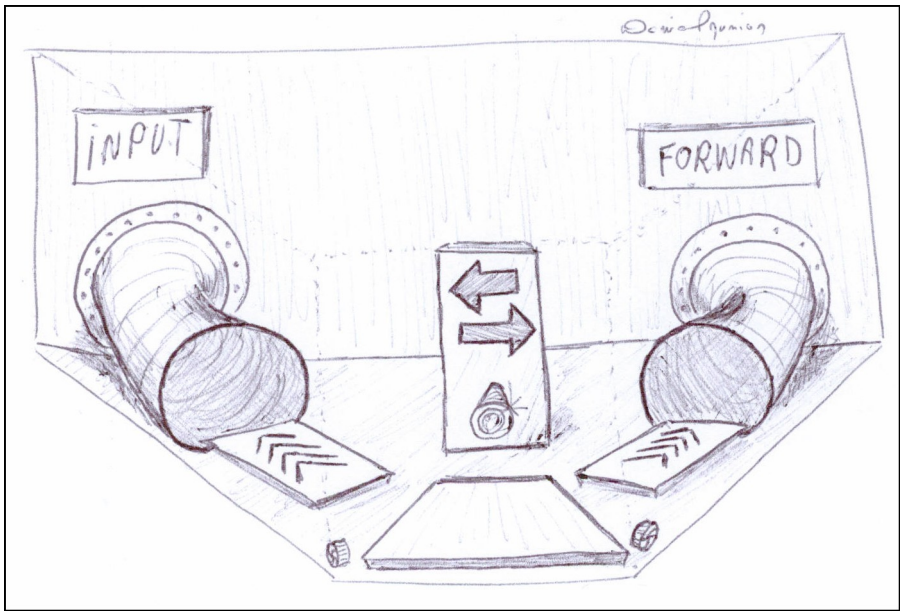

FIGURA 48: interior do primeiro roteamento

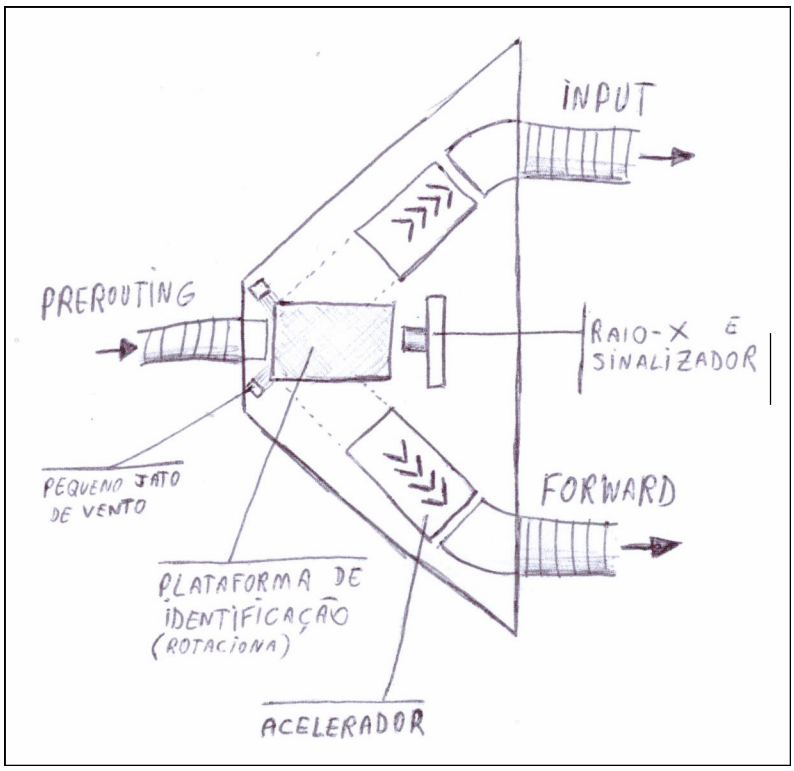

FIGURA 49: visão superior do primeiro roteamento

4.1.3. FORWARD

Quando o pacote não tem como destino o *host firewall*, ele é repassado (vai para o FORWARD). O FORWARD (Figura 50) recebe o pacote do primeiro roteamento e caso seja permitido enviará o pacote para o POSTROUTING. A análise realizada pelo FORWARD é demonstrada na Figura 51, a qual trata-se de um esboço do funcionamento do mesmo, utilizando conceitos de uma linha de produção.

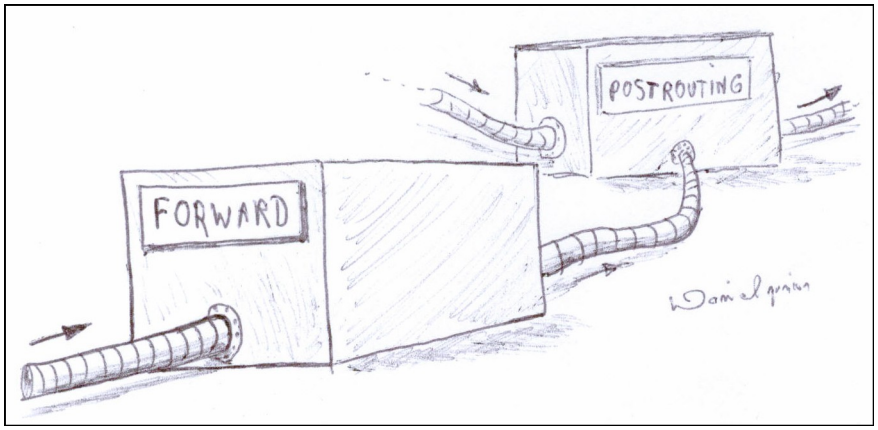

FIGURA 50: materialização do FORWARD na interface

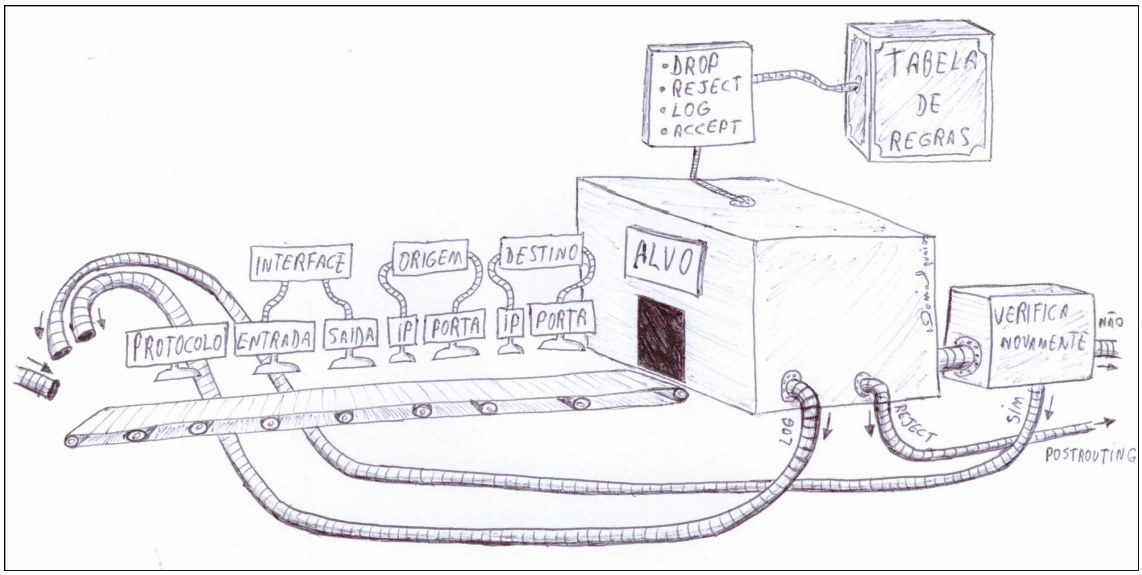

FIGURA 51: interior do FORWARD

O pacote chega e é colocado na esteira, a qual o conduzirá pelas checagens feitas por máquinas de raio-X. As verificações feitas são similares às realizadas no PREROUTING, dispensando uma nova explicação.

Feitas estas verificações, tem-se o alvo, isto é, a ação que o FORWARD deverá realizar diante deste pacote. As suas opções são: negação do pacote (DROP), rejeição (REJECT), registro em arquivo de log (LOG) e aceitar o pacote (ACCEPT). Estas ações serão realizadas mediante consulta à tabela de regras específicas de FORWARD.

A tabela de regras do FORWARD é demonstrada (Tabela 3) contendo quatro regras a título de exemplo. Observa-se que a estrutura de todas as tabelas de regras são iguais.

Nº da regra	Prot.	Placa de Rede		Origem		Destino		Ação
		IN	OUT	IP	Porta	IP	Porta	
1	*	*	*	0/0	*	*	53	Negar (DROP)
2	*	*	*	192.168.100.20	*	0/0	*	Rejeitar (REJECT)
3	*	*	*	192.168.100.0/24	*	13.7.6.5	3389	Registrar log (LOG)
4	*	*	*	192.168.100.0/24	*	13.7.6.5	3389	Aceitar (ACCEPT)

Tabela 3: regras de FORWARD

A descrição das regras é como segue:

- Regra 1: faz com que todo o tráfego originado de qualquer lugar e com destino à porta 53 seja negado (DROP). Neste caso, como se trata de FORWARD, nenhuma comunicação entre as redes adjacentes será realizado quando a porta destino for 53.
- Regra 2: faz com que todo o tráfego originado do IP 192.168.100.20 e tenha como

destino qualquer outra rede, seja rejeitado (REJECT). A ação de rejeição envia uma resposta ao IP origem informando da rejeição, sendo esta justificativa o diferencial em relação à negação.

- Regra 3: faz com que pacotes originados da rede 192.168.100.0/24 com destino ao IP 13.7.6.5 e porta 3389 devam ser registrados em arquivo de LOG. Conforme demonstrado na Figura 50, quando se trata de LOG, este volta para o início da esteira para ser analisado novamente através da próxima regra de controle.
- Regra 4: faz com que pacotes originados da rede 192.168.100.0/24 com destino ao IP 13.7.6.5 e porta 3389 sejam aceitos (ACCEPT).

Após aplicado o alvo, se o pacote não atendeu todos os requisitos de uma regra, ou seja, se todos os elementos da linha da regra forem diferentes aos dados do pacote, ele volta para o início da esteira para verificação perante as demais regras, caso contrário ele pode seguir à diante. Um exemplo para entendimento deste sutil detalhe é o que se segue:

Considere um pacote com as seguintes características: tipo TCP, originado do IP 19.0.0.5 e porta 20222, entrando pela placa de rede eth1 e que vai sair pela eth2 (o *firewall* tem conhecimento das placas existentes e os possíveis caminhos), e tenha como destino o IP 192.168.100.130 e porta 5900. Se no FORWARD existir uma regra conforme a Tabela 4, este pacote será verificado por esta regra e depois não haverá necessidade de nova verificação, pois todos os requisitos foram atendidos e podendo seguir em frente. Caso apareça um próximo pacote idêntico ao primeiro, com exceção da porta de origem como sendo 20223, este já não vai atender a todos os requisitos. Se apenas um requisito já não é atendido como este caso, o pacote deverá sofrer nova verificação, voltando ao início da esteira e verificado de acordo com as demais regras de controle. Esta situação é justamente um dos pontos mais complexos para o ensino em sala de aula, sendo de difícil abstração, mas que poderá ser resolvido com a implementação da interface proposta.

Nº da regra	Prot.	Placa de Rede		Origem		Destino		Ação
		IN	OUT	IP	Porta	IP	Porta	
1	TCP	eth1	eth2	19.0.0.5	20222	192168100130	5900	Negar (DROP)

Tabela 4: exemplo de regra de FORWARD com todos os requisitos preenchidos

Descrito este processo de análise, olhando ainda mais afundo na Figura 51, chega-se à estrutura do alvo. O interior é sugerido na Figura 52.

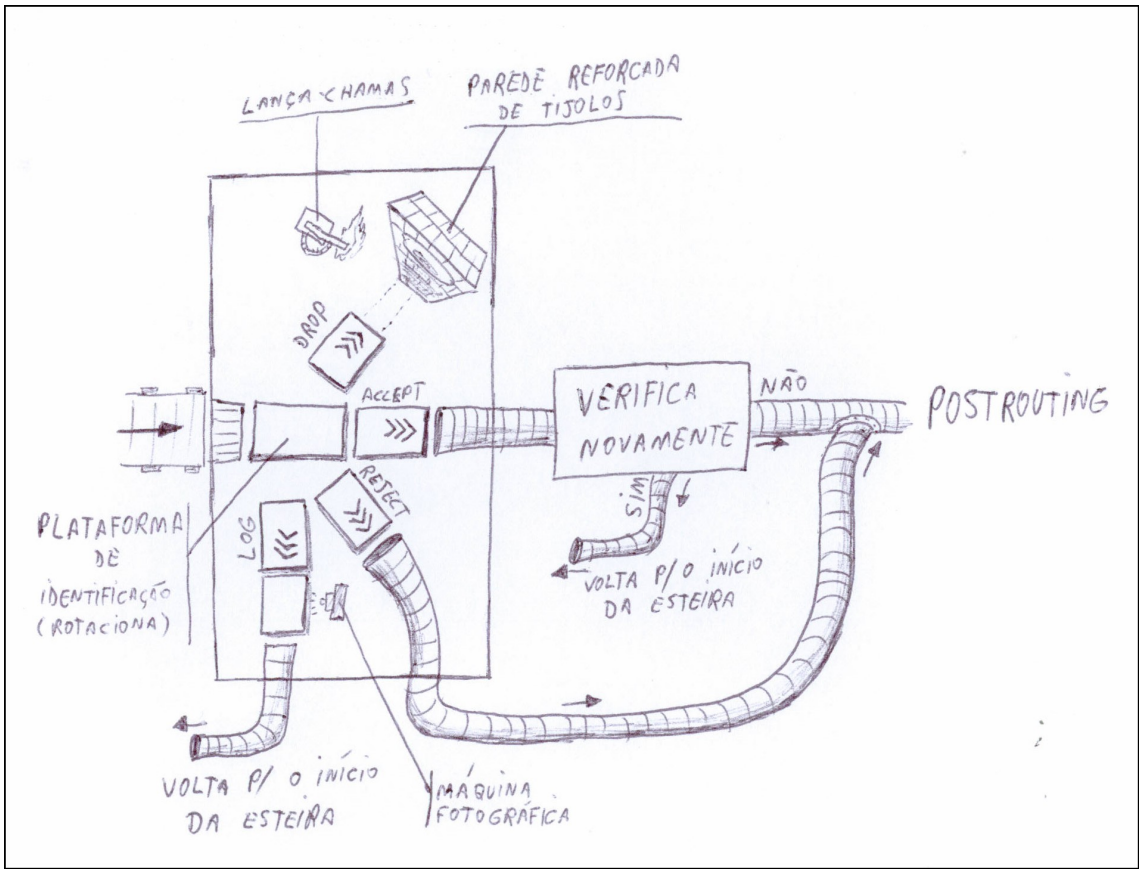

FIGURA 52: alvo do FORWARD

O pacote entra e uma plataforma de identificação já sabe o caminho que o pacote deverá tomar. Ela rotaciona posicionando o pacote no caminho determinado e então ele é empurrado para o seu destino.

O caminho do ACCEPT culmina na verificação se o pacote precisa ser analisado por outras regras, caso positivo ele volta, caso negativo ele segue adiante para o POSTROUTING.

O caminho de LOG possui uma máquina fotográfica, que assim como um radar em rodovias, registra o pacote e encaminha-o para o início da esteira.

O caminho de REJECT envia o pacote diretamente para o POSTROUTING, porém com a informação de rejeição, a ser identificada em um roteamento mais adiante. Observa-se que se o pacote já foi rejeitado, ele não precisa ser analisado por nenhuma outra regra.

Por fim o caminho do DROP posiciona o pacote e arremessa-o diretamente a um muro de tijolos reforçado, o qual é ainda incinerado por um lança-chamas, não havendo qualquer possibilidade de vida para este pacote, nem mesmo justificativa da sua morte a qualquer *host* na internet.

4.1.4. POSTROUTING

Após a exaustiva verificação no FORWARD, o pacote chega ao POSTROUTING (Figura 53) para então depois passar pelo segundo e último roteamento.

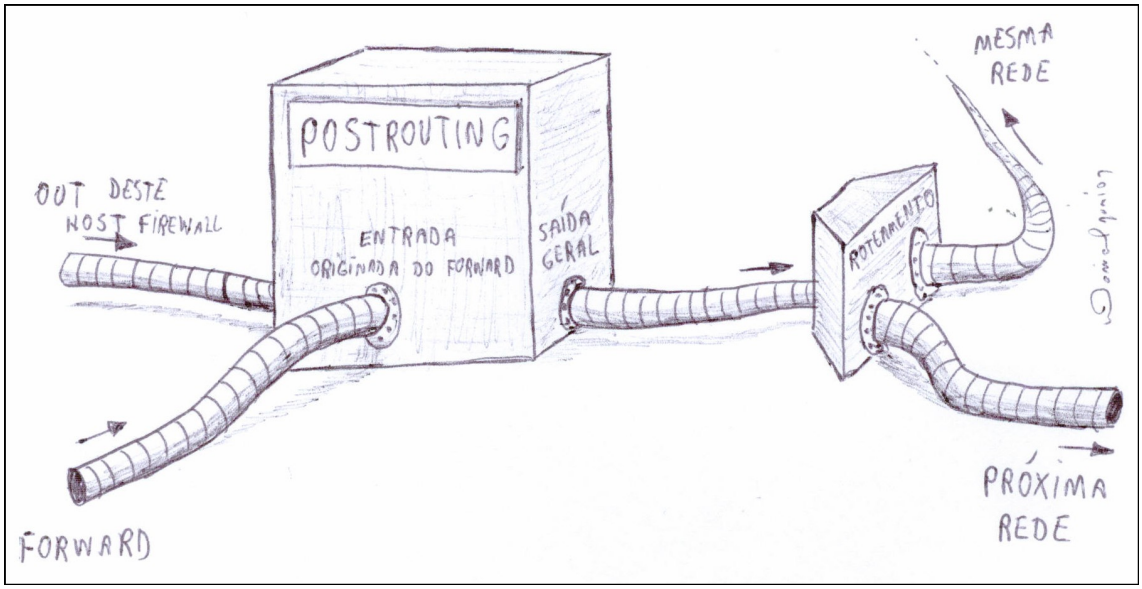

FIGURA 53: materialização do POSTROUTING na interface

O funcionamento interno do POSTROUTING é demonstrado na Figura 54. A verificação é a mesma realizada e descrita no PREROUTING, porém este recebe pacotes originados do FORWARD bem como pacotes originados da saída (OUT) do *host firewall* (explicado mais adiante). Também o alvo tem opções diferentes que são: MASQUERADE e SNAT. A Tabela 5 apresenta algumas regras de POSTROUTING envolvendo estas ações.

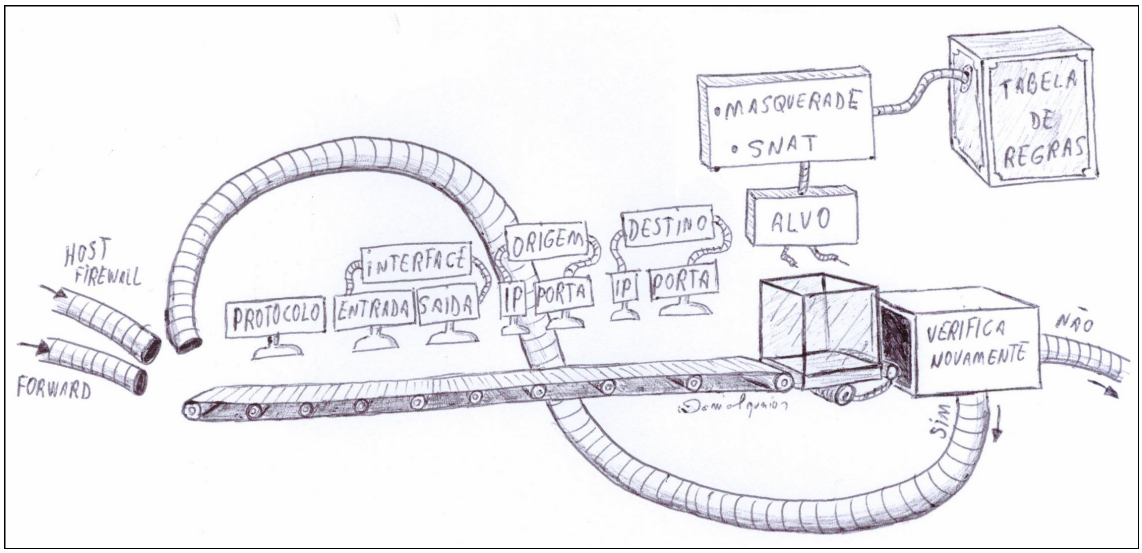

FIGURA 54: interior do POSTROUTING

Nº da regra	Prot.	Placa de Rede		Origem		Destino		Ação
		IN	OUT	IP	Porta	IP	Porta	
1	*	*	*	0/0	*	192.168.100.3	5900	MASQUERADE – ver qual é o IP da máquina *firewall* (por onde o pacote vai sair) e atribuí-lo ao pacote.
2	TCP	eth1	eth2	119.60.210.70	2003	192.168.100.3	3389	SNAT – alterar o endereço de origem do pacote para 192.168.100.254.

Tabela 5: regras de POSTROUTING

As regras da Tabela 5 são descritas da seguinte forma:

- Regra 1: faz com que todo o tráfego originado de qualquer lugar e com destino ao IP 192.168.100.3 na porta 5900, seja mascarado, isto é, tenha o seu endereço de origem alterado de forma que deste ponto em diante é como se o próprio firewall estivesse enviando o pacote. Obviamente é mantido um controle (Tabela 6) e caso o pacote precise de uma resposta, ela será associada e enviada ao verdadeiro host que originou o pacote.
- Regra 2: especifica que pacotes TCP originados do IP 119.60.210.70 porta 2003, que entram pela placa de rede eth1 e saem pela placa eth2 com destino ao IP 192.168.100.3 na porta 3389, tenham o seu endereço de origem alterado para 192.168.100.254. Em um primeiro momento o SNAT fez a mesma coisa que o

MASQUERADE, porém neste caso, ficou explicitado qual é o IP que deve ser substituído como nova origem do pacote. Assim como no MASQUERADE, o *firewall* mantem o controle para prover a resposta ao *host* correto.

n° de identificação do pacote	porta e IP origem	porta e IP destino
1	200.13.159.1:3245	192.168.100.3:5900
2	17.250.20.19:6017	192.168.100.3:5900

Tabela 6: controle de mascaramento feito no *firewall*

4.1.5. Segundo roteamento

Após concluído o trabalho de POSTROUTING, finalmente o pacote passará pela última etapa que é um segundo roteamento. Trata-se da edificação logo após o POSTROUTING conforme a apresentado na Figura 53. Este roteamento também é bem objetivo como o primeiro. A Figura 55 demonstra o seu interior onde uma máquina de raio-X identifica o destino do pacote como “mesma rede” e “próxima rede”. Mesma rede quando se trata de uma resposta deste *host* para alguém e próxima rede quando se trata de um pacote que está sendo repassado para frente. A Figura 56 exibe o interior de um outro ângulo, onde percebe-se mecanismos idênticos ao primeiro roteamento, como a plataforma de identificação que rotaciona para posicionamento e envio de pacotes.

Neste momento é encerrado o ciclo de vida do pacote no interior do *firewall*, pacote este destinado a outro local que não o *host firewall*.

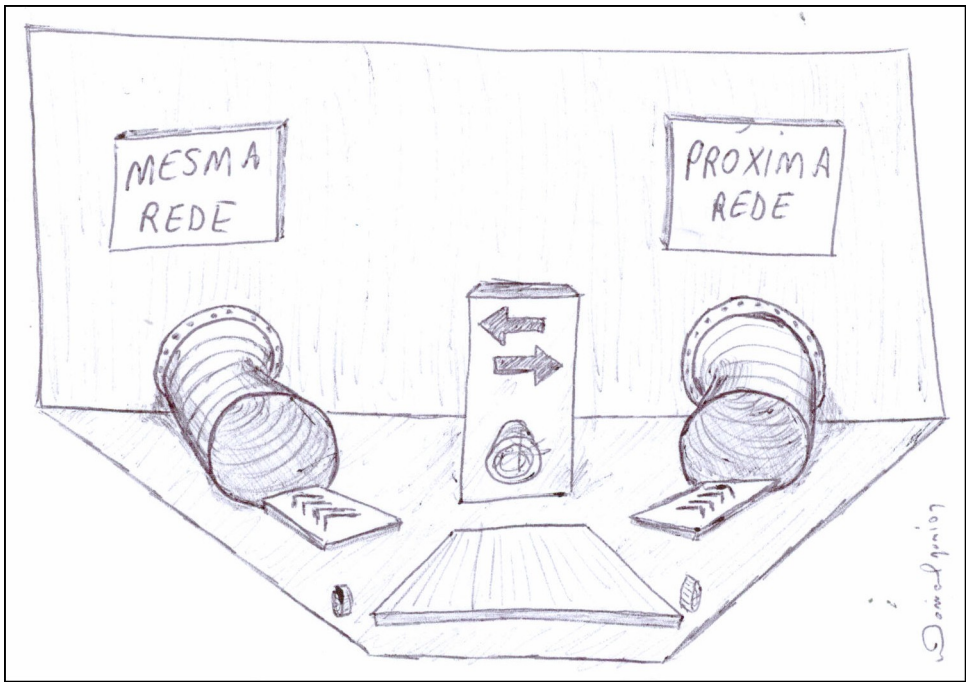

FIGURA 55: interior do segundo roteamento

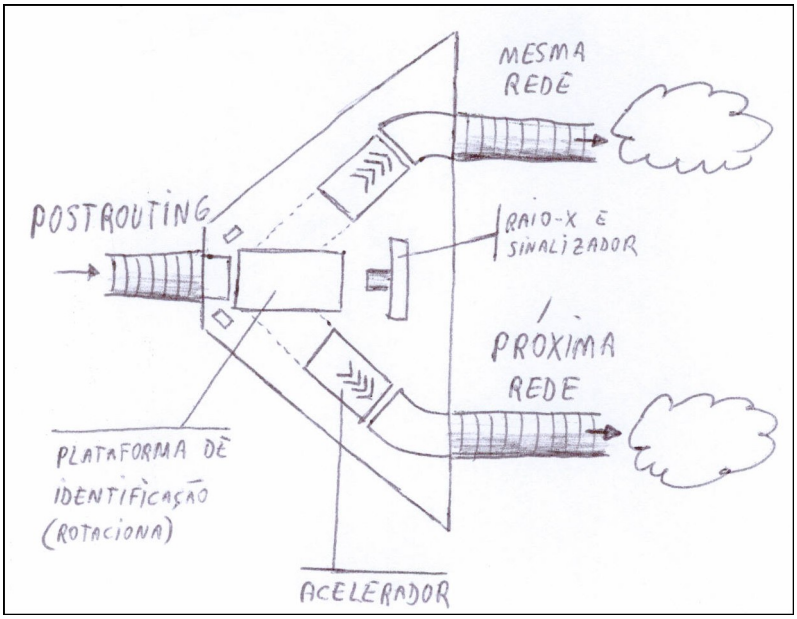

FIGURA 56: visão superior do interior do segundo roteamento

4.1.6. INPUT

Voltando ao primeiro roteamento (Figura 48), a outra opção disponível é o INPUT. Esta via recebe pacotes que são destinados ao próprio *host firewall*, o que inclui serviços

WEB, servidor de banco de dados, enfim, diversos serviços que não cabe aqui serem descritos, mas apenas saber que eles estão presentes neste próprio *host*.

Este *host* é um grande edifício (Figura 57). A função de *firewall* fica estabelecida no térreo. Os demais serviços como WEB e FTP, ficam estabelecidos nos andares superiores. Quando o pacote recém-chegado do primeiro roteamento se dirige à portaria que neste caso é o INPUT, o *firewall* decide-se entre três opções:

- Primeira: se o pacote pode subir para os andares superiores (serviços disponíveis).
- Segunda: se o pacote deve ser devolvido com algum aviso, isto é, rejeitado (em detalhe da mesma figura, pode-se observar o caminho rejeições saindo do INPUT diretamente para OUTPUT).
- Terceira: se ele deve ser simplesmente eliminado sem qualquer justificativa.

Para entender como é feita esta decisão, é necessário conhecer o interior do INPUT através da Figura 58. O pacote que chega, é jogado em uma esteira para ser submetido a várias verificações de raio-X de forma similar aos outros controles já descritos. Observa-se que um diferencial desta linha de verificação em relação às anteriores, é o alvo, o qual é constituído de uma outra edificação que tem o seu interior constituído conforme demonstra a Figura 59.

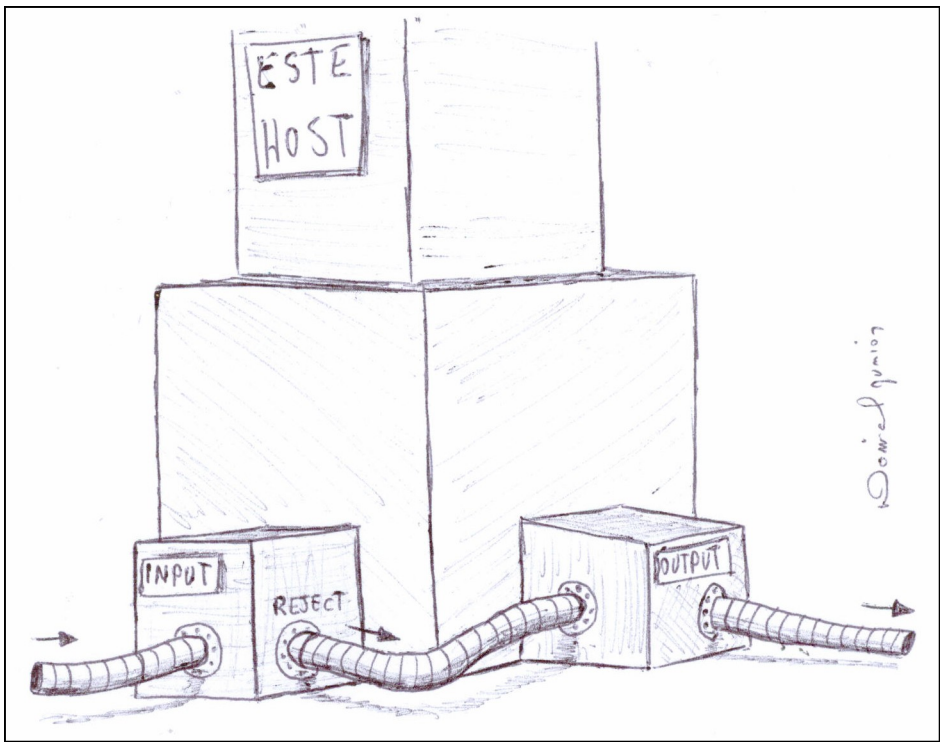

FIGURA 57: visualização do host firewall com INPUT e OUTPUT

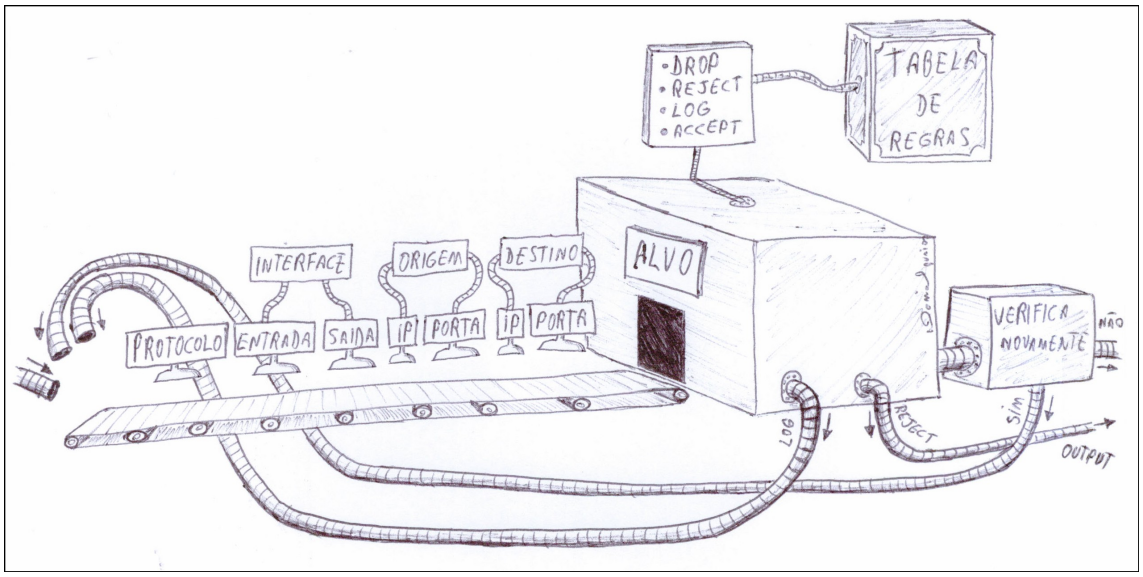

FIGURA 58: interior do INPUT

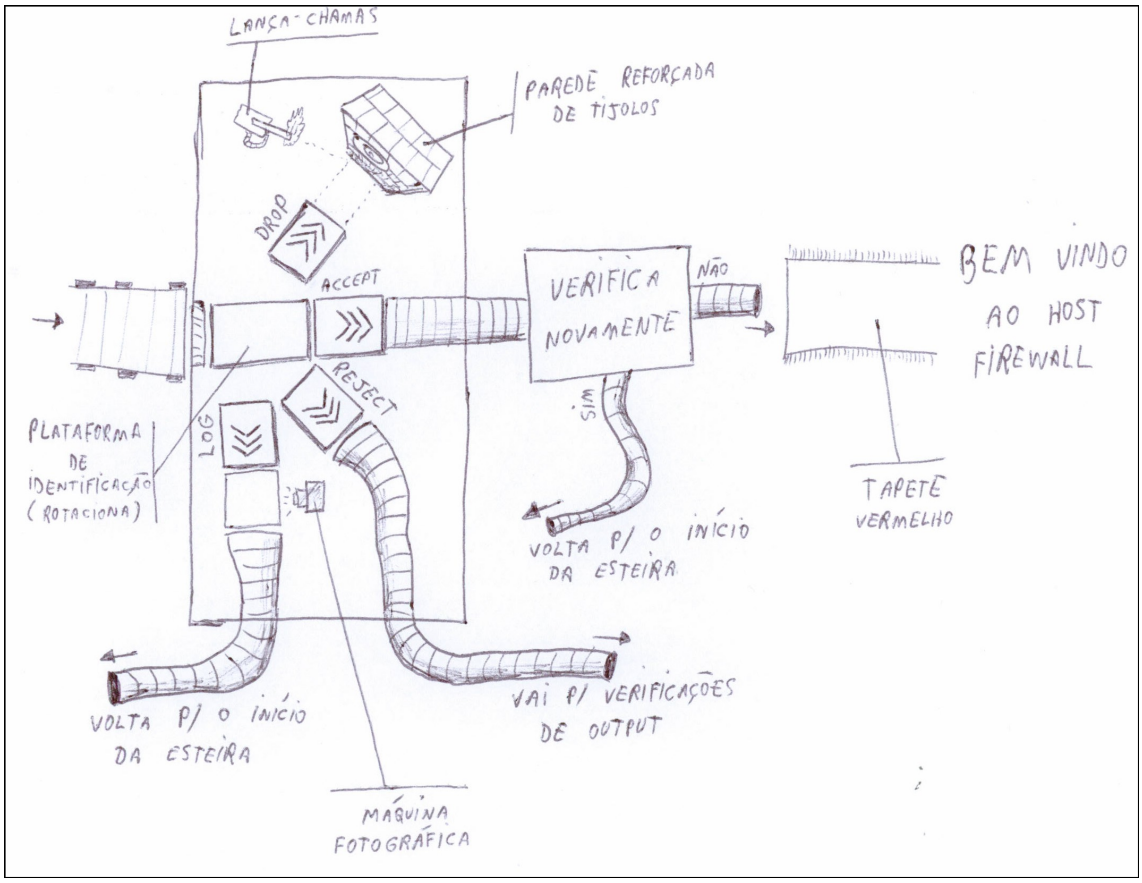

FIGURA 59: interior do alvo INPUT

Após a identificação das informações do pacote, ele será submetido a uma ação que

poderá ser DROP, REJECT, LOG e ACCEPT, já descritas anteriormente no item FORWARD. O pacote já tem o seu destino definido ao estacionar na plataforma de identificação e esta rotacionará direcionando-o para o caminho correto.

O caminho do ACCEPT culmina na verificação se o pacote precisa ser analisado por outras regras, caso positivo ele volta, caso negativo ele segue adiante para o *host*.

O caminho de LOG possui uma máquina fotográfica, que fotografa o pacote ao passar, fazendo assim um registro do mesmo e encaminha-o para o início da esteira.

O caminho de REJECT envia o pacote diretamente para a saída do *host*, isto é, o OUTPUT, pois é necessário informar à origem a rejeição do pacote, observando-se ainda que como o pacote foi rejeitado, não precisa ser analisado por nenhuma outra regra.

Por fim o caminho do DROP posiciona o pacote com destino à destruição, arremessando-o contra um muro de tijolos reforçado e incinerado por um lança-chamas, da mesma forma que no alvo do FORWARD.

Finalmente após tantas verificações, o que justifica bem o nome “muro de fogo” o qual transmite uma sensação de extrema dificuldade de se atravessar, o pacote é enviado por um tapete vermelho para o *host firewall*. O símbolo do tapete vermelho objetiva demonstrar justamente que o pacote merece todos os cuidados já que está habilitado a entrar.

A Figura 60 permitirá ao aluno ver a materialização de seus pensamentos em uma aula sobre *firewall*. O *host* é apresentado como um edifício cercado por uma enorme vala que o separa dos caminhos de entrada e saída. O transporte até este edifício só pode ser feito por plataformas voadoras denominadas IN e OUT, específicas para as finalidades conforme seus nomes.

Ao chegar pelo tapete vermelho, o pacote é posicionado na plataforma IN. Em seguida a porta destino deverá acender um indicador logo abaixo dela, atentando que ali entrará um pacote. Então a plataforma conduzirá o pacote até a porta, devendo ele adentrá-la e assim encerrar a jornada de INPUT para o *firewall.*

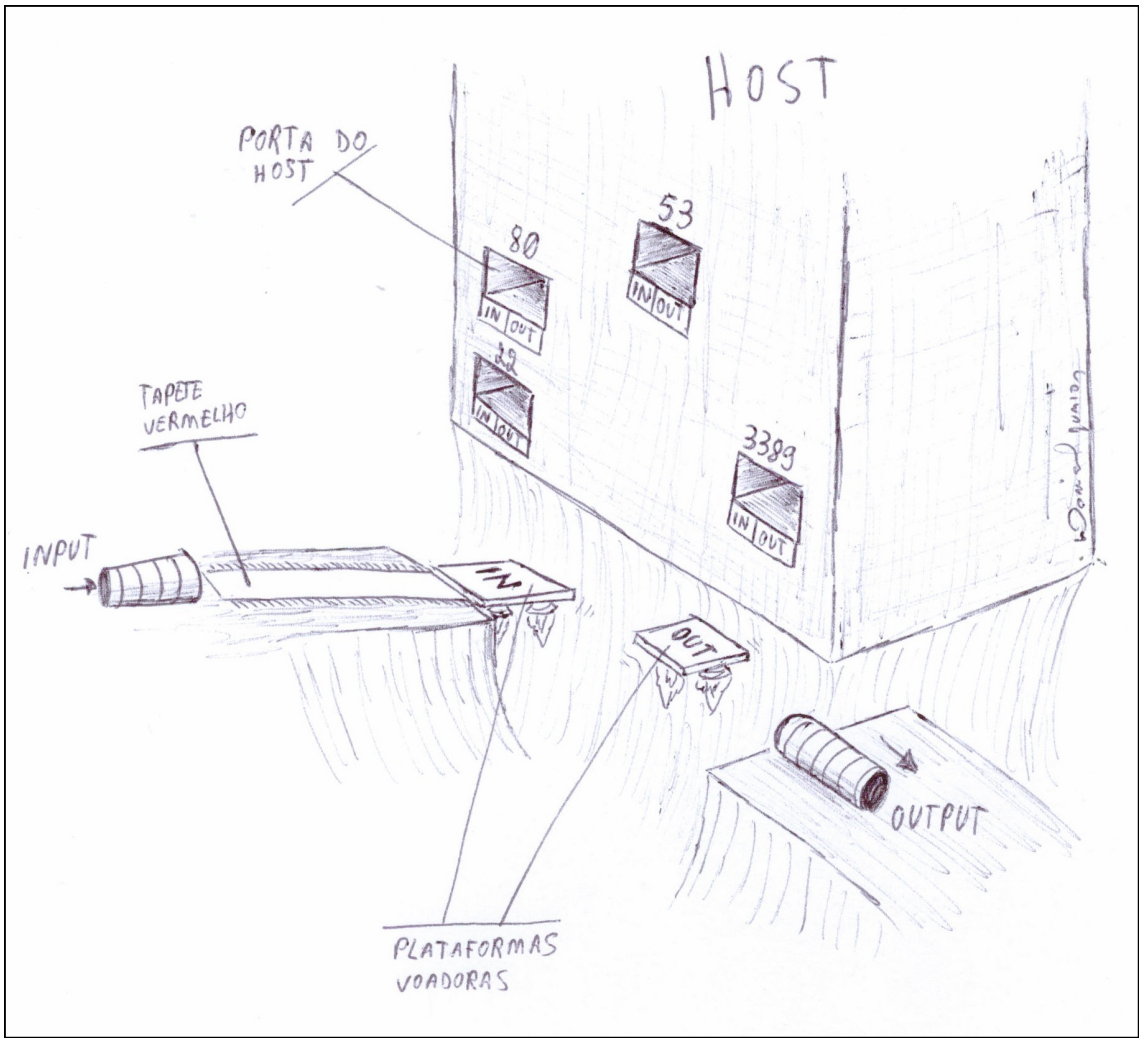

FIGURA 60: interior do host firewall (sistema de entrada e saída das portas)

4.1.7. OUTPUT

A jornada de um pacote originado do *host firewall* com destino a qualquer lugar começa na Figura 60. A porta que originou o pacote acende um indicador atentando que ali sairá um pacote. Então a plataforma OUT posiciona-se em frente a porta para que o pacote suba abordo. Em seguida ele é trazido à outra margem com destino ao OUTPUT.

A localização do OUTPUT já foi apresentado na Figura 57, e assim como o INPUT, ele fica acoplado ao prédio do *host.* O interior do OUTPUT é apresentado na Figura 61.

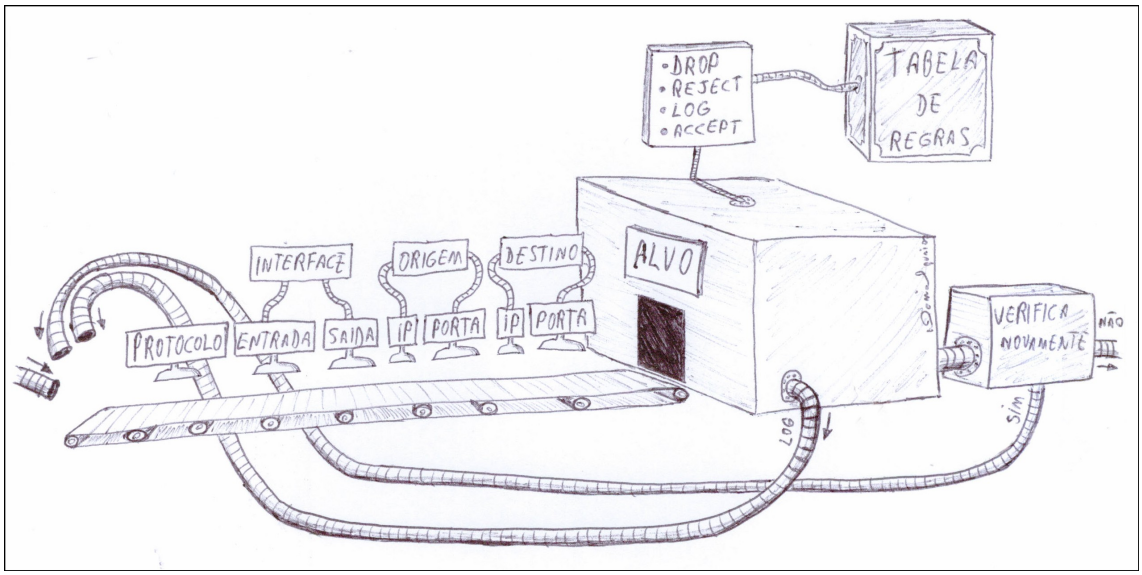

FIGURA 61: interior do OUTPUT

Como todas as outras linhas de verificação, aqui é feito da mesma forma. As máquinas de raio-X identificam o protocolo, placa de rede de entrada e saída, IP e porta origem e destino. Após identificadas estas informações, o pacote entra no alvo de OUTPUT que tem as mesmas ações que o FORWARD e o INPUT, ou seja: DROP, REJECT, LOG, ACCEPT. A Figura 62 apresenta o interior deste do alvo de OUTPUT.

O procedimento é idêntico aos demais alvos já apresentados. A plataforma detém o pacote enquanto ele é analisado perante as regras de controle. Em seguida, o pacote é submetido às ações de REJECT, DROP, ACCEPT ou LOG. Um detalhe a se observar na figura, é o REJECT que apenas tira uma foto do pacote e encaminha-o ao muro para ser destruído. Esta fotografia é a resposta de rejeição do pacote, visto que ele ainda não saiu para um outro *host*. O bloqueio aconteceu ainda dentro das dependências do próprio *host*, cabendo a ele registrar para si o bloqueio.

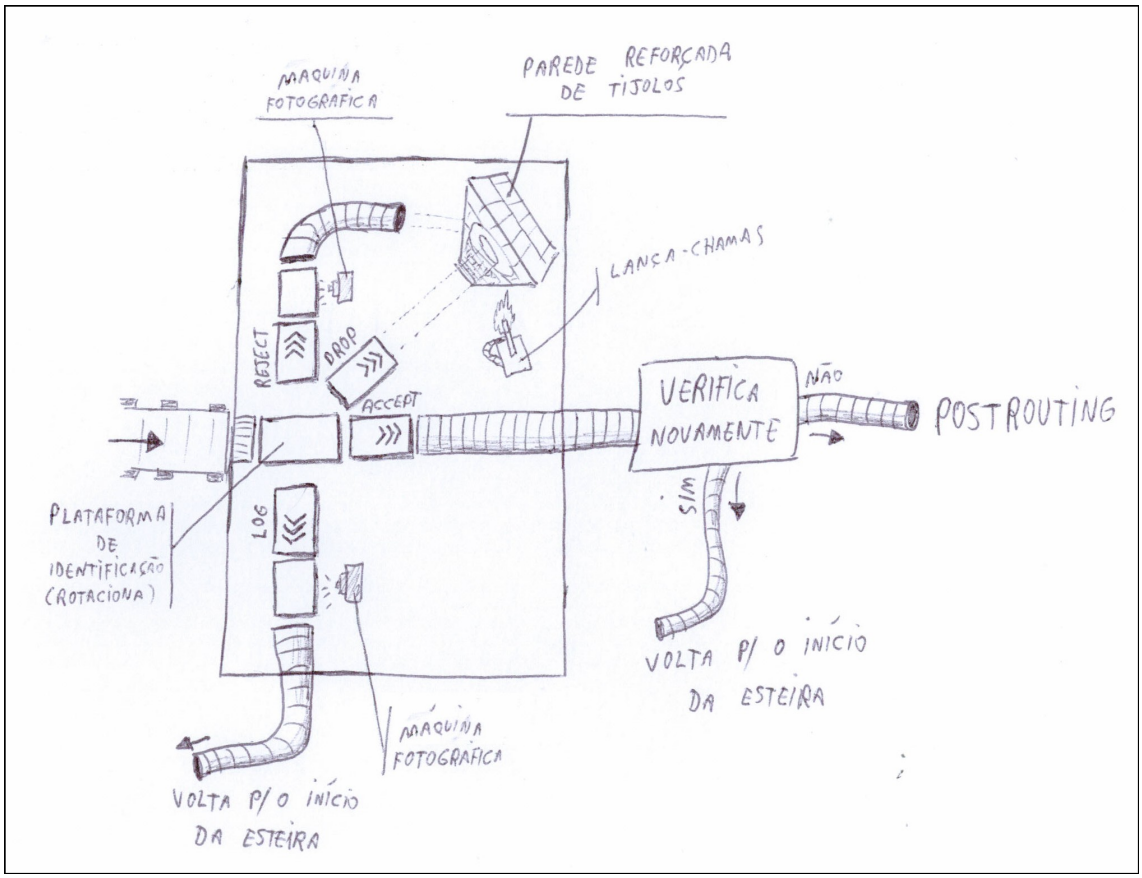

FIGURA 62: interior do alvo do OUTPUT

A Tabela 7 demonstra um modelo com regras de OUTPUT descritas a seguir:

- Regra 1: pacotes que saem do *host* pela placa de rede eth3 e com IP origem 192.168.200.1 devem ser destruídos.
- Regra 2: pacotes que saem do *host* com destino ao IP 13.7.8.8 devem ser rejeitados.

Nº da regra	Prot.	Placa de Rede		Origem		Destino		Ação
		IN	OUT	IP	Porta	IP	Porta	
1	*	*	eth3	192.168.200.1	*	*	*	Negar (DROP)
2	*	*	*	0/0	*	13.7.8.8	*	Rejeitar (REJECT)

Tabela 7: regras do OUTPUT

Uma vez liberado para prosseguir e sem nenhuma nova verificação necessária, o pacote é direcionado para o POSTROUTING seguido do segundo e último roteamento, finalizando assim a jornada do pacote dentro do *firewall*.

4.1.8. Representação do Pacote IP

O pacote IP é representado como uma bala de revolver (Figura 63). Esta metáfora é bem interessante pois o pacote assim como a bala, não tem condições de viajar por forças próprias. Ele viaja a velocidades sobre humanas, mas é necessário que alguém o impulsione. Todo e qualquer pacote de dados que viaja em uma rede de computadores foi enviado por algum dispositivo, seja ele uma placa de rede, um *switch*, um roteador, um dispositivo de laser, entre outros. Talvez soe de forma hilária, mas não é possível a um pacote parar no meio do cabo de rede e decidir retornar para pegar outro caminho ou parar para descansar e continuar posteriormente.

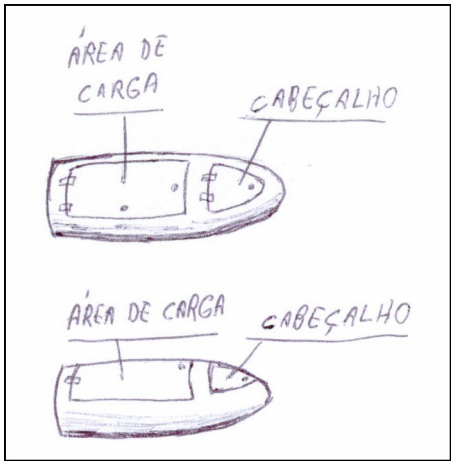

FIGURA 63: representação do pacote IP para a interface

Conforme mencionado, apenas os dados pertinentes a esta interface foram estabelecidos. Assim o pacote possui dois compartimentos: a área de carga útil e o cabeçalho que contém tipo de protocolo, IPs e portas. Estes dados são informados pelo usuário em um primeiro momento da interface. Após esta inserção, cabe apenas disparar o pacote e acompanhar as ações nele aplicadas.

4.2. ADEQUAÇÃO PERANTE AS QUALIDADES IDENTIFICADAS NESTA DISSERTAÇÃO

Uma vez apresentada a visão geral do ambiente proposto e considerando as qualidades

de interface levantadas nesta dissertação (Figura 42), é descrito a seguir a forma como cada uma pode ser atendida.

Para atender à qualidade “exclusão de informações desnecessárias”, a interface busca conter apenas representações inerentes ao processamento interno do *firewall*. De uma forma geral o ambiente gira em torno da máquina *firewall*. Em uma das extremidades, uma rede externa é representada por um roteador. Na outra extremidade uma rede interna é representada por três *hosts* e um *switch*, todos localizados na mesma “ilha” que o *firewall*. Esta representação é apenas para justificar a origem ou destino de um pacote que deva trafegar pelo *firewall*, sendo este último o protagonista do ambiente.

Demais informações como o serviço que o pacote está envolvido (WEB, FTP, entre outros), foram excluídos conforme já mencionado. Praticamente o ambiente trata a vida útil do pacote somente do momento em que ele entra no *firewall*, até o momento de eliminação ou saída do mesmo. As únicas informações presentes para isso são o protocolo, IP e porta de origem e destino. Estas informações são suficientes para o entendimento do mesmo, podendo obviamente outras informações serem acrescidas posteriormente, incrementando a interface. Até mesmo o funcionamento do serviço dentro do próprio *host firewall*, como por exemplo servidor WEB, não é necessária para o objetivo desta proposta. A interface demonstrará apenas até o momento de entrada ou saída neste *host.* A Figura 45 apresenta uma visão geral do ambiente interno, no qual pode-se observar a presença do *host firewall* e os caminhos possíveis a cada pacote de dados que entra e sai do *firewall*.

Para atender à qualidade “definição de representação visual e metafórica”, o ambiente propõe uma representação visual metafórica e artificial. Metafórica no sentido de utilizar ilhas, tubulações, leis da física, enfim, metáfora de objetos e conceitos que possivelmente estão presentes no modelo mental da maioria das pessoas, mesmo que involuntariamente. Artificial no sentido da criação de um ambiente que não existe forma natural no mundo real. O universo do ambiente proposto é composto de uma estrutura que compõe as redes e suas interligações, bem como os pacotes que só viajam exclusivamente dentro dos caminhos existentes. Não existe qualquer outro agente externo. Conforme já descrito sumariamente, partindo deste princípio, a representação de uma rede como uma ilha, induz ao pensamento de que a rede só é acessível por um determinado caminho que venha a ser estabelecido. Todos os caminhos existentes no ambiente, são compostos por tubulações, pelas quais os pacotes devem viajar. O conteúdo dentro do *firewall* é estabelecido como uma cidade industrial interligada também por tubulações. Cada edificação é composta ao estilo de uma linha de produção, cabendo ao pacote IP ser empurrado por estes caminhos. A metáfora da bala de

revolver para representar o pacote IP é bem conveniente descrito anteriormente.

O processo de verificação dos pacotes diante de uma lista de regras de controle, é representada por uma esteira, assim como uma linha de produção, onde o pacote ao passar, é analisado por máquinas de raio-X, assim como em aeroportos. Porém cada máquina busca determinada informação (protocolo, IP, porta, etc.), apresentando-a após a verificação. Tais informações devem ser bem destacadas assim que analisadas, afim de promover o relacionamento das condições identificadas com a tabela de regras existente. A metáfora da máquina fotográfica para registrar o pacote também é bem condizente com a ação de registro de LOG, o qual não armazena o pacote, e sim informações dele, assim como uma foto. O uso de lança-chamas e o ato de arremessar o pacote contra a parede deixam explicita a ação de destruição do pacote.

Para atender à qualidade “adequação da velocidade à percepção humana”, a criação de um pacote na rede origem ou rede destino poderá ser feita manualmente, em formulário simples onde o usuário informa o conteúdo do pacote. Após definidas as características do pacote, este é enviado ao *firewall* através de uma ação inicializada pelo usuário. Os pacotes chegam e são processados em todo o *firewall* um-a-um, ou seja, um único pacote passa por todas as análise que forem necessárias. Após ele sair do firewall ou ser destruído, o próximo pacote entra em cena. Todo este processo feito de forma lenta passando por cada ponto em velocidade adequada à percepção, podendo haver possibilidade de congelamento após cada ponto de processamento. Também é viável a possibilidade de liberação de um fluxo de pacotes, onde o usuário cria uma série de pacotes com características diferentes, e libera este fluxo o qual será enfileirado e processado pelo *firewall*, porém também em velocidade perceptível.

Para atender à qualidade “utilização de espaço e profundidade”, a utilização de recurso tridimensional no ambiente possibilita a percepção do pacote passando pelos locais específicos. As figuras de esboço apresentam a ideia de visualização desta característica, o que permite a visualização dos mais variados ângulos de visão. A configuração das análises é referenciada às tabela de regras de cada ponto de controle, o que possibilita o entendimento imediato do efeito de uma determinada regra de controle sobre o pacote de dados. O conjunto destas tabelas de regras formam a tabela Iptables.

Para a qualidade “utilização de memória espacial”, a qual talvez seja uma das qualidades mais importantes, porém sutil, ela é atendida pelo fato de definir locais específicos espacialmente para cada ponto de verificação. A própria disposição das edificações, da cidade de máquinas, bem como a própria tabela de regras dentro de cada prédio, são elementos que

justificam esta qualidade.

Por fim, para atender à qualidade “combinação de arte e engenharia”, está a forma disposta para o usuário perceber a leitura dos dados em um pacote, que no caso é uma metáfora de raio-X, bem como a ordem de disposição para a análise dos pacotes mediante as regras de controle. Esta porém é uma qualidade a ser melhor explorada em trabalho futuro de implementação desta interface.

4.3. FORMA DE UTILIZAÇÃO PELO ALUNO

Proponho no momento de inicialização da interface, uma prévia do ambiente, podendo o mesmo ser percorrido de forma vazia, apenas para conhecimento de cada etapa e caminhos existentes. Esta prévia seria uma espécie de voo panorâmico sobre o ambiente.

Em um segundo momento, o usuário insere uma regra ou um grupo de regras de controle nas tabelas do *firewall*. Esta inserção é realizada mediante o movimento de entrar em cada prédio e inserir ali determinada regra. Considerando que todas as regras foram definidas pelo usuário, é gerado uma tabela de regras compatível com IPTABLES, o que possibilita que o usuário poderá copiar e colar estas regras em um *firewall* real, e fazer apenas ajustes que achar conveniente. Também é interessante o recurso inverso, onde a partir de regras escritas para IPTABLES, sejam então carregadas para o ambiente proposto.

Em um terceiro momento, o usuário cria o pacotes de dados, informando o tipo de protocolo, o IP e porta de origem do pacote, bem como o IP e porta de destino. Também é interessante a possibilidade de criação de mais de um pacote idêntico, bem como a criação de pacotes com características diferentes. Um recurso interessante da interface é permitir ainda que sejam criados pacotes nos dois lados, rede interna e rede externa, porém conforme já mencionado, será processado um pacote por vez, afim de não comprometer a qualidade de adequação à velocidade humana.

Por fim, o usuário precisa executar o tráfego do pacote, desencadeando todo o processo de visualização dinâmica.

4.4. PROPOSTA DE METODOLOGIA DE DESENVOLVIMENTO

Em vista do tempo limite para conclusão de mestrado, não foi possível a

implementação prática desta proposta. Assim, esta dissertação limitou-se ao levantamento dos conceitos envolvidos acerca de interface, definindo o esboço do ambiente proposto observando detalhes de *design* a serem atendidos na implementação prática.

A implementação do projeto em um momento oportuno, deverá utilizar ferramenta gráfica 3D e demais recursos que possibilitem o funcionamento em multiplataforma, o que inclui ainda uma versão para dispositivos móveis.

4.5. CONCLUSÃO

Esta proposta de interface provê todas as qualidades previamente identificadas nesta dissertação, amarrando os conceitos de *design* e signos então levantados nos capítulos anteriores.

Através das qualidades atendidas, o ambiente da interface de uma forma geral possibilita uma consciência, uma percepção imediata de cada signo envolvido, evento também conhecido como primeiridade, onde caracteriza-se a estética. Todo o ambiente artificial e metafórico possibilita a associação de valores já estabelecidos para o indivíduo, elementos presentes no seu modelo mental. Esta situação é justamente a secundidade, ou seja, a ética que envolve os elementos da interface. Por fim, o esboço da interface foi proposto de forma a reduzir ao máximo a possibilidade de interpretação errônea acerca de cada elemento envolvido. Foi utilizado somente valores já conhecido à maioria dos usuários. Desta forma tem-se a terceiridade, a semiótica, ou seja, a lógica aplicada pelo usuário.

Estes alinhamentos consequentemente tornam a interface atraente ao usuário e eficaz no seu objetivo, ou seja, pode promover o conhecimento do funcionamento interno do *firewall* com maior precisão.

Os esboços aqui descritos, foram apresentados aos alunos afim de prover uma prévia da eficácia dos mesmos. Houve uma melhora significativa no entendimento do funcionamento interno do *firewall.* A representação metafórica e artificial aqui proposta, no primeiro impacto permitiu a continuidade do interesse por parte dos alunos. A característica da primeiridade foi certeira no sentido de trazer à mente dos alunos a impressão correta de cada objeto, sem duplicidade.

5. CONSIDERAÇÕES FINAIS

No decorrer desta pesquisa, foram abordados conceitos sobre signos, interface homem computador e *firewall*. Cada um destes elementos foi de suma importância para alcançar o resultado proposto. No quesito signos, esta pesquisa limitou-se apenas a abordar conceitos básicos como a relação triádica do signo, o signo como informação, bem como a visualização de dados no processo cognitivo. Estes elementos foram correlacionados aos conceitos de *design*, ou seja, tornando cada objeto de *design* envolvido como um signo pleno, ou seja, capaz de transmitir a informação durante o processo de aprendizagem, no qual tem o aluno como intérprete. O uso de recursos visuais amparados pelos conceitos de semiótica e interface homem computador foi de fundamental importância, produzindo um ambiente pedagógico amigável, divertido e satisfatório.

Em seguida, conforme proposto esta pesquisa possibilitou a discussão do *firewall* como agente de equilíbrio na internet, apresentando os possíveis ambientes nos quais ele pode estar inserido. Foram apresentadas suas funcionalidades mais pertinentes, bem como uma análise de interfaces específicas de configuração. Tais apreciações, em conjunto com o estudo sobre interface homem computador, permitiu que fosse levantada uma relação de qualidades imprescindíveis ao bom funcionamento da interface de ensino proposta.

Acredito em um primeiro momento que este projeto deva atender às qualidades de interface levantadas, no qual cada signo envolvido deva ser pleno, isto é, torne possível a interpretação das informações em cada elemento envolvido na interface. Todos os objetos envolvidos na interface, são presentes na mente da maioria das pessoas, o que poderá acarretar em uma melhor interpretação por parte de alunos.

Esta interface deve apresentar uma melhoria significativa em sala de aula quando utilizado pelo professor como ferramenta auxiliar. O processo de ensino amparado por este recurso visual, deve promover um entendimento muito mais eficiente, demonstrando dinamicamente o conteúdo que antes seria visível através de uma abstração, uma imagem mental da teoria passada em sala de aula.

5.1. TRABALHOS FUTUROS

Esta dissertação propicia alguns caminhos de pesquisa a serem continuados a partir

deste ponto. Tais trabalhos são:

a) registro de LOG do Iptables através de uma interface gráfica: este projeto seria algo direcionado a um ambiente de produção, ou seja, usuários experientes utilizariam tal interface para uma análise mais dinâmica de arquivo de LOG do *firewall*.

b) registro de LOG de outras ferramentas de *firewall* através de uma interface gráfica: a mesma linha descrita no item anterior, porém focado em outras ferramentas de *firewall.*

c) análise mais detalhada do cabeçalho Ipv4: esta talvez seja uma melhoria a ser implementada para esta mesma interface, acrescendo o pacote IP com todos os campos reais que um datagrama IP deve possuir, acrescentando mais tipos de análise.

d) estudo específico de *firewall* utilizando IPv6.

BIBLIOGRAFIA

ABNT, ABNT, NBR ISO/IEC 9126-1 - **Engenharia de software - Qualidade de produto - Parte 1: Modelo de qualidade**, ABNT, Rio de Janeiro-RJ, 2003.

AICHER, O. e KRAMPEN, M., [*Sistemas de signos na comunicação visual*], **Sistemas de signos em la comunicacion visual**, Barcelona, Gustavo Gili, 1979.

BAMBIRRA, Roberto Brandão, **Gestão do Conhecimento na Administração Pública Federal:** Estudo de Caso na Fundação Instituto Brasileiro de Geografia e Estatística (IBGE)**,** Dissertação de Mestrado, Universidade Estácio de Sá, Rio de Janeiro, 2009.

BARBOSA, Ákio Nogueira, **Um sistema para análise ativa de comportamento de firewall**, Dissertação de Mestrado, Escola Politécnica da Universidade de São Paulo-SP, 2006.

CRUZ, Kelly K. Damasceno, **Diferenças cognitivas entre usuários do ciberespaço**, Dissertação de Mestrado, PUC-SP/TIDD, 2008.

ECHEVERRÍA, Javier, [Os senhores do ar: Telépolis e o terceiro meio], **Los señores del aire: Telépolis y el tercer entorno**. Barcelona, Destino, 1999.

FLUSSER, Vilém, **O mundo codificado: por uma filosofia da comunicação**, Editora Cosac Naify, São Paulo, 2007.

FILHO, Oscar de Oliveira, **Ameaças e técnicas de defesa para informações em redes**, dissertação de pós-graduação em Redes de Computadores e Comunicação de Dados – Universidade Estadual de Londrina, Paraná, 2006.

FREITAS, Carla; CHUBACHI, Olinda; LUZZARDI, Paulo; CAVA, Ricardo. **Introdução à Visualização de Informações**. Revista de Informática Teórica e Aplicada. Instituto de informática da Universidade Federal do Rio Grande do Sul, n. 2, 2001.

HORN, Robert. **Information design**: emergence of a new profession. In JACOBSON, Robert (org.). Information Design. London: MIT Press, 1999.

JOHNSON, Steven, **Cultura da Interface – como o computador transforma nossa maneira de criar e comunicar**, Editora Jorge Zahar, Rio de Janeiro-RJ, 2001.

JOHNSON, Steven. **O mapa fantasma: como a luta de dois homens contra o cólera mudou o destino de nossas metrópoles**. Rio de Janeiro: Zahar, 2008.

LEAO, Lucia, **Cartografias em mutação: por uma estética do banco de dados**. In: ____ (Org.). Cibercultura 2.0. São Paulo: U.N. Nojosa, 2003;

LEVY, Pierre, **Cibercultura**, Tradução de Carlos Irineu da Costa, 2ª Edição, Editora 34, São Paulo-SP, 2000.

MANOVICH, Lev. Visualização de dados como uma nova abstração e anti-sublime. In: LEÃO, Lucia. (Org.). **Derivas: cartografias do ciberespaço**. São Paulo: Annablume, 2004.

MEGGS, Philip B., [História do design gráfico] **História del diseño gráfico**. México, Trillas, 1983.

NETO, Urubatan, **Dominando Linux Firewall Iptables**, Editora Ciência Moderna, Rio de Janeiro-RJ, 2004.

NOONAN, Wes, DUBRAWSKY, Ido, **Firewall Fundamentals**, Cisco Press, Indianapolis, USA, 2006.

PALU, Ari Junior, **Interface Administrativa para Firewall de Internet em Ambiente Linux**, Monografia UFLA, 2005.

PASTORE, Mike, DULANEY, Emmett, **Sybex CompTIA Security+**, Study Guide, 3ª Edição, Wiley Publishing, Inc., 2006.

PERKINS, Charles. **Firewalls**. 1a ed. São Paulo, Makron Books Brasil, 2002.

QUIGLEY, Aaron. **Aesthectics of large-scale relational information visualization in practice**. In FISHWICK, Paul. (org.) Aesthetic Computing. Cambridge, Mass.: MIT Press, 2006.

RANSDELL, J. Charles Peirce, **the idea of representation**, Tese de doutoramento inédita, New York, Columbia University, 1966;

RIBEIRO, Daniel Melo, **Visualização de Dados na Internet**, Dissertação de Mestrado, PUC-SP/TIDD, 2009;

ROYO, Javier, **Design Digital – Coleção Fundamentos do Design**, Editora Rosari, São Paulo-SP, 2008.

SANTAELLA, Lucia, **A Teoria Geral dos Signos: como as linguagens significam as coisas**, São Paulo, Cengage Learning, 2008;

TURBAN, E.; McCLEAN, E. R.; WETHERBE, J. C. **Tecnologia de informação para gestão:** transformando os negócios na economia digital. Porto Alegre: Bookman, 2004;

WEBLIOGRAFIA

ABNT, ABNT Catálogo, **ABNT NBR ISO/IEC 9126-1 - Engenharia de software - Qualidade de produto - Parte 1: Modelo de qualidade**, ABNT, 2003, disponível em <http://www.abntcatalogo.com.br/norma.aspx?ID=2815>, acessado em 17/03/2011 as 11:05.

ABNT, ABNT Catálogo, **ABNT NBR ISO 9241-151 - Ergonomia da interação humano-sistema Parte 151: Orientações para interfaces de usuários da World Wide Web**, ABNT, 2011, disponível em <http://www.abntcatalogo.com.br/norma.aspx?ID=86341>, acessado em 17/03/2011 as 11:07.

ABNT, **Conheça a ABNT**, disponível em <http://www.abnt.org.br/m3.asp?cod_pagina=929>, acessado em 17/03/2011 as 11:00.

DICIO, **Significado de Interface, Dicionário Online de Português**, disponível em <http://www.dicio.com.br/interface/>, acessado em 13/03/2011 as 10:12.

DICIO, **Significado de Usabilidade, Dicionário Online de Português**, disponível em <http://www.dicio.com.br/interface/>, acessado em 13/03/2011 as 10:30.

ESLINGER, Paul J., **Desenvolvimento do Cérebro e Aprendizado**, Revista Eletrônica de Divulgação Científica em Neurociência, n° 17, 2004, Universidade Estadual de Campinas, disponível em http://www.cerebromente.org.br/n17/mente/brain-development_p.htm>, Acessado em 24 de janeiro de 2011;

IPTABLES, **The netfilter.org "iptables" project**, disponível em <http://www.netfilter.org/projects/iptables/index.html>, acessado em 05/07/2011 as 15:01.

MANOVICH, Lev**. Information as an Aesthetic Event**. 2007. Disponível em <http://www.manovich.net/ >, acesso em 07/12/2008.

OLIVEIRA, Jorge Martins de, **Consciência**, Revista Eletrônica de Divulgação Científica em Neurociência, n° 5, 1998, Universidade Estadual de Campinas, disponível em <http://www.cerebromente.org.br/n05/opiniao/concien1.htm>, acessado em 24 de janeiro de 2011;

PEREIRA JR, Alfredo, **Uma abordagem naturalista da consciência humana**, Transf/Form/Ação, Editora UNESP, São Paulo-SP, v. 26, n. 2, p.109-141, 2003, Disponível em <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0101-31732003000200006&lng=pt&nrm=iso&tlng=pt>, acessado em 24 de janeiro de 2011, 13:30pm;

PETRY, Luis Carlos, **A im@gem pensa: Aspectos quânticos da imagem cibernética**, 2008, Revista Cibertextualidades, Disponível em <http://www.topofilosofia.net/swf_textos/E_a_imgem_pensa_RevFinal_04.swf> e <https://bdigital.ufp.pt/dspace/bitstream/10284/1347/3/cibertxt_3_p103-130_petry.pdf>, acessado em 19 de janeiro de 2010, 12:30am;

REIMER, Jeremy, **A History of the GUI**, Ars Technica, 2005, disponível em <http://arstechnica.com/old/content/2005/05/gui.ars/4>, acessado em 13 de março de 2011 as 8:35.

SANTAELLA, Lucia, **O que é semiótica**, Coleção Primeiros Passos, Editora Brasiliense, São Paulo, 1983, disponível em <http://www.scribd.com/doc/7153850/O-Que-e-Semiotica-Lucia-Santaella>, Acessado em 24 de janeiro de 2011;

SILVA, Gleydson Mazioli da, **Servidor SSH, Guia Foca GNU/Linux – Capítulo 15**, 2007, disponível em http://focalinux.cipsga.org.br/guia/avancado/ch-s-ssh.htm, acessado em 05/07/2011 as 13:55.

TDFSB, TDFSB, disponível em <http://www.determinate.net/webdata/seg/tdfsb.html>, acessado em 14/03/2011 as 00:01.