Centro Estadual de Educação Tecnológica Paula Souza
Faculdade de Tecnologia de Mauá

Implementação de um Firewall baseado em Software Livre para acesso ao Sistema Integrado de Administração Financeira e ao Sistema Integrado de Dados Orçamentários do Governo Federal

Autor: Tecgº Wallace Rodrigues de Santana

Orientador: Profº Ricardo Andrian Capozzi

Mauá
2005

Centro Estadual de Educação Tecnológica Paula Souza
Faculdade de Tecnologia de Mauá

Implementação de um Firewall baseado em Software Livre para acesso ao Sistema Integrado de Administração Financeira e ao Sistema Integrado de Dados Orçamentários do Governo Federal

Autor: Tecgº Wallace Rodrigues de Santana

Monografia apresentada à FATEC Mauá, como parte dos requisitos para obtenção do titulo de Tecnólogo em Informática com ênfase em Gestão de Negócios.

Orientador: Profº Ricardo Andrian Capozzi

Mauá
2005

Dedicatória

À minha mãe Geni, que sempre me ensinou a não desistir de meus sonhos.

A meu tio Alcides, que sempre me incentivou a lutar.

A minha cachorra Antonieta, que sempre encheu nossa casa de alegria.

Que Deus os tenha.

Agradecimentos

À minha esposa Carla, pelo carinho e compreensão.

Ao meu orientador Capozzi, pela confiança e ajuda.

A toda equipe de informática da CEAGESP.

Sumário

Lista de Figuras

Lista de Tabelas

Resumo

Preocupada com a segurança de seus ativos, a CEAGESP busca implementar uma política de segurança que visa aumentar a disponibilidade e a confidencialidade de dois dos principais sistemas implantados hoje na empresa: o SIAFI (Sistema Integrado de Administração Financeira) e o SIDOR (Sistema Integrado de Dados Orçamentários), ambos do Governo Federal.

O SIAFI e o SIDOR são sistemas de prestação de contas de empresas públicas para com o Governo Federal. O SIAFI é acessado através da rede do SERPRO e o SIDOR através da rede da Secretaria de Orçamento Federal.

Para estabelecer um canal de comunicação entre estas redes e a rede da CEAGESP de forma segura, a melhor alternativa é estabelecer uma rede privada virtual (VPN) ou túnel criptográfico. Porém, para a implementação desta VPN, faz-se necessário primeiramente a instalação de um *firewall* na borda do perímetro de segurança da rede da CEAGESP.

Este trabalho visa, portanto, implementar regras de *firewall* baseado em *software* livre para dar suporte aos sistemas SIAFI e SIDOR, e também para proteger a rede corporativa da CEAGESP contra ataques externos e acessos não autorizados.

Por final, será apresentada uma análise da viabilidade econômica entre a escolha de um *firewall* baseado em *software* proprietário, como o Check Point FireWall-1, e um *firewall* baseado em *software* livre, como o NetFilter IPTables.

1 Introdução

1.1 Objetivo

O objetivo deste trabalho é propor regras de *firewall* a serem implementadas em *software* livre para que a Companhia de Entrepostos e Armazéns Gerais de São Paulo, a CEAGESP, possa acessar com segurança o Sistema Integrado de Administração Financeira (SIAFI) e o Sistema Integrado de Dados Orçamentários (SIDOR), ambos do Governo Federal. O SIAFI é acessado através da rede de comunicação de dados do Serviço Federal de Processamento de Dados – SERPRO; e o SIDOR através da rede de comunicação de dados da Secretaria de Orçamento Federal – SOF. Será feita também uma análise da viabilidade econômica para a implantação de um *firewall* em *software* livre ao invés de *software* proprietário.

1.2 Motivação

A CEAGESP é uma empresa do governo federal vinculada ao Ministério da Agricultura, Pecuária e Abastecimento. Assim como todas as empresas e órgãos do governo federal, a CEAGESP deve prestar contas à União através de sistemas informatizados de controle financeiro e orçamentário. Alguns destes sistemas são gerenciados pelo SERPRO, que é vinculado ao Ministério da Fazenda.

Um destes sistemas é o SIAFI, que processa e controla a execução orçamentária, financeira e patrimonial da União, administrada pela Secretaria do Tesouro Nacional do Ministério da Fazenda. O outro sistema é o SIDOR, utilizado para processamento dos dados relativos à preparação da elaboração orçamentária, administrada pela Secretaria de Orçamento Federal do Ministério do Planejamento, Orçamento e Gestão.

As informações que transitam dos computadores da CEAGESP para as redes externas são sensíveis e necessitam de proteção. Para garantir que a comunicação entre estas redes seja feita de forma segura é necessário implementar sistemas eficazes de segurança. Segundo Tanenbaum (1997), “um dos métodos mais comuns é o uso da criptografia, que protege os dados em trânsito entre sites seguros”. Porém antes, deve-se

implementar um *firewall* que fica na borda do perímetro de segurança destas redes. É na implementação do *firewall* que este trabalho irá focar.

2 Conceitos

2.1 Segurança

Para Schetina *et al* (2002), a segurança é um processo e não um ponto no tempo, e pode ser dividido em quatro componentes principais: avaliação e política, proteção de ativos, monitoramento e detecção e resposta e recuperação.

Figura 1 – O processo de segurança, Schetina et al (2002)

De acordo com Schetina *et al* (2002), na fase de avaliação e política, as empresas determinam suas necessidades de segurança e definem os papéis e responsabilidades organizacionais. Elas também poderiam rever os mecanismos de segurança que já estão implantados e determinar se eles são suficientes para atender às necessidades da empresa. Essas respostas são convertidas em uma política de segurança, que define como a empresa planeja proteger seus ativos, onde quer que eles possam estar.

Ainda de acordo com Schetina *et al* (2002), quando a política tiver sido definida, a empresa passa para a fase de *proteção de ativos*, durante a qual ela implementa salvaguardas para tratar de todos os elementos da política de segurança. Isso pode ser feito por meio de procedimentos, como revisões regulares dos arquivos de *log* do sistema ou de implementações, como em um *firewall*.

Depois que as salvaguardas tiverem sido colocadas, a empresa precisa monitorar sua eficiência. Isso é realizado na fase de *monitoramento e detecção*. Por exemplo, se nunca se examinou o tráfego que passa através do *firewall*, então, com certeza nunca se saberá ele está realmente fazendo seu trabalho.

Finalmente, como não se pode esperar que as medidas de segurança sejam 100% eficazes o tempo todo, as empresas devem ter uma estratégia para *resposta e recuperação*.

Para Schetina *et al* (2002), depois que essas etapas tiverem sido tratadas, é o momento de começar tudo de novo e iniciar o processo de avaliação mais uma vez. Se a política, salvaguardas, monitoramento de capacidades e mecanismos de resposta não estiverem examinando minuciosa e regularmente, há uma boa chance de que eles logo se tornem obsoletos ou sejam superados por novas tecnologias, novos ataques ou alterações à empresa ou rede. Para que qualquer programa de segurança seja eficiente, ele deve ser suportado por todos os grupos dentro da empresa, desde o CEO até os usuários finais, o departamento de recursos, a equipe administrativa e a equipe da área de Tecnologia da Informação. Cada um desses grupos tem um papel na definição, implementação e monitoramento da definição da política de segurança da empresa e na sua concordância com ela. Sem o compromisso firme de cada grupo dentro de uma empresa, especialmente o gerenciamento sênior, o programa de segurança provavelmente não será eficaz.

2.1.1 Segurança da informação

De acordo com Albuquerque e Ribeiro (2002), o mais importante não é o quanto se deseja de segurança, mas sim o quanto se deseja de disponibilidade do sistema ou qual a necessidade de confidencialidade. No caso da CEAGESP, as necessidades mais urgentes hoje são a disponibilidade do sistema e sua confidencialidade.

2.1.1.1 Confidencialidade

Para Albuquerque e Ribeiro (2002), confidencialidade é a capacidade de um sistema de impedir que usuários não-autorizados vejam determinada informação, ao mesmo tempo em que usuários autorizados podem acessá-la.

2.1.1.2 Integridade

Segundo Albuquerque e Ribeiro (2002), integridade é o atributo de uma informação que indica que esta não foi alterada ou, se foi, o foi de forma autorizada; capacidade de um

sistema de impedir que uma informação seja alterada sem autorização ou, ao menos, de detectar se isso ocorreu.

2.1.1.3 Disponibilidade

De acordo com Albuquerque e Ribeiro (2002), disponibilidade indica a quantidade de vezes que o sistema cumpriu uma tarefa sem falhas internas sobre o número de vezes em que foi solicitado a fazer uma tarefa. A fração do tempo em que o site esteve no ar.

2.1.2 Segurança da informação no governo federal

Em reportagem publicada pela revista Tema em março/abril de 2004, constatou-se que com o aumento dos serviços públicos oferecidos pelo Governo Federal e disponibilizados na Internet, aumentou também a preocupação do governo com a segurança da informação. Ao mesmo tempo em que a disponibilização destes serviços aumenta o conforto e a satisfação do cidadão, aumentam também os riscos e ameaças para os sistemas informatizados disponibilizados.

Segundo João Rufino, que faz parte do Comitê Gestor da Segurança da Informação do Governo Federal (CGSI) e também é citado na matéria, “neste cenário, o principal desafio da segurança da informação está em como disponibilizar informações íntegras, confiáveis e com confidencialidade, sem expor, desnecessariamente, a privacidade de pessoas e organizações”.

2.1.3 Segurança por meio de Firewall

O *firewall* oferece uma das mais importantes opções para segurança da informação porque ele é o primeiro item a ser testado por quem, de fora, tenta acessar os computadores de uma rede corporativa. Como o *firewall* fica na borda do perímetro de segurança da rede, sua função é a de servir como primeiro ponto de verificação dos pacotes que tentam entrar na rede.

De acordo com o manual *Getting Started with Check Point FireWall-1*, da Check Point Software Technologies Ltd., quando se conecta uma rede à Internet, assegurar que ela estará livre de intrusos é uma questão crítica. A forma mais efetiva de proteger a ligação com a Internet é colocar um sistema de *firewall* entre a rede local e a Internet. O *firewall* garante que toda a comunicação entre a rede corporativa e a Internet esteja de acordo com a política de segurança da empresa.

Ainda de acordo com o referido manual, para fazer com que efetivamente seja oferecida uma segurança realista, o *firewall* deve rastrear e controlar o fluxo de toda comunicação que passa através dele. Para decidir sobre quais ações se deve tomar sobre serviços baseados em TCP/IP (como por exemplo, o que deve passar, ser rejeitado, encriptado ou feito *log* de tentativas de comunicação), um *firewall* deve obter, armazenar, restaurar e manipular informações derivadas de todas as camadas de comunicação e de outras aplicações. Isto não é suficiente para examinar pacotes isoladamente. O estado da comunicação – derivado de transmissões anteriores e de outras aplicações – é um fator essencial para estabelecer o controle sobre tentativas de comunicação. Ambos o estado de comunicação (derivado de transmissões anteriores) e o estado da aplicação (derivado de outras aplicações) talvez devam ser considerados quando se quer tomar decisões de controle.

2.1.3.1 Proteção contra ataques conhecidos

Apresentaremos aqui dois dos mais importantes ataques conhecidos "que os *hackers* usam para localizar, identificar e invadir um sistema", segundo Strebe e Perkins (2002). Os ataques de Ping da Morte e Inundações SYN são tipicamente ataques de recusa de serviço, que tem por objetivo, de acordo com Strebe e Perkins (2002), "impedir que um serviço seja fornecido travando ou sobrecarregando os computadores que oferecem esse serviço".

2.1.3.1.1 Ping da morte

De acordo com Strebe e Perkins (2002), a fim de testar a capacidade de um sistema e as restrições de tamanho dos pacotes, os pacotes ICMP podem ser criados com qualquer

coisa até 64 kB. Isso permite determinar o tamanho máximo do pacote entre o sistema-emissor e um sistema-alvo na Internet. Nos primórdios da Internet essa funcionalidade era importante porque muitos roteadores tinham limitações quanto ao tamanho máximo dos pacotes. Em pacotes de "ping" grandes, a parcela de dados com informações do pacote é preenchida com dados sem significado. O tamanho máximo dessa parcela é de 2^{16} (64536) *bytes* menos os dados de controle do pacote.

Os ataques "ping da morte" são propagados criando-se um pacote de solicitação de eco ICMP malformado no qual o tamanho alegado do pacote excede o tamanho máximo possível. Como o indicador de tamanho dos dados úteis tem 16 *bits* permitindo um tamanho máximo de pacote de 65536 *bytes* (o limite real é cerca de 65500 *bytes* devido aos dados de controle do cabeçalho do pacote), os pacotes que alegam serem maiores que 65500 *bytes* podem causar erros de TCP/IP no sistema receptor.

Em uma implementação TCP/IP típica, quando um cabeçalho de pacote é lido, conta-se com as informações contidas no cabeçalho para criar um *buffer* para os dados úteis. Quando o tamanho alegado do cabeçalho do pacote mais o tamanho dos dados úteis ultrapassam o limite máximo de 64 kB definido pela especificação TCP/IP, a implementação TCP/IP pode travar devido a erros na alocação de memória.

2.1.3.1.2 Inundação SYN

Segundo Strebe e Perkins (2002), o cliente solicitante transmite uma mensagem SYN para o serviço de um *host* solicitando atendimento e o servidor que recebe a solicitação responde com uma mensagem SYN-ACK aceitando a conexão. O cliente então responde com uma mensagem ACK após a qual o tráfego pode fluir pela conexão TCP bidirecional estabelecida.

Quando um servidor recebe a mensagem SYN inicial ele normalmente cria uma nova linha de execução (*thread*) para lidar com as solicitações da conexão do cliente. A criação dessa linha de execução exige tempo da CPU e reserva uma certa quantidade de memória. Quando a sessão TCP é fechada ou após um período de tempo suficiente, o servidor fecha a sessão TCP e a memória então reservada agora é liberada. A quantidade

de memória e o tempo de computação determinam o número de sessões simultâneas que um servidor de sessões pode suportar.

As inundações SYN são mensagens SYN artificiais enviadas aos servidores. Como uma inundação SYN afeta o computador atacado depende de sua implementação de TCP/IP.

Algumas implementações de pilha TCP/IP são capazes apenas de esperar pelas mensagens ACK de um número limitado de computadores, porque têm um *buffer* de memória limitado para estabelecer as conexões. Se esse *buffer* for preenchido com inicializações de conexões artificiais, o servidor irá parar de responder às tentativas de conexões subseqüentes até que as tentativas no buffer esgotem o tempo limite (*timeout*).

Em implementações que não limitam o estabelecimento de conexões, os ataques de inundação SYN têm um efeito similar. Como o servidor não sabe distinguir uma mensagem SYN legítima de uma falsa, ele reserva recursos de computação e de memória para estabelecer uma conexão. Sobrecarregando o servidor com um grande volume de solicitações, a capacidade máxima do servidor pode ser usada por essas tentativas de conexões artificiais e inúteis.

2.1.3.2 Proteção contra atacantes conhecidos

2.1.3.2.1 Atacantes externos

O principal protagonista de ataques externos a uma rede corporativa é o *hacker*, que segundo Oliveira (2001), é uma pessoa que possui uma grande facilidade de análise, assimilação, compreensão e capacidades surpreendentes com um computador. O *hacker* sabe perfeitamente que nenhum sistema é completamente livre de falhas, e sabe onde procurá-las utilizando técnicas das mais variadas.

2.1.3.2.2 Atacantes internos

Para Schetina *et al* (2002), a maior ameaça a uma empresa vem de pessoas internas. As pessoas que têm acesso às informações conhecem quais são os ativos críticos, onde eles se encontram e como estão protegidos. Essas pessoas normalmente são mais confiáveis do que as pessoas de fora. Têm acesso físico e, freqüentemente pela rede, aos seus sistemas. Elas gerenciam o *firewall* e não são monitoradas por um sistema de detecção de intrusos. Esses são todos os atributos que uma ameaça externa, como um criminoso ou um *hacker* adorariam ter. Freqüentemente só o que separa uma pessoa que tem acesso às informações dos seus ativos críticos são os seus escrúpulos e muitas vezes isso não é suficiente. Além disso, as mesmas vantagens que um funcionário da empresa tem para causar prejuízo, desde que haja a necessária intenção, amplificam os danos que ele pode causar por acidente. Um clique errado dado por um funcionário pouco experiente em um "Cavalo de Tróia" executável anexado a uma mensagem de correio eletrônico pode causar danos ao sistema e ao acesso remoto que talvez sejam impossíveis de conseguir através de um ataque direto feito por uma pessoa de fora.

2.1.3.3 O que o firewall não pode proteger

Para Strebe e Perkins (2002), nenhuma rede conectada à Internet pode ser completamente segura. Os *firewalls* são extremamente eficazes, são capazes realmente de manter distante a grande maioria dos *hackers*, mas há tantas maneiras diferentes de se tentar explorar as conexões de uma rede que nenhum método é totalmente seguro. Muitos administradores consideram erroneamente que seus problemas de segurança acabaram uma vez que seu *firewall* esteja operando e já tenha mostrado sua eficácia.

No entanto, o *firewall* só pode proteger as transmissões de dados que passam por ele. Segundo Strebe e Perkins (2002), é preciso também reforçar a idéia de um único ponto de controle no *firewall*. Se houver mais de um *firewall* na empresa (talvez um *firewall* conectando cada escritório remoto à Internet), deve-se ter absoluta certeza de que todos eles estejam configurados da mesma forma.

Ainda segundo Strebe e Perkins (2002), existe outra ameaça séria à segurança de uma rede: cruzar a fronteira escondida. Os modems oferecem a possibilidade a qualquer usuário da rede de discar para seus próprios provedores externos de acesso à Internet e assim desviar totalmente do *firewall*.

2.2 Firewall

Para Rodriguez *et al* (2001), um *firewall* é um sistema (ou grupo de sistemas) que reforça a política de segurança entre uma rede privada segura e uma rede não confiável como a Internet. Os *firewalls* tendem a preocupar-se com a proteção entre a Internet e a rede privada. Mas geralmente, um *firewall* deve ser considerado como um meio de dividir o mundo em duas ou mais redes: uma ou mais redes seguras e uma ou mais redes não seguras.

Ainda de acordo com Rodriguez *et al* (2001), um *firewall* pode ser um microcomputador, um roteador, um minicomputador, um *mainframe*, uma estação UNIX ou uma combinação destes que determina qual informação ou serviço pode ser acessado de fora e quem tem permissão para usar a informação e os serviços de fora. Geralmente, um *firewall* é instalado num ponto onde a rede privada segura e a rede externa não confiável se encontram, o qual é conhecido como ponto de obstrução.

E para entender como um *firewall* trabalha, deve-se considerar a rede como um edifício cujo acesso deva ser controlado. O edifício tem um salão de entrada, onde recepcionistas recebem os visitantes, guardas vigiam os transeuntes e câmeras de vídeo monitoram todas as ações das pessoas que circulam pelo edifício. Embora estes procedimentos talvez pareçam satisfatórios para controlar o acesso ao edifício, se uma pessoa não autorizada consegue entrar, não há nenhuma forma de proteger o edifício contra ações do intruso. De qualquer forma, se os movimentos do intruso puderem ser monitorados, será possível detectar qualquer atividade suspeita.

E conforme Rodriguez *et al* (2001), similarmente, um *firewall* é projetado para proteger as informações da empresa pelo controle do acesso entre a rede privada segura e a rede externa não confiável. De qualquer forma, é importante notar que mesmo que o

firewall seja projetado para permitir que o tráfego confiável passe através dele, que serviços vulneráveis sejam negados e ataques externos a rede interna sejam prevenidos, um ataque criado recentemente poderá penetrar o *firewall* a qualquer hora. O administrador da rede deve examinar todos os *logs* e alarmes gerados pelo *firewall* em uma base regular. De outra forma, não será possível proteger a rede privada de ataques externos.

2.2.1 Funções do Firewall

Conforme Strebe e Perkins (2002), "para manter um nível absolutamente mínimo de segurança na Internet que seja eficaz, é preciso controlar a segurança nas fronteiras usando *firewalls* que realizem todas as três funções básicas dos *firewalls*, filtragem de pacotes, conversão de endereços da rede e *proxy* de serviços de alto nível".

2.2.1.1 Filtragem de Pacotes

Segundo Strebe e Perkins (2002), "os filtros comparam os pacotes dos protocolos de rede (como o IP) e os pacotes dos protocolos de transporte (como o TCP) com um conjunto de regras contidas em um banco de dados e só encaminham os pacotes que atendam aos critérios especificados nesse banco de dados de regras". É a partir daí que estabeleceremos as primeiras regras do *firewall*, onde serão configurados quais pacotes poderão passar ou não. Ainda segundo Strebe e Perkins (2002), "os filtros de um modo geral seguem as seguintes regras: recusar tentativas de conexões dirigidas para dentro, mas permitir que passem as tentativas de conexão dirigidas para fora; eliminar pacotes TCP ligados a portas que não deveriam estar disponíveis para a Internet, mas permitir os pacotes que devam passar; restringir o acesso dirigido para dentro de certos intervalos de IP's".

A figura 2 mostra clientes remotos acessando serviços públicos dentro do *firewall*.

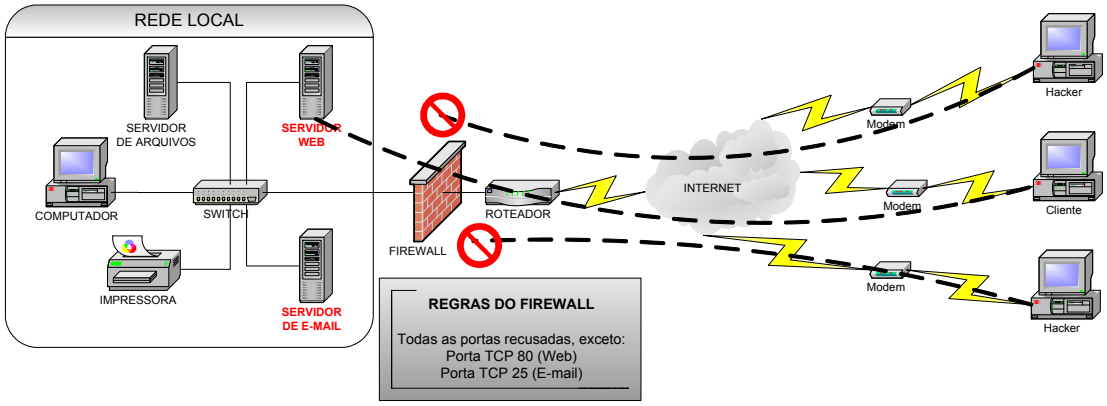

Figura 2 – Filtragem de pacotes, Strebe e Perkins (2002)

2.2.1.2 NAT

A NAT (*Network Address Translation* – Conversão de Endereços de Rede), de acordo com Strebe e Perkins (2002), "oculta os endereços IP internos convertendo todos os endereços de *hosts* internos para o endereço do *firewall*. Este então retransmite os dados dos *hosts* internos a partir de seu próprio endereço usando o número da porta TCP para saber quais conexões do lado público devem ir para que *hosts* do lado privado interno. Para a Internet, todo o tráfego da rede parece vir de um só computador extremamente ocupado".

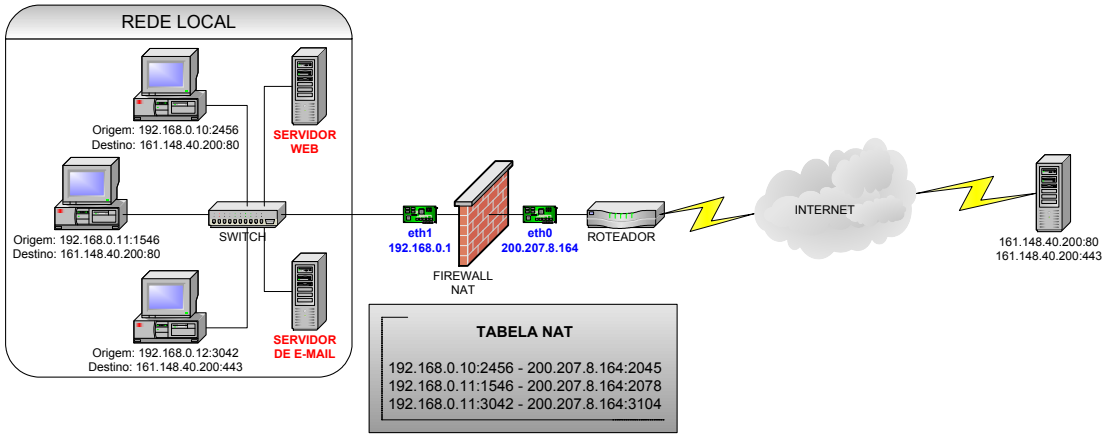

Figura 3 – Conversão de endereços de rede, Strebe e Perkins (2002)

2.2.1.3 PROXY

De acordo com Strebe e Perkins (2002), os servidores *proxy* foram desenvolvidos originalmente para colocar em *cache* as páginas Web que eram acessadas freqüentemente.

Nos primeiros dias da Internet, os enlaces de longa distância remotos eram lentos, a Web era relativamente pequena e as páginas Web eram estáticas. Quando a Web cresceu explosivamente, os *proxies* começaram a ficar menos eficazes em sua finalidade original – pois a Web agora é muito ampla e muitas páginas Web são dinâmicas, perdendo a validade assim que são transmitidas, fazendo com que os usuários de uma única organização tenham de passar por "um milhão" de páginas Web antes de uma delas ser visitada três vezes. Esses fatores representam, verdadeiramente, um problema de cache difícil de resolver. Mas, a nova Web também apresenta novos elementos e os servidores *proxy* mostraram um efeito colateral surpreendente e notável: eles podem ocultar todos os usuários reais de uma rede por trás de uma única máquina, eles podem filtrar URLs e podem impedir a passagem de conteúdo suspeito ou ilegal. A finalidade principal da maioria dos servidores *proxy* atuais é operar como *firewall* em vez de *cache* de páginas Web.

Ainda segundo Strebe e Perkins (2002), os *proxies* de aplicativos não precisam ser executados em *firewalls*; qualquer servidor pode realizar o papel de um *proxy*, seja dentro ou fora da sua rede. Sem um *firewall*, não há nenhuma segurança realmente, de modo que ambos são necessários. Pelo menos algum tipo de filtro de pacotes precisa ser usado para proteger o servidor *proxy* de ataques por recusa de serviço na camada de rede. Além disso, se o *proxy* não for executado no *firewall*, deverá ser aberto um canal através do *firewall* de um modo ou de outro. O ideal é que o próprio *firewall* realize a função do *proxy*. Isso irá evitar que os pacotes do lado público sejam encaminhados através do *firewall*. Os *proxies* são capazes também de realizar filtragem em nível de aplicativos para conteúdo específico. Por exemplo, alguns *proxies* HTTP *firewall* procuram por instruções em páginas HTML que façam referência a *applets* Java ou ActiveX embutidas e então retiram esse conteúdo das páginas. Isso evita que a *applet* seja executado nos computadores clientes e elimina o risco de o usuário acidentalmente descarregar um "Cavalo de Tróia". Esse tipo de filtragem é extremamente importante porque a filtragem, o uso de *proxies* e o mascaramento do IPs não são capazes de evitar que uma rede seja comprometida se os usuários forem convencidos (e enganados) a descarregar um cavalo de Tróia embutido em uma *applet* ActiveX, por exemplo.

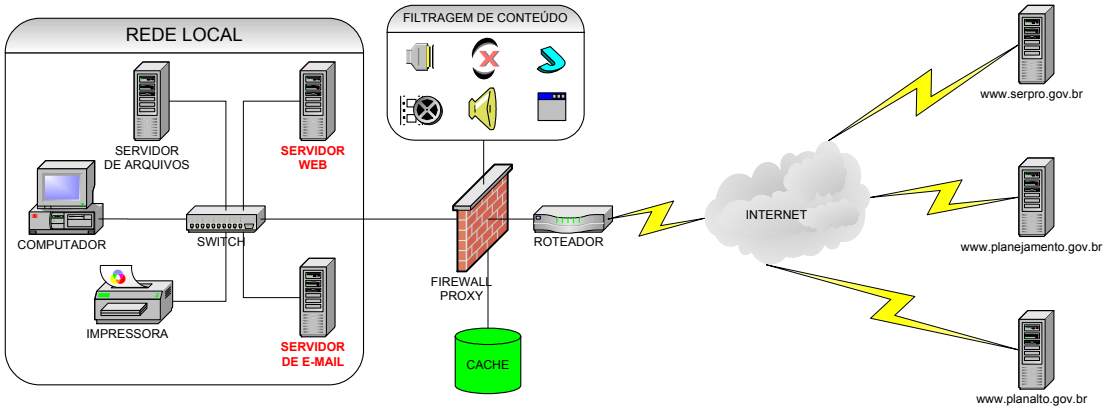

Figura 4 – Proxy de serviços de alto nível, Strebe e Perkins (2002)

2.2.2 Tipos de Firewall

Segundo Strebe e Perkins (2002), os *firewalls* originais eram filtros de pacotes, e as primeiras tentativas de tornar o TCP/IP seguro se basearam na idéia de que é bastante fácil para um roteador inspecionar o cabeçalho dos pacotes TCP/IP e simplesmente rejeitar aqueles que não estão de acordo com as especificações de aceitação.

2.2.2.1 Firewall sem inspeção de estados

De acordo com Strebe e Perkins (2002), os *firewalls* são roteadores nas fronteiras que aumentam a segurança determinando se um pacote deve ou não ser encaminhado com base na informação contida no cabeçalho de cada pacote individual. Teoricamente, os filtros podem ser configurados para operar com base em qualquer parte do cabeçalho do protocolo, mas a maioria só pode ser configurada para filtrar os campos de dados mais úteis, como: tipos de protocolo, endereços IP, portas TCP e UDP, número de fragmentos e informações sobre roteamento de origem.

2.2.2.2 Firewalls com inspeção de estados

Segundo Strebe e Perkins (2002), os *firewalls* sem inspeção de estados têm várias falhas, todas nascendo do fato de que um único pacote em uma comunicação não contém informações suficientes para determinar se ele deve ou não ser recusado, porque ele faz parte de uma comunicação maior. Os *firewalls* que realizam a inspeção de estados

resolvem esse problema retendo na memória os estados de todas as comunicações passando pelo *firewall* e usando esse estado guardado para determinar se os pacotes individuais devem ou não ser abandonados. A inspeção com estados filtra fluxos de comunicação inteiros, não apenas os pacotes, e conseguem se lembrar do estado das conexões da rede e das camadas da sessão gravando informações sobre o estabelecimento da sessão que passa através do *gateway* do filtro. Os filtros usam então essa informação para discriminar pacotes de retorno válidos das tentativas de conexão inválidas ou de invasão.

2.2.3 Topologia

De acordo com Strebe e Perkins (2002), uma vez que o *firewall* esteja sendo executado na fronteira entre a rede privada e a Internet, enfrentar-se-á um problema ao oferecer serviços públicos que os clientes precisam e, ao mesmo tempo, ao proteger a rede interna contra ataques de *hackers*. Assim, pode-se usar uma topologia de *firewall* único ou dual, de acordo com os serviços públicos que se queira oferecer.

2.2.3.1 Firewall único

Segundo Strebe e Perkins (2002), a solução mais simples e completa para proteção das fronteiras é a que adota um único *firewall*. Mas haverá um problema se forem oferecidos serviços públicos como um *site* Web, FTP ou um servidor de e-mail, pois deverá ser aberta uma conexão por meio do *firewall* a um cliente interno ou expor o servidor público à Internet sem a proteção do *firewall*. Os dois métodos representam um risco à segurança.

Ainda segundo Strebe e Perkins (2002), o problema com a instalação de servidores públicos, como os servidores de e-mail, fora do *firewall* é que eles ficam expostos ao risco dos ataques de *hackers* sem nenhuma restrição ou proteção. Esses computadores podem ser configurados de modo que não contenham informações confidenciais, mas é um fato que as tentativas de invasão podem facilmente provocar o mau funcionamento do serviço caso os servidores parem ou, no mínimo, causar embaraços se os *hackers* modificarem as páginas Web.

A figura 5 mostra servidores públicos de dentro do *firewall*.

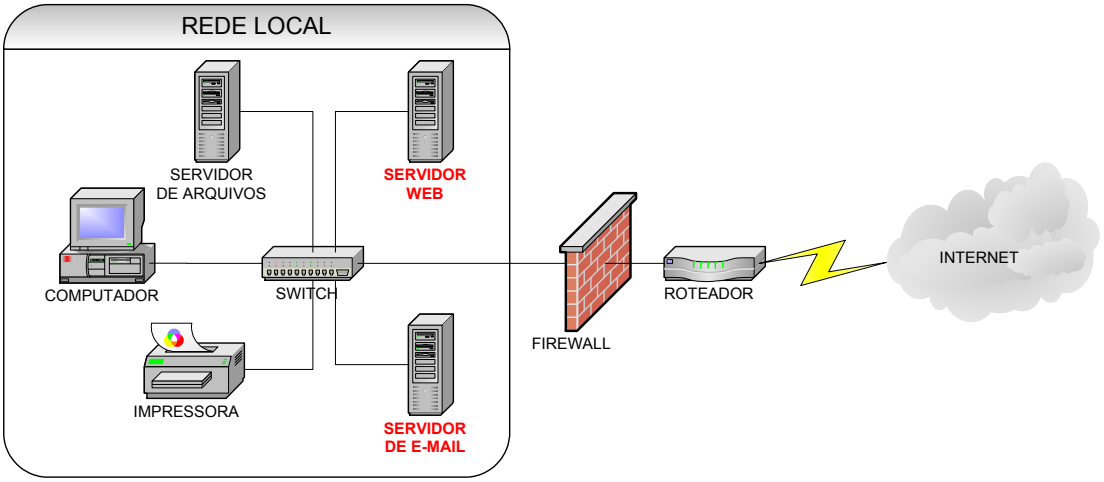

Figura 5 – *Firewall* único, Strebe e Perkins (2002)

2.2.3.2 Firewall dual

Para Strebe e Perkins (2002), é possível reduzir o risco de ter servidores públicos expostos com dois *firewalls* e dois níveis de proteção por *firewall*. Basicamente, coloca-se o primeiro *firewall* na conexão à Internet e protegem-se os servidores Web atrás dele. Isso irá fornecer uma proteção bastante segura e permitirá as conexões a partir da Internet para os serviços que se quer oferecer. Entre essa rede e a rede interna coloca-se um segundo *firewall* com uma norma de segurança mais rígida que simplesmente não permite conexões externas e oculta a identidade dos clientes internos. A rede que fica entre os dois *firewalls* é denominada DMZ (*demilitarized zone*, zona desmilitarizada).

A figura 6 mostra uma rede com dois *firewalls* fornecendo dois níveis de segurança.

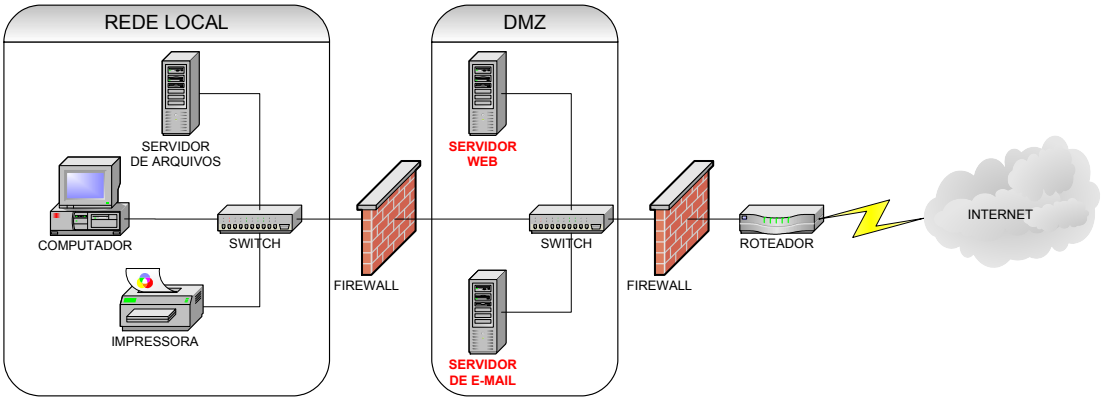

Figura 6 – *Firewall* dual, Strebe e Perkins (2002)

Um *firewall* dual pode ser composto por duas máquinas distintas executando um software de *firewall* ou simplesmente por uma única máquina equipada com dois ou mais adaptadores de rede, sendo cada adaptador destinado a cada sub-rede que se queira proteger. A figura 7 mostra um *firewall* único que executa a função de um *firewall* dual:

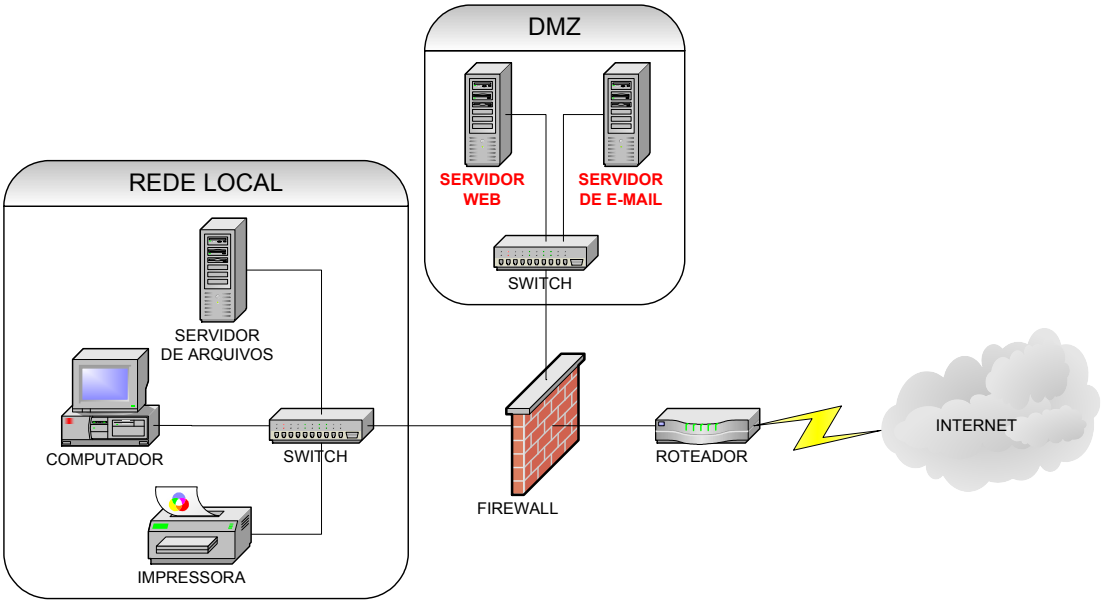

Figura 7 – *Firewall* dual virtual, Strebe e Perkins (2002)

2.2.4 Firewall com Debian GNU/Linux e NetFilter IPTables

2.2.4.1 Software Livre

O conceito de *software* livre iniciou-se quando Richard Stallman resolveu criar o projeto GNU. De acordo com Silva *apud* Stallman (2004), o projeto GNU começou com o objetivo de desenvolver um sistema operacional compatível com Unix totalmente livre. Livre se refere à liberdade, e não ao preço; significa que está livre para executar, distribuir, estudar, mudar e melhorar o *software*.

O projeto GNU não é somente desenvolvimento e distribuição de alguns *softwares* livres úteis. O coração do projeto GNU é uma idéia: que *software* deve ser livre, e que a liberdade do usuário vale a pena ser defendida. Se as pessoas têm liberdade mas não a apreciam conscientemente, não irão mantê-la por muito tempo. Se for um desejo que a liberdade dure, é necessário chamar a atenção das pessoas para a liberdade que elas têm em programas livres.

O método do projeto GNU é que programas livres e a idéia da liberdade dos usuários ajudam-se mutuamente. Conforme as pessoas encontrem programas GNU ou o sistema GNU e comecem a usá-los, elas também pensam sobre a filosofia GNU. O *software* mostra que a idéia funciona na prática. Algumas destas pessoas acabam concordando com a idéia, e então escrevem mais programas livres. Então, o *software* carrega a idéia, dissemina a idéia e cresce da idéia.

De acordo com Silva *apud* Stallman (2004), "nós devemos continuar a falar sobre a liberdade de compartilhar e modificar *software* – e ensinar outros usuários o valor destas liberdades. Se nós nos beneficiamos por ter um sistema operacional livre, faz sentido para nós pensar em preservar estas liberdades por um longo tempo. Se nós nos beneficiamos por ter uma variedade de *software* livres, faz sentido pensar sobre encorajar outras pessoas a escrever mais *software* livre, em vez de *software* proprietário".

2.2.4.2 GNU/Linux Debian

2.2.4.2.1 O projeto Debian

Segundo Perens *et al* (2002), "Debian é uma organização totalmente voluntária, dedicada ao desenvolvimento de *software* livre e a promover os ideais da Fundação do Software Livre (Free Software Foundation). O projeto Debian foi iniciado em 1993, quando Ian Murdock lançou um convite aberto para desenvolvedores de *software* para que eles contribuíssem para uma distribuição de *software* completa e coerente baseada no relativamente novo *kernel* Linux. Essa relativamente pequena associação de entusiastas dedicados, fundada originalmente pela Free Software Foundation e influenciada pela filosofia GNU evoluiu com o passar dos anos para uma organização que possui em torno de quinhentos desenvolvedores Debian".

Ainda segundo Perens *et al* (2002), "os Desenvolvedores Debian estão envolvidos em uma variedade de atividades, incluindo administração de sites Web e FTP, design de gráficos, análise legal de licenças de *softwares*, criação de documentação e, é claro, manutenção de pacotes de *software*".

2.2.4.2.2 O projeto GNU/Linux

De acordo com Perens *et al* (2002), "o projeto GNU desenvolveu um conjunto compreensivo de ferramentas de *software* livre para uso com o Unix e outros sistemas operacionais semelhantes ao Unix, como o Linux. Estas ferramentas permitem que usuários executem tarefas das mais simples (como copiar ou remover arquivos do sistema) até tarefas mais complicadas (como escrever e compilar programas e fazer edições sofisticadas em uma variedade de formatos de documentos)".

Como um sistema operacional consiste de vários programas fundamentais que são necessários para que o computador possa se comunicar e receber instruções dos usuários, ler e gravar dados no disco rígido, controlar o uso da memória e executar outros *softwares*, segundo Perens *et al* (2002), a parte mais importante de um sistema operacional é o *kernel*. Em um sistema GNU/Linux, o Linux é o componente *kernel*. O restante do sistema

consiste de outros programas, muitos dos quais foram escritos por ou para o projeto GNU. Devido ao *kernel* Linux sozinho não constituir um sistema operacional utilizável, os desenvolvedores Debian preferem usar o termo "GNU/Linux" para se referir ao sistema quando muitas pessoas casualmente o chamam de "Linux".

2.2.4.2.3 A distribuição Debian GNU/Linux

Para Perens *et al* (2002), a combinação da filosofia e metodologia Debian com as ferramentas GNU, o *kernel* Linux, e outros importantes *softwares* livres, formam uma distribuição de software única chamada Debian GNU/Linux. Esta distribuição é constituída de um grande número de pacotes de *software*. Cada pacote na distribuição contém executáveis, *scripts*, documentação, informação de configuração e possui um mantenedor que é primariamente responsável por manter o pacote atualizado, receber os relatórios de *bugs* e se comunicar com o(s) autor(es) original(is) do *software* empacotado. A base de usuários extremamente grande, combinada com o sistema de gerenciamento de *bugs* garante que os problemas sejam encontrados e corrigidos rapidamente.

Perens *et al* (2002) destaca ainda a atenção do Debian aos detalhes que permitem construir uma distribuição de alta qualidade, estável e escalável. Instalações podem ser facilmente configuradas para servir muitos propósitos, desde *firewalls* compactos passando por estações de trabalhos *desktop* científicas até servidores de redes de alto nível.

Segundo Perens *et al* (2002), a característica que mais distingue o Debian de outras distribuições GNU/Linux é seu sistema de gerenciamento de pacotes. Estas ferramentas dão ao administrador de um sistema Debian o controle completo sobre os pacotes instalados no sistema, incluindo a habilidade de instalar um único pacote ou automaticamente atualizar o sistema operacional inteiro. Pacotes individuais podem também ser mantidos e não atualizados. Pode-se até mesmo dizer ao sistema de gerenciamento de pacotes sobre o *software* que se compilou manualmente e quais dependências ele resolve.

Para proteger o sistema contra "Cavalos de Tróia" ou de outros *softwares* mal intencionados, o Debian verifica se os pacotes tiveram origem de seus mantenedores

Debian registrados. Ainda segundo Perens *et al* (2002), empacotadores Debian também têm um grande cuidado ao configurar seus pacotes de uma maneira segura. Quando problemas de segurança em pacotes fornecidos aparecem, consertos são geralmente colocados à disposição muito rapidamente. Com as simples opções de atualização Debian, consertos de segurança podem ser obtidos e instalados automaticamente através da Internet.

2.2.4.3 NetFilter IPTables

Segundo Silva (2004), no *kernel* do Linux 2.4, foi introduzido o *firewall* IPTtables (também chamado de NetFilter) que substitui o IPChains dos *kernels* da série 2.2. Este novo *firewall* tem como vantagem ser muito estável (assim como o *IPChains* e *IPFWAdm*), confiável, permitir muita flexibilidade na programação de regras pelo administrador do sistema, mais opções disponíveis ao administrador para controle de tráfego, controle independente do tráfego da rede local ou entre redes devido a nova organização das etapas de roteamento de pacotes.

O IPTtables é um *firewall* em nível de pacotes e funciona baseado no endereço/porta de origem/destino do pacote, prioridade, etc. Ele funciona através da comparação de regras para saber se um pacote tem ou não permissão para passar. Em *firewalls* mais restritivos, o pacote é bloqueado e registrado para que o administrador do sistema tenha conhecimento sobre o que está acontecendo em seu sistema.

Ainda de acordo com Silva (2004), o IPTables também pode ser usado para modificar e monitorar o tráfego da rede, fazer NAT, redirecionamento de pacotes, marcação de pacotes, modificação de prioridade de pacotes que chegam ou saem do sistema, contagem de *bytes*, divisão de tráfego entre máquinas, criação de proteções contra *anti-spoofing*, inundação SYN, negação de serviços DoS, etc. O tráfego vindo de máquinas desconhecidas da rede pode também ser bloqueado/registrado através do uso de regras simples. As possibilidades oferecidas pelos recursos de filtragem IPTables como todas as ferramentas UNIX maduras dependem de sua imaginação, pois ele garante uma grande flexibilidade na manipulação das regras de acesso ao sistema, precisando apenas conhecer

quais interfaces o sistema possui, o que deseja bloquear, o que tem acesso garantido, quais serviços devem estar acessíveis para cada rede, e iniciar a construção de seu *firewall*.

O IPTtables ainda tem a vantagem de ser modularizável, e outras funções podem ser adicionadas ao *firewall*, ampliando as possibilidades oferecidas.

2.2.4.3.1 Características do firewall IPTables

De acordo com Silva (2004), as principais características do NetFilter IPTables são:

- Especificação de portas ou endereço de origem ou destino;
- Suporte a protocolos TCP, UDP e ICMP (incluindo tipos de mensagens ICMP);
- Suporte a interfaces de origem ou destino de pacotes;
- Manipula serviços de *proxy* na rede;
- Tratamento de tráfego dividido em *chains* (para melhor controle do tráfego que entra ou sai da máquina e tráfego redirecionado);
- Permite um número ilimitado de regras por *chain*;
- Muito rápido, estável e seguro;
- Possui mecanismos internos para rejeitar automaticamente pacotes duvidosos ou mal formados;
- Suporte a módulos externos para expansão das funcionalidades padrões oferecidas pelo código de *firewall*;
- Suporte completo a roteamento de pacotes, tratadas em uma área diferente de tráfegos padrões;
- Suporte a especificação de tipo de serviço para priorizar o tráfego de determinados tipos de pacotes;
- Permite especificar exceções para as regras ou parte das regras;
- Suporte a detecção de fragmentos;
- Permite enviar alertas personalizados ao *syslog* sobre o tráfego aceito ou bloqueado;
- Redirecionamento de portas;
- *Masquerading*;

- Suporte a SNAT – *Source* NAT – para modificação do endereço de origem das máquinas para um único IP ou faixa de IP's;
- Suporte a DNAT – *Destination* NAT – para modificação do endereço de destino das máquinas para um único IP ou fixa de IP's;
- Contagem de pacotes que atravessaram uma interface ou regra;
- Limitação de passagem de pacotes ou conferência de regra (muito útil para criar proteções contra inundação SYN, "ping da morte", negação de serviços DoS, etc.).

2.3 Sistemas que se quer proteger

Os sistemas SIAFI e SIDOR, ambos do governo federal, podem ser acessados através da rede de comunicação do SERPRO, ou no caso do SIDOR, também pela rede da Secretaria de Orçamento Federal.

O que se quer proteger é a comunicação entre as redes da CEAGESP e do SERPRO. Apesar de Tanenbaum (1997) afirmar que a melhor maneira de se fazer isto é através de um túnel criptografado entre as duas redes, antes de se criar este túnel é extremamente aconselhável que seja implementado primeiro um *firewall* que fique na borda do perímetro de segurança destas redes.

2.3.1 SIAFI – Sistema integrado de administração financeira

O SIAFI é um sistema de informações centralizado em Brasília, ligado por teleprocessamento aos órgãos do Governo Federal distribuídos no País e no exterior. Essa ligação, que é feita pela rede de telecomunicações do SERPRO e também pela conexão a outras inúmeras redes externas, é que garante o acesso ao sistema às quase 13.800 Unidades Gestoras ativas no SIAFI.

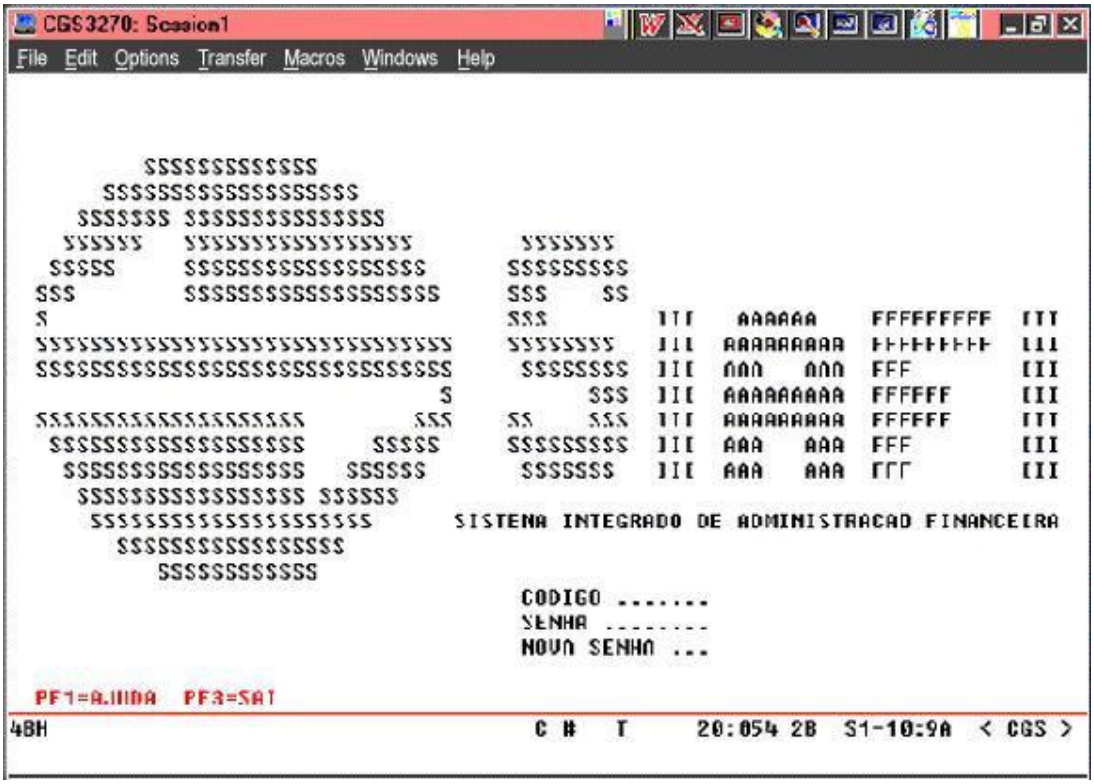

Figura 8 – Tela de acesso ao sistema SIAFI, STN (1999)

De acordo com STN (2005), o objetivo principal do SIAFI é servir de instrumento utilizado para registro, acompanhamento e controle da execução orçamentária, financeira e patrimonial do Governo Federal. Desde sua criação, o SIAFI tem alcançado satisfatoriamente seus principais objetivos, que são:

- Prover mecanismos adequados ao controle diário da execução orçamentária, financeira e patrimonial aos órgãos da Administração Pública;
- Fornecer meios para agilizar a programação financeira, otimizando a utilização dos recursos do Tesouro Nacional, através da unificação dos recursos de caixa do Governo Federal;
- Permitir que a contabilidade pública seja fonte segura e tempestiva de informações gerenciais destinadas a todos os níveis da Administração Pública Federal;
- Padronizar métodos e rotinas de trabalho relativas à gestão dos recursos públicos, sem implicar rigidez ou restrição a essa atividade, uma vez que ele permanece sob total controle do ordenador de despesa de cada unidade gestora;

- Permitir o registro contábil dos balancetes dos estados e municípios e de suas supervisionadas;
- Permitir o controle da dívida interna e externa, bem como o das transferências negociadas;
- Integrar e compatibilizar as informações no âmbito do Governo Federal;
- Permitir o acompanhamento e a avaliação do uso dos recursos públicos; e
- Proporcionar a transparência dos gastos do Governo Federal.

2.3.1.1 Vantagens do SIAFI

De acordo com STN (2005), o SIAFI representou tão grande avanço para a contabilidade pública da União que ele é hoje reconhecido no mundo inteiro e recomendado inclusive pelo Fundo Monetário Internacional. Seu desempenho transcendeu de tal forma as fronteiras brasileiras e despertou a atenção no cenário nacional e internacional, que vários países, além de alguns organismos internacionais, têm enviado delegações à Secretaria do Tesouro Nacional, com o propósito de absorver tecnologia para a implantação de sistemas similares.

Entre os ganhos que a implantação do SIAFI trouxe para a Administração Pública Federal, destacam-se:

- Contabilidade: o gestor ganha tempestividade na informação, qualidade e precisão em seu trabalho;
- Finanças: agilização da programação financeira, otimizando a utilização dos recursos do Tesouro Nacional, por meio da unificação dos recursos de caixa do Governo Federal na Conta Única no Banco Central;
- Orçamento: a execução orçamentária passou a ser realizada tempestivamente e com transparência, completamente integrada a execução patrimonial e financeira;
- Visão clara de quantos e quais são os gestores que executam o orçamento: os números da época da implantação do SIAFI indicavam a existência de aproximadamente 1.800 gestores. Na verdade, eram mais de 4.000 que hoje estão cadastrados e executam seus gastos através do sistema de forma “on-line”;

- Desconto na fonte de impostos: atualmente, o imposto devido já é recolhido no momento do pagamento;
- Auditoria: facilidade na apuração de irregularidades com o dinheiro público;
- Transparência: poucas pessoas tinham acesso às informações sobre as despesas do Governo Federal antes do advento do SIAFI. A prática da época era tratar essas despesas como "assunto sigiloso". Hoje a história é outra, pois na democracia o cidadão é o grande acionista do estado;
- Fim da multiplicidade de contas bancárias: os números da época indicavam 3.700 contas bancárias e o registro de aproximadamente 9.000 documentos por dia. Com a implantação do SIAFI, constatou-se que existiam em torno de 12.000 contas bancárias e se registravam em média 33.000 documentos diariamente. Hoje, 98% dos pagamentos são identificados de modo instantâneo na Conta Única e 2% deles com uma defasagem de, no máximo, cinco dias.

Além de tudo isso, o SIAFI apresenta inúmeras vantagens que o distinguem de outros sistemas em uso no âmbito do Governo Federal:

- Sistema disponível 100% do tempo e *on-line*;
- Sistema centralizado, o que permite a padronização de métodos e rotinas de trabalho;
- Interligação em todo o território nacional;
- Utilização por todos os órgãos da Administração Direta (poderes Executivo, Legislativo e Judiciário);
- Utilização por grande parte da Administração Indireta;
- Integração periódica dos saldos contábeis das entidades que ainda não utilizam o SIAFI, para efeito de consolidação das informações econômico-financeiras do Governo Federal – à exceção das Sociedades de Economia Mista, que têm registrada apenas a participação acionária do Governo – e para proporcionar transparência sobre o total dos recursos movimentados.

2.3.1.2 Principais atribuições do SIAFI

O SIAFI é um sistema informatizado que processa e controla, por meio de terminais instalados em todo o território nacional, a execução orçamentária, financeira, patrimonial e contábil dos órgãos da Administração Pública Direta Federal, das autarquias, fundações e empresas públicas federais e das sociedades de economia mista que estiverem contempladas no Orçamento Fiscal e/ou no Orçamento da Seguridade Social da União.

Segundo STN (2005), o sistema pode ser utilizado pelas Entidades Públicas Federais, Estaduais e Municipais apenas para receberem, pela Conta Única do Governo Federal, suas receitas (taxas de água, energia elétrica, telefone, etc.) dos Órgãos que utilizam o sistema. Entidades de caráter privado também podem utilizar o SIAFI, desde que autorizadas pela STN – Secretaria do Tesouro Nacional. No entanto, essa utilização depende da celebração de convênio ou assinatura de termo de cooperação técnica entre os interessados e a STN, que é o órgão gestor do SIAFI.

2.3.1.3 Considerações sobre a segurança do SIAFI

Segundo o tutorial do SIAFI, disponível no site da Secretaria do Tesouro Nacional do Ministério da Fazenda, acessado em maio de 2005, as ligações de usuários do SIAFI representam hoje um universo de aproximadamente 2.800 circuitos de comunicação na arquitetura SNA, com controladoras e terminais, as quais devem ser alteradas para a implantação do SIAFI XXI. Destas ligações, algumas já atendem os requisitos de infra-estrutura de rede requeridos para acesso ao novo sistema e para o SIAFI atual. Visando o aproveitamento da infra-estrutura de rede disponível, com redução das redundâncias existentes em nível de Governo Federal e otimizando operação destas redes, o SERPRO juntamente com os usuários responsáveis pelas respectivas unidades estarão avaliando as conexões existentes e disponibilizando a melhor alternativa para uso do SIAFI XXI.

Ainda segundo o tutorial, a Política de Segurança a ser adotada estabelecerá os aspectos de confidencialidade, integridade e disponibilidade para o SIAFI XXI, no que se refere a sistemas, servidores (*hardware*, ambiente operacional e produtos), redes de comunicação, controle de acesso, estações de trabalho, instalações físicas, pessoas, dados e

informações, classificação da informação e infra-estrutura de chaves públicas. Alinhados com a Política de Segurança, no segmento rede de comunicação, a solução deve prever facilidades de implementação física das normas e procedimentos nos níveis tático e operacional para garantir a segurança do tráfego de rede exigida para o SIAFI XXI.

2.3.1.3.1 Procedimentos de segurança para a REDE SIAFI

No que se refere à rede, a SERPRO adota uma solução de segurança em 3 níveis.

2.3.1.3.1.1 Nível 1 - Procedimentos básicos em relação à Internet

Estes procedimentos estabelecem segurança básica de proteção, para preservar a estrutura (*firewall*) e o conjunto de Intranets, dos tipos básicos de vulnerabilidades. As regras e customizações realizadas neste nível formam as premissas fundamentais da proteção do ambiente e não são alteradas sobre o risco da perda da segurança corporativa.

2.3.1.3.1.2 Nível 2 - Procedimentos de segurança da STN a Extranets e Internet

Neste nível de procedimentos a STN deve estabelecer quais os acessos e serviços que serão permitidos entre as redes que compõem a Intranet do SERPRO e a REDE SIAFI. Esse nível regula as conexões e/ou serviços estabelecidos entre redes consideradas externas para a STN (incluindo políticas específicas de acesso Internet).

Esse conjunto de procedimentos deverá ser aderente ao nível anterior.

Esse nível é implementado no *firewall* corporativo (DMZ SIAFI XXI) e no *firewall* de interligação das Intranets (incluindo acesso ao *mainframe*).

2.3.1.3.1.3 Nível 3 - Certificação digital por meio do SIAFI

Neste nível será feita a certificação digital dos usuários por meio da Autoridade Certificadora, garantindo a integridade de operação do Sistema.

2.3.1.3.2 Contingência para acesso a Internet

De forma a suprir a característica de contingência do ambiente sem perda de acesso, o *firewall* de alta disponibilidade prevê uma arquitetura da solução onde a meta é a utilização dos recursos redundantes previstos nas plataformas de *firewall*, de forma global e simultânea, conforme STN (2005). Sendo assim, a arquitetura prevê uma produção baseada na divisão de tráfego entre as duas plataformas e entre as DMZ's protegidas pelo *firewall*.

A solução de contingência garante a continuidade dos serviços produzidos na rede SIAFI, Intranet e áreas de publicação Internet, sem perda da segurança.

2.3.1.4 Formas de acesso permitidas pelo SIAFI

Para uso do SIAFI, cinco alternativas de acesso à Rede SERPRO são possíveis.

2.3.1.4.1 Acesso à Intranet do SERPRO

Nesta modalidade de conexão, a rede do usuário faz parte do *backbone* da rede SERPRO:

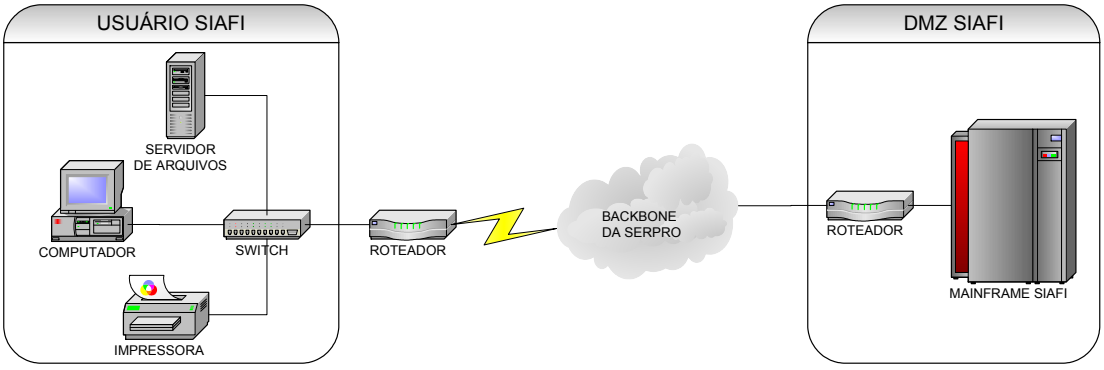

Figura 9 – Acesso ao SIAFI via Intranet, STN (2005)

2.3.1.4.2 Acesso VPN (Virtual Private Network – Rede Privada Virtual)

Nesta solução, os usuários do SIAFI estarão conectados a uma rede local que por sua vez possuirá um roteador conectado a um *switch* WAN no *backbone* da Rede do SERPRO. Existirá uma conexão permanente virtual (PVC) entre dois roteadores – o da LAN do cliente e o da regional do SERPRO mais próximo – que por sua vez terá uma conexão permanente virtual (PVC) com a zona desmilitarizada (DMZ) que abriga o roteador sumarizador de rotas da REDE SIAFI. Os usuários acessarão o SIAFI Atual através de emulação de terminais pelo aplicativo HOD (Host On Demand) desenvolvido pela IBM para ambientes WEB (Internet).

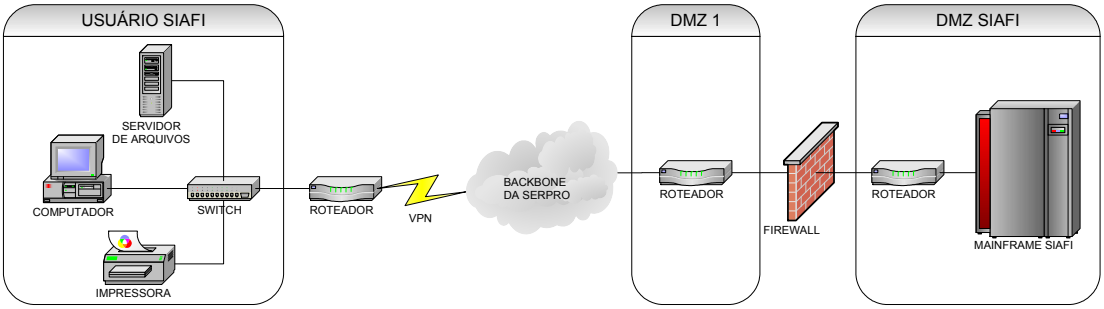

Figura 10 – Acesso ao SIAFI via VPN, STN (2005)

2.3.1.4.3 Acesso Extranet

Conforme STN (2005), as redes de Órgãos Governamentais que tenham interesse em acessar o SIAFI XXI terão sua conexão física estabelecida com a DMZ do SERPRO Regional Brasília. Os usuários acessarão o SIAFI Atual através de emulação de terminais pelo aplicativo HOD (Host On Demand) desenvolvido pela IBM para ambientes WEB (Internet).

A partir do SERPRO Regional Brasília, haverá um roteador que fará a sumarização de rotas e por sua vez terá uma conexão permanente virtual (PVC) com a zona desmilitarizada (DMZ) externa à DMZ STN, de acordo com a figura abaixo:

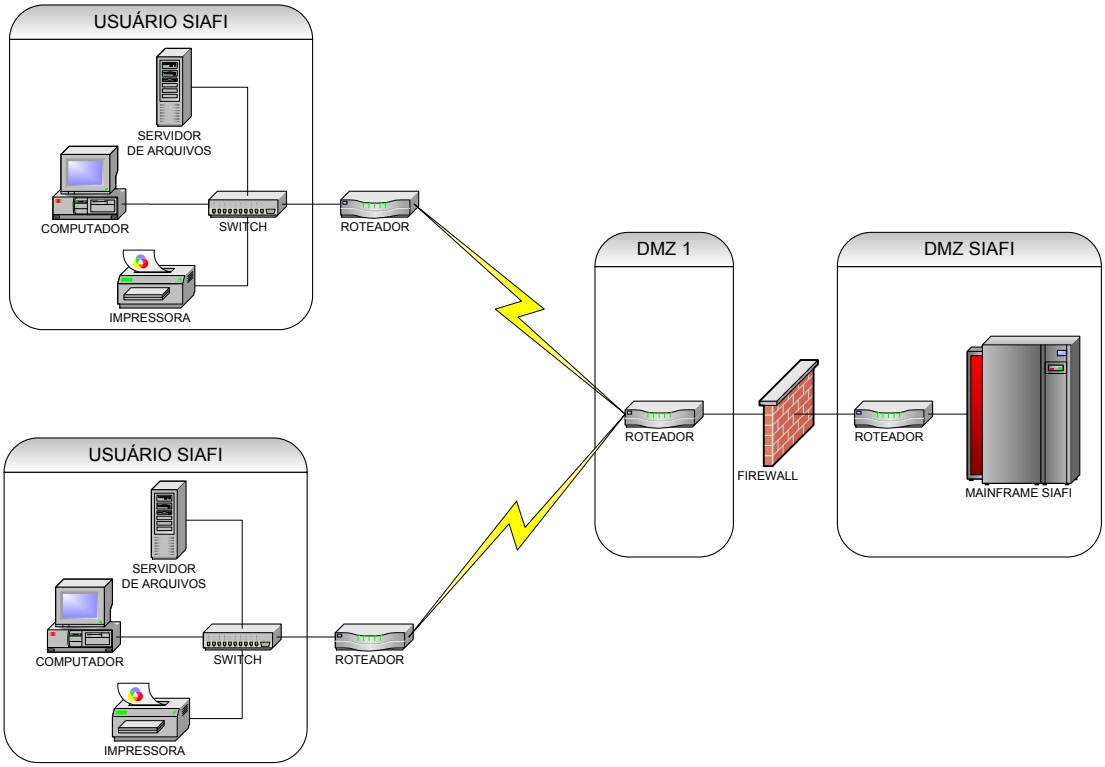

Figura 11 – Acesso ao SIAFI via Extranet, STN (2005)

2.3.1.4.4 Acesso seguro pela Internet

As unidades com um ponto de acesso, baixa utilização do SIAFI XXI e com capacidade de contratação de um provedor de serviço de Internet poderá fazer conexão com a rede SERPRO, utilizando-se de uma conexão representada a seguir:

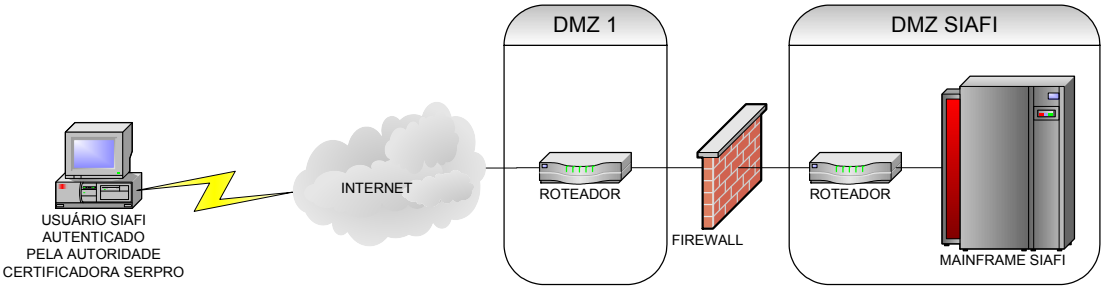

Figura 12 – Acesso ao SIAFI via Internet, STN (2005)

Com este tipo de conexão, por meio do acesso Internet, o usuário do SIAFI XXI terá os seus dados criptografados pelo protocolo SSL. O acesso ao SIAFI XXI será com autenticação forte utilizando certificados digitais emitidos pela unidade certificadora. O

acesso ao SIAFI Atual será feito com emulação de terminais através do aplicativo HOD (Host on Demand) desenvolvido pela IBM para funcionamento dentro de ambientes WEB (Internet).

2.3.1.4.5 Acesso discado seguro

As unidades com um ponto de acesso, baixa utilização do SIAFI XXI e sem capacidade de contratação de um provedor de serviço de Internet, poderão fazer conexão com a rede SERPRO, utilizando-se da conexão representada a seguir:

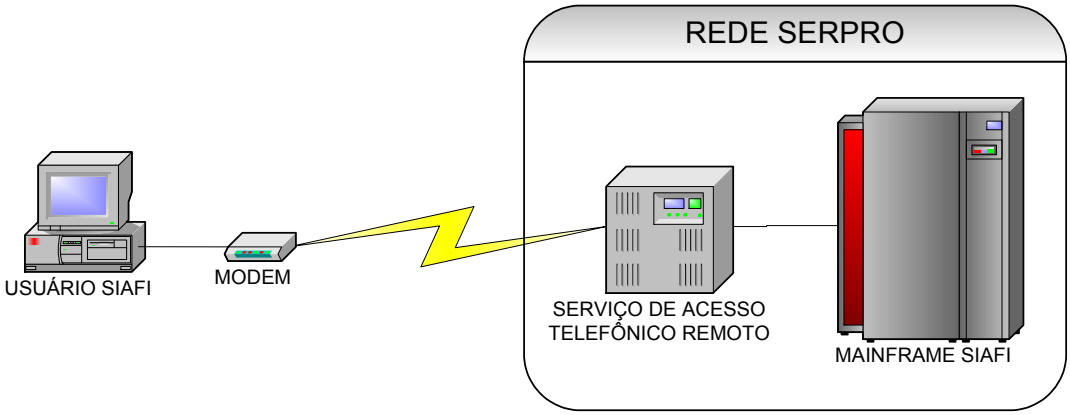

Figura 13 – Acesso ao SIAFI via conexão discada, STN (2005)

2.3.1.5 Forma de acesso ao SIAFI adotada pela CEAGESP

Para acessar o SIAFI, a CEAGESP usa o acesso via Internet. No *firewall* deve ser configurada uma regra que dê permissão aos usuários acessarem o seguinte endereço:

```
https://acesso.serpro.gov.br/HOD700/logonID.htm
```

Esta URL corresponde ao seguinte endereço IP:

```
161.148.40.200:443
```

Desta forma, o acesso ao SIAFI será feito com emulação de terminais através do aplicativo HOD (Host on Demand) desenvolvido pela IBM para funcionamento dentro de ambientes WEB (Internet).

2.3.2 SIDOR – Sistema Integrado de Dados Orçamentários

De acordo com o Glossário de Termos Legislativos e Orçamentários, da Câmara Federal de Deputados, o SIDOR é operado e gerenciado pela Secretaria de Orçamento e Federal (SOF) do Ministério do Planejamento, Orçamento e Gestão, com a finalidade de sistematizar os dados relativos aos orçamentos da União. Para a Secretaria do Tesouro Nacional, o SIDOR é também um conjunto de procedimentos, justapostos entre si, com a incumbência de cuidar do processamento de cunho orçamentário, através de computação eletrônica, cabendo sua supervisão à Secretaria de Orçamento Federal.

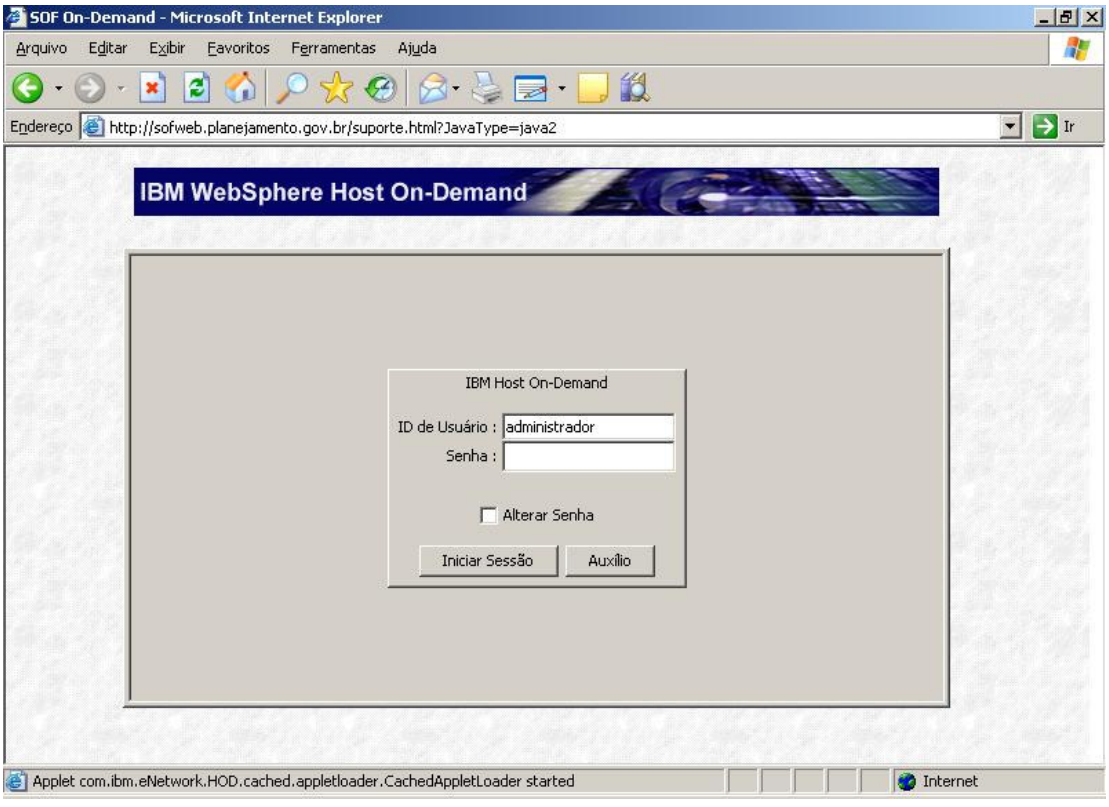

Figura 14 – Tela de acesso ao SIDOR, SOF (2005)

2.3.2.1 Formas de acesso permitidas pelo SIDOR

O SIDOR poder ser acessado através da rede SERPRO ou através da rede do próprio Ministério do Planejamento. Neste caso específico, a CEAGESP acessa o SIDOR através da rede do Ministério do Planejamento.

2.3.2.1.1 Através da rede SERPRO

Para acessar o SIDOR através da rede do SERPRO, pode ser usado as mesmas vias de acesso do SIAFI.

2.3.2.1.2 Através da Secretaria de Orçamento Federal

Outra forma de acessar o SIDOR é através da própria rede do Ministério do Planejamento, Orçamento e Gestão.

2.3.2.2 Forma de acesso ao SIDOR adotada pela CEAGESP

Para acessar o SIDOR, a CEAGESP usa o acesso via Secretaria de Orçamento Federal. No *firewall* deve ser configurada uma regra que dê permissão aos usuários acessarem o seguinte endereço:

```
http://sofweb.planejamento.gov.br
```

Esta URL corresponde ao seguinte endereço IP:

```
200.198.196.8
```

Ainda deve ser habilitados para o endereço acima a abertura das portas TCP 23, 8999 e 23000, saindo da rede local para a Internet.

Desta forma, o acesso ao SIDOR será feito com emulação de terminais através do aplicativo HOD (Host on Demand) desenvolvido pela IBM para funcionamento dentro de

ambientes WEB (Internet). O acesso via HOD é baseado em um *applet* que é executado na máquina cliente e abrindo conexões diretamente com uma máquina na rede da Secretaria de Orçamento Federal. Todo o tráfego é criptografado com chave de 128 *bits*.

Figura 15 – Página de acesso da Secretaria de Orçamento Federal, SOF (2005)

2.3.3 Diretrizes de acesso da CEAGESP

O objetivo da Norma Geral 002 da CEAGESP é determinar as regras de utilização da rede corporativa, os direitos de acesso dos funcionários e as punições aplicáveis para as atitudes consideradas violação das normas de utilização da rede, assegurando que os recursos computacionais disponibilizados ao usuário sejam utilizados para as finalidades aprovadas pela CEAGESP.

De acordo com esta norma, os recursos de uma rede corporativa são definidos pelos equipamentos e serviços utilizados pelos funcionários como os computadores, e-mails do domínio da empresa, Intranet, Internet, impressoras, dentre outros.

O DETIN – Departamento de Tecnologia da Informação – é o responsável pelo cadastramento dos usuários na rede corporativa da CEAGESP. Para os controles na utilização da rede quanto ao *login* e à manutenção de arquivos no servidor, ficam proibidas ao usuário da rede corporativa da CEAGESP as seguintes ações:

- Obter acesso não autorizado com tentativas de fraude na autenticação de usuário ou segurança de um servidor, rede ou conta, incluindo acesso aos dados não disponíveis ao usuário;
- Interferir nos serviços de qualquer outro usuário, servidor ou rede;
- Usar de programas ou comandos que interfiram no acesso de outro usuário;
- Acessar, armazenar, editar, expor e distribuir qualquer material de natureza pornográfica e racista;
- Criar ou remover arquivos fora da área alocada ao usuário para o desempenho de suas funções;
- Ausentar-se do seu local de trabalho sem encerrar os programas acessados, inclusive o *login* da rede;
- Emprestar ou divulgar senhas de acesso a outros funcionários;
- Instalar ou remover *softwares*;
- Abrir os computadores para qualquer reparo;
- Alterar as configurações de rede e de inicialização dos equipamentos disponíveis ao usuário.

2.3.3.1 Da utilização de e-mail

O DETIN – Departamento de Tecnologia da Informação – é o responsável pelo servidor de e-mail da CEAGESP, competindo-lhe fiscalizar a obediência pelos usuários no recebimento e envio de e-mails e no gerenciamento das contas, ficando assim proibidas as seguintes ações:

- Enviar e-mail a qualquer pessoa que não o deseje receber acatando o pedido de interrupção pelo destinatário;
- Enviar e-mails que tenham a finalidade de mala-direta como, por exemplo: publicidade, anúncios e informativos ou propaganda política;

- Reenviar mensagens em cadeia independentemente da vontade do destinatário em recebê-las;
- Enviar e-mails que sobrecarreguem o servidor ou a caixa postal de outro usuário;
- Forjar qualquer das informações do cabeçalho do remetente;
- Utilizar inadequadamente a linguagem em e-mails comerciais e/ou profissionais;
- Enviar e-mails com linguagem ofensiva e de baixo calão;
- Distribuir, através do e-mail, material pornográfico, racista, profano ou que atente à moral e aos bons costumes.

Aos usuários cabem ainda, obrigatoriamente, os seguintes procedimentos:

- A manutenção da caixa de e-mail, evitando acúmulo de mensagens e arquivos inúteis, cuja cota não deve ultrapassar os 40 MB;
- A utilização de programa gerenciador de e-mail homologado pelo DETIN - Departamento de Tecnologia da Informação;
- A utilização do protocolo IMAP para recebimento dos e-mails provenientes do domínio ceagesp.gov.br.

2.3.3.2 Da utilização da Internet

O acesso a Internet entendido como navegação a *sites*, *downloads* e *uploads* de arquivos, será fornecido aos usuários cadastrados junto ao DETIN – Departamento de Tecnologia da Informação – que ficará responsável por fiscalizar o cumprimento das seguintes proibições impostas aos usuários:

- Fazer *downloads* ou distribuir *softwares* e dados não legalizados durante o acesso a Internet;
- Divulgar as informações confidenciais da empresa em grupos de discussão, listas ou bate-papo;
- Efetuar *uploads* de *software* licenciado a Empresa ou de qualquer informação sem expressa autorização do gerente responsável;

- Utilizar *softwares* de comunicação instantânea como por exemplo, ICQ, Microsoft Messenger e afins;
- Utilizar *softwares* de *peer-to-peer* (P2P) como por exemplo, Kazaa, Morpheus e afins;
- Utilizar serviços de *streaming* como por exemplo, Rádios On-Line, Usina do Som e afins;
- Acessar *sites* cujo conteúdo seja racista, pornográfico ou profano;
- Utilizar a Internet para assuntos que não sejam relevantes à execução das atividades profissionais.

3 Implementando as regras do Firewall

3.1 Migrando as regras do Firewall-1 da Checkpoint

A configuração atual da rede da CEAGESP se baseia no Firewall-1 da Checkpoint para proteção da fronteira do perímetro de segurança. Para auxiliar a navegação na Internet, há também um servidor *proxy* Microsoft Proxy Server 2.0, para fazer *cache* das páginas Web.

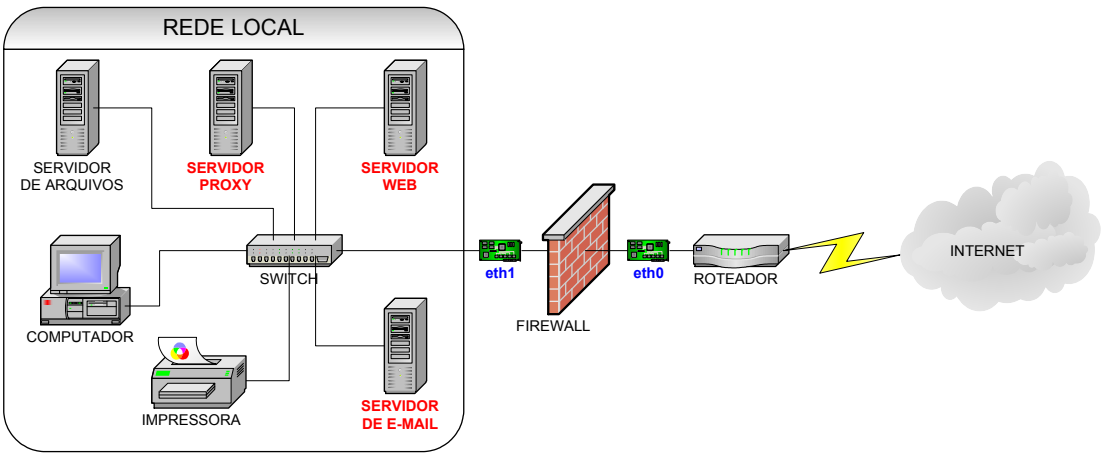

Figura 16 – Configuração de *Firewall* atual com PROXY

O Firewall-1 está baseado em um sistema Windows NT. Para configurar as regras do *firewall* utiliza-se uma interface gráfica como a mostrada abaixo:

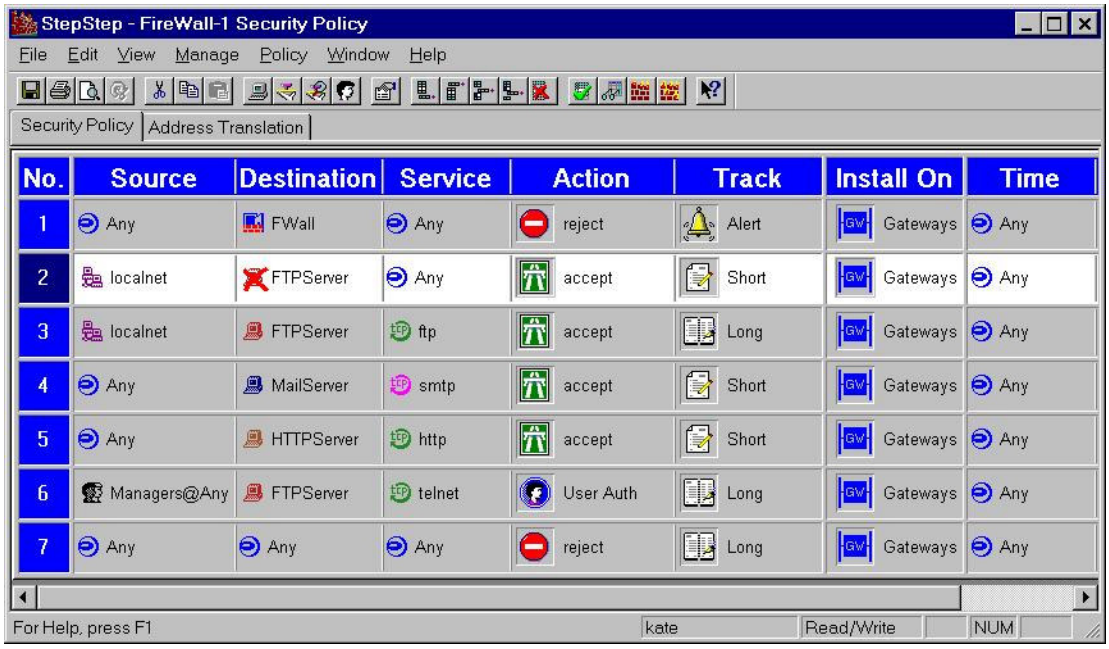

Figura 17 – Tela de configuração do Check Point Firewall-1, CheckPoint (2002)

Um resumo das principais regras do *firewall* está descrito na tabela abaixo. Por motivos de segurança e confidencialidade, algumas informações foram propositadamente omitidas.

#	ORIGEM	DESTINO	SERVIÇO	AÇÃO
01	mail2 (x.y.z.w) NAT – x.y.z.w	*qualquer*	*qualquer*	*aceitar*
02	web-gov (x.y.z.w) NAT – x.y.z.w	*qualquer*	HTTP (80) PORT URI	*aceitar*
03	*qualquer*	web-gov (x.y.z.w)	HTTP (80) PORT URI	*aceitar*
04	webmail (x.y.z.w) NAT – x.y.z.w	*qualquer*	DNS, FTP, HTTP, HTTPS, LOGIN, POP3, SMTP, TELNET	*aceitar*
05	*qualquer*	webmail (x.y.z.w) NAT – x.y.z.w	DNS (TCP, UDP), HTTP	*aceitar*
06	invasor (x.y.z.w /32)	*qualquer*	*qualquer*	*descartar*
07	invasor_trem_task (200.162.176.13/32)	*qualquer*	*qualquer*	*descartar*
08	*qualquer*	mail2 (x.y.z.w) NAT – x.y.z.w	SMTP, HTTP, ICMP-PROTO, DNS	*aceitar*
09	-	-	-	-

10	*qualquer*	trem.task.com.br (200.162.176.13/32)	*qualquer*	*descartar*
11	-	-	-	-
12	-	-	-	-
13	proxy_1 (x.y.z.w) NAT – x.y.z.w	*qualquer*	SMTP, HTTP, HTTPS, FTP	*aceitar*
14	router_Embratel (x.y.z.w)	mail2 (x.y.z.w) NAT – x.y.z.w web-gov (x.y.z.w) NAT – x.y.z.w	*qualquer*	*aceitar*
15	-	-	-	-
16	-	-	-	-
17	*qualquer*	*qualquer*	*qualquer*	*descartar*

Tabela 1 – Regras do Check Point Firewall-1

Na seqüência, uma breve explicação de cada regra:

- Regra 01 – permitir qualquer serviço originado do servidor de e-mail e da rede interna com destino à Internet;
- Regra 02 – permitir o serviço HTTP originado do servidor de web e da rede interna com destino à Internet;
- Regra 03 – permitir o serviço HTTP originado de qualquer lugar com destino ao servidor de web;
- Regra 04 – permitir os serviços de DNS, FTP, HTTP, HTTPS, LOGIN, POP3, SMTP e TELNET originados do servidor de e-mail e da rede interna com destino à Internet;
- Regra 05 – permitir os serviços DNS (TCP, UDP) e HTTP de qualquer lugar com destino ao servidor de e-mail e à rede interna;
- Regra 06 – descartar qualquer serviço originado do endereço especificado;
- Regra 07 – descartar qualquer serviço originado do endereço especificado;
- Regra 08 – permitir os serviços SMTP, HTTP, ICMP e DNS de qualquer lugar com destino ao servidor de e-mail e à rede interna;
- Regra 09 – omitida por motivos de segurança e confidencialidade;
- Regra 10 – descartar qualquer serviço originado de qualquer lugar com destino ao endereço especificado;
- Regra 11 – omitida por motivos de segurança e confidencialidade;

- Regra 12 – omitida por motivos de segurança e confidencialidade;
- Regra 13 – permitir os serviços SMTP, HTTP, HTTPS e FTP originados do servidor *proxy* e da rede interna com destino à Internet;
- Regra 14 – permitir qualquer serviço originado do roteador com destino aos servidores de e-mail, de web e à rede interna;
- Regra 15 – omitida por motivos de segurança e confidencialidade;
- Regra 16 – omitida por motivos de segurança e confidencialidade;
- Regra 17 – descarta qualquer serviço que não se enquadre nas regras anteriores.

3.2 Necessidades atuais

De acordo com a Norma Geral 002 da CEAGESP, os usuários deverão seguir as seguintes normas para acesso à Internet:

- Utilizar o protocolo IMAP para recebimento dos e-mails provenientes do domínio ceagesp.gov.br dentro da rede local;
- Não utilizar *softwares* de comunicação instantânea como ICQ, Microsoft Messenger e afins;
- Não utilizar *softwares* de *peer-to-peer* (P2P) como Kazaa, Morpheus e afins;
- Não utilizar serviços de *streaming* como Rádios On-Line, Usina do Som e afins;
- Não acessar *sites* cujo conteúdo seja racista, pornográfico ou profano.

Algumas destas normas podem ser implementadas através da configuração de um *firewall*. Outras porém, dependem também de um servidor *proxy*.

3.3 Implementando as regras no NetFilter IPTables

O *firewall* IPTables será instalado em um microcomputador com três placas de rede com o sistema operacional Debian Sarge 3.0 instalado. A primeira placa de rede será destinada para a conexão com a Internet; a segunda placa de rede será usada para dar acesso à zona desmilitarizada (DMZ) e a terceira placa de rede dará acesso à rede local.

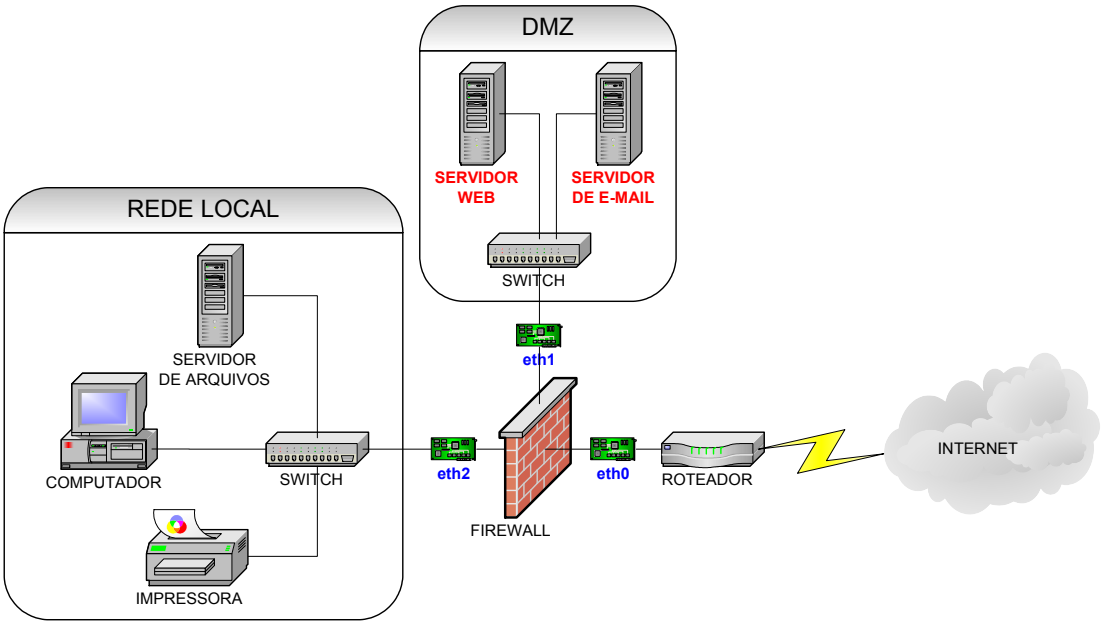

Figura 18 – Configuração de *Firewall* com DMZ

Arquivo de script para configuração do *firewall*:

Início do *script*:

```
$!/bin/bash
```

Declaração de variáveis auxiliares:

```
IPT='sbin/iptables'
NET_IFACE='eth0'
LAN_IFACE='eth1'
CLAN_IFACE='eth2'
LAN_RANGE='x.y.z.w/xx'
CLAN_RANGE='x.y.z.w/xx'
```

É assumido um sistema usando *kmod* para carga automática dos módulos usados por esta configuração do *firewall*:

```
/sbin/modprobe ip_conntrack
/sbin/modprobe ipt_MASQUERADE
```

```
/sbin/modprobe ipt_LOG
/sbin/modprobe iptable_nat
/sbin/modprobe ip_nat_ftp
```

Habilita o repasse de pacotes do *kernel*:

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

Limpa todas as regras existentes nas *chains* INPUT, OUTPUT E FORWARD:

```
$IPT –F
```

Limpa as regras existentes na tabela de NAT:

```
$IPT –t nat –F
```

Por padrão, descarta quaisquer pacotes que não estiverem especificados nas regras da tabela *filter*:

```
$IPT –t filter –P FORWARD DROP
```

Zera contador de *bytes* das *chains*:

```
$IPT –Z
```

Define a política padrão para descartar pacotes em cada *chain*:

```
/sbin/iptables –P FORWARD DROP
/sbin/iptables –P INPUT DROP
/sbin/iptables –P OUTPUT DROP
```

Proteção contra inundação SYN:

```
/sbin/iptables –A filter –p tcp --syn –m limit --limit
1/s –j ACCEPT
```

Proteção contra “ping da morte”:

```
/sbin/iptables –A filter –p icmp --icmp-type echo-
request –m limit --limit 1/s –j ACCEPT
```

Bloqueia outras conexões:

```
/sbin/iptables –A filtro –j DROP
```

Modifica o endereço IP destino dos pacotes de x.y.z.w vindo da interface eth0 para 192.168.1.x, para os serviços HTTP e DNS:

```
$IPT –t nat –A PREROUTING –p tcp –i eth0 –d x.y.z.w --
dport 80 --sport 1024:65535 –j DNAT --to 192.168.1.x:80

$IPT –t nat –A PREROUTING –p tcp –i eth0 –d x.y.z.w --
dport 53 --sport 1024:65535 –j DNAT --to 192.168.1.x:53

$IPT –t nat –A PREROUTING –p udp –i eth0 –d x.y.z.w --
dport 53 --sport 1024:65535 –j DNAT --to 192.168.1.x:53

$IPT –A FORWARD –p tcp –i eth0 –O eth1 –d 192.168.1.x --
dport 80 --sport 1024:65535 –m state --state NEW –j
ACCEPT

$IPT –A FORWARD –p tcp –i eth0 –O eth1 –d 192.168.1.x --
dport 53 --sport 1024:65535 –m state --state NEW –j
ACCEPT
```

```
$IPT –A FORWARD –p udp –i eth0 –O eth1 –d 192.168.1.x --
dport 53 --sport 1024:65535 –m state --state NEW –j
ACCEPT

$IPT –A FORWARD –t filter –i eth1 –m state --state NEW,
ESTABLISHED, RELATED –j ACCEPT

$IPT –A FORWARD –t filter –i eth0 –m state --state
ESTABLISHED, RELATED –j ACCEPT
```

Permite o tráfego entre a rede local e a DMZ:

```
$IPT –t filter –A INPUT –i lo –s 0/0 –d 0/0 –j ACCEPT
$IPT –t filter –A OUTPUT –o lo –s 0/0 –d 0/0 –j ACCEPT

$IPT –t filter –A INPUT –i $LAN_IFACE –m state --state
NEW –j ACCEPT
$IPT –t filter –A INPUT –i $CLAN_IFACE –m state --state
NEW –j ACCEPT
$IPT –t filter –A INPUT –m state --state ESTABLISHED,
RELATED –j ACCEPT
```

Permite o acesso a serviços HTTP, HTTPS e DNS:

```
$IPT –t filter –A FORWARD –d 0/0 --dport 80, 443, 53 –s
$LAN_RANGE –o $NET_IFACE –j ACCEPT

$IPT –t filter –A FORWARD –d 0/0 --dport 80, 443, 53 –s
$CLAN_RANGE –o $NET_IFACE –j ACCEPT

$IPT –t filter –A FORWARD –d $LAN_RANGE –s 0/0 --sport
80, 443, 53 –i $NET_IFACE –j ACCEPT
$IPT –t filter –A FORWARD –d $CLAN_RANGE –s 0/0 --sport
80, 443, 53 –i $NET_IFACE –j ACCEPT
```

Permite o acesso ao SIAFI:

```
$IPT –t filter –A FORWARD –d 161.148.40.200 --dport 443
–s $LAN_RANGE –o $NET_IFACE –j ACCEPT

$IPT –t filter –A FORWARD –d $LAN_RANGE –s
161.148.40.200 --sport 443 –i $NET_IFACE –j ACCEPT
```

Permite o acesso ao SIDOR:

```
$IPT –t filter –A FORWARD –d 200.198.196.8 --dport 8999,
23, 23000 –s $LAN_RANGE –o $NET_IFACE –j ACCEPT

$IPT –t filter –A FORWARD –d $LAN_RANGE –s 200.198.196.8
--sport 8999, 23, 23000 –i $NET_IFACE –j ACCEPT
```

Converte os endereços internos para o endereço do *firewall*:

```
$IPT –t nat –A POSTROUTING –o $NET_IFACE –j MASQUERADE
```

Permite o envio de pacotes ICMP, para fins de teste de conectividade:

```
$IPT –t filter –A OUTPUT –p icmp –s $LAN_RANGE –d 0/0 –j
ACCEPT
$IPT –t filter –A OUTPUT –p icmp –s $CLAN_RANGE –d 0/0 –
j ACCEPT
```

4 Viabilidade Econômica

Para a comparação entre o custo de implementação de um *firewall* baseado em software proprietário e um *firewall* baseado em software livre, levou-se em conta não só a quantidade de usuários que efetivamente irão usar os sistemas SIAFI e SIDOR, mas também todos os demais usuários e serviços que precisam usar uma conexão com a Internet.

A implantação de uma solução de *firewall* para sistemas separados numa mesma infra-estrutura de rede comprometeria todo o perímetro de segurança da rede. Como o objetivo principal é poder propor um sistema que monitore e controle o acesso à rede externa, é necessário limitar as possibilidades de acesso ao mundo exterior através do menor número possível de pontos de obstrução – ou interfaces entre a rede interna segura e a rede externa insegura.

Assim, a quantidade de usuários ou serviços que necessitam de acesso à Internet também devem ser considerados no projeto de implementação do *firewall*, pois o custo de implantação poderá ser diluído pela quantidade de usuários, o que irá gerar um custo por cliente mais baixo.

Sendo assim, o número de licenças ideal para atender a infra-estrutura de rede da CEAGESP é de quinhentas. Este número foi levantado pela equipe de informática da empresa, e levou em conta o número de usuários e serviços presentes na rede, bem como uma folga para expansões futuras.

4.1 Firewall proprietário

Segundo proposta comercial elaborada em maio de 2005 pela Compugraf à CEAGESP, o custo aproximado do CheckPoint Firewall-1 para quinhentos usuários ficaria em aproximadamente US$12.970,00, mais US$2.830,00 da subscrição anual. Considerando ainda o treinamento básico para operar o *software*, acrescenta-se mais R$4.440,00.

Nas tabelas comparativas abaixo, para conversão de dólar para real, foi considerada a seguinte cotação aproximada, pesquisada em maio de 2005:

US$ 1,00 = R$ 2,80

Na tabela abaixo é apresentado o custo inicial de implantação do Check Point FireWall-1 com sistema operacional próprio, o SecurePlataform Pro. A vantagem do SecurePlataform Pro é que o custo já está incluso na solução, e portanto não é necessário o gasto adicional com outros sistemas operacionais. A desvantagem é o suporte limitado a alguns distribuidores de *hardware* específicos, o que pode acarretar um custo maior para aquisição de *hardware* homologado.

	CUSTO
Servidor	R$ 4.000,00
Sistema Operacional Check Point SecurePlataform Pro	R$ 0,00
Firewall Check Point Express para 500 usuários	R$ 36.324,00
Subscrição anual	R$ 7.924,00
Treinamento Check Point VPN/FireWall-1 Management I e II NG	R$ 4.440,00
TOTAL	***R$ 52.688,00***

Tabela 2 – Custo do Check Point FireWall-1 com SecurePlataform Pro

Na tabela abaixo, foi considerado o Check Point FireWall-1 instalado em um servidor com o sistema operacional Windows Server 2003 Standard. Este tipo de configuração é indicado quando é necessário suporte a *hardware* específico não suportado pelo SecurePlataform Pro, ou quando a infra-estrutura de rede exige um servidor Windows, como por exemplo, redes baseadas em domínios do Windows.

	CUSTO
Servidor	R$ 4.000,00
Sistema Operacional Windows Server 2003 Standard	R$ 3.700,00
Firewall Check Point Express para 500 usuários	R$ 36.324,00
Subscrição anual	R$ 7.924,00
Treinamento Check Point VPN/FireWall-1 Management I e II NG	R$ 4.440,00
TOTAL	***R$ 56.388,00***

Tabela 3 – Custo do Check Point FireWall-1 com Windows Server 2003 Standard

4.2 Firewall baseado em Software Livre

Como o *firewall* baseado em *software* livre não possui custo com licenças, o gasto inicial se concentrará na aquisição dos equipamentos e no treinamento dos analistas de segurança.

Um treinamento bastante completo é oferecido pela 4Linux, empresa especializada em treinamento com foco em segurança. Abaixo uma lista dos principais cursos voltados para implementação de um *firewall*:

- 401 – Linux Security System Administration, 40 horas;
- 403 – Servidores Linux para Corporações, 40 horas;
- 409 – Inteligência e Arquitetura de Firewall, 16 horas;
- 415 – Segurança em Servidores Linux usando a BS7799, 40 horas;
- 418 – Detecção de Intrusos com Snort, 16 horas.

Estes cursos fazem parte de um pacote denominado Passaporte 4Linux.

	CUSTO
Servidor	R$ 4.000,00
Sistema Operacional Debian Sarge 3.0	R$ 0,00
Firewall NetFilter IPTables	R$ 0,00
Subscrição anual	R$ 0,00
Treinamento Passaporte 4Linux	R$ 3.789,00
TOTAL	***R$ 7.789,00***

Tabela 4 – Custo do NetFilter IPTables com Debian Sarge

4.3 Comparativo entre as soluções de Firewall

Entre as soluções de *firewall* propostas, pode-ser perceber através da tabela abaixo que o menor custo unitário por usuário é o do Debian Sarge 3.0 com NetFilter IPTables. Apesar do custo de implantação ser bastante atraente, outras características devem ser levadas em conta. Uma discussão sobre estas características será abordada na conclusão deste trabalho.

	CUSTO TOTAL	CUSTO POR USUÁRIO
Check Point FireWall-1 com SecurePlataform Pro	R$ 52.688,00	R$ 105,38
Check Point FireWall-1 com Windows Server	R$ 56.388,00	R$ 112,78
NetFilter IPTables com Debian Sarge	R$ 7.789,00	R$ 15,58

Tabela 5 – Comparativo entre as soluções de *firewall*

De acordo com a tabela acima, pode-se ver que o *firewall* baseado em NetFilter IPTables é 576% mais barato que o Check Point FireWall-1 com SecurePlataform Pro, e 624% mais barato que o Check Point FireWall-1 com Windows Server.

5 Conclusões

É fato que para um mínimo de proteção em uma rede corporativa conectada à Internet, é necessário pelo menos a instalação de um *firewall* na borda do perímetro de segurança da rede. A forma como o *firewall* é instalado, se na forma de *firewall* único ou dual, dependerá do nível de segurança que se quer ter e da quantidade de serviços que a empresa deseja oferecer ao mundo exterior. Outro fator importante é o custo, pois *firewalls* baseados em *software* proprietário são muito mais caros para implantar do que *firewalls* baseados em *software* livre.

Para oferecer o máximo de segurança, o *firewall* deve oferecer os serviços de filtragem de pacotes, tradução de endereços de rede e *proxy* de serviços de alto nível. No entanto, nem todos os *firewalls* comerciais oferecem todas estas funcionalidades. A exceção é o FireWall-1 da Check Point Software Technologies Ltd., que é considerado o mais completo do mercado.

Talvez por ser o *firewall* mais completo, o FireWall-1 é também o mais caro. O custo total de propriedade é alto e só se justifica caso a empresa queira ter um serviço de suporte altamente especializado e com alta disponibilidade. Este tipo de recurso é mais difícil em *software* livre, que na maioria das vezes é mantido por entusiastas.

Por outro lado, o NetFilter IPTables é também um *firewall* bastante robusto e completo, com exceção para o serviço de *proxy* de alto nível que não é oferecido. O custo para implantação do IPTables é bastante atraente, e a cada dia mais profissionais de segurança de redes estão se especializando na implementação de *firewall* IPTables.

Apesar do IPTables não oferecer todas as funcionalidades de um autêntico *firewall*, ele pode ser combinado com outros sistemas baseados em *software* livre, como o servidor *proxy* SQUID e o sistema identificador de intrusão SNORT.

Caso a empresa possua uma equipe de analistas especializados em segurança de redes, de certo que não será difícil implantar sistemas de segurança baseados em *software* livre. O avanço na conscientização sobre os benefícios do código aberto nos processos de

detecção de vulnerabilidades, na auditoria de sistemas computacionais e a crescente comunidade de especialistas em segurança baseado em *software* livre, vem criando meios de se oferecer suporte cada vez mais especializado e disponível para as empresas. E é a seriedade e o volume com que este movimento vem se desenvolvendo que faz com que os sistemas de segurança baseados em *software* livre se estabeleçam como alternativas viáveis do ponto de vista técnico e extremamente vantajosas do ponto de vista econômico.

6 Sugestões para trabalhos futuros

Como sugestão para complementar o processo de segurança da rede corporativa da CEAGESP, é necessário implementar outros sistemas que auxiliem o *firewall* na proteção do perímetro de segurança. Um destes sistemas é o *proxy* de serviços de alto nível SQUID. O SQUID é um *proxy* baseado em *software* livre que pode ser facilmente integrado com o NetFilter IPTables. Outro sistema complementar importante é o IDS (Intrusion Detect System – Sistema de Detecção de Intrusão) baseado em software livre denominado SNORT.

Outra forma de melhorar a segurança de um *firewall* baseado em *software* livre é estudar outras arquiteturas de implementação, como a instalação de múltiplos *firewalls* com o uso de zonas desmilitarizadas; modelos de *firewall* diferentes em cada ponto de obstrução da rede; montagem de *host* bastiões e *hosts* "potes de mel", entre outros.

Referencial Bibliográfico

ABNT, *NBR ISO/IEC 17799*: Tecnologia da Informação – Código de prática para a gestão da segurança da informação, Associação Brasileira de Normas Técnicas, Rio de Janeiro, 2001.

ALBUQUERQUE, Ricardo e RIBEIRO, Bruno, *Segurança no Desenvolvimento de Software*: como garantir a segurança do sistema para seu cliente usando a ISO/IEC, Editora Campus, Rio de Janeiro, 2002.

ANDREASSON, Oskar, *Iptables Tutorial 1.1.19*, 2003.

AOKI, Osamu, *Referência Debian*, 2005.

BRASILEIRO, Governo, *Guia Livre* – Referência de Migração para Software Livre do Governo Federal, Versão Ipiranga, 2004.

CASAD, Joe e WILLSEY, Bob, *Aprenda em 24 horas TCP/IP*, Editora Campus, Rio de Janeiro, 1999.

CEAGESP, *Norma Geral 002* – Rede Corporativa da CEAGESP – Política de Uso, Seção de Desenvolvimento, Organização e Métodos, 2004.

CHECK POINT, *Check Point FireWall-1 Architecture and Administration*, Version 4.0, Check Point Software Technologies Ltd., 1998.

CHECK POINT, *Getting Started with Check Point FireWall-1*, Version 4.0, Check Point Software Technologies Ltd., 1998.

CHECK POINT, *Managing Check Point FireWall-1 Using the Windows GUI*, Version 4.0, Check Point Software Technologies Ltd., 1998.

CONECTIVA, Equipe de Treinamento, *Segurança de Redes*: Firewall, 1ª Edição, Conectiva S.A., 2001.

COULSON, David, *Network Security IPTables*, Revista Linux Pro, março e abril de 2003.

DOWNES, Kevin, FORD, Merilee, LEW, H. Kim, SPANIER, Steve e STEVENSON, Tim, *Internetworking* – Manual de Tecnologias, 2ª Edição, Editora Campus, Rio de Janeiro, 2000.

FEIBEL, Werner, *Encyclopedia of Networking*, Second Edition, Sybex Inc., 1996.

GONZAGA, Diogo Correia, *Projeto de Implementação de um Servidor Firewall Livre Utilizando IPTables*, Instituto Nacional de Tecnologia da Informação, Brasília, 2004.

KIRCH, Olaf, DAWSON, Terry, *Linux Network Administrator's Guide*, O'Reilly & Associates, 2000.

OLIVEIRA, Wilson José de, *Segurança da Informação*: Técnicas e Soluções, Visual Books, Florianópolis, 2001.

PERENS, Bruce, RUDOLPH, Sven, GROBMAN, Igor, TREACY, James, DI CARLO, Adam, *Instalando Debian GNU/Linux 3.0 para Intel x86*, 2002.

RODRIGUEZ, Adolfo, GATRELL, John, KARAS, John e PESCHKE, Roland, *TCP/IP Tutorial and Technical Overview*, 7th Edition, IBM Redbooks, 2001.

SCHETINA, Erik, GREEN, Ken e CARLSON, Jacob, *Aprenda a desenvolver e construir sites seguros*, Editora Campus, Rio de Janeiro, 2002.

SCRIMGER, Rob, LASALLE, Paul, PARIHAR, Mridula e GUPTA, Meeta, *TCP/IP* – A Bíblia, Editora Campus, Rio de Janeiro, 2002.

SERPRO, *Revista Tema* – A Revista do SERPRO, Ano XXVIII, número 172, março/abril de 2004.

SERPRO, *Revista Tema* – A Revista do SERPRO, Ano XXVIII, número 173, maio/junho de 2004.

SILVA, Gleydson Mazioli da, *Guia Foca/GNU Linux*, CIPSGA – Comitê de Incentivo e Produção do Software GNU e Alternativo, 2004.

SOARES, Luiz Fernando Gomes, LEMOS, Guido e COLCHER, Sérgio, *Redes de Computadores*: das LANs, MANs e WANs às Redes ATM, Editora Campus, 2ª Edição, São Paulo, 1995.

SOF, *Portal SIDOR* – http://sofweb.planejamento.gov.br, Secretaria de Orçamento Federal, Ministério do Planejamento, Orçamento e Gestão, Brasília, acessado em maio de 2005.

STN, *Tutorial SIAFI* – Sistema Integrado de Administração Financeira do Governo Federal, Secretaria do Tesouro Nacional, MSD Software, Brasília, 1999.

STN, *Portal SIAFI* – http://www.tesouro.fazenda.gov.br, Secretaria do Tesouro Nacional, Ministério da Fazenda, Brasília, acessado em maio de 2005.

STREBE, Matthew, PERKINS, Charles, *Firewalls*, Editora Makron Books, São Paulo, 2002.

TANENBAUM, Andrew S., *Redes de Computadores*, 3ª Edição, Editora Campus, Rio de Janeiro, 1997.

TECHNET, Microsoft, *Academia Latino Americana de Segurança da Informação*, Microsoft TechNet Brasil, 2005.

Glossário

ACK – Pacote de reconhecimento

APPLET – Pequeno programa escrito em Java

BACKBONE – Redes principais que conectam redes menores

BUFFER – Área temporária de memória

Cache – Área de armazenamento de dados

CEAGESP – Companhia de Entrepostos e Armazéns Gerais de São Paulo

CEO – Chief Executive Officer

CGSI – Comitê Gestor da Segurança da Informação do Governo Federal

DMZ – Demilitarized Zone

DNS – Domain Name System

FTP – File Transfer Protocol

GNU – Acrônimo para *GNU's not UNIX*

GPL – General Public License

HOD – Host on Demand

HTML – HyperText Markup Language

HTTP – Hyper Text Transfer Protocol

HTTPS – Hyper Text Transfer Protocol Secure

IBM – International Business Machines

ICMP – Internet Control Message Protocol

IDS – Intrusion Detect System

IP – Internet Protocol

kB – Kilobyte, equivalente a 1024 bytes

Kernel – Núcleo de um sistema operacional

LOG – Registro de eventos

LOGIN – Identificação de usuários em uma rede

P2P – Peer-to-Peer

PING – Packet Internet Groper

POP3 – Post Office Protocol Version 3

SERPRO – Serviço Federal de Processamento de Dados

SIAFI – Sistema Integrado de Administração Financeira

SIDOR – Sistema Integrado de Dados Orçamentários

SMTP – Simple Mail Transfer Protocol

SNA – Systems Network Architecture

SOF – Secretaria de Orçamento Federal

SSL – Security Socket Layer

STN – Secretaria do Tesouro Nacional

Streaming – Fluxo de dados de som e imagem

SWITCH – Comutador de pacotes de redes

SYN – Pacote de sincronismo

TCP – Transport Control Protocol

Thread – Linha de execução em um processador

UDP – User Datagram Protocol

URL – Uniform Resource Locator

Anexos