Centro Universitário de Maringá
Curso Superior de Tecnologia em Redes de Computadores

PROJETO DE REDES
www.projetoderedes.com.br

MARCOS ANTONIO RODRIGUES

IMPLANTAÇÃO DO IPCOP FIREWALL EM MICROS E PEQUENAS EMPRESAS

Maringá
2007

MARCOS ANTONIO RODRIGUES

IMPLANTAÇÃO DO IPCOP FIREWALL EM MICROS E PEQUENAS EMPRESAS

Monografia apresentada ao Curso Superior de Tecnologia em Redes de Computadores, do Centro Universitário de Maringá como requisito parcial à obtenção do título de Tecnólogo.
Orientador: Prof. Alex Lopes Galvão

Maringá
2007

MARCOS ANTONIO RODRIGUES

IMPLANTAÇÃO DO IPCOP FIREWALL EM MICROS E PEQUENAS EMPRESAS

Relatório Final apresentado ao Curso Superior de Tecnologia em Redes de Computadores, do Centro Universitário de Maringá como requisito parcial para a obtenção do titulo de Tecnólogo, sob orientação do Prof. Alex Lopes Galvão, aprovada em 12 de Dezembro 2007.

BANCA EXAMINADORA

Orientador: _____

Prof. Alex Lopes Galvão

CESUMAR

Membro: _____

Prof. Elias C. Araújo de Carvalho

CESUMAR

Membro: _____

Prof. Cleber Lecheta Franchini

CESUMAR

Dedico à minha mãe, meu pai, irmãos, esposa, filhos e amigos pelos incentivos, confiança e força nos momentos de dificuldades para que eu alcançasse mais esta vitória.

AGRADECIMENTOS

À Deus por estar sempre comigo nesta vida. Agradeço a minha esposa Tânia Márcia Margato Rodrigues e a meus pais José Antonio Rodrigues Maria Venina Rodrigues por ter me incentivado a voltar a estudar e me ajudar conseguir chegar a este objetivo. Gostaria de mencionar minha gratidão pela preciosa orientação do professor Alex Lopes Galvão, agradeço ainda a Coordenadora do curso professora Márcia Cristina Dadalto Pascutti, ao professor Luis César de Mello e aos demais professores que contribuíram para minha formação acadêmica.

RESUMO

Este trabalho tem como objetivo elaborar um manual de instalação, configuração e gerenciamento do linux Ipcop Firewall, apresentando os recursos de segurança que este sistema oferece para micro e pequenas empresas. Para a elaboração deste manual foi preciso fazer um levantamento bibliográfico sobre Software Livre, Sistema Operacional e Linux, explicando cada um desses assuntos. Este Trabalho de Conclusão de Curso aborda a história, os conceitos e a filosofia de Software Livre, como funciona um sistema operacional, mostrando alguns tipos de sistema operacionais. Mostrará como surgiu o sistema operacional Linux e algumas distribuições existentes no mercado. Será elaborado um manual de instalação, configuração do sistema operacional IPCOP FIREWALL, mostrando a forma correta de instalação, configuração e gerenciamento desse sistema operacional.

Palavras-chave: software livre, sistema operacional, linux, firewall, Ipcop firewall.

ABSTRACT

The aim of this paper is to elaborate an installation manual, setup and management of Linux Ipcop Firewall, presenting safety resources that this system offers not only to personal computers but also to companies of small size. For the elaboration of this manual, it was necessary to make a bibliographical survey on Free Software, Operating System and Linux, explaining each one of these issues. This Course Conclusion Work brings the history, the concepts and the philosophy of Free Software. It also presents how an operating system works besides showing some operating system types. It will talk about how Linux operating system started as well as the distributions that there are in the market. Finally, an installation manual and an operating system setup Ipcop Firewall will be elaborated in order to present the proper form of installation, setup and management of this operating system.

Key words: Free Software, operating system, Linux, Firewall, Ipcop Firewall.

LISTA DE FIGURAS

LISTA DE SIGLAS

ADSL - Asymmetric Digital Subscriber Line
ARP - Address resolution protocol
ASL - Apache Software License
BSD - Berkeley Software Distribution
CPU - Unidade Central de Processamento
DHCP- Dynamic Host Configuration Protocol
DMZ - Demilitarized zone
DNS - Domain Name System
E/S - Entrada/Saída
FTP - File Transfer Protocol
GB - Gigabyte
GNU C/C++ - Linguagem de programação
GNU GPL - General Public License
HD - Hard Disk
HTTP - Hyper Text Transfer Protocol
HTTPS - HyperText Transfer Protocol Secure
ICMP - Internet Control Message Protocol
IDS - Intrusion Detection System
IP - Internet Protocol
IP'SEC - IP Security Protocol
IRC - Internet Relay Chat
ISA - Industry Standard Architecture
ISDN - Integrated services digital networks
KB - KiloBytes
LRU - Least Recently Used
MAC - Media Access Control
MB - MegaBytes
MIME - Multipurpose Internet Mail Extensions
NAT - Network Address Translation

NFS - Network File System
NIC - Network Information Center
NIS - Network Information Service
NTP - Network Time Protocol
PCI - Peripheral Component Interconnect
PDF - Portable Document Format
PERL - Linguagem de programação
PXE - Preboot Execution Environment
PPP - Point-to-Point Protocol
PSK - Phase Shift Keying
RAM - Random Access Memory
RPM - Red Hat Package Manager
ISA - Instruction Set Architecture
SCSI - Small Computer System Interface
SFTP - Secure File Transfer Protocol
SMP - Symmetric Multi-Processing
SSH - Secure Shell
SSL - Secure Sockets Layer
SWAP - Área de troca
TCL - Tool command Language
TCP - Transmission Control Protocol
TFTP - Trivial File Transfer Protocol
UDP - User Datagram Protocol
URL - Uniform Resource Locator
USB - Universal Serial Bus
UUCP - Unix to Unix Copy Protocol
VPN - Virtual Private Network

SUMÁRIO

1 INTRODUÇÃO

A Internet possibilitou que pessoas e empresas cruzassem fronteiras de modo fácil, rápido, nunca visto antes, criando um mundo virtual globalizado. Por isso hoje em dia, os usuários de micros e pequenas empresas necessitam, cada vez mais, do acesso a Internet seja para trabalho ou lazer. Embora a Internet tenha, e tem dado bons frutos, ela também oferece muitos perigos a usuários inexperientes. Alguns desses perigos são vírus, spams, worms, spywares, ações de Crackers e Hackers.

Há softwares que são fundamentais para acesso a internet e para a segurança a navegação, desenvolvendo processos básicos ou não e/ou administrados.

Algumas organizações acabam decidindo utilizar software proprietário de segurança mesmo sem obter sua devida licença, incorrendo assim na pirataria de software, que é uma prática ilegal. Com a intensificação do combate à pirataria, esta prática pode sair cara, como mostra a Lei de Software, Lei nº. 9.609, de 19 de fevereiro de 1998. O capítulo V Art. 12º da lei, enuncia que quem violar direitos de autor de programa de computador terá pena de detenção de seis meses a dois anos ou multa e se a violação consistir na reprodução, por qualquer meio, de programa de computador, no todo ou em parte, para fins de comércio, sem autorização expressa do autor ou de quem o represente a pena será reclusão de um a quatro anos e multa.

Para não incorrer nesta prática ilegal, as organizações tem dois caminhos.
O primeiro consiste em pagar as devidas licenças de uso. O segundo caminho consiste em buscar no software livre uma alternativa de qualidade e de baixo custo.

2 SOFTWARE LIVRE

Segundo a Free Software Foundation (2007) Software livre, se refere à liberdade dos usuários executarem, copiarem, distribuírem, estudarem, modificarem e aperfeiçoarem o software. Mais precisamente, ele se refere a quatro tipos de liberdade, para os usuários do software:

- A liberdade de executar o programa, para qualquer propósito (liberdade nº. 0).
- A liberdade de estudar como o programa funciona, e adaptá-lo para às suas necessidades (liberdade nº. 1). Acesso ao código-fonte é um pré-requisito para esta liberdade.
- A liberdade de redistribuir cópias de modo que se possa ajudar ao seu próximo (liberdade nº. 2).
- A liberdade de aperfeiçoar o programa, e liberar os seus aperfeiçoamentos, de modo que toda a comunidade se beneficie (liberdade nº. 3). Acesso ao código-fonte é um pré-requisito para esta liberdade.

Um programa é software livre se os usuários têm todas essas liberdades. Portanto, o usuário deve ser livre para redistribuir cópias, seja com ou sem modificações, seja de graça ou cobrando uma taxa pela distribuição, para qualquer um em qualquer lugar. Ser livre para fazer essas coisas significa (entre outras coisas) que o usuário não tem que pedir ou pagar pela permissão.

O usuário deve também ter a liberdade de fazer modificações e usá-las privativamente no seu trabalho ou lazer, sem nem mesmo mencionar que elas existem. Se o usuário publicar as modificações, ele não deve ser obrigado a avisar ninguém em particular, ou de nenhum modo em especial.

A liberdade de utilizar um programa significa a liberdade para qualquer tipo de pessoa física ou jurídica utilizarem o software em qualquer tipo de sistema computacional, para qualquer tipo de trabalho ou atividade, sem que seja necessário comunicar ao desenvolvedor ou a qualquer outra entidade em especial.

A liberdade de redistribuir cópias deve incluir formas binárias ou executáveis do programa, assim como o código-fonte, tanto para as versões originais quanto para as modificadas. Está ok, se não for possível produzir uma forma binária de

programação ou executável (pois algumas linguagens de programação não suportam este recurso), mas deve ser concedida a liberdade de redistribuir essas formas caso seja desenvolvido um meio de criá-las.

De modo que a liberdade de fazer modificações, e de publicar versões aperfeiçoadas, tenha algum significado, deve-se ter acesso ao código-fonte do programa. Portanto, acesso ao código-fonte é uma condição necessária ao software livre.

Para que essas liberdades sejam reais, elas têm que ser irrevogáveis desde que o usuário não faça nada errado; caso o desenvolvedor do software tenha o poder de revogar a licença, mesmo que o usuário não tenha dado motivo, o software não é livre (FREE SOFTWARE FOUNDATION, 2007).

2.1 REGRAS SOBRE A MANEIRA DE DISTRIBUIR SOFTWARE LIVRE

São aceitáveis, quando elas não entram em conflito com as licenças principais. Por exemplo, copyleft. “O copyleft diz que qualquer um que distribui o software, com ou sem modificações, tem que passar adiante a liberdade de copiar e modificar novamente o programa”. O copyleft garante que todos os usuários têm liberdade, ou seja, se você recebeu um software com uma licença livre que inclua cláusulas de copyleft, e se optar por redistribuí-lo (modificado ou não), terá que mantê-lo com a mesma licença com que o recebeu. Nem todas as licenças de software livre incluem a característica de copyleft. A licença GNU GPL (adotada pelo kernel Linux) é o maior exemplo de uma licença copyleft. Outras licenças livres, como a licença BSD ou a licença ASL (Apache Software License) não incluem a característica de copyleft. Esta regra não conflita com as liberdades, na verdade, ela as protege.

Portanto, o usuário pode ter pago para receber cópias do software GNU, ou o usuário pode ter obtido cópias sem nenhum custo. Mas independente de como o usuário obteve a sua cópia, este sempre tem a liberdade de copiar e modificar o software, ou mesmo de vender cópias.

“Software livre” não significa “não-comercial”. Um programa livre deve estar disponível para uso comercial, desenvolvimento comercial, e distribuição comercial. O desenvolvimento de softwares livres comerciais é muito importante.

Regras sobre como empacotar uma versão modificada são aceitáveis, se elas não acabam bloqueando a liberdade de liberar versões modificadas. Regras como: “se você tornou o programa disponível deste modo, você também tem que torná-lo disponível deste outro modo” também podem ser aceitas, da mesma forma. (Note que tal regra ainda deixa para você, a escolha de tornar o programa disponível ou não.) Também é aceitável uma licença que exija que, caso você tenha distribuído uma versão modificada e um desenvolvedor anterior, peça por uma cópia dele, você deva enviar uma.

No projeto GNU, é usado “copyleft” para proteger estas liberdades legalmente para todos. Mas também existe software livre que não é copyleft.

Às vezes regras de controle de exportação e sanções de comércio podem limitar a liberdade de distribuição de cópias de programas internacionalmente. Desenvolvedores de software não têm o poder para eliminar ou sobrepor estas restrições, mas o que eles podem e devem fazer é se recusar a impô-las como condições para o uso dos seus programas. Deste modo, as restrições não afetam as atividades e as pessoas fora da jurisdição deste governo.

Quando se fala de software livre, é melhor evitar o uso de termos como “dado” ou “de graça”, porque estes termos implicam que a questão é de preço, não de liberdade.

Finalmente, note que critérios como os estabelecidos nesta definição de software livre, requerem cuidadosa deliberação quanto a sua interpretação. Para decidir se uma licença se qualifica como de software livre, ela é baseada nestes critérios para determinar se ela segue no espírito assim como as palavras exatas. Se uma licença inclui restrições impensadas, ela é rejeitada (FREE SOFTWARE FOUNDATION, 2007).

2.2 TIPOS DE LICENÇAS MAIS COMUNS

Software proprietário: Esse tipo de licenciamento garante ao autor do software plenos poderes sobre venda, distribuição ou modificação do código fonte, afinal ele mesmo é quem define tais parâmetros de maneira desejada. Um usuário desse software normalmente deve pagar uma taxa pela utilização do mesmo, o que lhe garante uma ou mais licenças de uso. Caso queira instalar o software em mais máquinas do que sua licença permite, ele deve adquirir mais licenças do fornecedor. Normalmente não tem acesso ao código fonte, o que lhe impede de fazer modificações ou melhoras ao software, mesmo que seja para uso próprio, o que o torna altamente dependente do fornecedor para obter atualizações de falhas de segurança, por exemplo. Não pode redistribuir o software. Um exemplo de software proprietário é o sistema operacional Windows.

Software shareware: Possui características semelhantes ao software proprietário, mas com uma diferença importante: o usuário pode testar antes de comprar. É possível realizar a descarga do software pela internet ou adquiri-lo em uma mídia e instalar por um período de avaliação. Caso o usuário opte por continuar usando o software, deve pagar uma taxa de licença ao fornecedor. Alguns consideram uma prática inviável de comercialização de software, mas existem exemplos bem sucedidos. Existe também o shareware incompleto, que costuma ser uma versão do shareware que pode ser usada a vontade e indefinidamente como um freeware, mas não contém todas as características da versão completa. Um exemplo famoso de shareware é o software Winzip.

Software freeware: Programas de código fechado que são distribuídos gratuitamente pelo autor do software. Normalmente o usuário pode fazer cópias e distribuí-las gratuitamente, porém, não pode alterar o programa. Um exemplo de freeware é o Internet Explorer.

Domínio público: Programas em domínio público são considerados de propriedade coletiva de todos. O autor abre mão dos direitos de cópia, permitindo que se copie, altere ou redistribua o software, sem qualquer tipo de obrigação, inclusive permitindo que o software seja incorporado em trabalhos proprietários, sem nenhuma necessidade de pagamento ou respeito a restrições. Um exemplo de software em domínio público é o sistema operacional BSD (GOLDCHLEGER, 2001).

3 SISTEMA OPERACIONAL

Segundo Tanenbaum (2003), um sistema computacional moderno consiste em um ou mais processadores, memória principal, discos, impressoras, teclado, monitor, interfaces de rede e outros dispositivos de entrada e saída. Enfim, é um sistema complexo. Desenvolver programas que mantenham o controle de todos esses componentes e os utilizem corretamente de maneira otimizada é um trabalho extremamente difícil. Por isso, os computadores têm um dispositivo de software denominado sistema operacional, cujo trabalho é gerenciar esses componentes e fornecer aos programas do usuário uma interface com o hardware mais simples.

Na parte inferior está o hardware, que em muitos casos é ele próprio composto de dois ou mais níveis (ou camadas). O nível mais baixo contém dispositivos físicos: chips de circuitos integrados, fios, fontes de alimentação, tubos de raios catódicos e dispositivos semelhantes. Sua construção e seu funcionamento são atribuições da engenharia elétrica.

Em seguida vem o nível de micro arquitetura, no qual os dispositivos físicos são agrupados em unidades funcionais. Normalmente, esse nível contém alguns registradores internos à CPU (unidade central de processamento) e um caminho dos dados (data path) contendo uma unidade lógico-aritmética. Em cada ciclo de máquina, um ou dois operandos são trazidos aos registradores e combinados na unidade lógico-aritmética (por exemplo, pela adição ou por um E-booleano). O resultado é armazenado em um ou mais registradores.

Em algumas máquinas, a operação do caminho dos dados é controlada por um software denominado micro-programa. Em outras, é controlado diretamente por circuitos de hardware.

A função do caminho dos dados é executar um determinado conjunto de instruções. Algumas dessas instruções podem ser executadas em um ciclo de caminho dos dados; outras podem necessitar de múltiplos ciclos.

Essas instruções podem usar registradores ou outros recursos do hardware. Juntos, o hardware e as instruções visíveis a um programador de linguagem de montagem formam o nível ISA (*instruction set architecture* – arquitetura do conjunto de instruções). Esse nível é muitas vezes denominado linguagem de máquina.

A linguagem de máquina tem, em geral, entre 50 e 300 instruções. A maioria delas serve para mover os dados por meio da máquina, fazer operações aritméticas e comparar valores. Nesse nível, os dispositivos de entrada e saída são controlados carregando-se valores em registradores de dispositivos.

Pode-se comandar a leitura de um disco carregando-se os valores de endereço do disco, endereço da memória principal, contador de bytes e a direção (leitura ou escrita) em seus registradores. Na prática, vários outros parâmetros são necessários e o status que retorna à unidade leitora depois de uma operação é basicamente complexo. Além disso, para muitos dispositivos de E/S (entrada / saída) a temporização desempenha um papel fundamental na programação.

Para ocultar essa complexidade existe o sistema operacional. Ele consiste em uma camada de software que oculta (parcialmente) o hardware e fornece ao programador um conjunto de instruções mais conveniente. Por exemplo, read block from file (“leia um bloco de um arquivo”) é conceitualmente mais simples do que ter de se preocupar com os detalhes da movimentação das cabeças de leitura, como esperar que elas abaixem.

No topo do sistema operacional situa-se o restante do software do sistema. Nele encontramos o interpretador de comandos (também conhecido como Shell), o sistema de janelas, os compiladores, os editores e os programas similares independentes de aplicação. É importante notar que esses programas não constituem partes definitivas dos sistemas operacionais, mesmo que sejam normalmente fornecidos pelo fabricante do computador. Trata-se de um ponto crucial e sutil. O sistema operacional é (normalmente) aquela parte do software executada em modo supervisor ou modo núcleo (no caso, a parte mais interna de um sistema operacional). Os compiladores e os editores são executados em modo usuário. Se o usuário não gostar de um determinado compilador, ele será livre para escrever seu próprio compilador se o quiser; mas não lhe é permitido escrever sua própria rotina de tratamento de interrupção de relógio, que é parte do sistema operacional e está normalmente protegida pelo hardware contra tentativas de alterações pelo usuário.

Esta distinção, contudo, é às vezes confusa em sistemas embargados (que podem não ter um modo núcleo) ou sistemas interpretados (como sistemas operacionais baseados em Java, que usam interpretação, e não hardware, para

separar os componentes). Além disso, em computadores tradicionais, o sistema operacional é que se executa em modo núcleo.

Em muito sistema há programas executados em modo usuário, mas que auxiliam o sistema operacional ou realizam funções privilegiadas. Por exemplo, existe um programa, que permite aos usuários mudarem suas senhas. Esse programa não faz parte do sistema operacional e não é executado em modo núcleo, mas realiza uma função claramente delicada e precisa ser protegido de maneira especial.

Em alguns sistemas, essa idéia é levada ao extremo, e parte do que é tradicionalmente tido como sistema operacional (como o sistema de arquivos) é executado em espaço do usuário. Nesses sistemas, é difícil definir um limite claro. Tudo o que é executado em modo núcleo constitui sem dúvida parte do sistema operacional, mas alguns programas executados fora dele são inquestionavelmente também parte dele, ou pelo menos estão intimamente associados a ele.

Por fim, acima dos programas dos sistemas vem o programa de aplicação, que são comprados ou escritos por usuários para resolver problemas específicos, como processamento de texto, planilhas, cálculos de engenharia ou armazenamento de informação em um banco de dados (TANENBAUM, 2003).

3.1 TIPOS DE SISTEMAS OPERACIONAIS

3.1.1 Sistemas Operacionais de Computadores de Grande Porte

No topo estão os sistemas operacionais para computadores de grande porte – aqueles que ocupam uma sala inteira, ainda encontrada em centros de dados de grandes corporações. Esses computadores distinguem-se dos computadores pessoais em termos de capacidade de E/S. Um computador de grande porte com mil discos e milhares de gigabytes de dados não é incomum; um computador pessoal com essas especificações seria algo similar. Os computadores de grande porte estão também ressurgindo como sofisticados servidores Web, como servidores para

sites de comércio eletrônico em larga escala e ainda, como servidores para transações entre empresas (business-to-business).

Os sistemas operacionais para computadores de grande porte são, sobretudo orientados para o processamento simultâneo de muitos jobs, sendo que a maioria deles precisa de quantidades prodigiosas de E/S. Esses sistemas operacionais oferecem normalmente três tipos de serviços: em lote (batch), processamento de transações e tempo compartilhado. Um sistema em lote processa jobs de rotina sem a presença interativa do usuário. O processamento de apólices de uma companhia de seguros ou de relatórios de vendas de uma cadeia de lojas é em geral realizado em modo de lote. Sistemas de processamento de transações administram grandes quantidades de pequenas requisições – por exemplo, processamento de verificações em um banco ou em reservas de passagem aéreas. Cada unidade de trabalho é pequena, mas o sistema precisa tratar centenas ou milhares delas por segundo. Sistemas de tempo compartilhado permitem que múltiplos usuários remotos executem seus jobs simultaneamente no computador, como na realização de consultas a um grande banco de dados. Essas funções estão intimamente, relacionadas; sistemas operacionais de computadores de grande porte em geral realizam todas elas. Um exemplo de sistema operacional de computador de grande porte é OS/390, um descendente do OS/360 (TANENBAUM, 2003).

3.1.2 Sistemas Operacionais de Servidores

Um nível abaixo está o sistema operacional de servidores. Eles são executados em servidores, que são computadores pessoais muito grandes, em estações de trabalho ou até mesmo em computadores de grande porte. Eles servem múltiplos usuários de uma vez em uma rede e permitem-lhes compartilhar recursos de hardware e de software. Servidores podem fornecer serviços de impressão, serviços de arquivo ou serviços de Web.

Provedores de acesso à Internet utilizam várias máquinas servidoras para dar suporte a seus clientes. Sites Web usam servidores para armazenar páginas Web e tratar requisições que chegam. Sistemas operacionais típicos de servidores são Unix

e Windows 2000. O Linux está também ganhando terreno em servidores (TANENBAUM, 2003).

3.1.3 Sistemas Operacionais de Multiprocessadores

Um modo cada vez mais comum de obter potência computacional é conectar múltiplas (CPUS) em um único sistema. Dependendo precisamente de como estiverem conectadas e o que é compartilhado, esses sistemas são denominados computadores paralelos, multicomputadores ou multiprocessadores. Elas precisam de sistemas operacionais especiais, mas muitos deles são variações dos sistemas operacionais de servidores com aspectos especiais de comunicação e conectividade (TANENBAUM, 2003).

3.1.4 Sistemas Operacionais de Computadores Pessoais

A categoria seguinte é o sistema operacional de computadores pessoais. Seu trabalho é oferecer uma boa interface para um único usuário. São amplamente usados para processadores de texto, planilhas e acesso a Internet. Exemplos comuns são o Windows 98, o Windows 2000, o sistema operacional da Macintosh e o Linux. Sistemas operacionais de computadores pessoais são tão amplamente conhecidos que é provável que precisem aqui de pouca introdução. Na verdade, muitas pessoas nem mesmo sabem da existência de outros tipos de sistemas operacionais (TANENBAUM, 2003).

3.1.5 Sistemas Operacionais de Tempo Real

Outro tipo de sistema operacional é o de tempo real. Esses sistemas são caracterizados por terem o tempo como um parâmetro fundamental. Por exemplo,

em sistema de controle de processos industriais, computadores de tempo real devem coletar dados sobre o processo de produção e usá-los para controlar as máquinas na fábrica. É bastante comum a existência de prazos rígidos para a execução de determinadas tarefas. Por exemplo, se um carro está se movendo por uma linha de montagem, certas ações devem ser realizadas em momentos específicos. Se um robô soldador realiza seu trabalho muito cedo ou muito tarde, o carro está perdido. Se as ações precisam necessariamente ocorrer em determinados instantes (ou em determinado intervalo de tempo), tem-se então um sistema real crítico.

Outro tipo de sistema de tempo real é o sistema de tempo real não crítico, no qual o descumprimento ocasional de um prazo é aceitável. Sistemas de áudio digital ou multimídia pertencem a essa categoria. VxWorks e o QNX são sistemas operacionais de tempo real bem conhecidos (TANENBAUM, 2003).

4 LINUX

Segundo Tibet (2001) Linux é uma versão derivada do Minix, que por sua vez é uma versão Unix gratuita. O Linux foi desenvolvido por Linus Torvalds na Universidade Helsinque na Finlândia. Foi originalmente desenvolvido a partir do desejo de Linus de trabalhar com um sistema mais completo que o Minix, pequeno sistema Unix criado para fins didáticos por Andrew Tanembaum. O kernel do Linux não usa o código patenteado de nenhum fabricante, e grande parte do software distribuído para Linux é desenvolvido pelo projeto GNU ou GPL (General Public Licence) na Free Software Fundation em Cambridge – Massachussets.

O lançamento da primeira versão oficial do Linux se deu em 5 de outubro de 1991, já em sua versão 0.02. Até então o Linux já era capaz de executar o bash (GNU Born Again Shell) e o gcc (GNU C compiler), porém havia pouca coisa, além disso. O foco primário do Linus ainda era o desenvolvimento do kernel. Na verdade, o próprio Linus Torvalds até os dias atuais dedica-se apenas ao desenvolvimento do kernel em si, porém nem só de kernel se faz um sistema operacional, um sistema completo necessita de softwares de apoio, como devices drivers, protocolos de rede, ferramentas de desenvolvimento, utilitários e aplicativos.

Para o desenvolvimento de tais softwares, o Linux conta com uma legião de voluntários espalhados pelo mundo conectados via Internet, conhecida também como Comunidade Linux. Por essa razão podemos considerar o Linux um sistema operacional nascido e criado na Internet, e por esse motivo é fácil explicar a sua grande popularidade em tão pouco tempo, pois à medida que ele foi se desenvolvendo, a própria Internet foi atingindo a massa crítica que levou à sua explosão comercial nos dias de hoje.

O linux hoje se tornou uma alternativa viável, de qualidade e desempenho a qualquer sistema comercial atual, sendo considerado por muitos, a última palavra em se falando de sistemas na Internet devido a sua portabilidade, estabilidade, segurança e relação custo - beneficio. Atualmente em sua versão de kernel 2.2.13 é um sistema capaz tanto de servir como executar a função de estação de trabalho em qualquer ambiente de rede (TIBET, 2001).

4.1 DISTRIBUIÇÕES LINUX

Conforme vimos anteriormente um sistema operacional não é feito apenas de seu kernel. Para que possamos utilizá-lo necessitamos de outros programas escritos para executar uma série de funções. Várias empresas fizeram seus pacotes destes programas e do linux, de maneira que podem se facilmente instalados e utilizados. Estes pacotes são as famosas distribuições do Linux.

Uma distribuição típica irá conter:

- O próprio linux ou kernel do sistema operacional (em sua versão mais recente);
- Device drivers para o hardware disponível;
- Net3: suporte a redes Ethernet, Token-ring, PPP, etc;
- Ambiente gráfico - X Windows System;
- Desktop para ambiente gráfico (fvwm, fvwm95, Window maker, After dark, KDE, etc;)
- GNU File tool;
- GNU C/C++, Perl, TCL e outras ferramentas para desenvolvimento;
- Aplicativos e utilitários;
- GhostScript, interpretador e visualizador de documentos em Postscript;
- Tex e Látex para formatação de documentos científicos.

Porém, as distribuições não ficam limitadas a somente esses produtos. Elas podem oferecer uma variedade muito grande de outros produtos (TIBET, 2001).

4.1.1 Algumas distribuições

As distribuições aqui relacionadas foram escolhidas com base em experiências do autor.

4.1.1.1 Slackware

Uma das distribuições mais antigas, mas ainda em evidência, apesar de ser pouco atrativa aos novatos. É uma das poucas, senão a única que ainda pode ser instalada a partir de disquetes. O Slackware é atraente a pessoa que tem bastante experiência em administração Unix e que gosta de baixar o código-fonte de programas, compilá-los, instalá-los, configurá-los e gerenciá-los com as próprias mãos, a moda antiga. E, no entanto, a distribuição que fornece mais liberdade ao administrador por não impor restrições e que exige mais conhecimento dos utilitários e pacotes de software do sistema (TIBET, 2001).

4.1.1.2 Open Linux

A distribuição da empresa norte-americana Caldera, responsável pela manutenção de diversos produtos comerciais para Linux. O Open Linux, apesar do nome, é a distribuição que possui mais pacotes de código fechado, tendo um visual bem familiar ao mundo comercial. Essa distribuição foi a primeira a fornecer o Netscape quando este ainda era um produto fechado. O servidor Oracle, lançado para Linux, foi disponibilizado primeiro para essa distribuição. A Caldera também detém, entre outros, os direitos de comercialização do servidor Novell para Linux coincidência ou não, o fundador da empresa Caldera é um ex-proprietário da Novell. O Caldera Open Linux tem pouco compromisso com software livre (TIBET, 2001).

4.1.1.3 Red Hat Linux

A Red Hat é, hoje em dia, a distribuição mais popular. Além de contar com o famoso (RPM), o gerenciador de pacotes mais difundido na Internet, é mantido por uma empresa que se preocupa com o Free Software, mantendo vários funcionários com a tarefa exclusiva de escrever softwares que serão divulgados na Internet com

seus respectivos códigos-fontes. A sua popularidade pode estar ligada a preocupação com o usuário leigo, sendo assim a distribuição de mais fácil instalação, contando com softwares de apoio ao usuário bem intuitivos para tal tarefa. É a única distribuição atualmente que tem clone em nossa língua, o Conectiva Linux (TIBET, 2001).

4.1.1.4 Debian GNU/Linux

A Debian começou com o projeto da Free Software Fundation e posteriormente se desligou do projeto e tomou vida própria. É a mais preocupada com free software de todas as distribuições. Apenas pacotes que tenham o código-fonte disponível sem restrições podem fazer parte dessa distribuição. A distribuição com o maior número de pacotes entre todas e com a maior equipe de desenvolvimento. Porém, apresenta desvantagens em relação à facilidade de instalação e seleção dos pacotes, pois obriga o usuário a escolher um por um todos os pacotes a serem instalados. Uma parte dos usuários do Red Hat migra para esta distribuição após adquirirem experiência suficiente (TIBET, 2001).

5 FIREWALL

Ferretto et al. (2002.) definem que Firewall foi desenvolvido para impedir o acesso não autorizado às redes privadas. O Firewall é um mecanismo de segurança resistente a invasões, composto por um único sistema, ou por um conjunto de componentes básicos que o constituem e formam a sua arquitetura.

Agindo como um ponto de intersecção entre duas redes, ou mais, o Firewall centraliza a comunicação entre elas e também pode controlar todo o tráfego que passa por ele, tendo como finalidade e princípio proteger uma determinada rede das outras (FERRETTO, 2002).

O Firewall deve estar sempre presente em todas as comunicações entre redes públicas e privadas ou entre duas ou mais redes privadas que exijam maior segurança. Esse controle tem como base a política de segurança implementada no Firewall, bloqueando ou permitindo a passagem de tráfego entre as redes, de acordo com as autorizações desta política.

Desta forma, o Firewall provê um meio de controle do tráfego que passa por ele e cria um perímetro de defesa em torno da rede que protege. Todos os recursos de hardware e software que se encontram dentro deste perímetro estarão protegidos pelo Firewall (FERRETTO, 2002).

5.1 BENEFÍCIOS

Segundo Ferretto et al. (2002.) o Firewall gerencia os acessos entre duas redes distintas, evitando que a rede protegida fique facilmente vulnerável e exposta a ataques externos. Como centraliza e também pode controlar todo o tráfego que entra ou sai da rede, pode inibir a entrada ou saída de serviços estratégicos que tornem a segurança vulnerável e age como um ponto de obstrução – choke point, mantendo pessoas não autorizadas, como hackers, crackers, vândalos, espiões, etc., do lado de fora do perímetro da rede protegida (FERRETTO, 2002).

Além disso, possui a vantagem de ser o local onde a segurança pode ser monitorada de forma prática, e caso ocorram problemas, pode ser o local onde estão

acionados os procedimentos de defesa necessários – disparo de alarmes, registro de ocorrências, contra-ataque, bloqueio à passagem de todo o tráfego, etc. Devido a sua característica centralizadora, é o local ideal para se fazer auditorias, o levantamento de necessidades e usos que justifiquem os gastos com a comunicação (FERRETTO, 2002).

Desta forma, o Firewall agrega vantagens que visa garantir os seguintes princípios básicos de segurança da informação:

- Disponibilidade: garantia que a informação estará disponível para acesso no momento desejado;
- Sigilo: garantia que a informação seja inteligível apenas para os usuários, máquinas ou processos autorizados;
- Controle de acesso: garantia que a informação só possa ser acessada por pessoas ou processos autorizados;
- Autenticidade: garantia da identificação correta da origem da informação ou dos participantes, ou seja, a origem é conhecida. Dela deriva a integridade e o não repúdio;
- Integridade: garantia que a informação original não foi alterada;
- Não repúdio: garantia que os participantes não podem negar ação anterior da qual participam (FERRETTO, 2002).

5.2 LIMITAÇÕES

Segundo Ferretto et al. (2002.) para que um Firewall seja eficaz é necessário que todo o tráfego de entrada e saída de rede a ser protegida, passe por ele. O Firewall não pode proteger a rede de tráfego que não passa por ele. É essencial que nenhuma conexão com a rede externa, mesma via modem, seja feita em qualquer ponto da rede, pois este tipo de conexão exclui os esquemas de segurança, pré-estabelecidos e conseqüentemente a política de segurança. (FERRETTO, 2002).

O Firewall não é capaz de proteger uma rede dos ataques que não passam por ele. Da mesma forma, o Firewall não pode impedir que usuários mal intencionados copiem as informações em disquetes ou outra mídia qualquer e as

divulguem. Também não consegue impedir que uma pessoa, usando a senha de outra, acesse a rede em seu lugar. (FERRETTO, 2002).

O mais grave na aplicação de uma política de segurança é justamente a falta de cuidado dos próprios usuários do sistema, tais como: uso de senhas fracas ou sua divulgação, contas abertas, baixa de arquivos infectados e execução dos mesmos sem antes passar pela verificação do antivírus. Assim, nem o Firewall perfeitamente configurado pode garantir segurança. Por isso, a consciência das responsabilidades e o treinamento dos usuários são estritamente necessários (FERRETTO, 2002).

O Firewall não proporciona nenhum tipo de proteção contra intrusos que já conseguiram penetrar, de alguma forma, no seu perímetro de defesa. O Firewall, também, não consegue proteger a rede da execução de códigos maliciosos e são suscetíveis a eles. Um Firewall de nada será útil se houver propagação de vírus na rede protegida ou se programas mal comportados, desenvolvidos sem cuidado ou que apresentam alguma falha, permitam a entrada de intrusos ou coloquem a rede em risco de ataques (FERRETTO, 2002).

5.3 PREJUÍZOS

Segundo COLLE et al. (2006), controlar o uso de recursos e do tempo dos funcionários tem sido uma prioridade para muitas organizações sendo que em outras a questão da privacidade dos usuários é considerada.

Com a chegada da Internet, ficou muito mais fácil e rápido ter acesso a informações e comunicar-se com o mundo, para o bem ou para o mal. Muita gente acha que não há problema em acessar um ou outro site de entretenimento ou e-mail pessoal durante o horário de expediente. Mas, vale lembrar que o funcionário é pago para, durante esse tempo, prestar seus serviços à empresa. Se a intenção é tirar alguns minutinhos para relaxar e esfriar a cabeça o certo é procurar fazer algo que não seja uma ameaça para as organizações, usar a Internet para fins pessoais, em casa. O uso do correio eletrônico é uma “ferramenta de produtividade”, estudos mostram que o número de mensagens irá dobrar a cada ano, até 2007, e esse aumento irá diminuir a produtividade de mais de 60% dos usuários (COLLE, 2006).

As empresas em geral, não são tão rígidas com essas “escapadinhas” para o mundo virtual. O problema é quando o funcionário perde o limite de tempo, ou, pior ainda, do conteúdo dos sites acessados. Usar a Internet no trabalho para “surfar” em sites de pornografia ou relacionados a assuntos ilegais é algo altamente não-recomendável. Muitas empresas controlam a navegação dos usuários internos e podem até demitir o funcionário que for flagrado ao usar indevidamente a rede. Esse foi o caso de um ex-funcionário de uma grande instituição financeira, acusado de utilizar o correio eletrônico da empresa para repassar imagens pornográficas. A causa foi parar na 3ª Turma do Tribunal Regional do Trabalho da 10ª Região (Brasília), que reconheceu, por unanimidade, a justa causa na demissão (COLLE, 2006).

Se os equipamentos e softwares utilizados para acessar a Internet pertencem à empresa e há cláusula expressa no contrato de trabalho dispondo que o computador só pode ser utilizado para fim de trabalho e que seu uso será monitorado, a simples consulta de e-mail particular pode ser motivo para a aplicação de justa causa. Muitos funcionários reclamam da monitoração feita pelas empresas, alegando que sua privacidade é violada (COLLE, 2006).

As empresas estão mais cautelosas. Não é invasão de privacidade checar o que seus funcionários andam fazendo pela Internet. É direito da corporação ter controle o que está ou não sendo produzido, afinal, é ela quem paga o salário no fim do mês (COLLE, 2006).

O que faz um funcionário quando não está exercendo seu trabalho, mas se encontra nos limites da empresa? Este tempo gasto com atividades alheias ao trabalho, com periodicidade excessiva, consequentemente traz perda de produtividade, prejuízos financeiros. Estes prejuízos nem sempre são de fácil constatação e mensuração. Muitas empresas não se dão conta do enorme prejuízo que sofrem por não terem uma boa política de acesso a Internet e um bom controle de acesso (COLLE, 2006).

As corporações estão classificando o e-mail pessoal e as conexões de Internet de seus empregados como fator potencial de distração no trabalho, vazamento de informações e problemas com a pornografia. Por isso, estão considerando limitar ou mesmo proibir o uso pessoal da Web, a razão é simples: grande parte dos problemas de vírus nas empresas vem por causa do uso pessoal da Internet por parte dos empregados (COLLE, 2006).

Com relação aos problemas legais, uma empresa pode ser processada se um de seus funcionários usar a rede corporativa para baixar ilegalmente música e outros conteúdos protegidos por *copyrigth*. (COLLE, 2006)

5.4 A NECESSIDADE DE FIREWALL

Segundo Ferretto et al. (2002.), a finalidade principal de um Firewall é proteger uma rede de ataques externos, ou seja, provenientes de outra rede. É importante observar que no ambiente de negócios na Internet, atualmente, o Firewall, por si só, não é suficiente para fornecer todos os níveis de segurança necessários. Firewalls são geralmente muito eficientes em manter pessoas não autorizadas do lado de fora das redes empresariais. Isto é feito delimitando-se os tipos de conexões que serão permitidas e os serviços que serão suportados. Isto funciona bem quando as fronteiras da rede são claramente definidas e quando há pouca ou nenhuma necessidade de computação colaborativa (FERRETTO, 2002).

Os processos atuais de negócios baseados na Web mudaram as regras da computação empresarial. As empresas precisam, cada vez mais, disponibilizar informações, assim como ter acesso a diversas aplicações no mundo dos negócios. Em cada nova aplicação permitida, o risco de brechas na segurança é multiplicado. Cada novo usuário implica, também, um risco ampliado de espionagem, maus usos de contas ou que informações caiam em mãos erradas, deliberadamente ou não. Considerando o acesso estendido a parceiros, clientes e fornecedores provenientes da rede externa, uma solução gerenciada centralmente é necessária para controlar a complexidade do sistema. É possível delimitar o acesso a informações críticas residentes na rede protegida, por trás do Firewall, assim como definir e controlar quais informações que podem sair da empresa para a rede externa (FERRETTO, 2002).

Ataques ou invasões podem originar-se de dentro ou de fora das fronteiras convencionais da empresa. Muitas brechas na segurança originam-se do lado de trás do Firewall, ou seja, dentro da própria empresa. Para evitar que informações confidenciais caiam em mãos erradas, a habilidade de monitorar o conteúdo de arquivos saindo da rede interna para a Internet, ou só trafegando na rede interna é

tão ou mais importante, quanto a habilidade de monitorar o conteúdo de arquivos entrando da Internet para a rede interna (FERRETTO, 2002).

O Firewall tem a capacidade de impor limites no fluxo da informação que sai para a rede externa, como o bloqueio de protocolo, podendo impedir o estabelecimento de conexões de bate papo tipo IRC, por exemplo, e outros serviços considerados perigosos ou simplesmente dispensáveis. Porém, este bloqueio pode ser driblado se o aplicativo utilizar outros protocolos ou portas diferentes daquelas utilizadas normalmente (FERRETTO, 2002).

Em geral, Firewalls não são capazes de exercer controle rigoroso sobre o conteúdo através do monitoramento e bloqueio de informações não autorizadas, assim como impedir todo e qualquer acesso não autorizado. Também não disponibilizam procedimentos antivírus nativamente, assim como o controle sobre códigos maliciosos embutidos em Applets, Java ou arquivos Activex (FERRETTO, 2002).

Estes arquivos podem possuir conteúdos perigosos, capazes de paralisar as redes empresariais. A filtragem de conteúdo e medidas antivírus efetivas, baseadas no gateway, são ambas necessárias para garantir uma proteção adequada à empresa (FERRETTO, 2002).

Embora a segurança nos desktops e servidores sejam importantes, medidas relacionadas a conteúdo não autorizado e programas malignos são mais efetivas e eficientemente empregadas em gateway para a Internet, que atuam como Firewalls, operando como o único ponto de comunicação da empresa com o restante do mundo (FERRETTO, 2002).

5.5 CONSIDERAÇÕES ESPECIAIS

Segundo Ferretto et al. (2002.) devido a importância e responsabilidade de um Firewall na segurança de uma rede, faz-se necessária a adoção de algumas considerações para resguardá-lo (SHELDON, 1996):

- Limitar as contas no Firewall ao estritamente necessário, tal como a conta do administrador. Se possível, deve ser desabilitado o login da rede;

- Usar autenticação para garantir um grau de segurança maior do que o uso de login/senha;
- Dispositivos do tipo desafio/resposta são facilmente integrados aos mais populares sistemas operacionais;
- Remover todos os programas desnecessários instalados num Firewall: compiladores, editores de texto, jogos, etc. Eles podem conter alguma brecha que permita que os hackers a explorem;
- Não se deve rodas protocolos vulneráveis em um Firewall, tais como: TFTP, NIS, NFS, UUCP, etc;
- Desabilitar o protocolo Finger. Através dele, um usuário remoto pode obter informações sobre todas as contas de um sistema;
- Nos Gateways de e-mail, desabilitar os comandos EXPN e VRFY, os quais podem ser utilizados por hackers para obter informações sobre os endereços dos usuários;
- Desabilitar todos os serviços que não estão sendo utilizados num Firewall;
- Utilizar Firewall somente como Firewall;
- Habilitar a criação de logs no Firewall e constantemente analisá-los com o apoio de ferramentas específicas;
- Desenvolver políticas de contenção;
- Utilizar o host do Firewall apenas para sua atividade especifica.

Características Firewall;

- Combinação mais completa e segura do mercado de Proxy a nível de aplicação;
- VPN com vários algoritmos de criptografia;
- Bloqueio de sites Web indesejáveis;
- Suporte a NAT bi-direcional;
- Medidas anti-spamming integradas;
- Possui capacidades externas de log, permitindo exportar informações para analisadores ou programas de detecção de intrusos (FERRETTO, 2002).

5.6 POLÍTICAS DE SEGURANÇA PARA FIREWALL

Segundo Ferretto et al. (2002.) a política de segurança é um dos fatores mais importantes para garantir a segurança corporativa. Isso porque ela trata justamente do ativo: as pessoas. É o conjunto formado por diretrizes, normas, procedimentos e instruções que irá nortear os usuários quanto ao uso adequado dos recursos e eles disponibilizados (FERRETTO, 2002).

É onde se definem regras, comportamentos, proibições e até punições por má utilização. Deve estar de acordo com a cultura da empresa e seus recursos tecnológicos (FERRETTO, 2002).

Regras de manutenção e criação de senhas, rotinas de backup, fragmentação de material descartado, limites para uso de e-mail e a definição de trilhas de auditoria são alguns dos pontos abordados. Sendo o padrão comum existir uma diretriz básica, onde enfoca a proteção de dados/informações da empresa, sendo complementada por normas que abrangem assuntos específicos (FERRETTO, 2002).

Políticas de segurança, para serem efetivas, devem ser divulgadas tanto aos usuários dos sistemas quanto aos responsáveis pela manutenção dos mesmos (SHELDON, 1996).

É importante ressaltar que um Firewall não é somente um dispositivo, para fornecer segurança a uma rede. O Firewall é parte de uma política estratégica e consistente de segurança organizacional, que possibilita a criação de um plano de defesa para proteger os recursos computacionais. O Firewall é peça fundamental na segurança de uma organização, mas deve ser lembrado que de nada adianta se este não estiver configurado adequadamente (FERRETTO, 2002).

6 IPCOP FIREWALL

O IPCOP FIREWALL é uma distribuição do sistema operacional Linux sendo que sua finalidade é proteger a rede em que é instalado. E extremamente fácil de instalar e configurar por qualquer utilizador, desde o mais inexperiente até o mais técnico utilizador.

É distribuído sob a licença GNU (General Public License), uma de muitas vantagens que ele possui, é que seu código fonte é aberto permitindo que peritos em segurança WORLDWIDEWEB (Rede de alcance mundial), examinem e reparem problemas de segurança. O logotipo do IPCOP é mostrado na figura 1.

Figura 1 Ipcop_Banner_Half_Size

6.1 SURGIMENTO DO IPCOP FIREWALL

O IPCOP foi iniciado em outubro de 2001, de uma bifurcação, do projeto Smoothwall. Pois surgiu na época uma proposta que o Smoothwall, passa a ser cobrado, um grupo de pessoas foi contra a esta proposta, e se retiram do projeto Smoothwall.

Este grupo que se retirou do projeto Smoothwall, decidiu iniciar um novo projeto, pois eles queriam ter um projeto de código fonte aberto que atendesse suas necessidades, e que outras pessoas pudessem se beneficiar.

Como possuíam os códigos fontes eles os recodificaram e o relançaram com o nome de IPCOP FIREWALL. Este grupo estipulou metas que todo membro tem que seguir, para fazer parte do grupo. Essas metas são:

- Fornecer uma distribuição de Firewall estável;
- Fornecer uma distribuição de Firewall seguro;

- Fornecer uma distribuição de Firewall que seja software livre;
- Fornecer uma distribuição de Firewall altamente configurável;
- Fornecer uma distribuição de Firewall de fácil configuração;
- Fornecer Suporte confiável;
- Fornecer um ambiente agradável para o usuário discutir e ter ajuda;
- Fornecer upgrades/patches estáveis, assegurando, fácil implementação para IPCOP FIREWALL;
- Se esforce para adaptar o IPCOP FIREWALL às necessidades da Internet.

6.2 CARACTERÍSTICAS DE INSTALAÇÃO

6.2.1 Interfaces

O IPCOP suporta 4 interfaces de rede e classifica cada uma delas com cores, variando essas de acordo com a função de cada interface.
Green (rede interna);
Red (rede externa ou Internet);
Orange (DMZ);
Blue (conexão access point).

Alem das 4 interfaces o IPCOP FIREWALL suporta também VLAN, e suporte à nome alternativo para a interface red.

6.2.2 Hardware

Suporte a arquitetura i386 e alfa.
Memória mínima de 12 MB até 4 GB.

Disco rígido ide, scsi, controladora disco sata e raid com 250 MB no mínimo.
Placa ethernet ISA, PCI.
Núcleo SMP disponível para i386 HT / multicore ou múltiplos CPU.

6.2.3 Instalação

O IPCOP Firewall pode ser instalado das seguintes formas:

- Boot disquete;
- Boot cd room ide, SCSI;
- Boot usb;
- Boot placa ethernet com PXE habilitado (necessitando de avdhcp e tftp servidor instalado);
- Instalação http/ftp.

6.2.4 Idiomas Disponíveis

O IPCOP FIREWALL esta disponível nos seguintes idiomas:

Holandês, Sul-Africano, Português Brasileiro, Búlgaro, Catalão, Chinês, Tcheco, Dinamarquês, Inglês, Finlandês, Francês, Alemão, Grego, Húngaro, Italiano, Japonês, Lituano, Norueguês, Persa, Polonês, Português, Romano, Russo, Eslovaco, Esloveno, Espanhol, Sueco, Tailandês, Turco, Urdu, Vietnamita.

6.2.5 Serviço de Backup

- Disquete;
- Interface web;
- USB.

6.2.6 Serviços Disponíveis.

- Cliente/Servidor DHCP;
- DNS dinâmico;
- Http/ftp proxy (squid);
- IDS (snort) em todas as interfaces;
- LOG (local e remoto);
- Cliente/ Servidor ntp;
- Servidor ssh;
- Informação de trafego (interface red).

6.2.7 Características do Firewall

- Statefull Firewall é uma característica utilizada por Firewalls que tem a finalidade de analisar os pacotes TCP detalhadamente. Ele cria um poderoso sistema, evitando ataques do tipo *Stealth Scans, i*sso permite que o Firewall Statefull seja tecnicamente melhor do que um Firewall Filtro de Pacotes, devido à sua criticidade na análise dos pacotes de uma rede;
- Suporte a Nat h323, irc, msn, pptp, proto-gre, quake3;
- Nat programável para interface Laranja;
- PING de resposta configurável para todas as interfaces.

6.2.8 Vpn Ip’sec

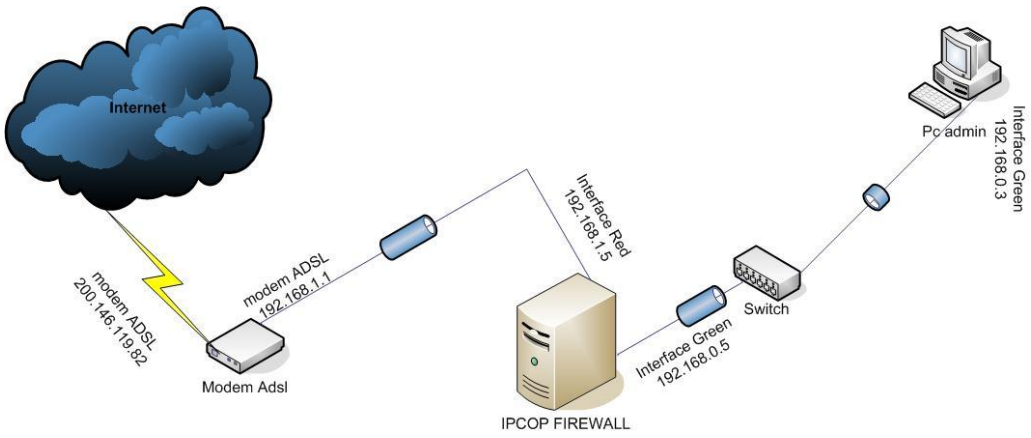
- Certificado ou PSK;
- Conexão Host a rede (Roadwarrior);
- Conexão Rede a Rede. (Net-to-Net).

7 MANUAL DE INSTALAÇÃO DO LINUX IPCOP FIREWALL

Neste capítulo será mostrado como se instala o IPCOP FIREWALL, para que micros e pequenas empresas possam ter uma ferramenta poderosa, eficiente para proteger sua rede dos perigos da Internet, e também monitorar as atividades de seus funcionários na rede mundial de computadores. Será construída uma rede conforme diagrama detalhado mostrado na figura 2.

- IP valido do modem ADSL 200.146.119.82.
- IP inválido do modem ADSL 192.168.1.1.
- IP inválido interface Red (eth0) 192.168.1.5.
- IP inválido interface Green (eth1) 192.168.0.5.
- IP inválido PC administrador 192.168.0.3.

Figura 2 Diagrama detalhado da rede



O material usado neste manual foi gerado através de uma máquina virtual usando o software VMWARE Workstation, e também o software Wink 2.0 para extrair os screenshots.

Depois de obtido o material necessário para elaboração do manual, o IPCOP FIREWALL foi instalado em um computador com, 1 processador AMD-k6(tm)-2/500 MHz com 256 MB de memória ram, 1 HD de 10 GB de espaço, 2 placas Realtek RTL8139 Family PCI fast Ethernet NIC, 1 Gravadora Cd room, 1 switch 3COM 16

portas, 1 modem adsl modelo Altavia 670R da Parks, com a opção “Boot cd room ide”.

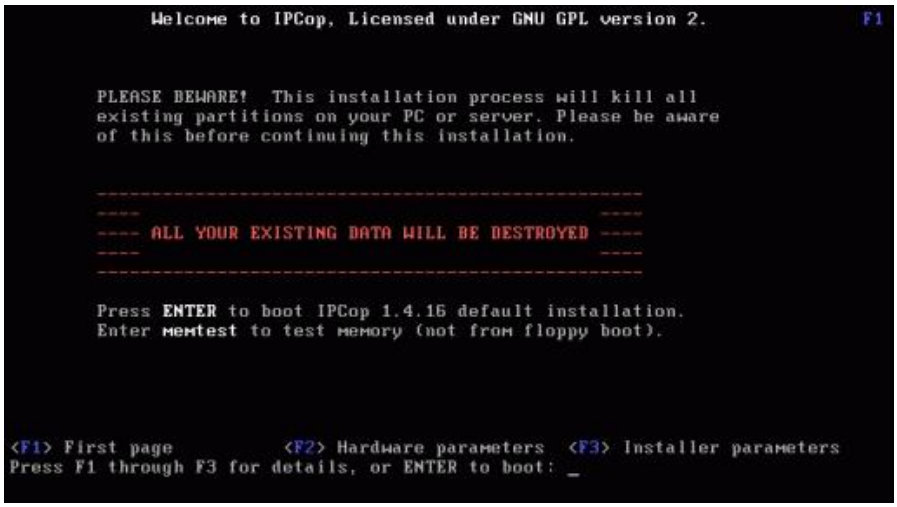
Lembrando que o IPCOP FIREWALL é um sistema operacional que roda sozinho, só pode ser instalado em uma máquina dedicada como Firewall, não é recomendado instalar em uma máquina que tenha outro sistema operacional, pois esta instalação irá apagar todos os dados do HD.

É preciso fazer o download do arquivo ipcop-1.4.16-install-cd.i386.iso no seguinte endereço http://downloads.sourceforge.net/ipcop/ipcop-1.4.16-install-cd.i386.iso?modtime=1184673271&big_mirror=1, este endereço é a fonte oficial para download do IPCOP FIREWALL, após o download é preciso gravar este arquivo em uma mídia cd rom.

7.1 INICIANDO A INSTALAÇÃO.

Com o arquivo gravado na mídia cd rom insere-se a mesma no computador que será instalado o IPCOP FIREWALL. Entra-se na bios do computador e habilita o computador para dar boot pelo cd room. Reinicia-se o computador com a mídia no leitor cd room, e espere até o cd rom ser lido, irá aparecer a tela inicial de instalação do IPCOP, conforme mostra a figura 3.

Figura 3 Tela inicial da instalação

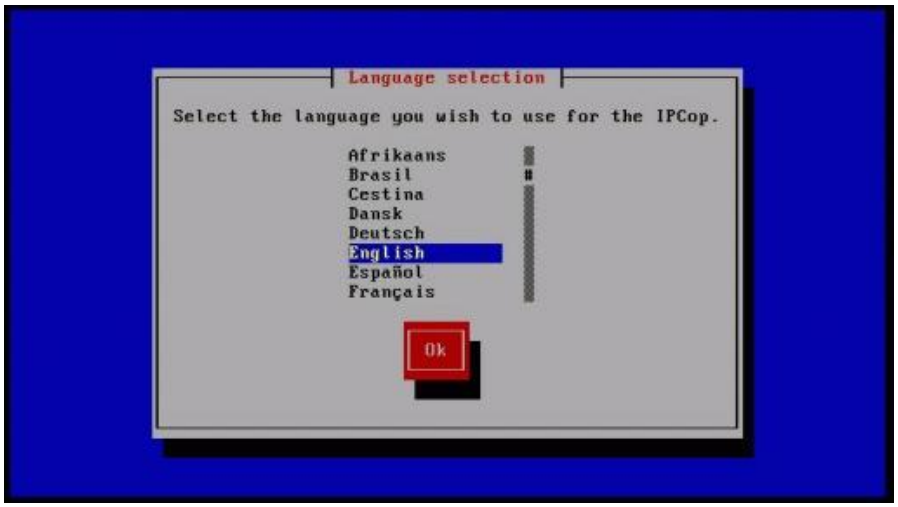


Durante a instalação serão usadas as seguintes teclas para navegação entre as opções:

- TAB, para posicionar e selecionar as opções;
- ENTER, para prosseguir a instalação;
- ESPAÇO, para selecionar opções;
- Seta esquerda, Seta direita, Seta abaixo, Seta acima, também servem para posicionar e selecionar opções.

Depois de clicar “ENTER”, para dar inicio a instalação será feita a leitura de compatibilidade de hardware da máquina e será apresentada a tela “Language selection” mostrada na figura 4, para que seja escolhido do idioma de instalação do sistema. Neste manual escolhemos o idioma English, por ser de fácil atualizações futuras de ferramentas do sistema, e por ser uma linguagem universal, tecle “ENTER” para seguir para a próxima tela.

Figura 4 Language selection



A próxima tela é somente uma mensagem de boas vindas do sistema, como mostra a figura 5, tecle “ENTER” para iniciar a instalação.

Figura 5 Mensagem de boas vindas

A tela “Select installation media”, mostrada na figura 6 é para informar qual o tipo de instalação que será realizada. Selecione “CDROM/USB-KEY” e pressione “TAB” até chegar a opção “OK” e tecle “ENTER”.

Figura 6 Select installation media

A tela “IPCOP v1.4.16 – The Bad Packets Stop Here” está informando que o HD será formatado automaticamente e serão criadas as partições necessárias para a instalação do sistema, como mostra a figura 7, clique “ENTER” para continuar a instalação. (OBS: tudo que estiver no HD será perdido).

Figura 7 IPCOP v1.4.16 – The Bad Packets Stop Here

A tela “Restore”, conforme mostra a figura 8, é para escolher alguma forma de backup, nesta instalação não será usada esta opção, clique a tecla “TAB” até chegar a opção “SKIP”. Para marcar esta opção pressione a tecla “ESPAÇO”, depois pressione a tecla “TAB” até chegar à opção “OK” e clique “ENTER” para continuar a instalação.

Figura 8 Restore

A partir da tela “Configure networking” é onde se deve ter muita atenção, pois é nela que se começa a ser configurada a rede, e qualquer descuido pode-se ter problemas, conforme a figura 8.

Conforme a Figura 2 o IPCOP possui 2 interfaces de rede sendo elas, a interfaces Green e Red e é nesta parte onde a instalação detecta o driver da placa de rede da interface GREEN, e informa-se o endereço IP da placa.

Selecione a opção “Probe” e tecle “ENTER” para a instalação detectar o primeiro driver da placa de rede.

Figura 9 Configure networking

Se tudo ocorreu bem a instalação reconhecerá o driver de placa rede, e mostrará o driver reconhecido e aparecerá a opção “OK”, assinalada clica-se “ENTER” para continuar a instalação.

Figura 10 Detecção placa rede

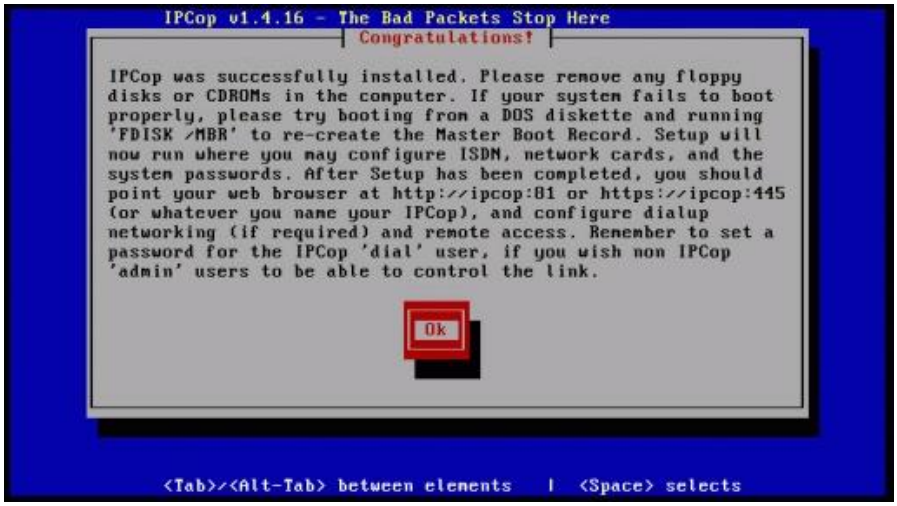
Se a mensagem “Error: Auto Detecting failed” aparecer é porque a placa de rede não é suportada pelo sistema, ou está com algum problema, deve-se providenciar a troca da placa de rede não suportada, ou com problema.No endereço http://www.ipcop.org/index.php?module=pnWikka&tag=IPCopHCLv01, está disponível uma lista de placas de redes suportadas pelo sistema.

A tela “GREEN interface” solicitará que seja digitado o endereço IP para a interface Green como mostra a figura 11. Neste manual usaremos o endereço 192.168.0.5, clique na tecla “TAB” até chegar a opção “OK”, clique “ENTER”, para finalizar.

Figura 11 Configure networking

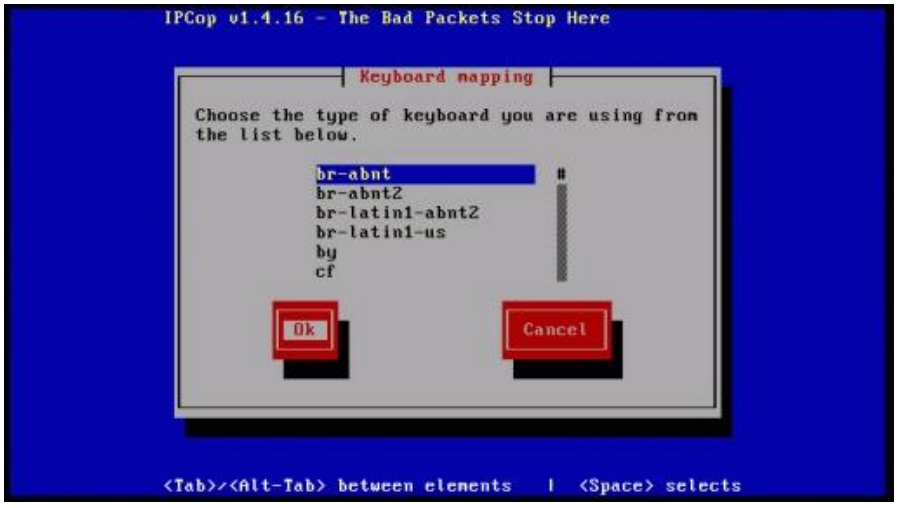
A tela “Congratulations!” informa que o sistema foi instalado com sucesso, como mostra a figura 12.

Figura 12 Congratulations!



A tela “Keyboard mapping” é para configurar o layout do teclado. Neste manual será usada a opção br-abnt, mova o cursor com as teclas “acima, abaixo” até encontrar a configuração do teclado, pressione a tecla “TAB” para ir para a opção “OK”, clique na tecla “ENTER” para continuar a instalação.

Figura 13 Keyboard mapping

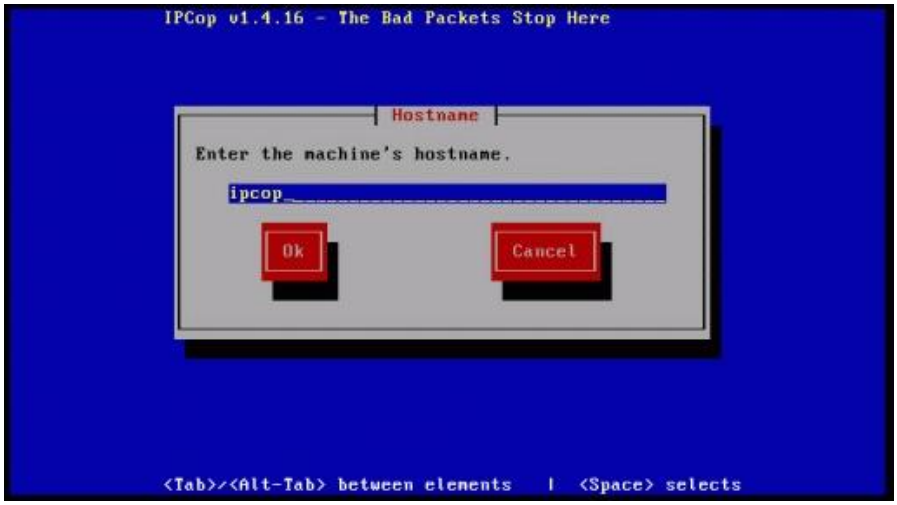


A tela “Timezone” é para configurar a zona de tempo, neste manual foi escolhida a zona Brazil/East (Brasil/Leste) como mostra a figura 14.

Figura 14 Timezone

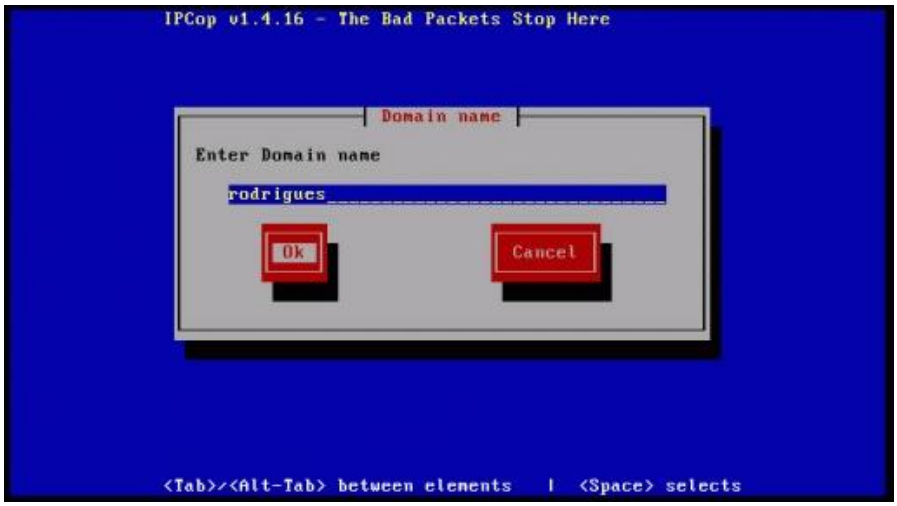
Na tela “Hostname” é solicitado que se informe o nome para o servidor, como mostra a figura 15. Neste manual usaremos o nome IPCOP, pode-se colocar qualquer nome que desejar desde que não tenha nenhum outro computador na rede com o nome.

Figura 15 Hostname



Na tela “Domain name” é solicitado que se informe o domínio que o Firewall fará parte.como mostra a figura 16. Neste manual usaremos o domínio “RODRIGUES”, lembre-se que para os computadores se comunicarem eles têm que pertencerem no mesmo domínio.

Figura 16 Domain name



A próxima tela é para se configurar conexão ISDN como mostra a figura 17. A conexão ISDN usa o sistema telefônico comum, com isso se paga pulsos telefônicos. Tem-se à disposição duas linhas de 64 K cada uma, que podem ser usadas tanto para conexão à Internet quanto para chamadas de voz. Na hora que conectar-se a Internet tem-se a opção de usar as duas linhas, conectando-se a 128 k, ou então deixar a segunda linha livre para uma chamada de voz, mas em compensação acessando a apenas 64 k.

O grande problema desse tipo de conexão é que se usar as duas linhas para conectar a Internet, a tarifa é cobrada em dobro. Por isso que ela não é usada largamente, além disso, ela não está disponível em muitas cidades. Para desabilitar esta função clicamos “TAB” até o cursor se posicionar em “Disable ISDN” e clicamos “ENTER” para continuar a instalação.

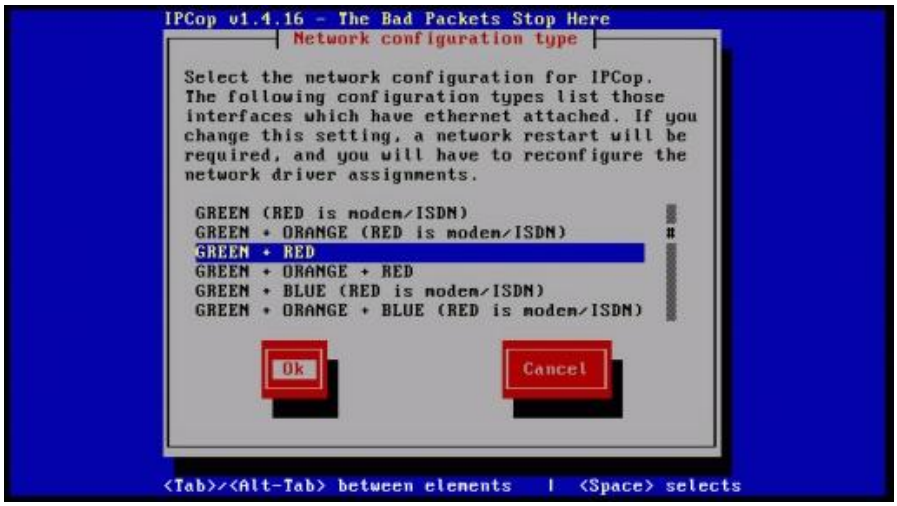
Figura 17 ISDN configuration menu

A tela “Network configuration menu” é onde se configura o tipo de rede, detecta o driver da interface “RED”, informa o IP da interface “RED”, informa os IP’s dos servidores DNS, o IP do Gateway da rede e tem a opção de habilitar um servidor DHCP para a rede interna, como mostra a figura 18. Escolhe-se a opção “Network configuration type” para informar qual o tipo de rede.

Figura 18 Network configuration menu

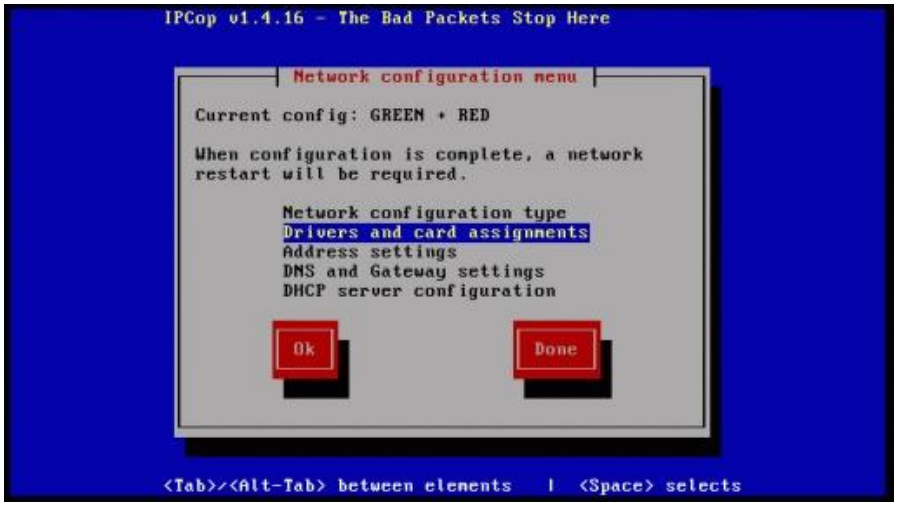
Na tela “Network configuration type” escolhe-se a opção “GREEN + RED”, pressiona-se as teclas ”TAB”, “ENTER” para a instalação gravar o tipo de rede que será usado, como mostra a figura 19.

Figura 19 GREEN + RED



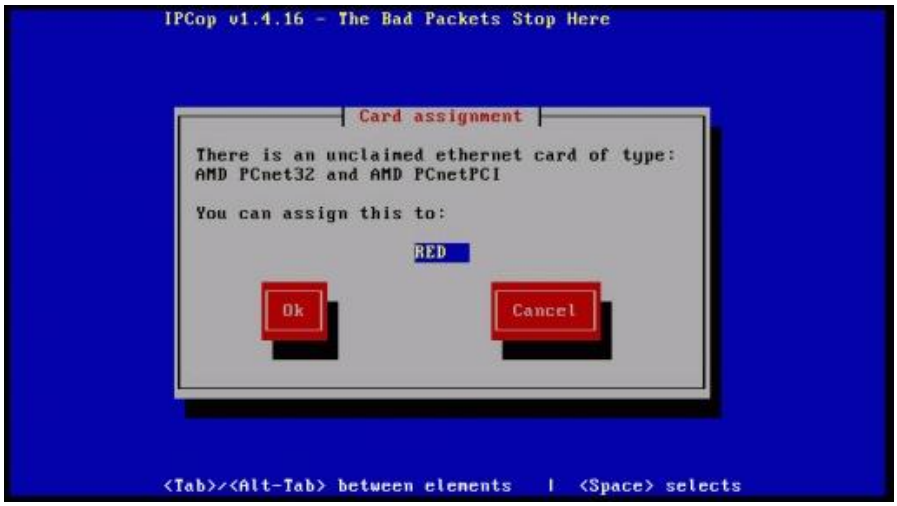
A instalação voltará a tela “Network configuration menu”, seleciona-se a opção “Drivers and card assignments”, como mostra a figura 20. Pressione “ENTER” para entrar na opção, e pressione “ENTER” novamente para a instalação detectar o driver da interface “RED”.

Figura 20 Drivers and card assignments



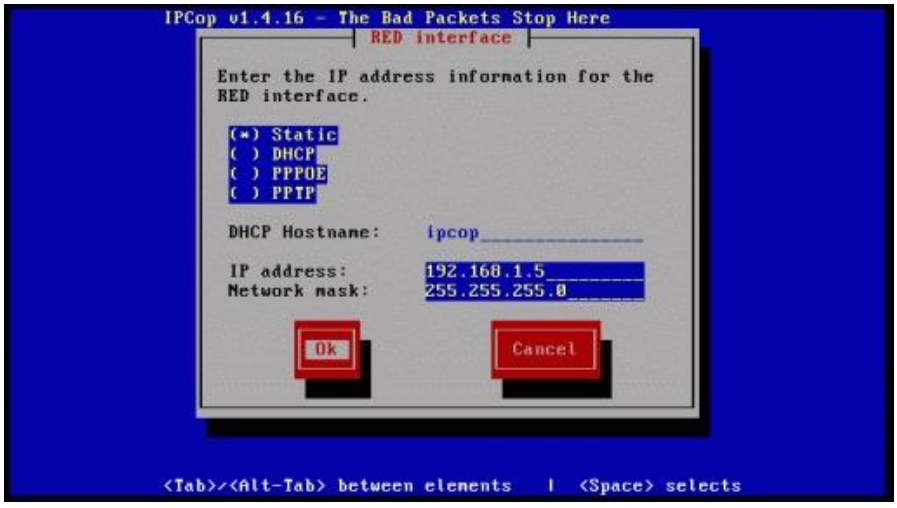
Se tudo correr bem será apresentada a tela “Card assignment” e a interface “RED” selecionada, como mostra a figura 21. Pressione “ENTER” e será apresentada a mensagem “ALL cards successfully allocated”, esta mensagem quer dizer o driver foi reconhecido.

Figura 21 Card assignment



A instalação voltara à tela “Network configuration menu”, nesta tela escolhe-se a opção "Address settings” pressiona-se “ENTER” será apresentado as interfaces “GREEN e RED”, seleciona-se a interface “RED”, pressiona-se “ENTER”, e será apresentada a tela “RED interface” estará marcada a opção “STATIC”, pressiona-se a tecla “TAB” até chegar a opção “IP address” e digita-se o IP, 192.168.1.5, pressiona-se a tecla “TAB” até a opção “OK” e tecla-se “ENTER” para terminar a configuração da interface “RED”, conforme a figura 22.

Figura 22 RED interface



A instalação voltará na tela “Address settings”, pressiona-se “ENTER” duas vezes até chegar a opção “Done”, e clica-se “ENTER” para voltar à tela “Network configuration menu”.

Na opção “DNS and Gateway settings” pressionando “ENTER” aparecerá a tela para ser digitado o DNS primário, DNS secundário e Default Gateway. Os DNS usados para este manual são, primário 200.221.11.100, secundário 200.221.11.101, (Obs. Para saber os IP’s dos servidores dns válidos pode-se entrar em contato a operadora que disponibiliza o serviço a sua empresa, ou com o provedor). O Default Gateway é o endereço IP do modem ADSL que neste caso é 192.168.1.1.

Figura 23 DNS and Gateway settings

Depois de configurado a opção “DNS and Gateway settings” a instalação voltara à tela “Network configuration menu” restando a opção “DHCP Server configuration”.

Na opção de configuração do servidor DHCP a seguir, existe um bug e tem que ser tomado muito cuidado, pois qualquer descuido a instalação terá que ser feita de novo, este bug ocorre da seguinte forma.

Se for escolhido não configurar o servidor escolhendo a opção “DONE” a instalação mesmo assim entra na configuração, e se mover o cursor até a opção “Cancel” e clicar “ENTER” a instalação pula a fase onde é solicitada que se informe as senhas dos usuários “ROOT”, “ADMIN”, “BACKUP” e encerra a instalação.

Com isso não tem como logar no sistema, pois as senhas de login não foram informadas. Se for escolhido configurar o servidor, a instalação obriga a fazer duas

vezes a configuração do servidor, para depois solicitar as senhas dos usuários “ROOT”, “ADMIN”, “BACKUP”.

Para contornar este bug, tanto para configurar ou não o servidor deve-se seguir os seguintes procedimentos. Selecionar a opção “DHCP Server configuration” escolher a opção “DONE” pressionar “ENTER”.

A instalação entrará na tela de configuração, para não configurar o servidor deve-se pressionar “TAB” até chegar à opção “DONE” depois “ENTER”, caso for configurar o servidor siga os procedimentos abaixo.

Para configurar o servidor habilite a opção “Enabled”, pressiona-se “TAB”. Preencham-se os campos, “Start address”, “End address”, “Primary DNS”, as opções “Start address e End address” informar o endereço IP inicial e o endereço IP final que o servidor usará para atribuir IP’s automaticamente para computadores que forem conectados à rede, como mostra a figura 24. Neste trabalho estamos informando que o endereço inicial é 192.168.0.30 e o endereço final é 192.168.0.40, “Primary DNS” é para endereço IP do servidor DHCP, como mostra a figura 24.

Figura 24 DHCP Server configuration

Após informar o endereço IP na opção “Primary DNS”, pressiona-se “TAB” até chegar à opção “OK”, a seguir pressiona-se “ENTER” para encerrar a configuração do servidor DHCP.

Terminada a configuração do servidor DHCP, o sistema solicitará que sejam informadas as senhas dos usuários “root”, “admin”, e de “backup”. (Obs. Nunca digite a mesma senha para os usuários root e admin).

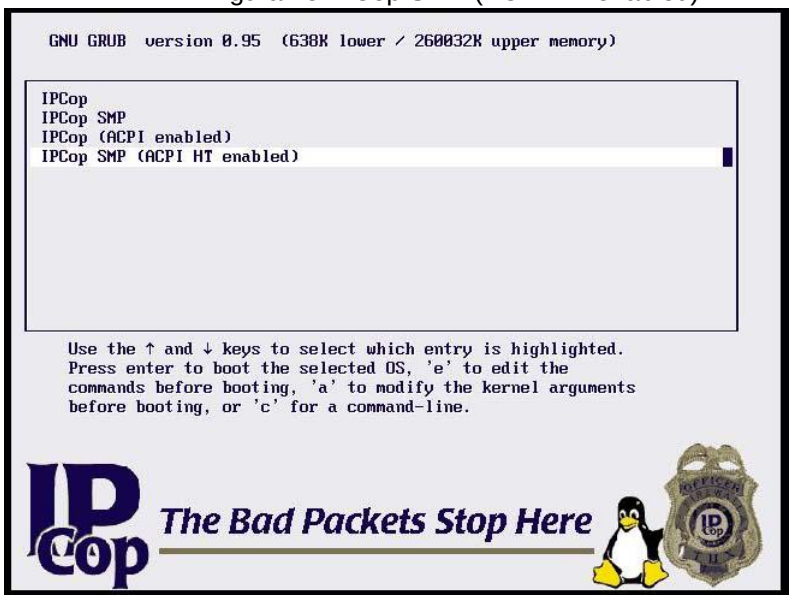
Na primeira tela digita-se a senha do usuário “root” e confirma-se a senha, pressione “ENTER”, siga este procedimento para o usuário admin, e para backup.

Depois de digitar a senha de backup o sistema informará que a instalação foi completada e solicitará que o computador seja reiniciado. Clique “ENTER” para reiniciar o computador.

Lembre-se de tirar a mídia do cd rom, e entrar na bios do computador e mudar a opção de boot, para que seja dado boot pelo HD.

Depois de reiniciado o computador e ter colocado para dar boot pelo HD, será apresentada a tela inicial de boot do sistema. O cursor estará na opção “IPCOP”, move-se o cursor até a opção “IPCOP SMP (ACPI HT enabled)” e pressiona-se “ENTER”, como mostra a figura 25.

Figura 25 IPCop SMP (ACPI HT enabled)



Depois de inicializado, o IPCOP fará a leitura de hardware, arquivos de inicialização habilitarão os módulos necessários para seu funcionamento, e apresentará a tela de login, como mostra a figura 26.

Figura 26 IPCop login

8 MANUAL DE CONFIGURAÇÃO E GERENCIAMENTO DO LINUX IPCOP FIREWALL

Neste capítulo será apresentada a forma correta de configurar e gerenciar o IPCOP FIREWALL, sendo que estas configurações são feitas quase todas via interface Web. Foi utilizado um computador com Windows XP Professional instalado, navegador Internet Explorer 7.0, o software WINSCP e software PUTTY.

- Winscp: cliente gráfico para acesso remoto usa FTP, SFTP.
- Putty: cliente acesso remoto em modo texto.

Primeiramente faz-se o download dos softwares winscp e putty nos seguintes endereços, site oficial do winscp http://winscp.net/eng/index.php, endereço oficial do site putty http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html.

Terminados os downloads, instala-se o software winscp, e cria-se um diretório em c:\arquivos de programas\PuTTy e copia-se o software putty.exe para este diretório.

A instalação default do IPCOP já vem pré configurada e funcionando, podendo atender as necessidades, porém para melhorar algumas funções há a necessidade de instalar o servidor de addons (Addons Server). Com o servidor addons instalado melhora-se a segurança e desempenho do servidor.

Addons são softwares que melhoram algumas ferramentas do sistema, ou inclui nova ferramenta. Existem vários addons para o IPCOP na Internet, mas alguns são exclusivos para uma determinada versão do IPCOP.

Sempre que encontrar um addon para o IPCOP procure saber se a fonte que disponibiliza é confiável, nunca instale este addon no servidor principal sem fazer testes primeiro, pois se este addon for incompatível para a versão do IPCOP, podem ocorrer problemas sérios, até mesmo inviabilizar o sistema.

Para a instalação do Addons Server, crie um diretório em C:\IPCOP, logo após faça o download do arquivo “addons-2.3-CLI-b2.tar.tar” no endereço http://firewalladdons.sourceorge.net/ e salve-o no diretório criado.

Para prosseguir com as configurações é necessário habilitar a opção de acesso via SSH do IPCOP. Abra um navegador de internet e digite na barra de

endereço do navegador https:// ip da interface GREEN :445 (https://192.168.0.5:445). Será apresentado um erro de segurança que deve ser ignorado, este erro é apresentado em qualquer navegador.

Se estiver usando o navegador Internet Explorer será apresentado a seguinte mensagem “Erro do Certificado:Navegação Bloqueada”, clica-se em “Continuar neste site (não recomendado)”,conforme a figura 32.

Após aparecer a página principal do IPCOP clique em “Connect”, no campo “Nome de usuário” informe o nome “admin” e no campo “Senha” informe a senha que foi digitada na instalação. (obs. Somente o usuário admin tem permissão de acesso a interface web do ipcop). Vá até a opção “SYSTEM” procure por “SSH Access” marque a clique em “Save”.

Feche o navegador, e execute o programa Winscp, (caso queria mudar o idioma do Winscp feche o programa, baixe o arquivo de tradução compactado no endereço http://winscp.net/translations/dll/pt.zip, descompacte este arquivo no diretório c:\arquivos de programas\Winscp, depois execute o programa Winscp clique a opção “Languages” e escolha o idioma “Portugueses – Português (Brasil)”).

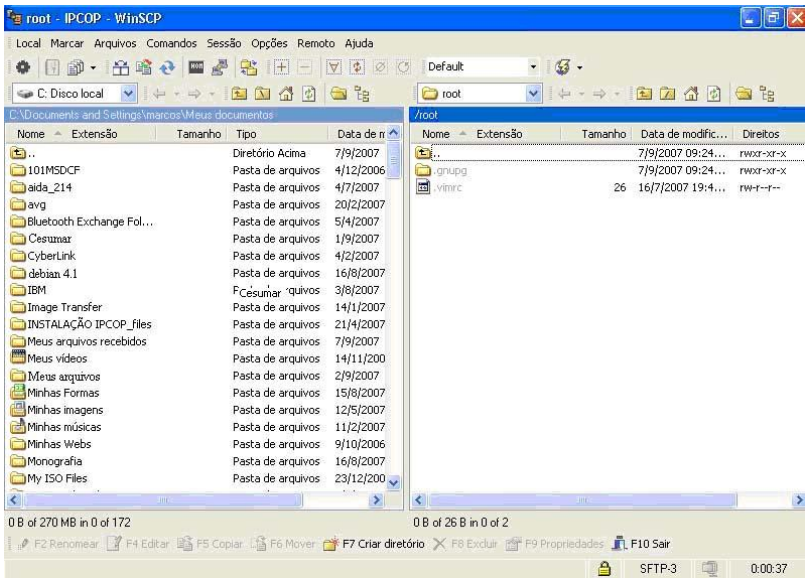
Execute novamente o Winscp, agora habilitado o idioma Português clique na opção Nome do Host, digite o IP da interface Green, em Número de porta digite a porta 222, em Usuário digite “root” e na opção senha digite a senha do usuário root, clique em “Login”, conforme mostra a figura 27.

Figura 27 WinSCP Login

Se quiser salvar esta configuração para não ter que ficar digitando as informações toda vez que executar o Winscp basta clicar em Salvar, é perguntado se realmente deseja salvar, clique OK, depois deve-se escolher com que nome deseja salvar a configuração.

Se não for informado nenhum nome será salvo como root@192.168.0.5, logo após clique em “Login”, surgira a pergunta se deseja realmente prosseguir, clique OK, e será aberta a sessão WinSCP, conforme mostra a figura 28.

Figura 28 Sessão WinSCP



A sessão Winscp apresenta a esquerda o diretório C:\Documents and Settings\marcos\Meus documentos que é computador com Windows XP professional, e a direita o diretório /root que é computador com o IPCOP.

Agora é necessário posicionar o winscp para o diretório onde foi feito o download do arquivo “addons-2.3-CLI-b2.tar.tar”. Para fazer isso dê dois cliques com o mouse na tarja azul no lado esquerdo e será aberta uma janela, clique na opção procurar, procure pelo diretório onde foi salvo o arquivo, selecione o diretório e clique “OK” e “OK” , o Winscp ficará posicionado no diretório c:\ipcop.

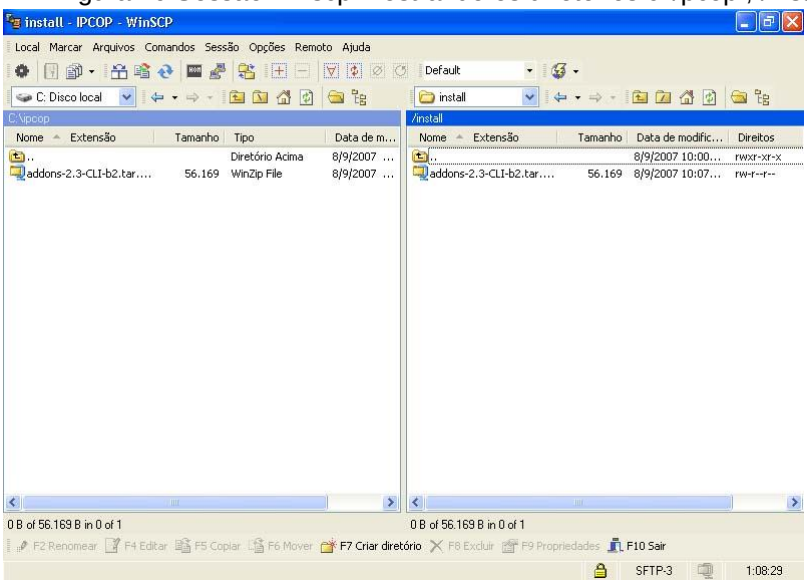
Agora posicione o mouse no lado direito e clique duas vezes na tarja azul, será apresentada uma janela, mude de /root para / clique “OK”, o programa se posicionará na raiz do IPCOP.

Cria-se um diretório “INSTALL” na raiz do ICOP para enviar os addons que serão instalados. Para criar o diretório, posicione o mouse no espaço em branco da

raiz do IPCOP, clique na tecla direita do mouse e posicione o mouse em “NEW” depois em “DIRECTORY” e digite “INSTALL” e clique “OK”.

Depois de criado o diretório clica-se nele com mouse para entrar no diretório, o winscp mostrará no lado esquerdo o diretório C:\IPCOP e no lado direito /install, conforme figura 29. Veja que o diretório c:\IPCOP esta com o arquivo “addons-2.3-CLI-b2.tar.tar” que foi baixado, move-se este arquivo para /install. Para mover clique com a tecla esquerda do mouse no arquivo fique segurando, e arraste o arquivo para o lado direito e depois solte o botão, será perguntado se deseja copiar o arquivo para o diretório /install clique “OK” para que seja copiado.

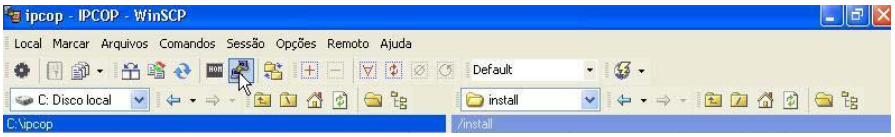
Figura 29 Sessão winscp mostrando os diretórios c:\ipcop , /install



Depois que o arquivo foi copiado para /install deve-se descompactá-lo para que possa ser instalado, para fazer a descompactação, clique com o botão direito do mouse no arquivo vá até a opção “Comandos personalizados” selecione a opção “UnTar/GZip” e clique nela, será perguntado se realmente deseja descompactar o arquivo, clique “OK”, e qual o caminho que o arquivo será descompactado. Deixe como está e clique “OK” pois ele será descompactado dentro do diretório /install mesmo.

Note que foi criado um diretório “addons” com os arquivos descompactados dentro, para instalar o addon Server, no menu do winscp a uma opção chamada “Abrir sessão no PuTTy” clica-se na opção e winscp abrirá o software PuTTY, conforme figura 30.

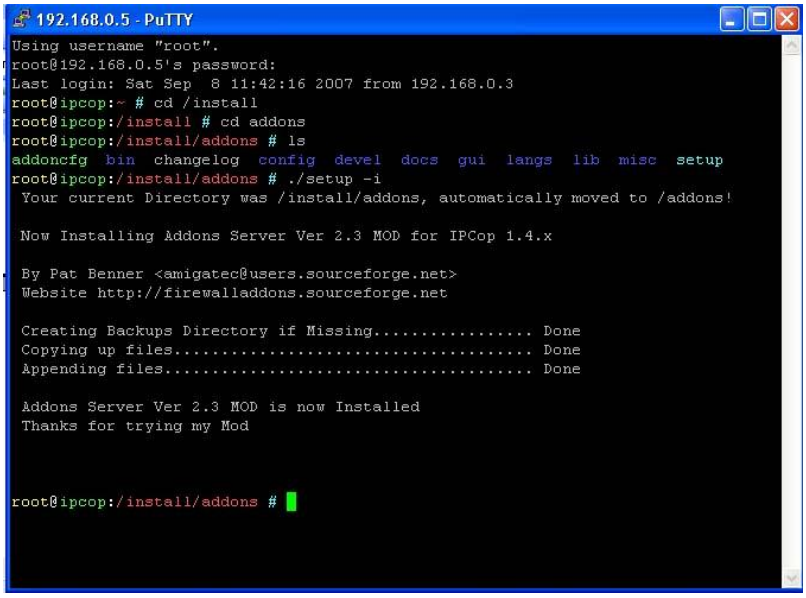
Figura 30 Abrir sessão no PuTTy



Este software emula um terminal de acesso remoto, será apresentado um sinal de alerta, se deseja mesmo criar a sessão remota, clique “SIM” e será apresentada a tela do terminal onde é solicitada a senha do usuário “root” digita-se a senha e o terminal será habilitado.

Dentro do terminal digita-se cd /install para ir até o diretório onde está o subdiretório addons que contém os arquivos de instalação do addon Server, digita-se cd /addons para entrar no diretório, e o comando ls para listar os arquivos de instalação. Para instalar o addon Server digita-se o comando ./setup –i e será instalado o programa, conforme a figura 31.

Figura 31 Instalação addon server



Depois que é instalado, o addon Server é acrescentado à página principal do ipcop, menu “ADDONS” este menu contém as seguintes opções:

1. ADDONS –NEWS;
2. ADDONS;
3. ADDONS-UPDATE;

4. ADDONS-INFO.

A opção ADDONS-NEWS traz informações sobre addons novos, ou que foram modificados, é só clicar na opção “Refresh addons news” que são mostradas as informações.

A opção ADDONS informa quais addons estão disponíveis para o ipcop, para ver esses addons é só clicar em “Refresh addons list” e será mostrada uma lista com vários addons. Para saber informações sobre um addon, clica-se na opção “informação” que possui um link pro site do desenvolvedor, ou para um site que possui o arquivo para download.

A opção ADDONS-UPDATE mostra quais addons precisam de atualizações.

A opção ADDONS-INFO mostra informações detalhadas de um addon.

Na opção ADDONS quando se clica em “Refresh addons list” aparecem vários addons, caso queira instalar um ou mais addons tem que ter muito cuidado, pois há addons nesta lista que não funciona na versão 1.4.16, e pior ainda que não funcionar ele pode estragar a instalação toda do IPCOP, um exemplo é o addon Copplus2.1-b1.

Neste trabalho serão apresentados 3 addons importantes para segurança e monitoramento de usuários, que são:

1. BlockOutTraffic;
2. Ipcop-advproxy;
3. Ipcop-urlfilter.

O objetivo do BlockOutTraffic é criar uma política DROP ou REJECT para todo tráfego que passar pelo IPCOP. Todo tráfego que era permitido pela instalação default do IPCOP é bloqueado pelo BlockOutTraffic.

É necessário então, criar regras para permitir trânsito de pacotes. Estas regras são criadas usando a interface Web do IPCOP, que estará disponível depois da instalação do addon.

Acessando o endereço http://blockouttraffic.de/files/BlockOutTraffic-2.3.2-GUI-b3.tar.gz pode-se fazer o download dos arquivos para instalar o BlockOuTraffic, salve o arquivo em c:\ipcop, use o programa winscp para copiar o arquivo para o diretório /install do ipcop.

Antes de descompactar o arquivo crie um diretório com o nome Block e copie o arquivo BlockOutTraffic-2.3.2-GUI-b3.tar.gz para este diretório, pois os arquivos de instalação foram compactados sem um diretório, e na descompactação esses arquivos serão adicionados no diretório /install, esse procedimento é somente para que os arquivos compactados não fiquem juntos com arquivos de instalação.

Descompacte o arquivo com o programa winscp, execute o PuTTY e digite o comando cd /install/Block, lembrando que tem que digitar os nomes dos diretórios igualmente como foi criado, se foi criado o diretório Block com letra maiúscula tem que se digitar o início com letra maiúscula, pois o IPCOP é Linux e ele difere maiúsculas de minúsculas.

Estando no diretório digite o seguinte comando para instalar o addon BlockOutTraffic, ./setup –i, após ter digitado o comando será instalado o addon.

Agora serão instalados os addons ipcop-advproxy, ipcop-urlfilter. Estes addons tem que ser instalados juntos, pois funcionam em conjunto, são eles que fazem os bloqueios de sites, palavras, e também monitora os usuários da rede interna quando navegam na Internet.

Para fazer o download do ipcop-advproxy, ipcop-urlfilter acesse o site http://www.advproxy.net/ clique em “Download Advanced Proxy”, procure pela opção “Download Advanced Proxy for IPCop 1.4.4 - 1.4.16” e clique em “I agree with these terms”, salve o arquivo no diretório c:/ipcop.

Para fazer o download do ipcop-urlfilter procure a opção “URL filter add-on” clique nela, procure a opção “Download URL filter” e clique nela, procura agora a opção “Download URL filter for IPCop 1.4.8 - 1.4.15” e clique na opção “I agree with these terms” para fazer o download.

Terminado o download dos dois addons copie-os com o winscp para o diretório /install, descompacte-os usando o winscp. Serão criado dois diretórios, um chamado ipcop-advproxy, e outro ipcop-urlfilter. Usando o PuTTY acesse o diretório ipcop-advproxy com o comando cd /install/ipcop-advproxy, e instale o addon com o comando ./install.

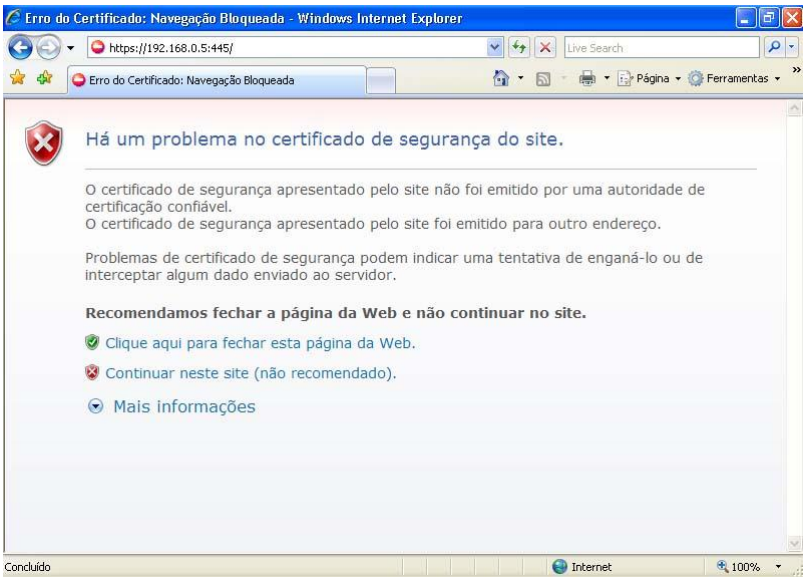
Após ter instalado o ipcop-advproxy, digite o comando cd /install/ipcop-urlfilter para entrar no diretório de instalação do addon ipcop-urlfilter e digite o comando ./install.

Depois de instalados os addons, a interface web do ipcop é alterada da seguinte forma, no menu “SERVIÇOS”, a opção “proxy” é alterada para “PROXY

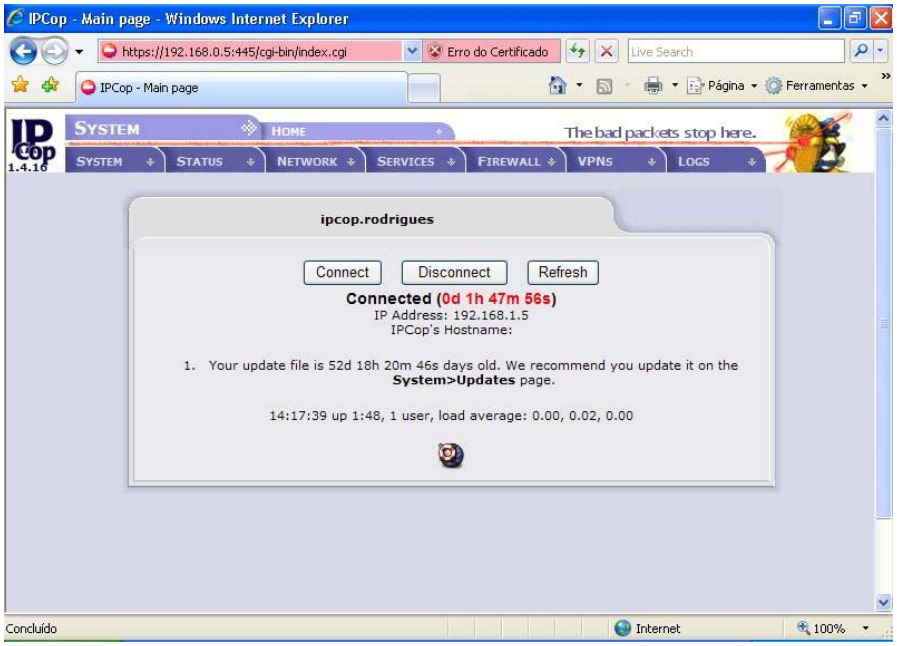
AVANÇADO”, e é acrescentado o item “URL FILTER”, no menu “FIREWALL” é acrescentado as opções “BLOCK OUTGOING TRAFFIC” e “ADVANCED BOT CONFIG”, também foram acrescentados três opções no menu “LOGS”, sendo elas “LOGS DO PROXY” e “LOGS DE FILTROS URL”.

Para acessar a página de configurações do IPCOP, inicializa-se o navegador IE e digita-se “https:// o IP da interface Green seguido de :445”, (https://192.168.0.5:445), será apresentado a seguinte mensagem “Erro do Certificado:Navegação Bloqueada”, clica-se em “Continuar neste site (não recomendado)”, para ter acesso a página do IPCOP, conforme a figura 32.

Figura 32 Acesso a página de configurações do IPCOP

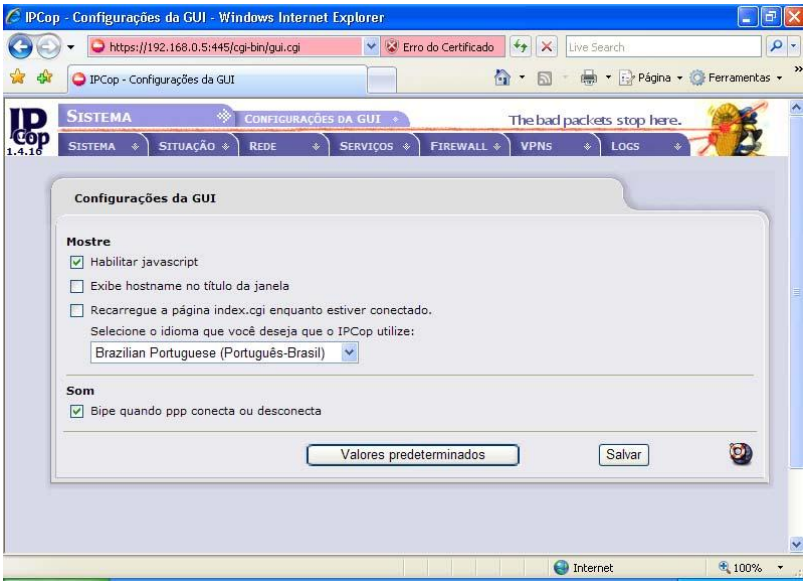


Após aparecer a página principal do IPCOP clica-se em “Connect”, conforme a figura 33. Será solicitada a senha de usuário administrador do IPCOP, este usuário tem poderes para fazer a administração do IPCOP. Digita-se admin e a senha que foi digitada na instalação.



Para mudar o idioma do IPCOP para Português (Brasileiro), vá com o mouse até o menu System na opção GUI SETTINGS, e procure pela opção “Brazilian Portuguese (Português-Brasil)”, clique em “Save” para mudar o idioma.

Figura 34 Brazilian Portuguese (Português-Brasil)



8.1 PÁGINA PRINCIPAL

É através da página principal que se tem acesso aos menus de configurações e logs do sistema. Esses menus sãos:

- SISTEMA;
- SITUAÇÃO;
- REDE;
- SERVIÇOS;
- FIREWALL;
- VPNS;
- LOGS.

O menu Rede não será abordado neste trabalho porque ele é configurado somente quando se usa conexão discada, o que não é o caso deste manual. E o menu Vpns serve para fazer tunelamento na Internet entre duas redes, ou um host e uma rede, não sendo este o objetivo deste manual.

8.2 MENU SISTEMA

O menu Sistema contém as seguintes opções, conforme mostra a figura 35:

1. Principal;
2. Atualizações;
3. Senhas;
4. Acesso SSH;
5. Configurações da GUI;
6. Cópia de Segurança;
7. Desligar;
8. Créditos.

A opção 1 é somente a página inicial da interface web do IPCOP FIREWALL.

A opção 2 é onde se faz atualizações para uma nova versão do sistema, caso seja disponibilizado uma atualização esta opção informa que é preciso fazer a atualização. Além de informar que é preciso fazer a atualização é apresentado o link para fazer o download das atualizações, também a opção de limpeza de cache do Proxy (squid).

A opção 3 é usada para alterar a senha do administrador e do usuário de conexão de discagem.

A opção 4 é usada para habilitar o servidor de conexão SSH.

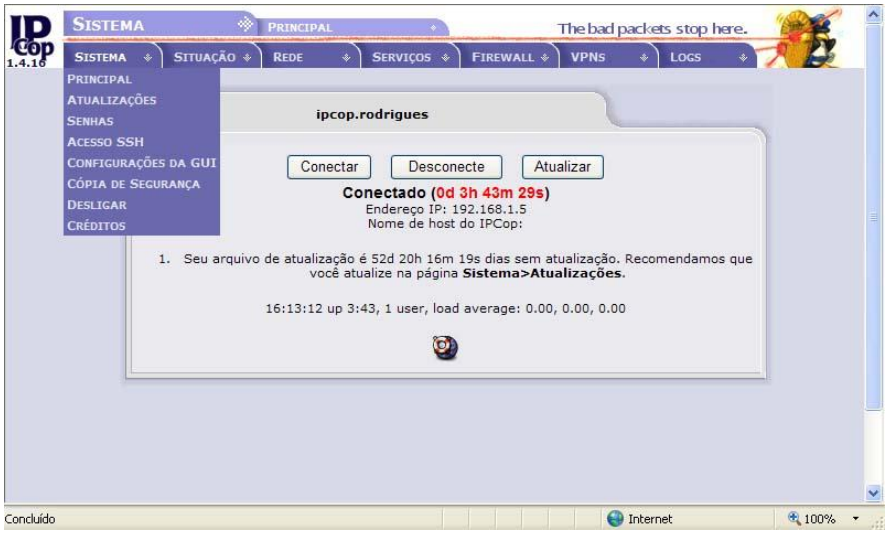
A opção 5 é usada para alterar o idioma da interface Web do sistema.

A opção 6 é usada para fazer backup, havendo a possibilidade de fazer backup do sistema em disquetes, HD, mídias removíveis.

A opção 7 serve para reinicializar, desligar ou programar o sistema para desligar ou reinicializar com hora e dia automaticamente.

A opção 8 é apresentação das pessoas que fazem parte do grupo que mantem o ipcop ativo.

Figura 35 Menu Sistema



8.3 MENU SITUAÇÃO

No menu Situação estão as opções mostradas na figura 36;

1. Situação do Sistema;
2. Situação da Rede;
3. Gráfico do Sistema;
4. Gráfico de Trafego;
5. Conexões.

A opção 1 apresenta os serviços que o sistema possui, e quais estão sendo executados e quais estão parados, exibe também o uso da memória, uso do disco,

os Inodes usage. Quais usuários estão logados no sistema e o tempo que eles estão logados, mostra os módulos carregados e qual a versão do kernel do Linux é usado pelo sistema.

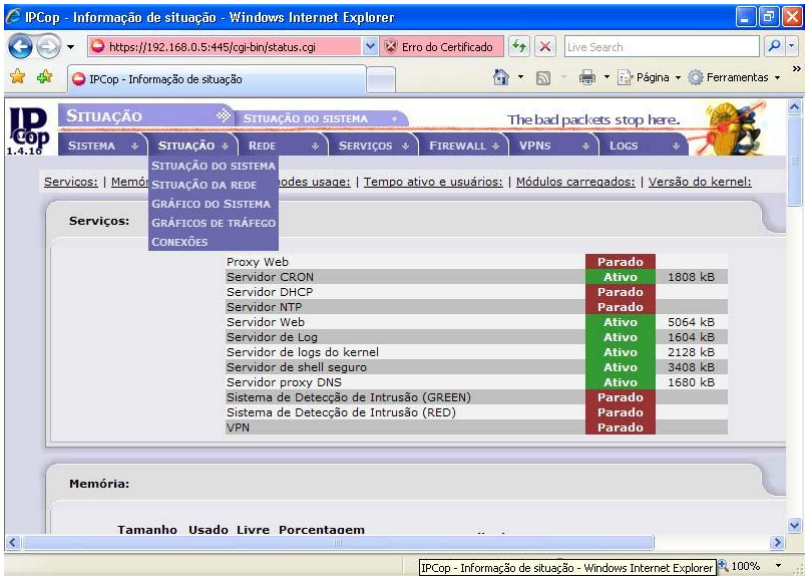
A opção 2 apresenta as interfaces do sistema detalhadamente tais como endereço IP, endereço MAC, a tabela de roteamento, a tabela de entrada ARP.

A opção 3 mostra estatísticas de uso da CPU, da memória RAM, SWAP, e do HD, em modo gráfico se clicar em uma dessas opções pode-se ter estatística individual mostrando dia, mês e ano.

A opção 4 mostra o tráfego das interfaces Green e Red, clicando numa dessas opções são mostrados gráficos por dia, mês e ano.

A opção 5 rastreia as conexões entre o sistema e a rede interna.

Figura 36 Menu situação



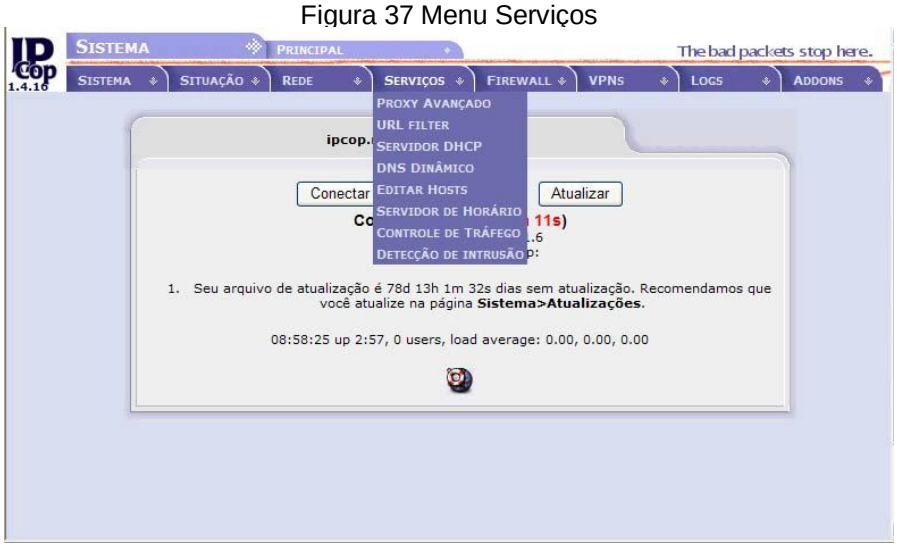
8.4 MENU SERVIÇOS

Este menu contém as opções mostradas na figura 37:

- Proxy Avançado;
- Url filter;
- Servidor DHCP;
- DNS dinâmico;
- Editar hosts;

- Servidor de horário;
- Controle de tráfego;
- Detecção de intrusão.

Figura 37 Menu Serviços



8.4.1 Proxy Avançado

A opção Proxy Avançado é um servidor Proxy que atua sobre as requisições dos usuários na rede interna, ele funciona da seguinte forma: quando um usuário da rede interna vai navegar na Internet ele abre o navegador e digita o endereço que quer acessar, na verdade o usuário está acessando o servidor Proxy.

A solicitação do usuário vai até o servidor, é o servidor quem realmente navega, ele vai ao endereço solicitado, armazena no cache e depois repassa as informações para o usuário. Este endereço fica armazenado por um tempo no cache do Proxy, se algum outro usuário solicitar este endereço ele repassa automaticamente sem a necessidade de entrar de novo na Internet.

Por isso um servidor Proxy é muito importante, pois diminui bastante o tráfego entre a Internet e a rede interna.

O Proxy avançado é instalado através do addon ipcop-advproxy, ele sobrepõem o proxy da instalação original para que o firewall seja mais seguro e eficiente. Para configurar dividiremos em partes para melhor entendimento.

1. Configurações comuns.

2. Proxy principal.
3. Configurações de logs.
4. Gerenciamento de cache.
5. Portas de destino.
6. Controle de acesso base na rede.
7. Restrições de tempo.
8. Limites de transferência.
9. Limitação para download.
10. Filtro mime.
11. Web browser.
12. Privacidade.
13. Filtro url.
14. Método de autenticação.

A. Configurações comuns

Na opção 1 Configurações Comuns habilita-se as seguintes opções:

Habilitação ligada Green, esta opção diz ao Proxy que a rede Green pode trafegar pelo Proxy. Na opção Porta Proxy por default vem habilitada a porta 800, geralmente o Proxy trabalha nas 3128 ou 8080, mas se quiser colocar outro número de porta há esta possibilidade, mas lembre-se “NUNCA USE UMA PORTA PARA O PROXY QUE ESTEJA SENDA USADO POR OUTRO SERVIÇO”, pois certamente haverá conflito de portas.

Marque a opção “Transparência ligada”, caso esta opção não seja habilitada cada computador que estiver conectado à rede, terá que ser configurado o navegador manualmente. Em “Hostname visível” é para informar o nome do servidor Proxy.

Na opção “E-mail do administrador do cache” informa-se o e-mail da pessoa que administra o servidor Proxy, nas opções “Linguagem de mensagens de erro” e “Design de mensagens de erro” deixe padrão, porque elas só funcionam no idioma inglês. Há bilite “Suprimir informações da versão”, pois habilitando esta opção não é apresentada à versão do servidor Proxy esta sendo usada, conforme a figura 38.

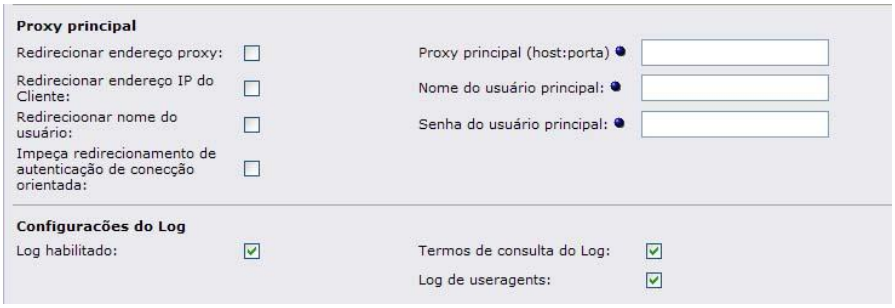
Figura 38 Configurações comuns

B. Proxy principal, configurações do log

A opção Proxy principal não é configurada, pois ela só é configurada quando se tem um servidor Proxy principal.

Habilite a opção ‘Configurações do “Log” para que o sistema gere informações sobre a navegação pela Internet. A figura 39 mostra as opções Proxy principal e configurações do log.

Figura 39 Proxy principal, configurações do log



C. Gerenciamento de Cachê

As opções disponíveis em gerenciamento de cachê são mostradas na figura 40.

- Tamanho da memória cache em (NB): É a quantia de memória RAM que é usado para fazer cache de objetos. Este valor não deve exceder mais de 50% de RAM instalada. O mínimo para este valor é 1MB, o default é 2 MB.
  Este parâmetro não especifica o tamanho do processo de máximo. Só coloca um limite de memória RAM ADICIONAL que o Servidor Proxy usará para fazer cache de objetos.

- Tamanho do cache em (MB): É a quantia de espaço do disco (MB) que será usado para fazer cache. O default é 50 MB. Mude esta opção para um cache maior, mas nunca coloque o tamanho total da unidade de disco, o uso máximo do disco é 20%.

- Tamanho mínimo do objeto em (KB): É o tamanho mínimo de objetos que serão salvos em cache. O valor é especificado em kilobytes, o tamanho mínimo padrão é 0 KB, que significa não existir tamanho mínimo.

- Tamanho máximo do objeto em (KB): É o tamanho máximo de objetos que serão salvos em cache. O valor é especificado em kilobytes, o tamanho máximo padrão é 4096 KB.

- Número de subdiretórios de nível-1: O valor padrão para o Número de subdiretórios de nível-1 é 16.
  Cada nível-1 contém 256 subdiretórios, então um valor de 256 níveis-1 usa um total 65536 subdiretórios para cache, o valor recomendado é 16. Só se deve aumentar este valor somente quando for necessário.

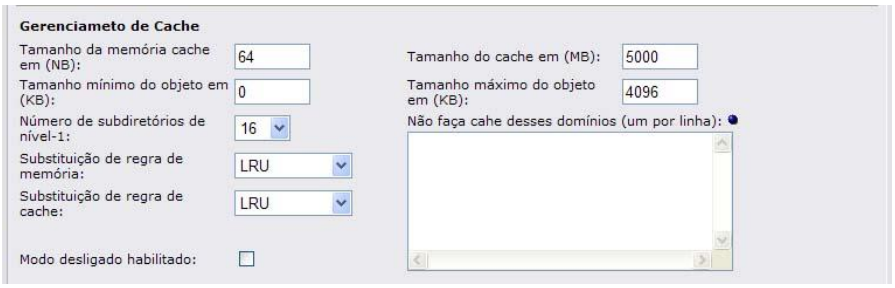
- Não faça cache desses domínios (um por linha): Esta opção é para não fazer cache de determinados domínios.
- Substituição de regra de memória: O parâmetro de política de substituição de regra de memória determina quais objetos serão

substituídos da memória, para criar espaço para novos objetos, a política padrão é LRU.

- Substituição de regra de cache: O parâmetro de política de substituição de cache decide que objetos permanecerão em cache e quais objetos serão substituídos, para criar espaço para novos objetos. A política default para substituição de cache é LRU.

- Modo desligado habilitado: Esta opção é desligar o gerenciamento de cache.

Figura 40 Gerenciamento de Cache



D. Portas de destino

Esta opção enumera as portas de destino permitido para os padrões HTTP e SSL e codificaram pedidos HTTPS, as portas podem ser definidas como um número de porta única ou varias portas. A figura 41 mostra um exemplo de portas de destino.

Figura 41 Portas de destino

E. Controle de acesso baseado na rede

Esta opção serve para controlar o acesso dos usuários da rede interna, ao Servidor Proxy. A figura 42 mostra as opções a serem configuradas.

- Subnets permitidas (uma por linha): Nesta opção são definidas quais redes têm permissão para acessar o Servidor Proxy, a rede GREEN e AZUL (se disponível) devem ser incluídas aqui.

- Desabilite o acesso por Proxy interno a Green de outras subredes: Esta opção é para desabilitar o Proxy para acessar outras subredes internas.

- Endereços IP sem restrição (um por linha) / Endereços MAC sem restrição (um por linha): Estas opções são para o caso de um computador ter acesso irrestrito ao servidor Proxy, insere-se o IP e endereço MAC da placa de rede do computador.

(OBS: Estas funções também funcionam independentes, mas o correto é inserir o IP e MAC para o caso de alguém tentar burlar o servidor Proxy.)

- Endereços IP banidos (um por linha) / Endereços MAC banidos (um por linha): Estas opções são para o caso de um computador não ter

acesso ao servidor Proxy, insere-se o IP e o endereço MAC da placa de rede do computador.

(OBS: Estas funções também funcionam independentes, mas o correto é inserir o IP e MAC para o caso de alguém tentar burlar o servidor Proxy.)

Figura 42 Controle de acesso baseado na rede

F. Restrição de tempo, Limites de transferência, Limitação para Download

As opções disponíveis em Restrição de tempo, limite de transferência e limitação para download são mostradas na figura 43.

- Restrição de tempo

  A opção é configurada quando se quer restringir o acesso a Internet em um determinado período, o padrão é permitir acesso em qualquer dia e horário. Para negar acesso num determinado dia e horário, selecionam-se os dias e o horário e mude a opção “Acesso” para negar, depois clique em “Salvar e reiniciar”.

- Limites de transferências

  Esta opção é configurada quando se quer restringir o tamanho máximo de arquivos download e upload da Internet, sendo que o padrão é 0 para ambos. Se for definido o tamanho máximo do arquivo em 1MB, arquivos maiores não serão baixados ou enviados.

- Limitação para Download

  Esta opção é configurada quando se quer restringir a velocidade de downloads de arquivos, podendo restringir a velocidade de 64 kBit/s até 5120 KBit/s.

Figura 43 Restrição de tempo, Limites de transferência, Limitação para Download

G. Filtro tipo MIME, Web browser

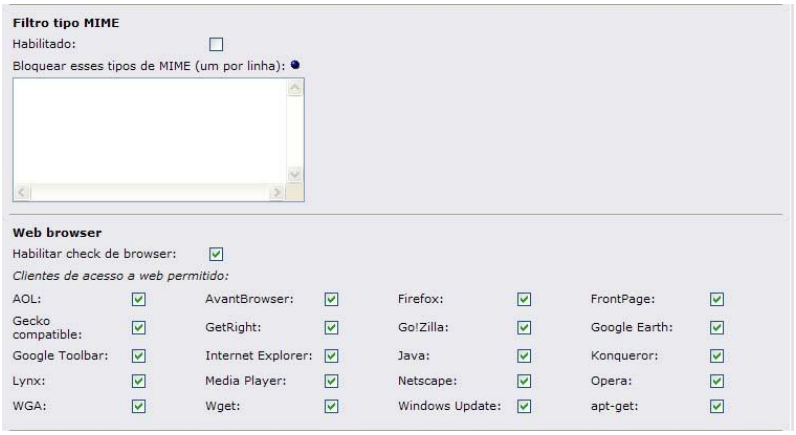
A opção Filtro tipo mime é usada para bloquear MIMES, para habilitar esta opção clique em “Habilitado”, depois no campo “Bloquear esses tipos de MIME (um por linha):” digita-se os tipos de mimes que se quer bloquear, conforme mostra a figura 44.

Exemplo: Caso queira bloquear acesso a arquivos com extensão PDF, digite no campo “Bloquear esses tipos de MIME (um por linha):”.pdf”

Web browser

A opção Web browser permite que seja controlado o tipo de navegador que terá acesso a sites da Web, para habilitar marque a opção “Habilitar check de browser:”, e marque os tipos de navegadores que poderão acessar a Web.

Figura 44 Filtro tipo MIME, Web browser



H. Privacidade, Filtro URL, Método de autenticação

Esta opção Privacidade é habilitada quando se quer ter privacidade durante a navegação na Internet, conforme mostrado na figura 45.

No campo “Falso Useragent para sites externos:” é informada uma string, e toda vez que um usuário da rede interna for navegar na Internet o servidor Proxy, muda o cabeçalho de navegação que é submetido para sites externos.

Exemplo: Ensira a string “Mozilla/5.0 (Windows; U; Windows NT 5.1; En-os EUA; Rv:1.7.3) Gecko/20041002 Firefox/0.10”, esta string fará com que servidores Web externos acreditam que todos os usuários da rede interna estejam usando o Firefox Browser:

Na opção “Feferenciador falso submetido a sites externos:”, quando se clica em um hyperlink, a URL de origem é enviada para o site da web de destino. Inserindo, por exemplo a string “Http://xxxxxxxxxxxxxxxxxxxxxxxxxxxx“, a URL de origem é trocada por uma falsa, ficando o usuário da rede interna, anonimamente.

A opção “filtro URL”, só funciona se o addon ipcop-urlfilter estiver instalado, ela é habilitada para que o Servidor Proxy possa fazer filtros de URLS, domínios, expressões.

O método de autenticação, não é configurado para Servidores Proxy transparentes.

Figura 45 Privacidade, Filtro URL, Método de autenticação

8.4.2 URL Filter

O URL Filter é um dos addons mais importantes do IPCOP, é ele quem faz bloqueios de acesso a domínios, urls, palavras, arquivos indesejáveis. É possível bloquear toda navegação à Internet, ou liberar a navegação somente a sites autorizados pela empresa. Ele só funciona se o addon Proxy avançado estiver instalado. Serão mostradas a seguir as opções de configurações desse addon.

A. Bloquear categorias e Blacklist personalizada

A opção “Bloquear categorias” é um banco de dados que contém varias categorias de blacklist (lista negra), que representam ameaças à segurança da navegação na Internet, para habilitar marque todas as opções. A figura 46 mostra todas as opções.

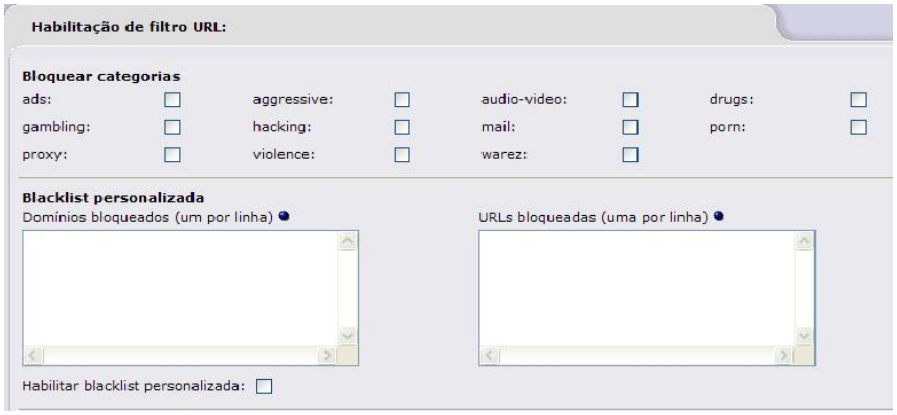
A opção “Blacklist personalizada” bloqueia domínios e urls indesejáveis, para habilitá-la marque a opção “Habilitar blacklist personalizada”.

Exemplo: Caso se queria bloquear o domínio cesumar.br adiciona-se o domíno na opção “Domínios bloqueados” (é permitido um domínio por linha).

Caso queira bloquear somente uma URL de um domínio em vez do domínio todo, adiciona-se a URL que será bloqueada na opção, “URLs bloqueadas”.

Exemplo: Caso se queira bloquear a URL cesumar.br/moodle adiciona-se a URL na opção “URLs bloqueadas”, (é permitido uma URL por linha), com isso os usuários poderão acessar o domíno cesumar.br, mas não poderão acessar a URL cesumar.br/moodle.

Figura 46 Bloquear categorias, Blacklist personalizada



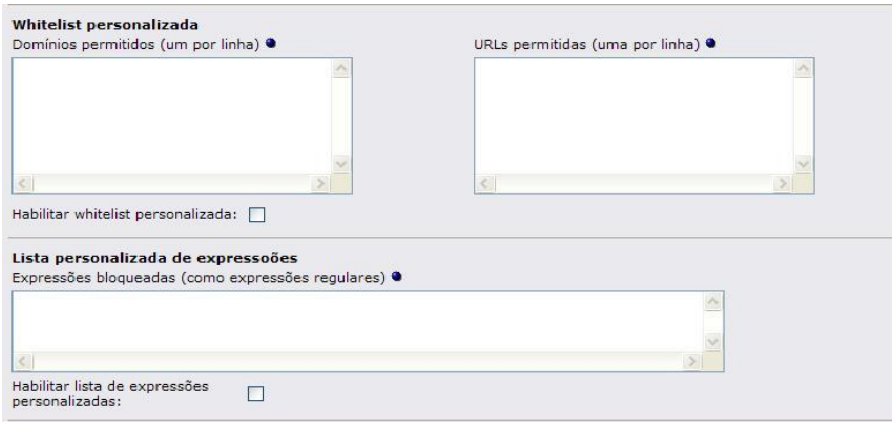
B. Whitelist personalizada e Lista personalizada de expressões

A opção Whitelist é habilitada quando se deseja especificar domínios e URLs para os usuários da rede interna acessarem. Para habilitar marque a opção “Habilitar whitelist personalizada”, conforme mostra a figura 47.

A opção “Lista personalizada de expressões” é habilitada quando se deseja bloquear acesso por expressões ou palavras. Para habilitar marque a opção “Habilitar lista de expressões personalizadas”.

Exemplo: Caso queira bloquear as palavras sexo e nudez, adicione estas palavras no campo “Expressões bloqueadas”, se algum usuário tentar acessar um endereço da Internet que contenha uma dessas palavras, a navegação dele será bloqueada.

Figura 47 Whitelist personalizada, Lista personalizada de expressões



C. Bloqueamento por extenção de arquivo, Redirecionar arquivo local e Controle de tempo de acesso

A opção “Bloqueamento por extenção” é habilitada quando se quer bloquear download de arquivos executáveis, compactados, vídeo ou áudio.

A opção “Redirecionamento arquivo local” ativa o redirecionamento de pedidos de download de arquivo para o repositório local. Com isso aumenta a velocidade e a largura de banda da rede.

A opção “Controle de acesso à rede” tem duas opções, a opção “Endereços IP não filtrados (um por linha)” é para dar privilégio a um usuário para navegar na Internet sem restrições, ou seja, todas as regras contidas no URL Filter não serão aplicadas para este usuário.

Já na opção “Endereços IP descartados (um por linha)” é para bloquear o acesso de um usuário a Internet, ou seja, o URL Filter ignorará todas as regras e bloqueia de imediato o usuário.

As opções “Controle de tempo de Acesso e Definir cota do usuário” são para definir dias, horas, minutos de acesso a Internet para usuários individualmente. Todas opções descritas neste item são mostradas na figura 48.

Figura 48 Bloqueamento por extenção de arquivo, Redirecionar arquivo local e Controle de

D. Configuração de páginas bloqueadas

Nesta opção é onde são configuradas as mensagens que irão aparecer para os usuários que tenham restrição de acesso a Internet. A figura 49 mostra todas as opções desta tela.

Mostrar categoria de página bloqueada: deveria mostrar o nome da categoria a qual esta página foi adicionada para bloqueio. (Bug).

Mostrar URL de página bloqueada; mostra a URL da página que tentaram acessar na mensagem.

Mostrar IP de página bloqueada; mostra o IP do usuário que tentou acessar a página bloqueada na mensagem.

Use DNS Error para bloquear URLs: se habilitada mostra uma mensagem no navegador de página não encontrada.

Habilitar imagem de background: se habilitada deveria mostrar uma imagem personalizada de background para a página bloqueada. (Bug).

Linha de mensagem 1; insira aqui a 1º mensagem que será mostrada para o usuário que tentar acessar algum conteúdo proibido.

Linha de mensagem 2: insira aqui a 2º mensagem que será mostrada para o usuário que tentar acessar algum conteúdo proibido.

Linha de mensagem 3; insira aqui a 3º mensagem que será mostrada para o usuário que tentar acessar algum conteúdo proibido.

Exemplo de mensagem:

“ACESSO NEGADO"

“Acesso a página solicitada foi negada”

“Por favor, contacte o Administrador da rede caso exista Algum erro".

Figura 49 Configuração de páginas bloqueadas

E. Configurações avançadas

Estas opções ativam os seguintes serviços:

- Habilitar listas de expressões: ativa a lista de expressão personalizada.
- Habilitar SafeSearch: verificação de palavras-chave, frases, url.
- Bloquear “ads” com janelas em branco: bloqueia anúncios e banners indesejados.
- Bloquear sites acessados por esses endereços IP: bloqueia sites acessados por endereço IP. O mesmo site estará disponível se acessado pelo nome de domínio, se não estiver bloqueado por outra regra.
- Bloquear todas as URLs não explicitamente permitidas: bloqueia acesso a todos os sites, somente os site que estiverem na opção “Whitelist personalizada” poderão ser acessados.
- Habilitar Log: Ativa logs do URL Filter.
- Log nome de usuário: inclui o nome do usuário no log.
- Repartir log por categorias: divide o log por categoria de Blacklist.

- Número de processos filtrador: quantidade de processos filtrados que estão ativos, o valor default é 5.
- Allow custom whitelist for banned clients: todas as solicitações de navegação a Internet, de clientes proibidos serão bloqueadas a revelia. Os clientes proibidos somente poderão acessar sites que estiverem indicados na opção “Whitelist personalizada”. A opção “Habilitar whitelist personalizada” deve estar habilitada.
- Salvar: salva todas as configurações habilitadas no URL Filter.
- Salvar e reinicializar: salva todas as configurações habilitadas no URL Filter e reiniciar, o serviço para ativar as regras.

Todos os serviços descritos acima são mostrados na figura 50.

Figura 50 Configurações avançadas

F. Manutenção de filtro URLs

As opções de manutenção de filtro URL são mostradas na figura 51.

- Atualização de blacklist: faz atualização de uma blacklist existente no sistema.
- Atualização automática da blacklist: habilitando esta opção o sistema procura na Internet uma blacklist atualizada e baixa automaticamente a lista, depois de baixada a lista atualizada, clica-se em “Salvar configurações atualizadas”. Tem-se a opção de escolher a baixa automática diariamente, semanalmente ou mensalmente, e também

possui quatro fontes para downloads. Caso queira indicar uma fonte para download é só indicar na opção “Fonte URL customizada”.

Figura 51 Manutenção de filtro URL

G. Editor blacklist, configuração de backup de filtro URL e Restaurar filtro de configuração URL

- Editor blacklist: serve para incluir uma nova categoria de filtro, editar uma categoria existente.
- Configuração de backup de filtro Url: faz backup de toda blacklist, incluindo as opções “Blacklist personalizada, Whitelist personalizada”.
- Restaurar filtro de configuração URL: restaura o backup blacklist

Todas essas opções são mostradas na figura 52.

Figura 52 Editor blacklist, Configuração de backup de filtro URL, Restaurar filtro de configuração URL

8.4.3 DHCP

Este menu é usado para fazer manutenções no servidor DHCP, tais como, mudar a faixa de IP's que o servidor DHCP distribui aleatoriamente, atribuir IP fixo a uma determinada máquina, verificar quais máquinas estão conectadas à rede com IP's distribuidos pelo servidor DHPC.

8.4.4 DNS Dinâmico

Esta opção é somente configurada para conexões que possuem IP's dinâmicos. A Internet possui um número limitado de endereços de IP. Quando se conecta a um provedor de Internet, o provedor atribui um endereço de IP dinâmico para o computador utilizar enquanto estiver conectado. Se o computador tiver a necessidade de hospedar um servidor web, ou outro serviço qualquer, que exija que outros computadores o achem na Internet, eles precisam saber qual o seu endereço IP. Como o IP dinâmico muda constantemente fica impossível que outros computadores localizem o servidor web, ou outro serviço hospedado no computador que usa IP dinâmico.

O serviço dns dinâmico é oferecido por provedores externos, sendo que alguns desses provedores cobram pelo serviço, e outros não. O dns dinâmico é um software que atribui um hostname estático a um endereço de IP dinâmico. Assim quando o provedor de acesso muda o ip dinâmico do computador este software avisa ao provedor de dns dinâmico IP novo.

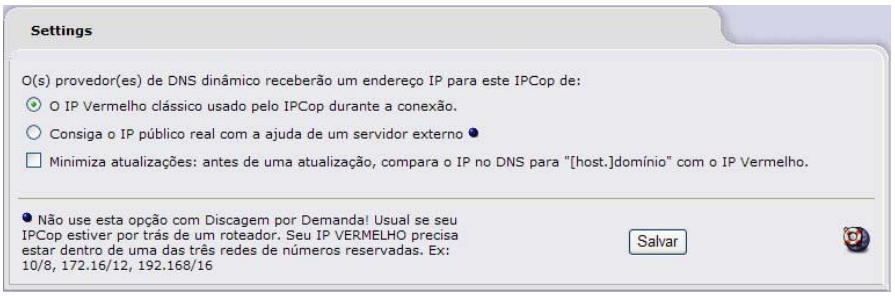
Para configurar esta opção siga os passos abaixo.

A SETTINGS

Para habilitar Dns dinâmico marque as opções "Consiga o IP público real com a ajuda de um servidor externo", "Minimiza atualizações: antes de uma atualização,

o IP no DNS para “[host.]domínio” com o IP Vermelho” depois clique em salvar. Conforme mostra a figura 53.

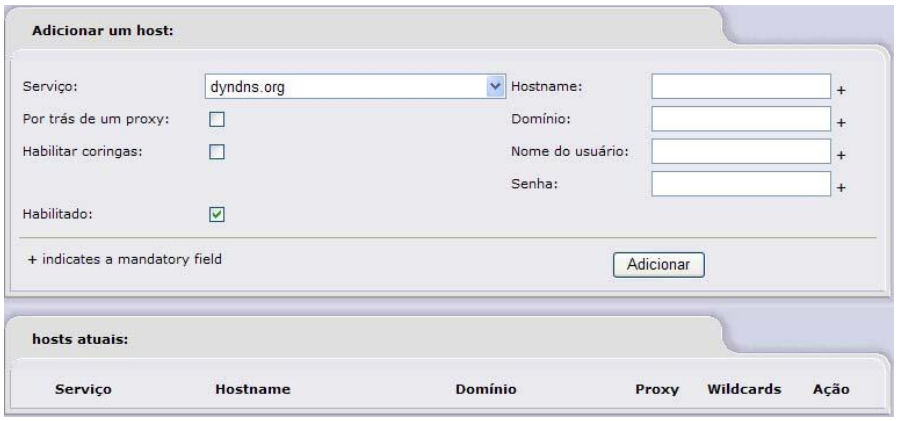
Figura 53 Settings



B ADICIONAR UM HOST

Para adicionar um host tem-se que acessar uns dos servidores externos cadastrados no IPCOP e abrir uma conta de usuário, depois preencha os campos Hostname, domínio, Nome do usuário e senha, clique em Adicionar, que são mostrado na figura 54.

Figura 54 Adicionar um host



8.4.5 Editar Hosts

Esta opção adiciona nome aos hosts da rede. Para isso, preencha os campos Endereço IP do Host, Hostname, Nome do domínio e marque a opção “Habilitado”, clique em “Adicionar”, conforme mostra a figura 55.

Figura 55 Editar hosts

8.4.6 Servidor de Horário

O servidor de horário é configurado quando se quer que os relógios dos computadores da rede interna sejam atualizados por um servidor de horas externo. Esta tarefa pode ser executada automaticamente ou manualmente.

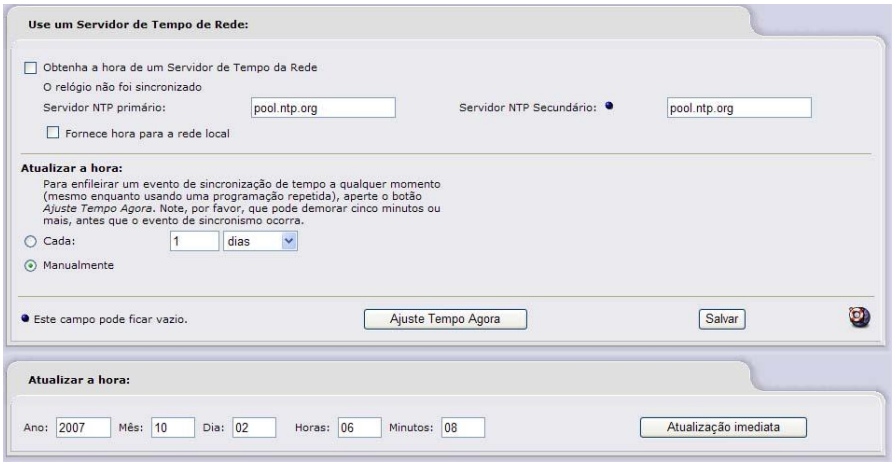
As opções de habilitação do servidor de horário são mostradas na figura 56.

Marque as seguintes opções, “Obtenha a hora de um Servidor de Tempo da Rede”, “Fornece hora para a rede local” e escolha a forma de execução Manualmente ou automática.

Para habilitar a forma de atualização manualmente marque somente a opção “Manualmente”.

Para habilitar a forma de atualização automática marque a opção “Cada”, informando que a atualização será em horas, dias, semanas ou meses.

Figura 56 Servidor de horário

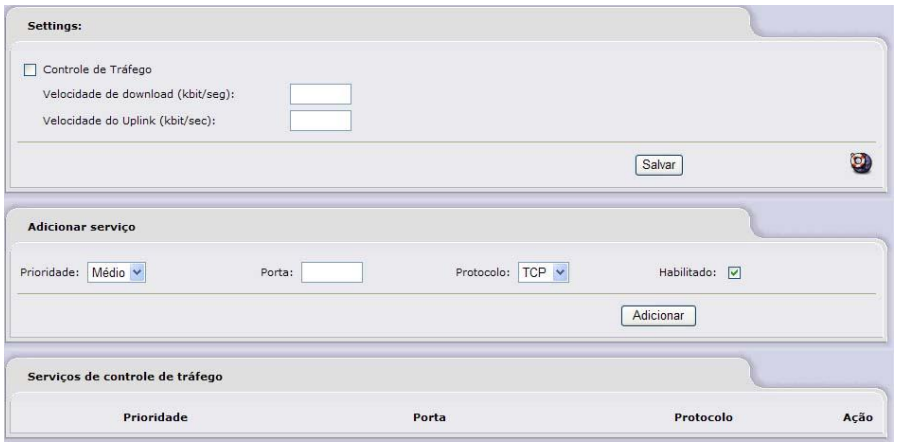


8.4.7 Controle de Tráfego

Esta opção é para controlar o tráfego entre a Internet e a rede interna, ou seja, ele prioriza tráfego de alguns serviços melhorando o desempenho da rede. O tráfego é configurado em categorias de prioridades Alta, Média e Baixa.

Para habilitar marque a opção “Controle de trafego”, informe as velocidades de download e Uplink, escolha qual será a prioridade da conexão, Alta, Média, Baixa, a porta usada pelo serviço e o tipo de protocolo usado por ela, marque a opção “habilitada”, e clique em adicionar, conforme mostrado na figura 57.

Figura 57 Controle de Tráfego

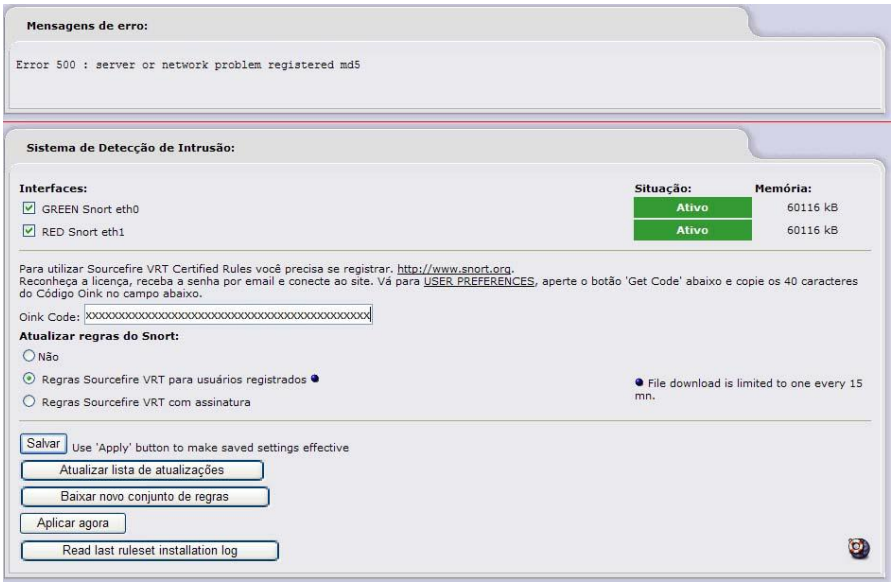


8.4.8 Detecção de Intrusâo

Um sistema de detecção de intrusão, analisa o conteúdo dos pacotes recebidos pelo Firewall e procura por códigos maliciosos conhecidos que possam prejudicar os computadores da rede interna. O IPCOP usa o Snort para fazer a detecção de intrusão.

Para habilitar esta opção, faça o cadastro no site www.snort.org depois do cadastro gere o “Oink Code”, copie e cole o código gerado no campo “Oink Code”, como mostra a figura 58. Marque as opções “GREEN Snort e RED Snort” e “Regras Sourcefire VRT para usuários registrados”, depois clicar em “Salvar”. Para manter o snort atualizado o administrador do IPCOP recebe frequentemente e-mail sobre novas regras que estão disponíveis para atualização, e também é necessário entrar na opção “Detecção de Intrusão” e fazer a atualização manual de novas regras, clicando em “Baixar novo conjunto de regras” e finalmente em “Aplicar agora”.

Figura 58 Detecção de intruso



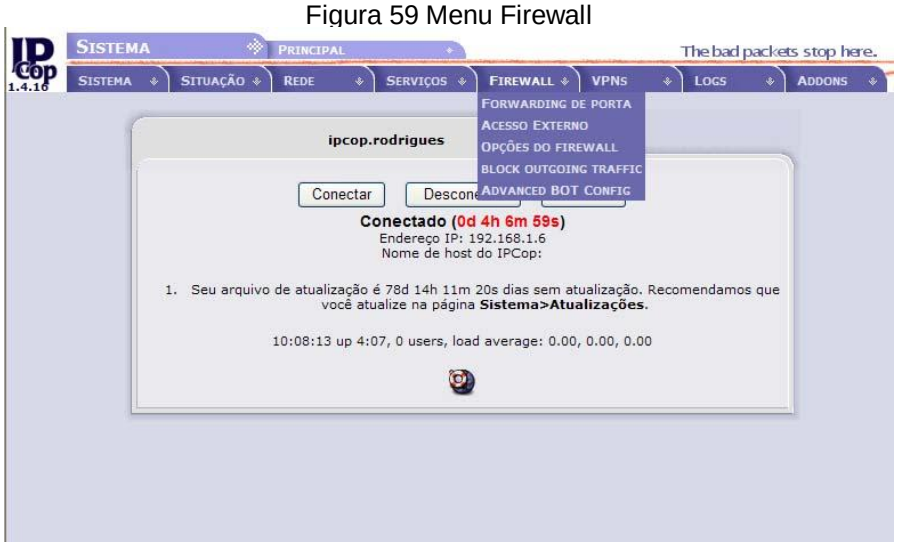
8.5 FIREWALL

O menu Firewall é importantíssimo, pois nele estão serviços essencias para a segurança do sistema e de toda a rede. Através dele pode-se adicionar regras

ipatbles, fazer bloqueios de portas, serviços e redirecionamentos de portas, permitir acesso de usuários externos à rede interna. A figura 59 apresenta as opções do menu firewall, sendo elas:

- FORWARDING DE PORTA;
- ACESSO EXTERNO;
- OPÇÕES DO FIREWALL;
- BLOCK OUTGOING TRAFFIC;
- ADVANCED BOOT CONFIG.

Figura 59 Menu Firewall



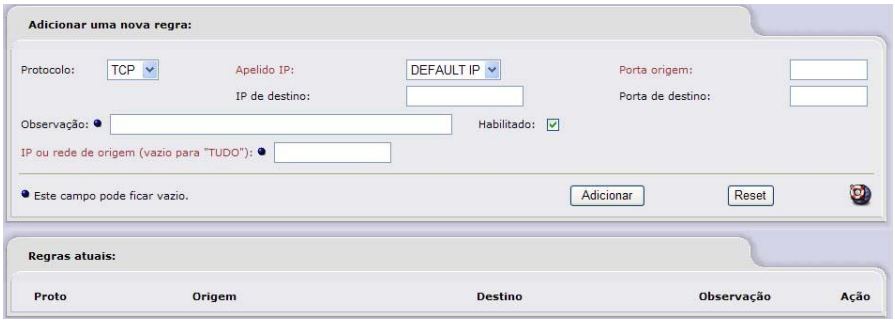
8.5.1 Forwarding de Porta

Nesta opção é onde são feitos os redirecionamentos de portas. Se há um serviço na rede interna e alguém tem que acessar este serviço através da Internet este serviço só será acessível se for feito o redirecionamento da porta para o computador que estiver instalado o serviço.

Por exemplo, tem-se um Servidor Windows 2003 na rede interna e este servidor está rodando o serviço Terminal Server, para que usuários acessem este serviço da Internet, é preciso redirecionar a porta para o IP do Servidor Windows 2003. O Terminal Server usa a porta 3389 TCP e UDP para redirecionar faz-se o seguinte: No campo “Porta de Origem” digite o numero da porta 3389, no campo “IP

de destino” informa-se o endereço IP do Servidor Windows 2003. Em “Porta de destino” informe a porta 3389, em “Observação” digite o nome do serviço que esta sendo feito o redirecionamento “Terminal Server”, marque a opção “Habilitado”, depois é só clicar em “Adicionar”, repita o procedimento só mudando a opção “Protocolo” para UDP. A figura 60 mostra todas essas opções.

Figura 60 Forwarding de porta

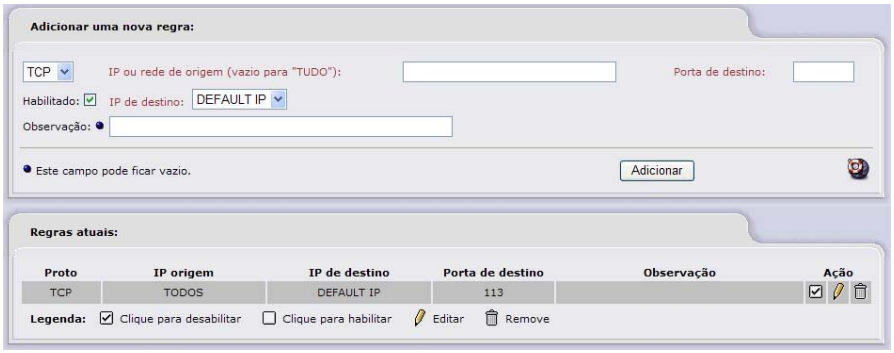


8.5.2 Acesso Externo

Esta opção libera a entrada de um serviço da Internet para a rede interna, no capítulo 8.5.1 foi configurado o redirecionamento de portas do serviço de Terminal Server, não adianta nada configurar o redirecionamento de porta se esta opção não for configurada.

Para liberar o acesso externo digite na opção “Porta de destino” o número da porta que está sendo liberada, no caso a porta 3389, marque a opção “Habilitado”, no campo “Observação” digite o nome do serviço “Terminal Server” e clique em adicionar, repita o procedimento mudando somente a opção “TCP”, para UDP, conforme mostra a figura 61.

Figura 61 Acesso externo



8.5.3 Opções do Firewall

Esta opção bloqueia a entrada do comando ping da Internet para interface Red (IPCOP), e da interface Green (rede interna) para a interface Red (IPCOP). Para habilitar esta opção marque a opção desejada, e depois clique em “Salvar”, como mostra a figura 62.

Figura 62 Opções do Firewall

8.5.4 Block Outgoing Traffic

Esta opção controla o tráfego entre as interfaces GREEN e RED (origem, destino, serviços, etc) ela controla quais serviços da Internet podem ser utilizados pelos computadores da rede interna. As regras são criadas usando uma interface

WEB bastante intuitiva e, é claro, disponível através da página de administração do IPCOP.

Segundo Gaspar (2006) as principais características do Block Outgoing Traffic são:

- Fácil interação com as regras através de uma página WEB;
- Controle do tráfego que vai ou passa através do IPCOP;
- Possibilidade de criar restrições de Tráfego por endereços MAC, IP e interfaces;
- Cadastro de objetos (p. ex: endereços, serviços e interfaces);
- Cadastro de grupos de endereços e de serviços;
- Regras com restrições de tempo (p. ex: intervalo de hora ou dia da semana para ser aplicada);
- Controle de acesso para rede BLUE (Wireless);
- Controle e monitoração do tráfego das regras através de Logs do Firewall.

Para configurar clique na opção “Editar”, irá aparecer a tela de configuração, preencha os seguintes campos, “Admin MAC”, com o endereço MAC do computador que irá administrar o IPCOP, o campo “HTTPS Port (Default is 445)” com o número de porta 445, que é porta de acesso à página de administração do IPCOP. Se a rede interna tiver algum tipo de serviço que é acessado pela Internet, marque a opção “Connection state:”, pois ela permitirá o tráfego de uma conexão já existente.

Marque a opção “Logging:”, para criar registros ou logs do tráfego que não coincidir com as regras configuradas no Block Outgoing Traffic, no campo “Default Deny action:”, escolha qual será a política que o Block Outgoing Traffic irá trabalhar, lembrando que a política DROP bloqueia os pacotes tanto de entrada quanto de saída sem enviar um aviso. A política REJECT também bloqueia os pacotes de entra ou saída, mas envia uma mensagem ICMP informando que o destino foi unreachable (Inalcançável).

A opção “Advanced Mode:” é para acrescentar regras avançadas para customizar as necessidades da rede, só habilite esta opção se o administrador do IPCOP tiver bastante conhecimento sobre firewalls, pois esta opção abre o firewall.

Marque a opção “Check for BlockOutTraffic updates”, para o sistema avisar caso seja disponibilizado uma nova versão, ou atualização deste serviço.

Para continuar a configuração do BlockOutTraffic, é necessário fazer a configuração do capítulo 8.5.5 e depois voltar a este capítulo.

Terminadas as configurações do capítulo 8.5.5 clica-se no menu “FIREWALL” na opção “BLOCKOUTGOINGTRAFFIC” para abrir a página onde são adicionadas as regras para o “BlockOutTraffic”.

Segundo Gaspar (2006) a página “New Rule” é divida seções:

1. Origem: identifica a origem do pacote com as opções:
    - Default Interface;
    - “Adress Format” (IP ou MAC) e “Source Address” (Endereço de origem IP/MAC);
    - Redes Padrões: Rede de origem, padrão rede GREEN;
    - Custom Address: Endereços (hosts) cadastrados pelo usuário;
    - Address Group: Grupos de endereços (hosts) criados pelo usuário;
    - Invert (exclusão): altera o sentido da regra em relação ao endereço digitado, ou seja, serve para excluir o argumento da regra. No caso do endereço, refere-se a qualquer endereço de entrada, exceto o endereço ou grupo identificado.

2. Destino: identifica o destino do pacote com as opções:
    - IPCop Access: acesso ao Firewall IPCop;
    - Other Network/Outside: outra rede, cujo padrão é Any(qualquer destino), Custom address (um host específico), Address Group (um grupo específico de hosts), Destination IP or Network (o campo pode ser preenchido com um endereço de um host ou rede);
    - Invert (exclusão): idêntico a opção Source. No caso do destino, refere-se a qualquer endereço de destino, exceto o endereço, rede ou grupo identificado;
    - Use Service: pode conter a opção “Service Groups” (quando o usuário cadastra grupos de serviços), “Custom Services” (para serviços

cadastrados) e “Default Services” (para serviços cadastrados por padrão no IPCop).

3. Additional:

- Rule enable (habilitar a regra): você pode apenas cadastrar a regra, sem no entanto, habilitá-la. Se marcar esta opção, a regra ficará ativa automaticamente após o cadastro;
- Log rule (Log da regra): marque esta opção se desejar registrar em Log o tráfego da regra;
- Rule Action: Ação a ser aplicada à regra (ACCEPT ou DROP);
- Remark: Comentário sobre a regra.

4. Timeframe: habilitando a opção “Add Timeframe” você pode escolher o intervalo de dias do mês, o dia a semana, ou intervalo de hora em que a regra estará ativa. Obs. os campos seguidos por uma bola azul (●) são opcionais.

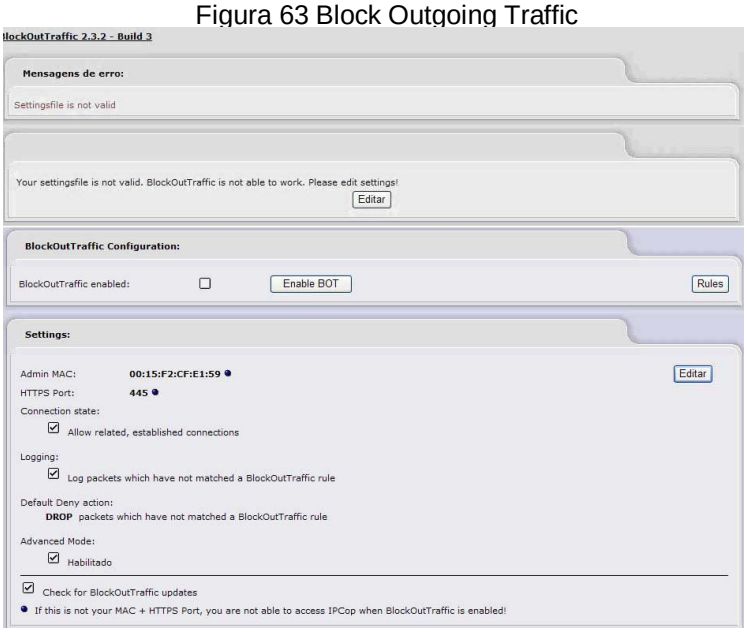
Para permitir que a rede GREEN use os serviços do IPCOP selecione:

Origem (source):

- Default interface: Green
- Redes Padrões: Green Network
- Destino (destination):
- IPCop access
- Marque a opção "use Service", e em "Service Group", escolha a opção "IPCOP_ADMIN" (é grupo que foi definido anteriormente para os serviços relacionados ao IPCop), clique em “Salvar” para adicionar a regra.

Para habilitar o “BlockOutTraffic” clique em “Settings”, depois em “Enable BOT”.

Figura 63 Block Outgoing Traffic



8.5.5 Advanced Bot Config

Através do Advanced Bot Config pode-se criar um cadastro de serviços e endereços (serviços e endereços são objetos que guardam informações globais sobre “números de portas/protocolos” e “endereços de hosts”) que não sejam padrão do programa. A seção “Default services settings” contém um cadastro padrão de 250 serviços, caso haja necessidade de adicionar um serviço pode-se fazê-lo através da opção “Services settings”.

Para terminar a configuração do capítulo 8.5.4 tem que ser adicionado os serviços ssh, https e proxy. Estes serviços são para administrar o IPCOP quando o Block OuttTraffic for ativado.

Caso as configurações do capítulo 8.5.4 sejam ativadas sem que sejam adicionados os serviços ssh, https e proxy, a administração via Web do IPCOP não sera acessada pelo navegador, causando grandes transtornos, pois para restaurar as configurações padrões terão que ser feitas pela interface texto do IPCOP, e por uma pessoa que tenha conhecimentos avançados.

Adicionando os serviços ssh, https e proxy.

No campo “Serviço de Nome” digite o primeiro serviço a ser adicionado, no campo “Portas” digite a porta usada pelo serviço e no campo “Protocolo”, assinale que tipo de protocolo o serviço usa, clique em “Adicionar” para salvar a configuração, repita o processo para os outros dois serviços.

Exemplo:

Nome do Serviço	Porta	Protocolo
Ipcop_https	445	TCP
Ipcop_proxy	3128	TCP
Ipcop_ssh	222	TCP

Além de cadastrar serviços, pode-se agrupar os serviços em um único objeto.

A seguir são descritos os serviços que podem acrescentados:

- Criar grupos de serviços (Service Grouping): agrupar os serviços cadastrados;
- Cadastro de hosts (Address Settings) através do endereço (IP ou MAC);
- Criar grupos de Endereços (Address Grouping): agrupar os objetos de endereço;
- Adicionar uma nova interface: cadastrar uma nova interface (p. ex VPN).

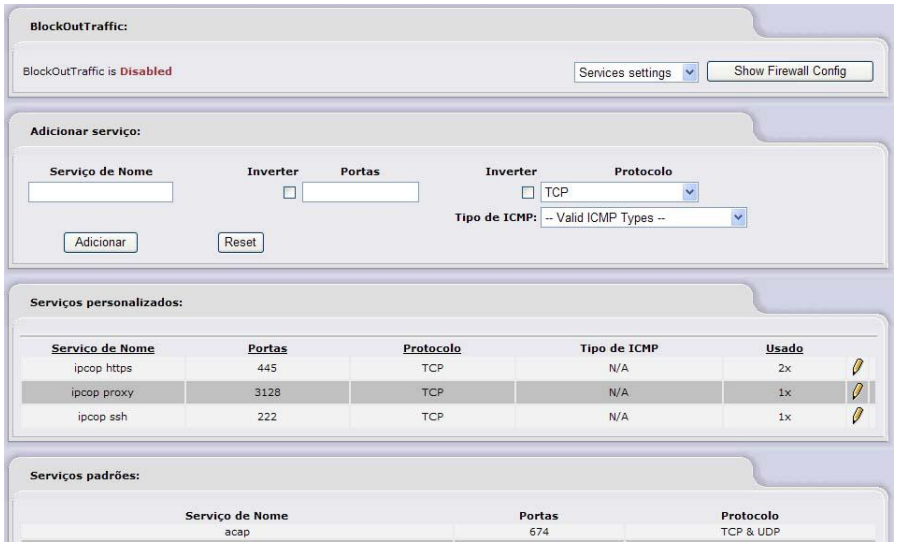
Para agrupar os serviços adicionados selecione a opção “Service Grouping” no menu dropdown, clique na opção “Show Firewall Config”, irá aparecer a página onde se faz o agrupamento dos serviços.

Selecione a opção “Service Group name:“ e informe um nome para o agrupamento. Exemplo, “IPCOP_ADMIN”. Selecione a opção “Serviços personalizados:”, clique em “Adicionar”.

Este procedimento cria o agrupamento “IPCOP_ADMIN”, e já inclui o serviço Ipcop_https dentro grupo “IPCOP_ADMIN”, agora adicione os serviços, Ipcop_proxy, Ipcop_ssh no grupo “IPCOP_ADMIN”, selecione o marque o grupo no menu dropdown “Service Group name”, no menu dropdown “Serviços personalizados” selecione um dos serviços que falta adicionar ao grupo, e clique em “Adicionar”, repita este procedimento para o outro serviço.

Terminada esta etapa, volta-se ao capítulo 8.5.4, para adicionar a regra que permite administrar o IPCOP e a regra que permite aos usuários da rede interna acessarem a Internet, depois que o “BlockOutTraffic” for habilitado.

Figura 64 Advanced Bot Config



8.6 LOGS

Este menu na instalação padrão contém 6 tipos de logs, que são, Configuração do Log, Resumo do Log, Logs do Proxy, Logs do Firewall, Logs do IDS e Logs do sistema. A quantidade de logs deste menu aumenta quando é instalado um addon no sistema, e ele possui Log será acrescentado a este menu, exemplo disso é o Logs de filtros URL, que foi acrescentado ao menu quando foi instalado o addon ipcop-urlfilter-1.9.

Os logs são essenciais ao sistema, pois é através deles que o administrador do sistema pode saber se o sistema está funcionando normalmente, e vigiar o tráfego entre a rede interna e a Internet e também saber o que os usuários da rede interna andam fazendo na Internet. A seguir será mostrado para que serve cada um dos logs.

8.6.1 Configuração do Log

A Configuração do Log possui 3 níveis de configurações sendo, opções de visualização do log, Resumos do Log, Registro remoto. A figura 65 mostra a tela de configuração do log.

Opções de visualização do log:

- Ordenado em ordem cronológica inversa: ordenar a ordem de apresentação do log.
- Linhas por página: É a quantidade de linhas que serão apresentadas no resumo do Log.

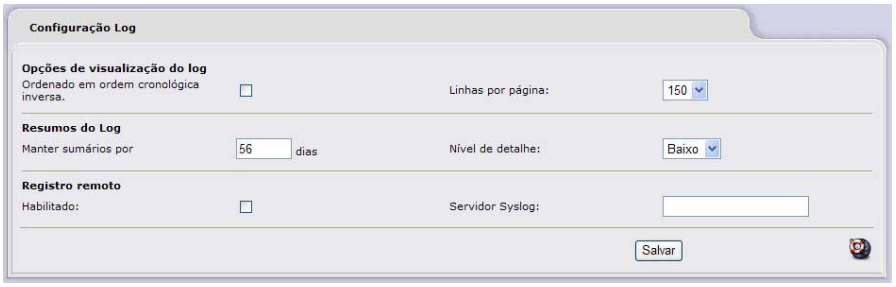
Resumos do Log:

- Manter sumários por quantidade de dias que os logs serão mantidos no sistema.
- Nível de detalhe: Qual nível de detalhe se é baixo, médio ou alto.

Registro remoto:

- Habilitado: habilita o envio do log para um servidor de log remoto.
- Servidor Syslog: endereço do servidor remoto.

Figura 65 Configuração do Log



8.6.2 Resumo do Log

O Resumo do Log mostra para o administrador do sistema a quantidade de pacotes (TCP, UDP, ICMP) que transitou na rede, de onde se originou o pacote e qual o seu destino, informa também as portas usadas, a interface de origem e o endereço IP de destino.

Figura 66 Resumo do Log

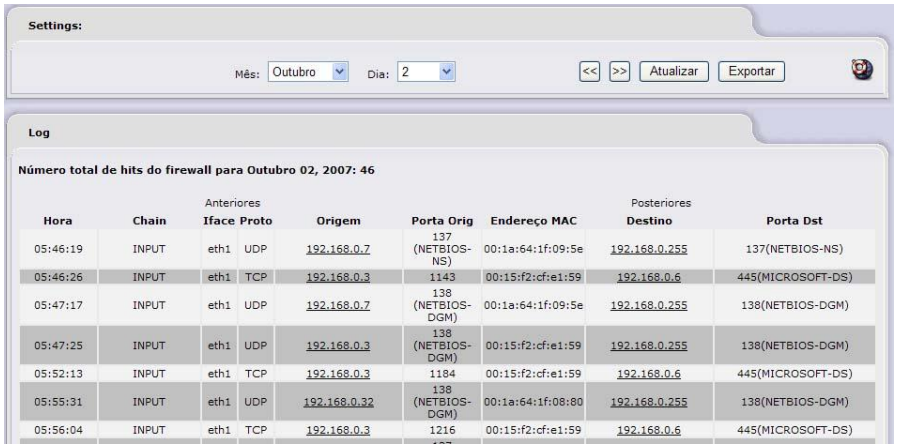
8.6.3 Logs do Proxy

O Logs Proxy mostra a hora, o endereço IP da máquina do usuário da rede interna e o endereço do Website que ele acessou ou tentou acessar.

Figura 67 Logs de Proxy

8.6.4 Logs do Firewall

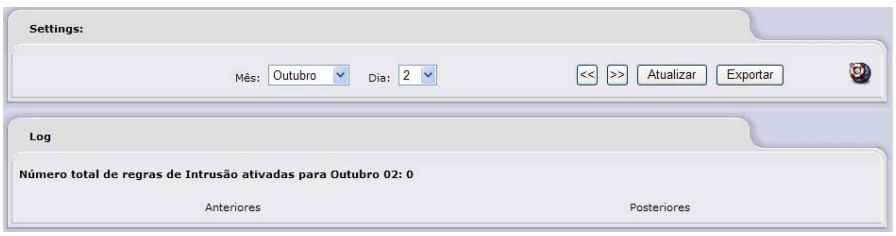
A opção Logs do Firewall mostra detalhadamente o tráfego no firewall. E mostrada a hora, a política adotada pelo firewall, qual a interface que originou o tráfego, qual o protocolo usado, qual IP que originou o tráfego, qual a porta de origem. Se o tráfego foi originado por uma máquina da rede interna, é mostrado o endereço MAC da máquina que originou o tráfego, o endereço IP de destino, a porta e o serviço de destino. Conforme a figura 68.



8.6.5 Logs do IDS

A opção Logs do IDS mostra as tentativas de invasão à rede interna. Este log mostra os endereços IP's e porta que originaram a tentativa de invasão, mostra o endereço IP e a porta da máquina que sofreu a tentativa de invasão.

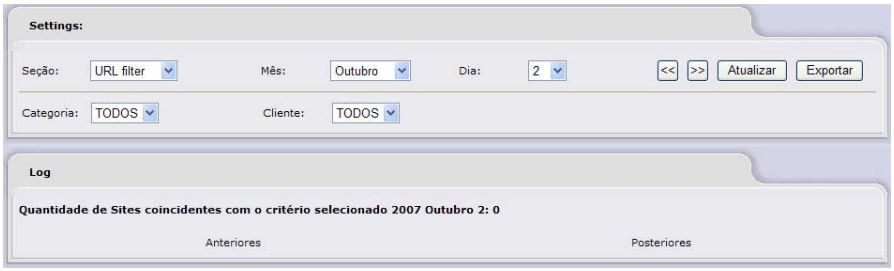
Figura 69 Logs do IDS



8.6.6 Logs do Filtro URL

O Logs do Filtro URL mostra os sites acessados na Internet, pelos usuários da rede interna. Ele mostra a hora que o usuário acessou o site, a categoria que este site pertence, o endereço IP da máquina que tentou acessar o site e o endereço URL do site.

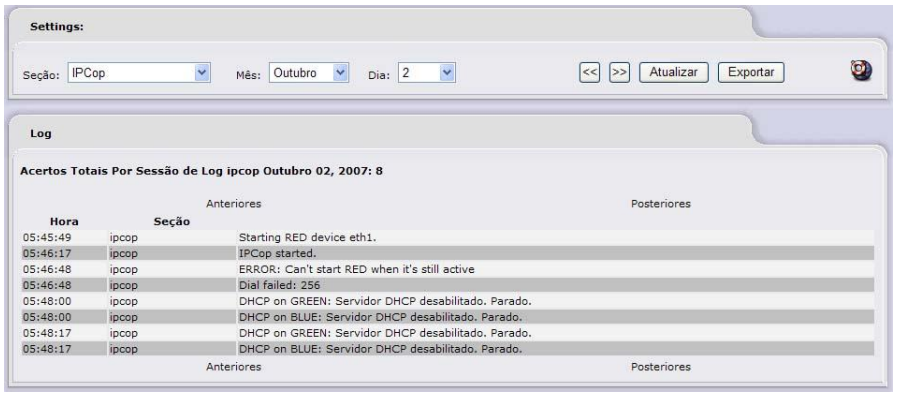
Figura 70 Logs do Filtro URL



8.6.7 Logs do Sistema

O Logs do Sistema mostra a hora que um serviço teve erro de funcionabilidade, ou se o serviço foi desativado, ou ativado.

Figura 71 Logs do sistema



9 CONCLUSÕES

A segurança das informações é vital para a sobrevivência de qualquer organização. Ainda mais nos dias de hoje, quando as empresas se lançam na Internet fazendo com que suas informações trafeguem neste meio, sem nenhum tipo de segurança. Proteger-se de hackers, vírus e outras ameaças é um ponto que dever ser lembrado e que a segurança deve ser encarada como um processo contínuo.

Muitas empresas erram gravemente adotando o software proprietário, como a única forma de solução de segurança aumentando seus custos. Em muitos casos empresas simplesmente ignoram essa segurança, por causa do alto custo de implantação através de software proprietário e migram para a pirataria. Estas empresas têm pensamentos errôneos a respeito de software livre, pois a grande discussão sobre software livre no ambiente corporativo tem sido qual sua vantagem (ou desvantagens) de custo, difícil implantação.

O objeto desse trabalho foi mostrar que IPCOP FIREWALL é uma ferramenta poderosa, intuitiva, de fácil implantação, podendo ajudar na segurança de micros e pequenas empresas contra os perigos que Internet propicia nos dias atuais

A contribuição deste trabalho foi mostrar que IPCOP Firewall evita e diminui os perigos que a Internet oferece.

Como trabalhos futuros, pretende-se estender este manual, mostrando a implementação de outros addons.

REFERÊNCIAS

BRASIL. Lei nº. 9.609 – de 19 de fevereiro de 1998. Dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências. Brasília, DF19 fev. 1998. Disponível em <http://www.planalto.gov.br/ccivil/Leis/L9609.htm>. Acesso em: 01 maio 2007.

FREE SOFTWARE FOUNDATION, The Free Software Definition. Boston. 2007. Disponível em: <http://www.gnu.org/philosophy/free-sw.html>. Acesso em: 01 maio 2007.

GOLDCHLEGER, Andrei. Open source Vs Código fechado. Disponível em <http://www.ime.usp.br/~is/ddt/mac339/projetos/2001/demais/andrei/>. Acesso em: 27 maio 2007.

TANENBAUM, Andrew S. Sistemas Operacionais Modernos. Tradução de Ronaldo A. L. Gonçalves, Luis A. Consularo. São Paulo: Prentice Hall, 2003. 707

TIBET, Chuck V. Linux Administração e Suporte. São Paulo: Novatec Editora Ltda., 2001. 379 p.

FERRETTO, Luiz Filipe Fagundes, et al. Implementações básicas de segurança para ambientes com processamentos críticos. Brasília: UNEB. 2002. Disponível em<http:www.eln.gov.br/Conhecimento/GestaodoConhecimento/monografia_Rute.doc>. Acesso em: 01 de Ago. 2007.

COLLE,Andrew Del, et al. Prejuízos causados as organizações por acessos a conteúdos indevidos. Curitiba: SPEI. 2006. Disponível em <http://www.assespropr.org.br/uploadAddress/Prejuizos_Causados_pelo_acesso_a_conteudos_indevidos.pdf>. Acesso em: 17 de Ago. 2007.

GASPAR, Antonio Edivaldo de O, Iniciando a configuração do Boot. 2006. Disponível em <http://blockouttraffic.de/files/GettingStarted_ptBr.pdf>. Acesso em: 25 set. 2007.

IPCop Mission Statement
<http://www.ipcop.org/index.php?module=pnWikka&tag=IPCopMissionStatement>. Acesso em: 02 out. 2007.

IPCop 1.4.x Features
<http://www.ipcop.org/index.php?module=pnWikka&tag=IPCop14xFeatures>. Acesso em: 02 out. 2007.

Administrative Guide
Copyright © 2002-2004 Chris Clancey, Harry Goldschmitt, John Kastner, Eric Oberlander, Peter Walker
<http://www.ipcop.org/1.4.0/en/admin/html/ >. Acesso em : 02 out. 2007.

IPCOP_BANNER_HALF_SIZE. GIF. Altura: 234 pixels. Largura: 60 pixels., 96 dpi 8 BIT CMYK. 3.741 Bytes. Formato GIF. Disponivel em: <http://www.ipcop.org/index.php?module=pnWikka&tag=IPCopArt>. Acesso em: 02 out. 2007.