PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
ESCOLA POLITÉCNICA E DE ARTES
GRADUAÇÃO EM ENGENHARIA DA COMPUTAÇÃO

JONAS NUNES RESENDE FILHO

CUSTOMIZAÇÃO DO IPCOP COMO SOLUÇÃO DE SEGURANÇA EM REDES DE PEQUENAS E MÉDIAS EMPRESAS

GOIÂNIA
2025

JONAS NUNES RESENDE FILHO

CUSTOMIZAÇÃO DO IPCOP COMO SOLUÇÃO DE SEGURANÇA EM REDES DE PEQUENAS E MÉDIAS EMPRESAS

Trabalho de Conclusão de Curso apresentado à Escola Politécnica e de Artes, da Pontifícia Universidade de Goiás, como parte dos requisitos para obtenção do título de Bacharel em Engenharia da Computação.

Orientador (a): Profª. Drª. Solange da Silva

Banca examinadora:

Prof. Me. Gildenor de Souza Amorim Cavalcante

Prof. Me. Rafael Leal Martins

GOIÂNIA
2025

JONAS NUNES RESENDE FILHO

CUSTOMIZAÇÃO DO IPCOP COMO SOLUÇÃO DE SEGURANÇA EM REDES DE PEQUENAS E MÉDIAS EMPRESAS

Trabalho de Conclusão de Curso aprovado em sua forma final pela Escola Politécnica e de Artes, da Pontifícia Universidade Católica de Goiás, para obtenção do título de Bacharel em Engenharia da Computação, em: / / .

■

_____

Orientador (a): Profª. Drª. Solange da Silva

_____

Prof. Me. Gildenor de Souza Amorim Cavalcante

_____

Prof. Me. Rafael Leal Martins

AGRADECIMENTOS

Primeiramente, quero expressar minha eterna gratidão à minha família, especialmente a Deus, por todo o apoio, amor e paciência que me proporcionaram. Vocês foram minha principal fonte de força em todos os momentos de dúvida ou dificuldade. Sem vocês, nada disso seria possível, e sua constante presença me deu a coragem necessária para seguir em frente.

Aos meus amigos, agradeço por estarem ao meu lado durante toda essa jornada. O apoio, a motivação e as risadas compartilhadas nos momentos de descontração foram fundamentais para aliviar os momentos mais difíceis. Vocês foram essenciais para manter meu equilíbrio e garantir que eu mantivesse o foco e a energia, especialmente quando o caminho se tornava desafiador.

A minha gratidão se estende também aos professores que contribuíram significativamente para o meu crescimento acadêmico e pessoal. Cada um de vocês, com seus ensinamentos e dedicação, forneceu as bases necessárias para que eu alcançasse este resultado. O conhecimento técnico adquirido nas suas aulas foi essencial, mas foi a inspiração que vocês me deram que realmente fez a diferença.

Um agradecimento imenso à minha orientadora, Profª Drª. Solange, por sua orientação constante e sua paciência incomparável. Seu conhecimento vasto e sua capacidade de me motivar foram vitais para o progresso deste trabalho. Com sua ajuda, consegui superar obstáculos e me aprimorar tanto profissionalmente quanto pessoalmente.

Por fim, agradeço a todos que, direta ou indiretamente, fizeram parte deste processo. Este trabalho é o reflexo do esforço coletivo de todos aqueles que me apoiaram. A cada um de vocês, meu mais sincero e profundo obrigado.

RESUMO

O objetivo geral deste trabalho é realizar uma análise detalhada da customização do IPCop em redes empresariais, abrangendo desde a configuração básica até práticas avançadas de segurança. Segundo os procedimentos técnicos, esta pesquisa é bibliográfica e documental. O estudo permitiu concluir que o IPCop é uma solução eficiente para a proteção de redes, oferecendo uma ampla gama de recursos, como filtragem de pacotes, *proxy*, autenticação de usuários e monitoramento em tempo real. Sua facilidade de configuração torna-o uma opção acessível, mesmo para administradores com conhecimentos limitados na área de segurança da informação. Entre os principais desafios está a adaptação do IPCop a ambientes que nem sempre foram planejados para suportar camadas dinâmicas de proteção. Isso exige não apenas conhecimentos técnicos, mas também uma abordagem voltada à escalabilidade e à manutenção contínua do sistema. Destaca-se ainda a importância da definição de políticas claras e da adoção de práticas éticas na administração do *firewall*, especialmente em contextos onde a integridade das comunicações e a proteção de dados são fundamentais para a continuidade dos negócios. Conclui-se que a customização do IPCop atende de forma eficaz às demandas de segurança em redes organizacionais, permitindo o controle de tráfego, segmentação e ajustes conforme as necessidades locais. Sua estrutura modular possibilita a integração de novos recursos, ampliando sua capacidade de proteção e adaptabilidade a diferentes contextos corporativos.

Palavras-chave: IPCop; Customização de firewall; Redes empresariais; Segurança em TI; Pequenas e médias empresas.

ABSTRACT

The main objective of this work is to conduct a detailed analysis of the customization of IPCop in small and medium-sized business networks, covering everything from basic configuration to advanced security practices. According to technical procedures, this research is bibliographic and documental. The study concluded that IPCop is a viable and efficient solution for protecting networks in small and medium-sized enterprises, offering a wide range of security features—from packet filtering to real-time traffic monitoring. Its ease of customization and configuration makes it an accessible option even for administrators with limited knowledge of network security. Furthermore, IPCop's flexibility allows it to adapt to various scenarios and requirements, providing an adequate level of protection without the need for significant infrastructure investment. One of the critical challenges in customizing IPCop for small and medium-sized business networks is adapting this firewall solution to environments that were not originally designed to support dynamic security layers. This requires not only improvements in configuration and integration with other technologies, but also a design approach focused on scalability and ongoing system maintenance. Additionally, the importance of clear policies and ethical practices in firewall administration is emphasized, especially in environments where data protection and communication integrity are essential for business continuity and for minimizing risks associated with potential security failures. It is concluded that IPCop customization can effectively meet the security demands of small and medium-sized business networks, providing data traffic control, network segmentation, and continuous monitoring. The system’s modular structure allows additional features to be integrated as needed, enhancing protection capacity and adaptability to different corporate scenarios.

Keywords: IPCop; Firewall customization; Business networks; IT security; Small and medium-sized enterprises.

LISTA DE FIGURAS

LISTA DE ABREVIATURAS E SIGLAS

ADSL	*Asymmetric Digital Subscriber Line*
AES	*Advanced Encryption Standard*
ASA	*Adaptive Security Appliance*
CA	*Certificate Authority*
CHAP	*Challenge Handshake Authentication Protocol*
CIA	*Confidencialidade, Integridade e Disponibilidade*
Cisco	*Cisco Systems*
DDoS	*Distributed Denial of Service*
DHCP	*Dynamic Host Configuration Protocol*
Endian	*Endian Firewall*
FTP	*File Transfer Protocol*
GNU	*General Public License*
GOV.BR	*Governo Brasileiro*
GUI	*Graphical User Interface*
HTTP	*HyperText Transfer Protocol*
HTTPS	*Hypertext Transfer Protocol Secure*
IDS	*Intrusion Detection System*
IP	*Internet Protocol*
IPCop	*Firewall de código aberto*
IPS	*Intrusion Prevention System*

IPTables	*IP Table Rules (ferramenta de firewall no Linux)*
IPsec	*Internet Protocol Security*
ISO	*International Organization for Standardization*
LAN	*Local Area Network*
LGP	*Lei Geral de Proteção de Dados*
MFA	*Multi-Factor Authentication*
NAT	*Network Address Translation*
NGFW	*Next Generation Firewall*
PAN-OS	*Palo Alto Networks Operating System*
PAP	*Password Authentication Protocol*
PME	*Pequenas e Médias Empresas*
RADIUS	*Remote Authentication Dial-In User Service*
RAID	*Redundant Array of Independent Disks*
RED	*Rede Externa (interface de rede do IPCop)*
SMBs	*Small and Medium-sized Businesses*
SQL	*Structured Query Language*
SSH	*Secure Shell*
TCP	*Transmission Control Protocol*
TI	*Tecnologia da Informação*
URL	*Uniform Resource Locator*
USB	*Universal Serial Bus*
VCI	*Virtual Channel Identifier*

vi *Editor de texto no Unix/Linux*

VM *Virtual Machine*

VPN *Virtual Private Network*

VPI *Virtual Path Identifier*

SUMÁRIO

1 INTRODUÇÃO

No contexto atual de transformação digital, a segurança da informação tornou-se uma prioridade estratégica para organizações de todos os portes. As pequenas e médias empresas (PMEs), em particular, enfrentam desafios únicos em relação à proteção de suas redes de computadores, uma vez que muitas vezes carecem dos recursos financeiros e técnicos disponíveis para grandes corporações. A adoção de práticas de segurança adequadas é essencial para proteger a integridade, confidencialidade e disponibilidade das informações críticas para os negócios, especialmente em um ambiente cada vez mais marcado pela proliferação de ataques cibernéticos e pela crescente dependência de tecnologias digitais (Stallings, 2021).

A segurança da informação é um campo vital para a proteção dos ativos digitais de uma organização, englobando práticas e tecnologias destinadas a garantir a confidencialidade, integridade e disponibilidade das informações. De acordo com Stallings (2021) a segurança da informação envolve um conjunto de estratégias e controles técnicos que protegem os dados contra acesso não autorizado, alteração ou destruição, além de assegurar que as informações estejam disponíveis para os usuários autorizados quando necessário.

Além disso, a implementação de medidas de segurança eficazes requer uma compreensão profunda dos riscos associados e a capacidade de adaptar as soluções às necessidades específicas da organização. Brooks (2019) destaca a importância de uma abordagem baseada em risco, onde as organizações identificam e avaliam suas vulnerabilidades para implementar controles que ofereçam uma proteção proporcional às ameaças enfrentadas.

As PMEs são alvos frequentes de cibercriminosos, que exploram as vulnerabilidades dessas empresas para realizar ataques como *phishing*, *ransomware* e negação de serviço (DDoS). Esses ataques podem causar danos significativos, desde a interrupção das operações até a perda irreparável de dados sensíveis. Além disso, a conformidade com regulamentações de proteção de dados, como a Lei Geral de Proteção de Dados (LGPD) no Brasil, exige que as empresas adotem medidas de segurança robustas para evitar penalidades severas e danos à reputação (Kremer, 2021).

Firewalls são dispositivos ou sistemas que controlam o tráfego de rede entre diferentes zonas de segurança, funcionando como a primeira linha de defesa contra ameaças externas. Segundo Tanenbaum e Feamster, (2021) *firewalls* podem ser configurados para filtrar o

tráfego com base em uma variedade de critérios, como endereços IP, portas e protocolos, o que permite que as organizações bloqueiem ou permitam o tráfego de acordo com suas políticas de segurança.

Além disso, *firewalls* modernos frequentemente incorporam funcionalidades avançadas, como inspeção profunda de pacotes e filtragem de aplicativos, para detectar e bloquear ameaças mais sofisticadas. Um estudo conduzido por Northcutt e Rose (2020) em "*Network Intrusion Detection*" enfatiza como *firewalls* integrados com sistemas de detecção de intrusões (IDS) podem melhorar significativamente a capacidade de uma organização de responder a ameaças e mitigar ataques em tempo real.

A segurança em redes de computadores é uma área fundamental para proteger a integridade e a confidencialidade dos dados que transitam por redes corporativas. A segurança de redes envolve a proteção dos dados contra interceptação, alteração e acessos não autorizados, utilizando tecnologias como criptografia, autenticação e controle de acesso (Forouzan, 2017).

Além disso, a gestão de redes seguras também inclui a proteção contra ameaças internas e externas. O autor ressalta a importância de uma abordagem holística para a segurança das redes, que deve considerar tanto a proteção de *hardware* quanto a segurança dos protocolos e aplicações utilizados na comunicação (Bonaventure, 2021).

O IPCop é uma solução de *firewall* de código aberto projetada para proteger redes de computadores, especialmente adequada para pequenas e médias empresas. Ele oferece uma gama de funcionalidades, incluindo filtragem de pacotes, suporte a VPN e proxy, que permitem uma personalização significativa para atender às necessidades específicas de cada organização. Segundo a documentação oficial do IPCop, a ferramenta é projetada para ser fácil de configurar e gerenciar, tornando-a uma opção viável para empresas que precisam de uma solução de segurança robusta sem a complexidade associada a sistemas comerciais (Ipcop project, 2024).

Justifica estudar este tema porque, este trabalho visa responder à seguinte questão de pesquisa: **Quais são as funcionalidades e benefícios da customização do IPCop como solução de segurança em redes de pequenas e médias empresas?**

Este trabalho tem como objetivo geral explorar a etapa de customização do IPCop em redes de pequenas e médias empresas, abordando desde a configuração básica até as práticas avançadas de segurança.

Os objetivos específicos são:

- Descrever o funcionamento do IPCop como firewall em redes de PMEs;
- Demonstrar o passo a passo da instalação e configuração do IPCop;
- Demonstrar as funcionalidades do IPCop.

Espera-se que os resultados deste trabalho possam contribuir:

- Informando aos administradores de redes corporativas sobre as vantagens do uso de soluções de código aberto como o IPCop;
- Demonstrando como o IPCop pode ser adaptado para atender às necessidades específicas de segurança de PMEs;
- Encorajando mais empresas a adotarem práticas de segurança cibernética robustas para proteger seus ativos digitais.

Quanto aos aspectos metodológicos, esta pesquisa, em relação aos procedimentos técnicos, é uma pesquisa bibliográfica e experimental.

Esta monografia está organizada em seis capítulos, sendo estruturada da seguinte forma: O Capítulo 1 apresenta a introdução com o contexto do trabalho, a questão de pesquisa, objetivos e resultados esperados. O Capítulo 2 traz o referencial teórico com conceitos, definições e trabalhos relacionados ao tema. No Capítulo 3 estão descritos os procedimentos metodológicos, mostrando como foi feito para atingir o objetivo geral. O Capítulo 4 descreve a instalação do software IPCop. O capítulo 5 está descrito suas funcionalidades. Por fim, o Capítulo 6 traz as considerações finais do estudo.

2 REFERENCIAL TEÓRICO

Este capítulo é constituído de duas partes: uma de conceitos e definições e outra de trabalhos relacionados.

2.1 Conceituação e definições

A segurança em redes de computadores é um tema amplamente discutido no cenário tecnológico atual, especialmente devido ao crescimento do número de dispositivos conectados à internet. Dados do governo brasileiro indicam que, em 2022, 90% dos lares no Brasil já tinham acesso à internet, totalizando 65,6 milhões de domicílios conectados (GOV.BR, 2022). Esta massificação do uso da rede aumentou a necessidade de mecanismos de proteção, tanto para usuários domésticos quanto para empresas.

A segurança da informação em redes envolve um conjunto de práticas e tecnologias voltadas à proteção de dados e sistemas contra acessos não autorizados, ataques cibernéticos e violações. Nesse contexto, os *firewalls* se destacam como uma das principais soluções de segurança, atuando na defesa perimetral das redes, controlando o tráfego de entrada e saída com base em políticas predefinidas (Stallings, 2021).

De acordo com a Cisco *Systems*, um *firewall* pode ser definido como um sistema de segurança projetado para monitorar e controlar o tráfego de rede, baseado em regras estabelecidas pelo administrador do sistema. Ele age como uma barreira entre redes internas confiáveis e redes externas, como a internet, bloqueando ou permitindo a passagem de dados com base nas regras configuradas (Cisco, 2023).

A tríade CIA, composta pelos princípios de Confidencialidade, Integridade e Disponibilidade, é fundamental para a segurança da informação. Confidencialidade diz respeito à proteção das informações, evitando que sejam acessadas por pessoas não autorizadas, garantindo que dados sensíveis fiquem restritos apenas a indivíduos com permissão. Integridade refere-se à garantia de que as informações permaneçam precisas e inalteradas, prevenindo modificações não autorizadas ou erros. Já a Disponibilidade assegura que as informações e os sistemas estejam acessíveis aos usuários autorizados quando necessário. Esses três pilares são cruciais para implementar práticas de segurança robustas, garantindo a proteção, a precisão e o acesso adequado aos dados, o que fortalece a confiança e a eficiência dos sistemas de informação (Stallings, 2021).

2.2 Firewall

Um *firewall*, apresentado na Figura 1, é uma barreira de segurança que monitora e controla o tráfego de rede com base em políticas definidas. Ele atua como uma primeira linha de defesa entre redes internas seguras e externas, como a Internet, bloqueando ou permitindo a passagem de dados com base em regras preestabelecidas. Os *firewalls* são essenciais para proteger sistemas e dados contra acessos não autorizados e ataques cibernéticos (Cisco Systems, 2023).

Figura 1 – Visualização de um Firewall em uma rede

Fonte: FREEPIK, 2024.

Os *firewalls* podem ser classificados em diferentes tipos, cada um oferecendo características e níveis de proteção distintos. São eles:

Firewalls Stateless: Esses *firewalls* realizam uma filtragem básica de pacotes e não mantém informações sobre o estado das conexões de rede. Eles verificam cada pacote de

forma independente, sem considerar o contexto do tráfego anterior. Essa abordagem torna os *firewalls stateless* mais rápidos e simples, mas também limita a sua capacidade de oferecer proteção avançada contra ameaças mais complexas (Zwicky; Cooper & Chapman, 2021).

*Firewalls Stateful***:** Ao contrário dos *firewalls stateless*, os *firewalls stateful* monitoram o estado das conexões e mantém informações sobre o tráfego atual. Eles verificam os pacotes em relação ao estado da conexão, oferecendo uma proteção mais robusta ao acompanhar a integridade da comunicação. Isso permite que eles detectem e bloqueiem pacotes que não se encaixam em uma conexão estabelecida, proporcionando uma camada adicional de segurança (Shinder, 2020).

Firewalls de Próxima Geração (NGFW)**:** Esses *firewalls* combinam as funcionalidades dos *firewalls* tradicionais com capacidades avançadas, como inspeção profunda de pacotes, filtragem de aplicativos e proteção contra ameaças sofisticadas. Os NGFWs são projetados para lidar com ameaças modernas de forma mais eficaz, oferecendo uma abordagem mais completa para a proteção da rede (Check Point, 2023) e (Palo Alto Networks, 2024).

Firewalls de Aplicação**:** Focados em proteger aplicativos específicos contra-ataques direcionados, como SQL *injection* e cross-site *scripting*, os *firewalls* de aplicação operam em um nível mais granular. Eles são capazes de identificar e bloquear ameaças que outras abordagens podem não detectar, proporcionando uma proteção mais detalhada para as aplicações (Fortinet, 2023).

Os *firewalls* são utilizados para:

- Controle de Acesso: Permitir ou bloquear tráfego com base em regras de segurança.
- Proteção Contra Ameaças: Identificar e prevenir ataques cibernéticos e vulnerabilidades.
- Monitoramento de Rede: Analisar e registrar o tráfego de rede para detectar padrões suspeitos.

São implementados em diversos ambientes, incluindo redes corporativas, centros de dados, pequenas e médias empresas, e até mesmo para uso doméstico, dependendo das necessidades de segurança e orçamento (Oliveira & Martins, 2022).

Os *firewalls* desempenham um papel fundamental na proteção de redes contra ameaças cibernéticas, e diferentes tipos de *firewalls* atendem a necessidades específicas de segurança. Entre os mais conhecidos está o *Palo Alto Networks* (PAN-OS), criado em 2005, amplamente adotado em ambientes corporativos e data *centers*. Este *firewall* é notável por sua

segurança de próxima geração (NGFW), oferecendo inspeção profunda de pacotes e integração com serviços de nuvem. Embora seja altamente eficaz, seu custo elevado e a complexidade na configuração podem ser desvantagens para algumas organizações (Palo Alto Networks, 2024).

Outro *firewall* amplamente reconhecido é o Fortinet FortiGate, desenvolvido em 2002. É conhecido por oferecer um bom equilíbrio entre desempenho e custo-benefício, sendo ideal para ambientes corporativos, pequenas e médias empresas (SMBs) e redes de filiais. Com uma gama ampla de produtos, o FortiGate proporciona segurança avançada, embora sua interface possa ser confusa e sua curva de aprendizado seja um ponto a considerar (Fortinet, 2024).

O *Check Point Next Generation Firewall*, criado em 1994 e disponível como NGFW desde 2001, é amplamente utilizado em ambientes corporativos e governamentais. Este *firewall* é elogiado por sua segurança avançada e a integração robusta com outras soluções de segurança. No entanto, seu custo elevado e a complexidade na gestão podem representar desafios para alguns usuários (Check Point, 2023).

O Cisco ASA com *FirePOWER*, lançado em 2005, é conhecido por sua confiabilidade e integração com outras soluções de segurança da Cisco. Ideal para ambientes corporativos e redes de filiais, suas funcionalidades são mais limitadas quando comparadas aos NGFWs modernos, e sua interface de usuário pode parecer antiquada (Cisco, 2023).

O Endian *Firewall*, criado em 2003, é uma solução o*pen-source* adequada para pequenas e médias empresas, bem como para uso residencial e em *home labs*. Oferece recursos como *Virtual Private Network* (VPN), filtragem de web e detecção de intrusões, mas pode não ter o mesmo nível de recursos avançados que *firewalls* empresariais e o suporte na versão gratuita é limitado (Endian, 2024).

2.3 TOKEN

Um *token* é uma representação digital de um valor que é usado para autenticar e autorizar um usuário ou sistema a acessar recursos protegidos. Ao contrário de autenticações baseadas em senhas, que podem ser vulneráveis a ataques de força bruta ou *phishing*, os *tokens* proporcionam um método mais seguro e eficiente de autenticação e autorização. Em um sistema típico de autenticação, como o *OAuth* 2.0, após o login bem-sucedido, o servidor gera um *token* que pode ser utilizado para validar o usuário durante a interação com

Application Programming Interface (APIs), sem a necessidade de enviar credenciais repetidamente (Stallings, 2020).

Um *token* de acesso é geralmente usado para garantir que o usuário ou serviço tem permissão para acessar recursos específicos por um tempo determinado. Ao fazer login em um sistema, o servidor gera um *token* após verificar as credenciais do usuário. Esse *token* contém informações sobre a identidade do usuário e sobre os recursos aos quais ele tem acesso, permitindo autenticação contínua sem necessidade de reautenticação constante. O *token* de acesso geralmente tem um tempo de expiração para limitar o risco de comprometer as informações, após o qual o usuário precisará realizar a autenticação novamente ou utilizar um *refresh token* para obter um novo *token* (Ferreira; Lemos, 2018).

A segurança dos *tokens* é fundamental para a integridade de um sistema. Quando não são protegidos adequadamente, os *tokens* podem ser interceptados ou falsificados, resultando em sérios riscos de segurança. Para mitigar esses riscos, os *tokens* devem ser transmitidos sobre canais seguros, como HyperText Transfer Protocol Secure (HTTPS), e devem ser protegidos com criptografia. Além disso, um bom sistema de gerenciamento de *tokens* deve incluir políticas como a expiração de *tokens* e o uso de *refresh tokens* para renovar a validade, o que impede o uso indevido de tokens antigos ou comprometidos. O uso de *tokens* também deve ser integrado a outros mecanismos de segurança, como a autenticação multifatorial ou *Multi-Factor Authentication* (MFA), para aumentar a proteção (ISO/IEC 27001,2022).

Tokens são essenciais em ambientes que fazem uso de APIs para integração de sistemas. No contexto de *OAuth 2.0*, um sistema cliente pode obter um *token* de acesso para realizar operações em nome do usuário sem expor suas credenciais diretamente. Isso é muito comum em serviços que permitem login via *Google*, *Facebook* ou outros provedores, no qual o *token* gerado pelo provedor é usado para autenticar o usuário no aplicativo. A utilização de *tokens* oferece vantagens como maior segurança e a possibilidade de definir permissões específicas, permitindo que o usuário controle quais dados são acessados por diferentes serviços (Tanenbaum; Feamster; Wetherall, 2021).

Em sistemas modernos de segurança, os *tokens* têm se mostrado uma solução eficaz para autenticação e autorização. Ao eliminar a necessidade de enviar senhas a cada requisição e fornecer métodos robustos de controle de acesso, os *tokens* oferecem uma camada adicional de proteção contra ataques e vazamentos de dados. Seu uso é fundamental em sistemas distribuídos, como na nuvem e em serviços baseados em APIs, onde a flexibilidade e a segurança são essenciais para garantir a integridade e a confiabilidade das comunicações

(Stallings, 2020).

2.4 Cibersegurança

A cibersegurança é um pilar fundamental para a proteção de dados no mundo digital, e a criptografia é uma das principais ferramentas para garantir a segurança e a confidencialidade da informação. A criptografia assegura a integridade dos dados transmitidos, protegendo-os contra acessos não autorizados. Tecnologias como o *Advanced Encryption Standard* (AES) são amplamente utilizadas para proteger a comunicação digital, especialmente em transações financeiras e em dados pessoais. Sem criptografia, a segurança de dados e comunicações estaria comprometida, uma vez que as ameaças cibernéticas se tornam cada vez mais sofisticadas (Diogenes, 2024).

Além da criptografia, a autenticação e o controle de acesso desempenham um papel vital na proteção de sistemas e redes. Sistemas robustos de autenticação, como a autenticação multifatorial (MFA), aumentam a segurança de uma rede, garantindo que apenas usuários autorizados possam acessar informações sensíveis. A combinação de algo que o usuário sabe (como uma senha) e algo que o usuário tem (como um dispositivo de autenticação) ajuda a reduzir a eficácia de ataques de *phishing* e outros tipos de fraude digital. Assim, os métodos de controle de acesso são cruciais para limitar os danos em caso de violação de segurança (Palma; Costa; Sabino, 2024).

A segurança de redes envolve diversas camadas de proteção, incluindo a utilização de *firewalls*, sistemas de detecção de intrusão ou *Intrusion Detection System* (IDS) e redes privadas virtuais ou Virtual Private Net*work* (VPNs). As redes precisam ser protegidas contra ameaças externas e internas. A segurança em redes sem fio, por exemplo, exige o uso de protocolos de segurança como Wi-Fi Protected Access 3 (WPA3) para redes domésticas e empresariais, além de políticas rigorosas de criptografia de dados. Ferramentas de monitoramento contínuo permitem detectar e mitigar atividades suspeitas de forma mais eficiente (Silva, 2024).

À medida que as ameaças cibernéticas se tornam mais sofisticadas, as organizações precisam adotar estratégias proativas de defesa. A implementação de políticas de segurança e a educação contínua dos funcionários são fundamentais para reduzir as vulnerabilidades. A defesa em profundidade, que envolve múltiplas camadas de segurança, é uma abordagem recomendada para mitigar riscos e garantir a resiliência frente a ataques como *ransomware*. A

gestão de riscos cibernéticos e a capacidade de resposta rápida a incidentes são essenciais para proteger dados críticos e garantir a continuidade dos negócios (Ferreira, 2021).

2.5 Trabalhos Relacionados

No contexto da implementação e customização do IPCop como solução de segurança em redes de pequenas e médias empresas, diversos estudos têm sido conduzidos para explorar as melhores práticas e metodologias eficazes. Trabalhos recentes destacam a integração do IPCop com outras ferramentas de segurança, como firewalls e sistemas de monitoramento, visando melhorar a proteção contra ataques cibernéticos e garantir a segurança da rede. Além disso, pesquisas sobre o impacto da personalização do IPCop em ambientes corporativos apontam para uma maior confiabilidade e controle sobre o tráfego de dados, além de uma gestão eficiente das conexões de rede. Estes estudos também discutem os desafios enfrentados na implementação do IPCop, como a necessidade de configuração adequada e a adaptação às necessidades específicas de cada empresa. A revisão dessas pesquisas é fundamental para entender os benefícios e limitações do IPCop como uma solução de segurança, contribuindo para a inovação e fortalecimento da infraestrutura de TI nas pequenas e médias empresas.

A seguir, essa seção apresenta alguns trabalhos relacionados ao tema em estudo.

2.5.1 Perbandingan Kinerja IPCop dengan Honeypot dalam Mengamankan Server Linux dari Serangan Hacker

No trabalho de Burju Manik e Imran Lubis (2021), o IPCop, implementado como sistema de segurança no servidor, demonstrou ser uma solução eficaz na proteção contra ataques de hackers. Ele é capaz de bloquear completamente tentativas de ping, impedindo que hackers descubram informações sobre o servidor alvo, o que dificulta a identificação e exploração de vulnerabilidades. A configuração adequada do IPCop permite que o servidor se mantenha protegido contra acessos não autorizados, funcionando como uma barreira robusta contra invasões. Com isso, o IPCop assegura a integridade do servidor, oferecendo uma defesa ativa e eficaz contra ataques externos.

Além disso, o IPCop pode ser facilmente configurado e executado em ambientes como o Manjaro Linux e Windows 10, conforme demonstrado na pesquisa. Sua capacidade de bloquear ataques de maneira eficiente é um dos pontos fortes da ferramenta, tornando-a uma escolha sólida para pequenas e médias empresas que necessitam de segurança robusta em seus

servidores. Em comparação com outras soluções, como o Honeypot, o IPCop se destaca pela simplicidade e eficácia na proteção direta do servidor, garantindo que ele se mantenha fora do alcance de ataques, enquanto outros sistemas podem direcionar os hackers para servidores virtuais.

2.5.2 Simulasi Pemanfaatan IPCop sebagai PC Router dalam Jaringan Local (LAN) di Laboratorium FE-UMI

Conforme o trabalho de Alexander Simanullang, Junika Napitupulu, Jamaluddin e Mufria J. Purba (2018), o IPCop pode ser uma excelente solução para a construção e gerenciamento de redes locais (LAN) com endereços IP diferentes, como demonstrado no estudo realizado na Faculdade de Economia da Universidade Methodist da Indonésia. Ao utilizar o IPCop como *PC Router*, é possível gerenciar o tráfego de dados entre duas redes locais, garantindo que ambas as redes possam acessar a internet por meio de um único ponto de roteamento. A configuração do IPCop oferece uma abordagem segura e eficiente, facilitando a integração entre diferentes segmentos de rede e otimizando a comunicação entre os dispositivos.

Além disso, a personalização do IPCop pode ser ampliada com funcionalidades como a interface *ORANGE*, modelagem de largura de banda (*bandwidth shaping*) e firewall. Essas características são fundamentais para garantir que a rede local seja protegida contra ameaças externas, ao mesmo tempo em que se proporciona uma alocação eficiente de recursos de rede. O uso do IPCop permite que administradores de rede controlem e limitem a largura de banda disponível para os usuários, além de proporcionar uma camada adicional de segurança com o firewall integrado, protegendo a rede contra acessos não autorizados.

2.5.3 Analisis Efektifitas Bandwidth Menggunakan IPCop (Studi Kasus: Balai Besar Teknologi Energi)

No trabalho de Viva Arifin e R. Inge Fitriana (2012), o IPCop, com seu recurso de *Proxy* Avançado, é uma ferramenta essencial para gerenciar e otimizar a largura de banda em ambientes de rede. No caso do Centro de Tecnologia de Energia (B2TE), a implementação do IPCop permitiu limitar o uso da largura de banda, garantindo que cada usuário não consuma mais do que a quantidade alocada, evitando congestionamentos e desperdícios de recursos. A configuração de limitações específicas para download, como a restrição de 512 Kbps para

cada host, ajuda a manter a eficiência da rede e a equilibrar o uso de dados entre os usuários.

Além disso, o IPCop oferece uma funcionalidade de *traffic shaping*, que permite limitar a velocidade de download e upload, proporcionando uma distribuição mais eficiente da largura de banda. Com o uso de duas linhas de modem ADSL, a capacidade de banda é mais bem aproveitada, e a restrição de velocidade de download de 512 Kbps para cada usuário assegura que nenhum usuário sobrecarregue a rede. Esse controle ajuda a garantir que todos os usuários tenham acesso equitativo à internet, melhorando a performance da rede e evitando que downloads excessivos de dados prejudiquem a comunicação no ambiente corporativo.

3 MÉTODO

Este trabalho quanto à natureza caracteriza-se como um resumo de assunto, já que se baseia em apenas organizar uma área de conhecimento, indicando sua evolução histórica e estado de arte (Wazlawick, 2014).

Quanto aos objetivos, essa pesquisa é exploratória, aquela em que o autor não tem necessariamente uma hipótese ou objetivo definido em mente. Ela pode ser considerada, muitas vezes, como o primeiro estágio de um processo de pesquisa mais longo (Wazlawick, 2014).

Referente aos procedimentos técnicos, trata-se de uma pesquisa bibliográfica e documental.

A revisão bibliográfica envolve a análise de materiais já publicados, como livros, teses, recursos online e revistas, entre outros. Sua principal vantagem é permitir uma abordagem mais ampla de diversos fenômenos, além do que seria possível se pesquisar diretamente (Gil, 2017).

De acordo com Gil (2017), as etapas da revisão bibliográfica são:

a) Escolha do tema: O tema escolhido é “Customização do IPCop como Solução de Segurança em Redes de Pequenas e Médias Empresas”;

b) “Customização do IPCop como Solução de Segurança em Redes de Pequenas e Médias Empresas”;

c) Revisão preliminar da literatura: Foi realizado um levantamento bibliográfico preliminar de periódicos e artigos relacionados ao uso de Inteligência Artificial em sistemas de controle inteligente. A pesquisa abrangeu a base de dados da CAPES, o repositório da PUC GO e também foi conduzida utilizando o Google Acadêmico;

d) Formulação da pergunta de pesquisa: Quais são as funcionalidades e benefícios da customização do IPCop como solução de segurança em redes de pequenas e médias empresas?

e) Identificação das fontes: As fontes bibliográficas relevantes estão sendo identificadas, incluindo dissertações, periódicos científicos, obras de referência e outros materiais que ofereçam informações pertinentes para responder à pergunta de pesquisa;

f) Análise do conteúdo: Na análise do conteúdo foram examinadas as informações e dados coletados das fontes selecionadas, relacionando-os à pergunta de pesquisa. A consistência dos argumentos apresentados será avaliada durante essa fase;

g) Redação do Texto: Escrita do TCC2.

A pesquisa documental é uma abordagem metodológica semelhante à pesquisa bibliográfica, mas se diferencia principalmente pelas fontes utilizadas. Enquanto a pesquisa bibliográfica se baseia nas reflexões e contribuições de diferentes autores sobre um determinado tema, a pesquisa documental se concentra em materiais que já foram analisados anteriormente, mas podem ser reinterpretados de acordo com os objetivos específicos do estudo (Gil, 2017).

De acordo com Gil (2017), a pesquisa documental também tem etapas, mas este estudo se concentra em apenas uma delas, que é:

a) Customização do IPCop: Customização do IPCop em redes de pequenas e médias empresas, abordando desde a configuração básica até as práticas avançadas de segurança.

4 IPCOP

Este capítulo aborda as principais definições e funcionalidades do IPCop, destacando suas aplicações em diversos ambientes de rede e sua importância na segurança de sistemas computacionais. Além disso, investiga-se como o IPCop pode ser uma solução eficaz para Pequenas e Médias Empresas (PMEs), fornecendo uma defesa robusta e economicamente viável contra ameaças cibernéticas.

4.1. Sobre o IPCOP *FIREWALL*

O IPCOP *FIREWALL* é uma distribuição baseada no sistema operacional Linux, desenvolvida para garantir a segurança da rede em que é implementado. Ele se destaca pela simplicidade na instalação e configuração, podendo ser usado tanto por iniciantes quanto por usuários mais experientes. Licenciado sob a *General Public License (*GNU), o IPCOP *FIREWALL* oferece a vantagem de ser *open source*, permitindo que especialistas em segurança de todo o mundo possam analisar seu código-fonte e corrigir possíveis vulnerabilidades (Meneguite, 2010).

Em outubro de 2001, um grupo de desenvolvedores decidiu criar o IPCOP como um novo projeto, após discordarem da proposta de tornar o *Smoothwall* um *software* pago. Eles preferiram seguir com um *firewall* de código aberto, permitindo que qualquer pessoa pudesse usá-lo e aprimorá-lo. Assim, separaram-se do projeto original e, usando o código existente, reformularam o sistema e o lançaram como IPCOP *FIREWALL* (IPCop Firewall, 2007).

4.2 Instalação e Configuração do IPCOP

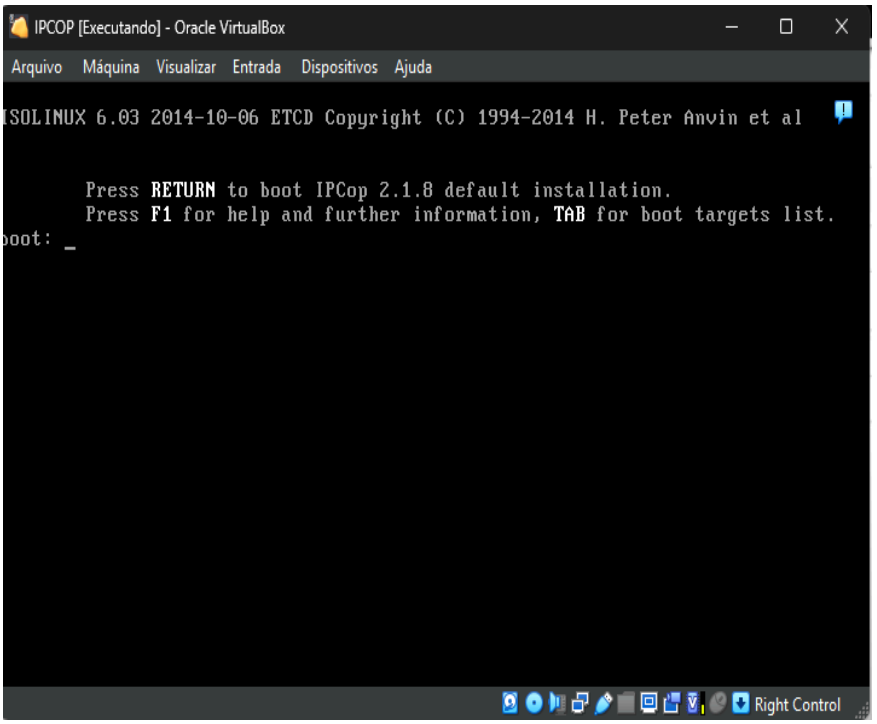
Para configurar o IPCOP em uma máquina virtual foi utilizado o *Oracle VirtualBox*. É importante definir os requisitos de hardware e as configurações de rede corretamente. O IPCOP é um *firewall* leve baseado em Linux e seus requisitos mínimos de sistema são bem acessíveis. A máquina virtual precisa de apenas 512 MB de RAM e 2GB de espaço em disco, suficiente para armazenar logs e configurações básicas. O processador pode ser configurado com apenas 1 núcleo, pois o IPCOP não exige muitos recursos para operações padrões.

Uma das configurações essenciais ao configurar a *Virtual Machine* (VM) do IPCOP é a rede. No *VirtualBox*, pode-se desativar o adaptador 1 e ativar o adaptador 2 para que ele seja usado como a principal interface de rede. O Adaptador 2 deve ser configurado em modo *Bridge* para conectar a máquina virtual diretamente à rede física ou em modo *Network Address Translation* (NAT) para conectar à Internet, dependendo das suas necessidades. Com essa configuração, o IPCOP poderá atuar de maneira eficaz como *firewall*, isolando e controlando o tráfego entre a rede interna e a conexão externa, conforme necessário.

O processo de instalação do IPCOP é relativamente simples e intuitivo. Após baixar a imagem *International Organization for Standardization* (ISO) do IPCOP no site oficial, basta carregá-la na VM e iniciar o processo de instalação. Durante a instalação, o assistente guiará você pela configuração das interfaces de rede, definição de senhas e outras configurações de segurança básicas.

Após configurar todos os requisitos e ajustes de rede na máquina virtual o IPCOP está pronto para ser inicializado. Com a ISO carregada e os adaptadores de rede configurados, basta iniciar a VM para que o IPCOP comece o processo de inicialização e instalação, como mostrado na Figura 2.

Figura 2 – Tela de inicialização do IPCOP

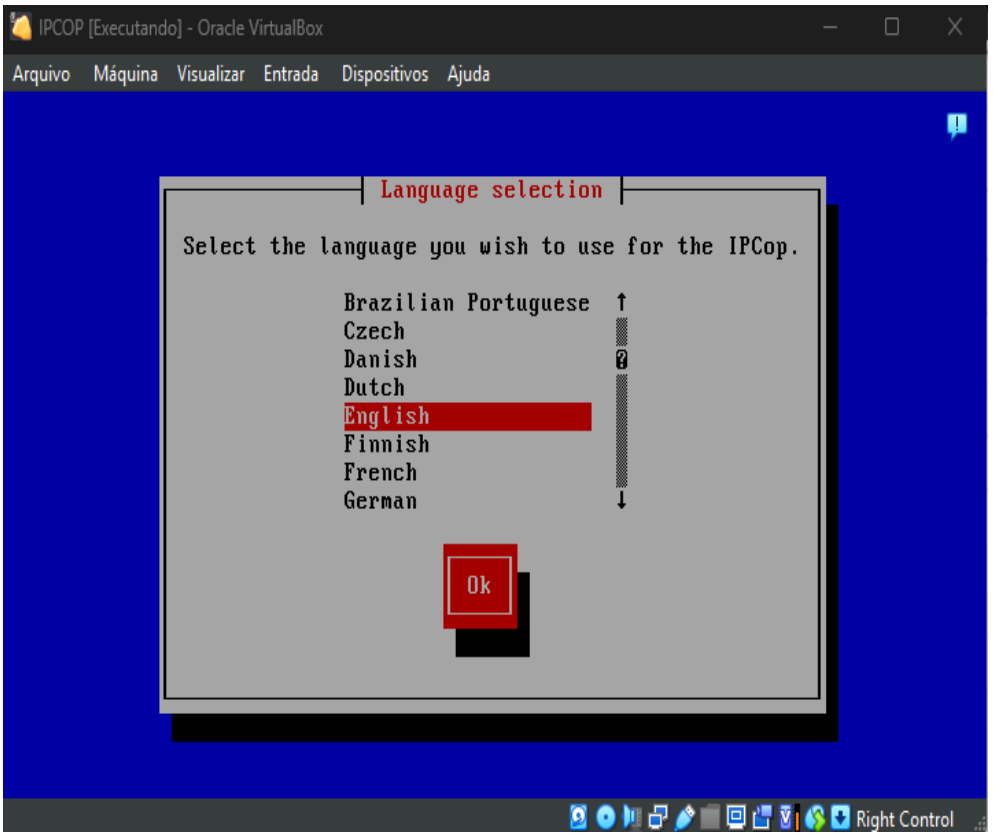


Fonte: autoria própria, 2024

Após iniciar a instalação do IPCOP e pressionar a tecla enter na primeira tela, existe uma opção para selecionar o idioma do sistema. Esse passo permite escolher a língua em que as instruções e o menu de configuração serão exibidos, facilitando o entendimento durante a instalação e a administração da *firewall*. Selecione o idioma desejado usando as setas do teclado e pressione enter para confirmar.

A escolha do idioma ajudará a tornar o processo de configuração mais acessível e intuitivo, principalmente para usuários que preferem operar o sistema em sua língua nativa, como mostrado na Figura 3. Depois de definir o idioma, o assistente de instalação continuará com as próximas etapas, guiando você pela configuração de rede e outros ajustes iniciais.

Figura 3 – Tela de seleção do idioma

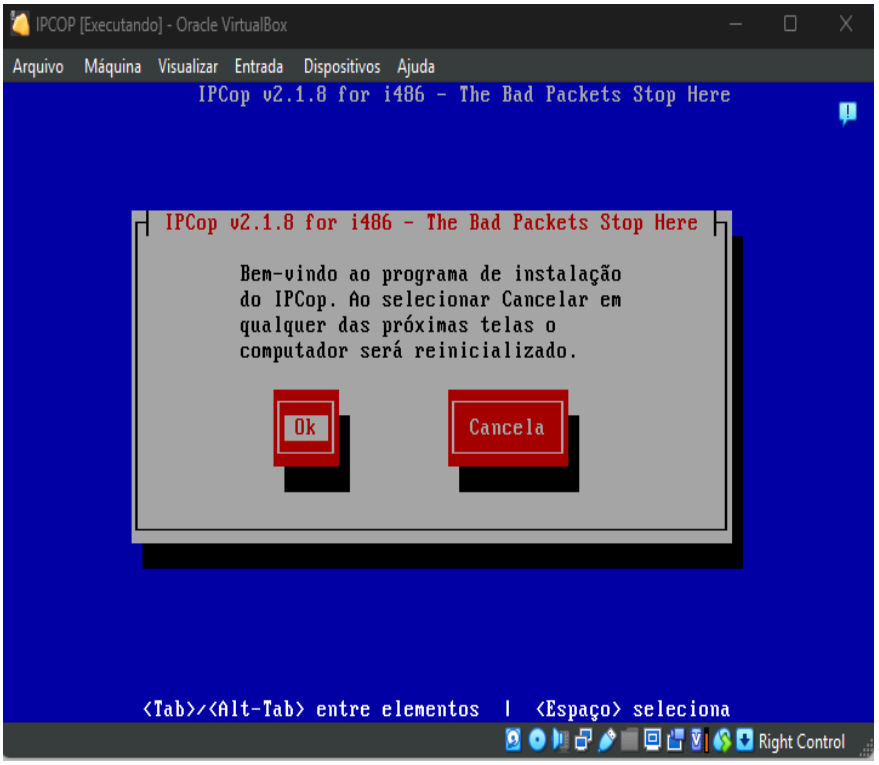


Fonte: autoria própria, 2024

Após a tela de seleção de idioma na instalação do IPCop, será exibida uma tela com as opções “OK” ou “Cancelar”. Nessa etapa, o sistema está pedindo uma confirmação para continuar o processo de instalação. Caso escolha “OK”, a instalação prosseguirá para a próxima fase na qual o IPCop começará a configurar o sistema e realizar as etapas iniciais, como a detecção de hardware e a configuração da rede.

Caso escolha o botão “Cancelar”, o processo de instalação será interrompido imediatamente e o computador será reiniciado. Isso ocorre porque a instalação não pode continuar sem a confirmação do usuário. Ao cancelar, o sistema reverte as mudanças feitas até aquele ponto e reinicia, permitindo que se reinicie o processo de instalação ou inicie outro sistema operacional se necessário, como mostrado na Figura 4.

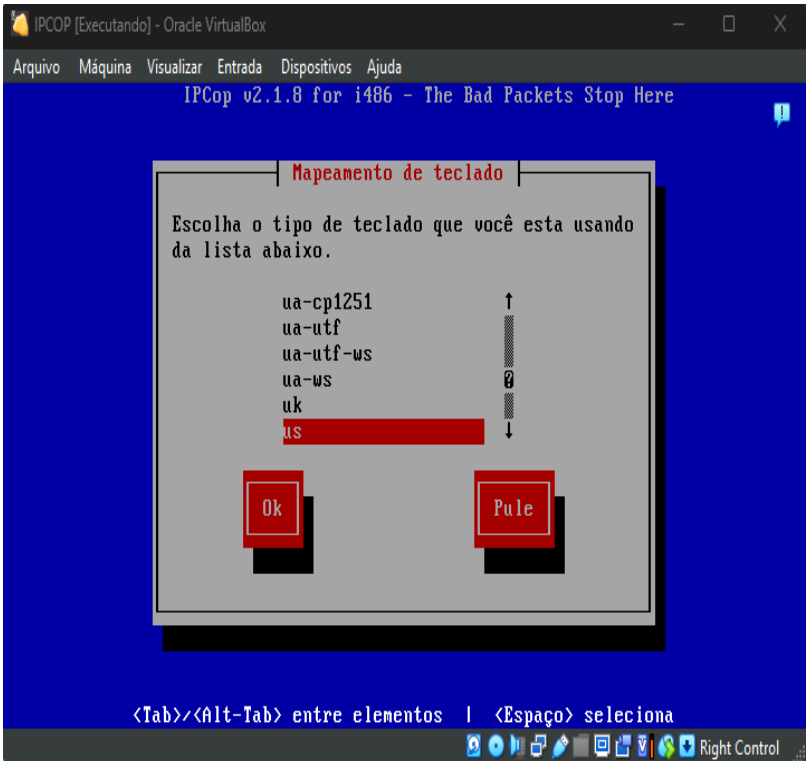
Figura 4 – Tela de instalação



Fonte: autoria própria, 2024

Após essa etapa, aparecerá uma tela para escolher o tipo de teclado que está sendo usado. O IPCop oferece várias opções de *layout* de teclado, permitindo que possa selecionar o mais adequado para o seu uso. Escolha a opção correta para garantir que a digitação durante a instalação seja feita corretamente, como mostrado na Figura 5.

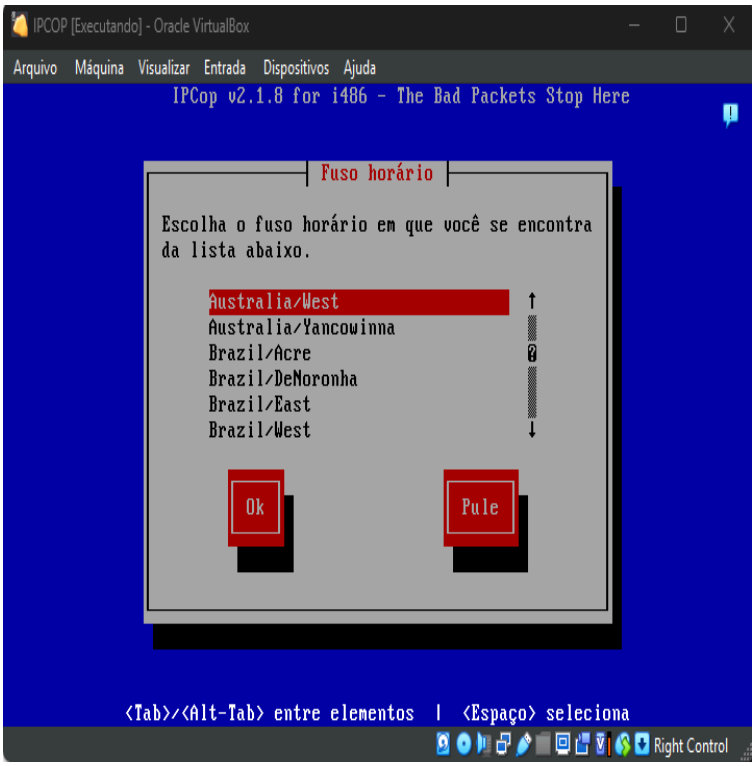
Figura 5 – Tela de seleção do teclado



Fonte: autoria própria, 2024

Após a escolha do tipo de teclado, a próxima tela que se encontrará durante a instalação do IPCop será a de seleção do fuso horário. Nessa etapa, o sistema pede que seja escolhida a região e o fuso horário onde está localizado, garantindo que a hora e a data sejam configuradas corretamente no sistema, como mostrado na Figura 6.

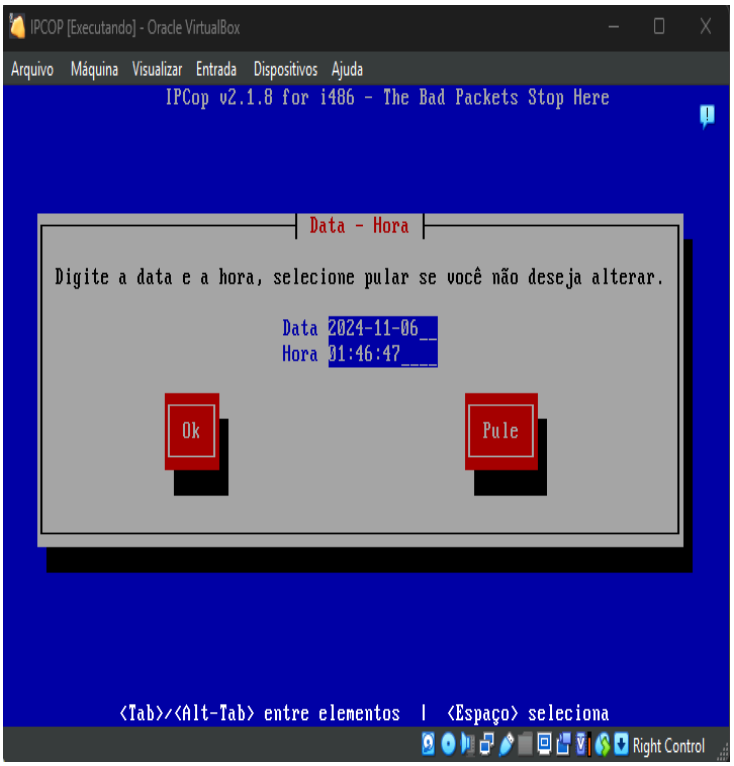
Figura 6 – Tela de seleção do fuso horário



Fonte: autoria própria, 2024

Após a seleção do fuso horário, o IPCop exibirá uma tela para se ajustar manualmente a data **e** hora do sistema, caso deseje. Essa etapa permite que se insira a data e hora exatas, o que pode ser útil caso não queira confiar no relógio de hardware do computador ou se a sincronização automática não estiver funcionando, como mostra a Figura 7.

Figura 7 – Data e Hora



Fonte: autoria própria, 2024

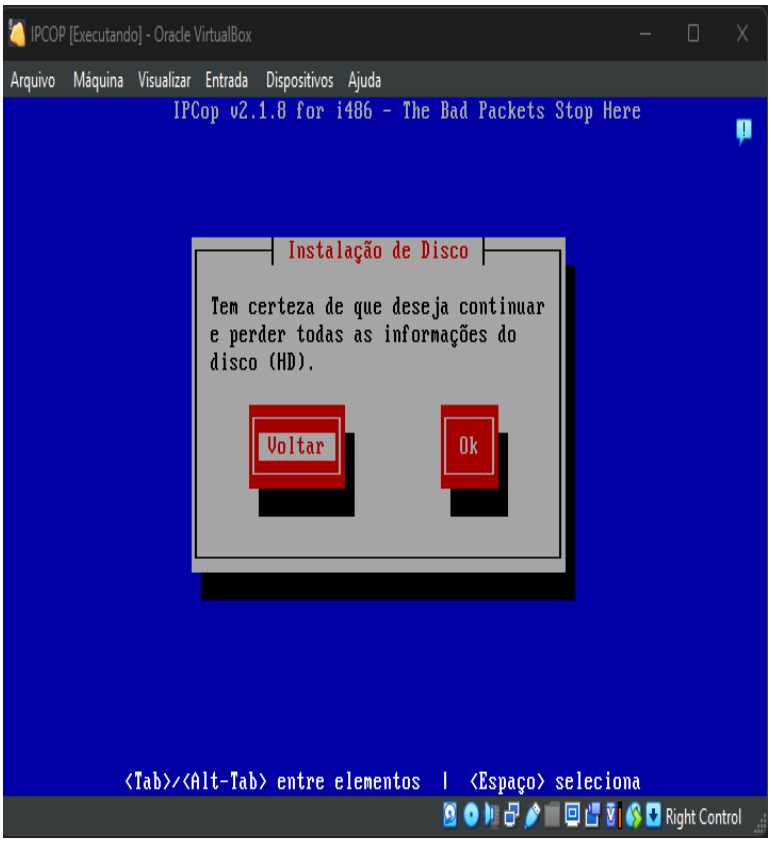
Após a configuração da data e hora, será visto uma tela de instalação do disco no IPCop, na qual serão apresentadas opções de “OK” e “Cancelar”. Nessa etapa, o sistema está pedindo sua confirmação para o início da formatação e instalação do IPCop no disco rígido, como exibido na Figura 8.

Figura 8 – Instalação de Disco

Fonte: autoria própria, 2024

Após a tela de instalação do disco com as opções “OK” ou “Cancelar”, aparecerá uma tela de confirmação. Nessa tela, o IPCop irá exibir um aviso sobre o que acontecerá se caso continuar com a instalação, como a formatação do disco e a remoção de todos os dados existentes, como mostrado na Figura 9.

Figura 9 – Confirmação de Instalação de Disco



Fonte: autoria própria, 2024

Após a tela de confirmação será exibida uma tela com três opções para selecionar o destino da instalação: Disco Rígido, *Flash* e Voltar. Caso escolha a opção Disco Rígido, o IPCop será instalado no disco rígido do computador e todos os dados existentes no disco serão apagados. Se optar por *Flash*, a instalação será feita em um dispositivo USB (*Universal Serial Bus*), como um p*en driv*e, permitindo que o IPCop seja executado a partir do *flash* drive em outros computadores. A opção Voltar permite que se retorne à tela anterior caso queira revisar ou corrigir sua escolha antes de continuar com a instalação, como mostrado na Figura 10.

Figura 10 – Instalação de Disco

Fonte: autoria própria, 2024

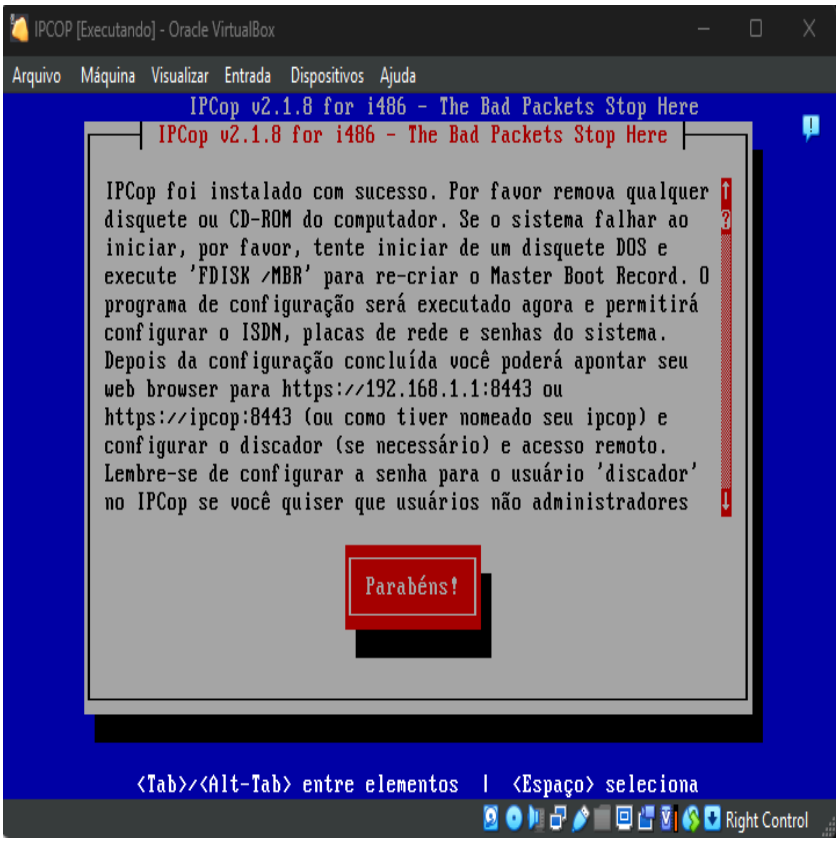
A tela “Restaurar”, conforme mostra a figura 11, serve para escolher alguma forma de *backup*, nesta instalação não será usada esta opção. Utilize a tecla 'TAB' para navegar entre as opções até que a opção 'PULE' seja selecionada.

Figura 11 – Restaurar

Fonte: autoria própria, 2024

A tela a seguir se refere ao IPCop ter sido instalado com sucesso e informa alguns avisos para não ocorrer algum problema futuro, conforme a tela da Figura 12 é exibida abaixo.

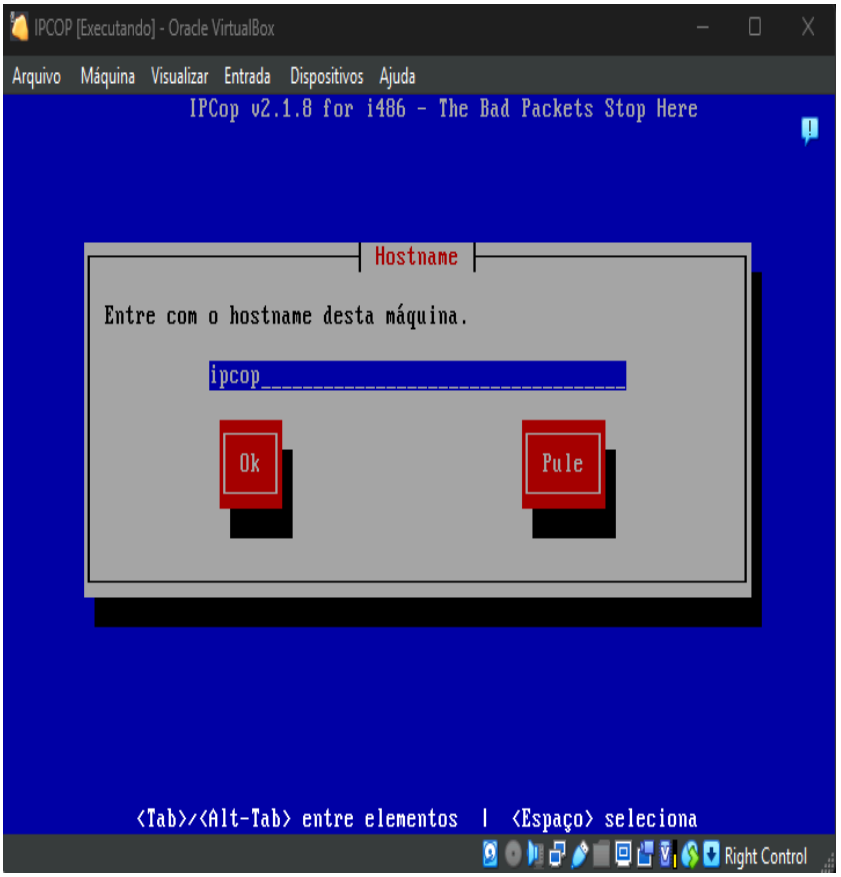
Figura 12 – IPCop instalado com sucesso



Fonte: autoria própria, 2024

Na tela "*Hostname*" é solicitado que se informe o nome do servidor, como mostra a Figura 13. Esse nome será utilizado para identificar o servidor dentro da rede, facilitando sua localização e gerenciamento. Certifique-se de escolher um nome descritivo e único para evitar conflitos ou dificuldades futuras na identificação.

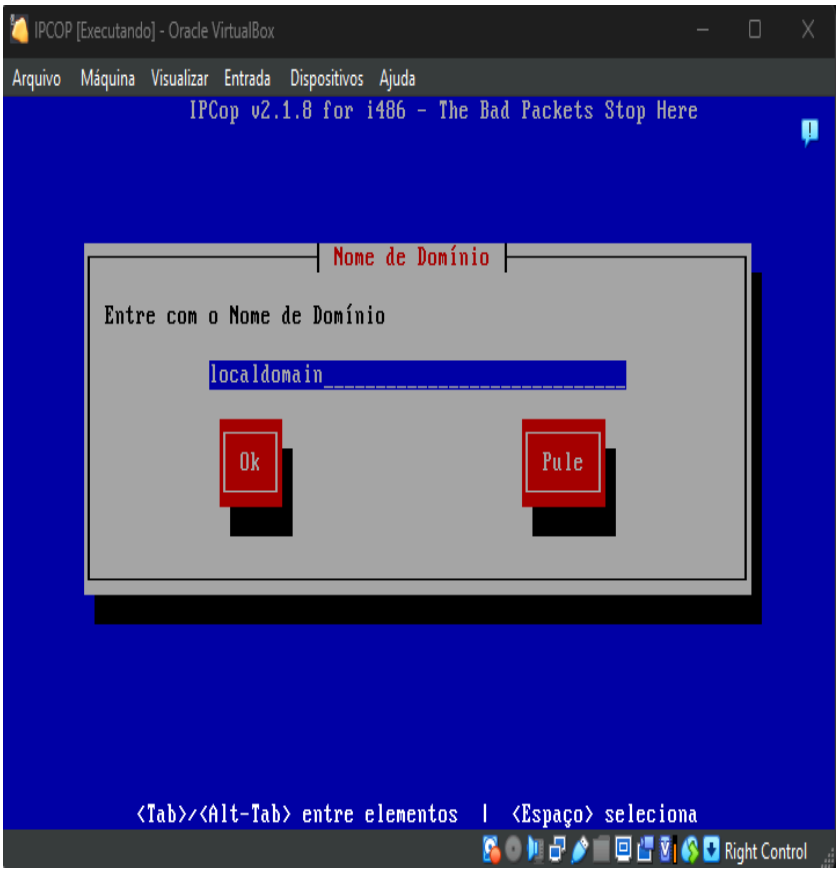
Figura 13 – *Hostname*



Fonte: autoria própria, 2024

Na tela “Nome de Domínio” é solicitado que se informe o domínio que o *Firewall* fará parte, como mostra a Figura 14. Esse domínio é essencial para integrar o Firewall à infraestrutura de rede, garantindo que ele funcione de maneira adequada dentro do ambiente configurado. Certifique-se de inserir o nome do domínio corretamente, pois erros podem impactar a comunicação entre dispositivos na rede.

Figura 14 – Nome de Domínio



Fonte: autoria própria, 2024

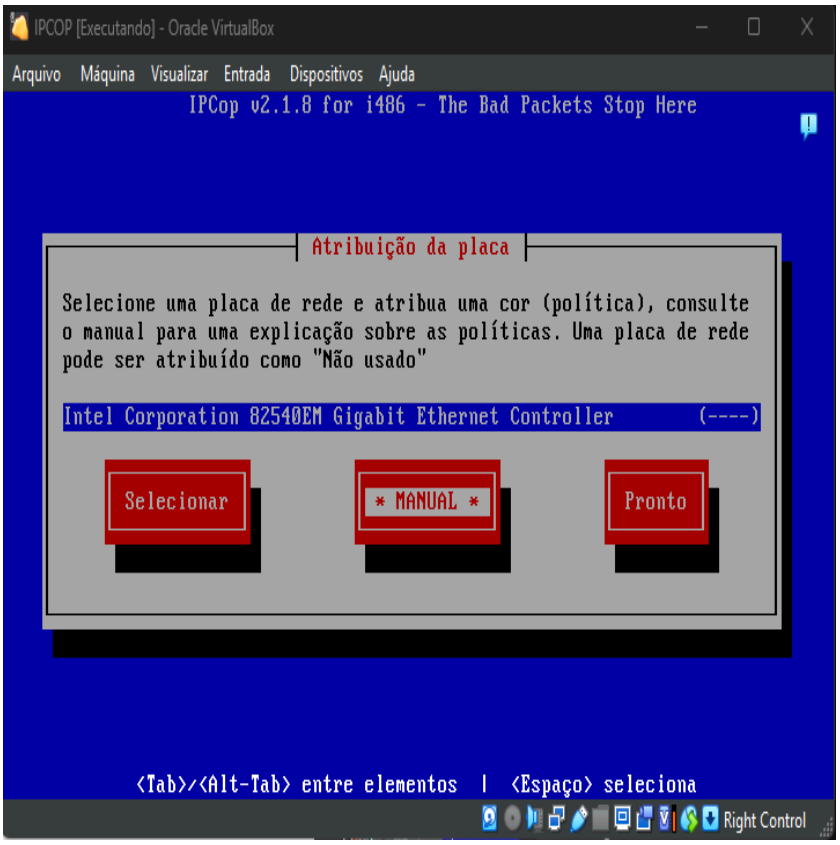
Na tela “Interface *RED*” é solicitado que se informe o tipo de configuração, como mostra a Figura 15. Essa configuração define como a interface será conectada à rede externa, sendo uma etapa crucial para o funcionamento do *Firewall*. Escolha a opção que melhor se adequa à topologia da rede, garantindo que o tráfego externo seja devidamente gerenciado e monitorado.

Figura 15 – Interface *RED*

Fonte: autoria própria, 2024

Na tela “Atribuição da placa” é solicitado que se informe uma placa de rede e a cor, como ilustra a Figura 16. Essa etapa é importante para associar corretamente cada interface física à sua função dentro do sistema. Certifique-se de selecionar a placa correspondente e atribuir a cor de forma consistente com o padrão de configuração adotado na rede, facilitando a identificação e o gerenciamento futuro.

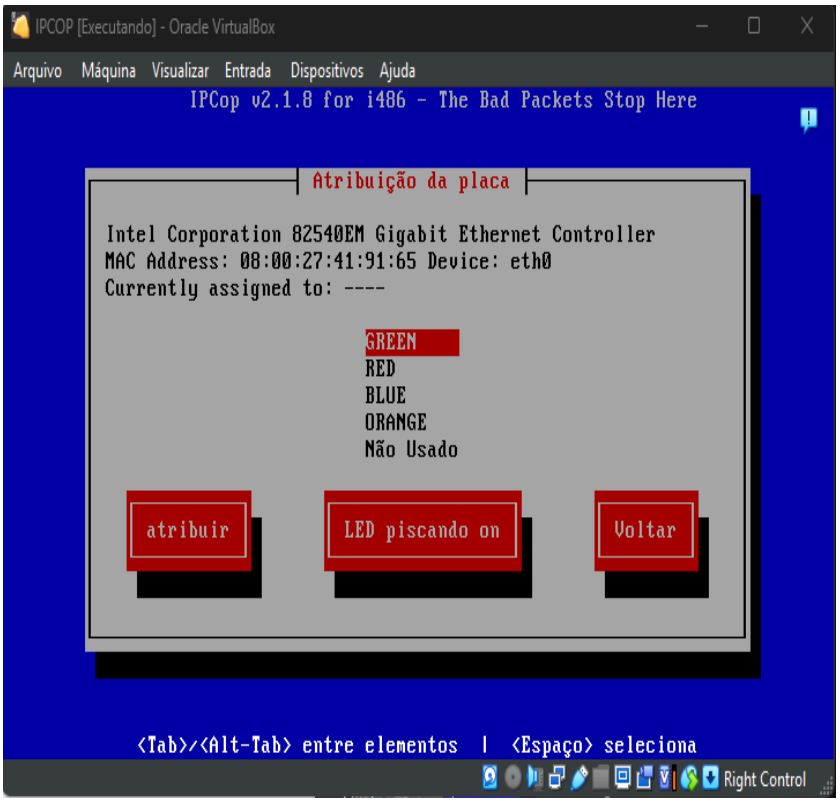
Figura 16 – Atribuição da placa



Fonte: autoria própria, 2024

Na etapa seguinte, exibida na tela “Atribuição da placa”, é requisitada a definição da cor da interface, conforme ilustrado na Figura 17. A escolha da cor é crucial para identificar visualmente a função de cada interface na configuração do sistema. Neste caso, selecione a cor “GREEN”, que representa a área destinada à rede local, onde estão localizados os computadores, impressoras e servidores da organização.

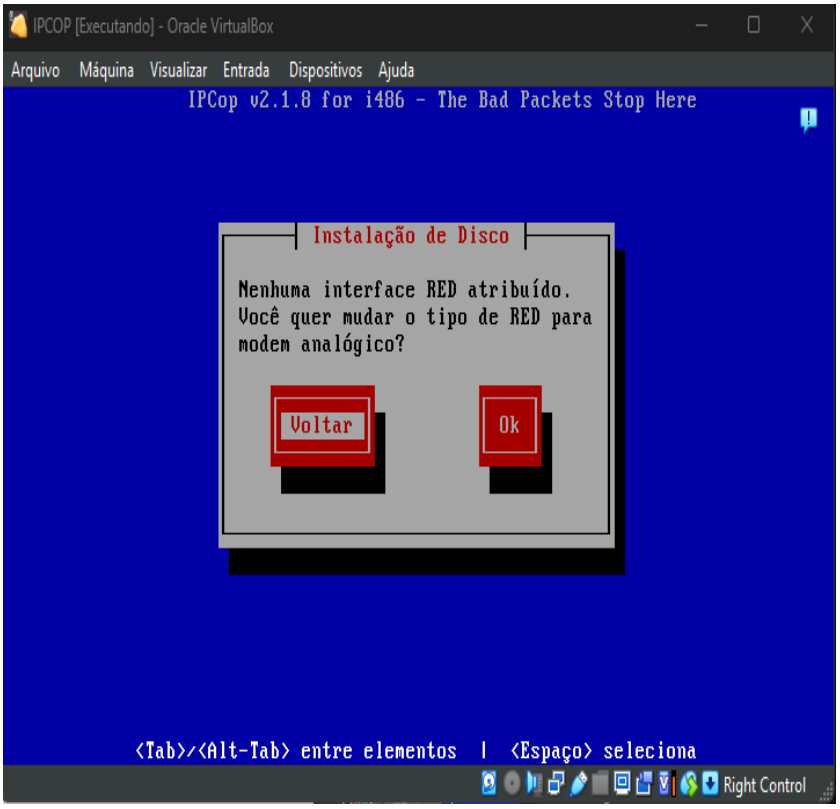
Figura 17 – Atribuição da placa (cor)



Fonte: autoria própria, 2024

Na tela “Instalação de Disco”, será solicitado que você informe se deseja alterar o tipo RED para modem analógico, conforme ilustrado na Figura 18. A cor RED representa a área voltada para o acesso externo à internet, sendo a região onde os dados de fora da rede, como requisições de sites e aplicativos, são recebidos. Caso não seja necessário realizar essa alteração, selecione a opção "Voltar" para retornar à etapa anterior e revisar ou ajustar outras configurações do sistema.

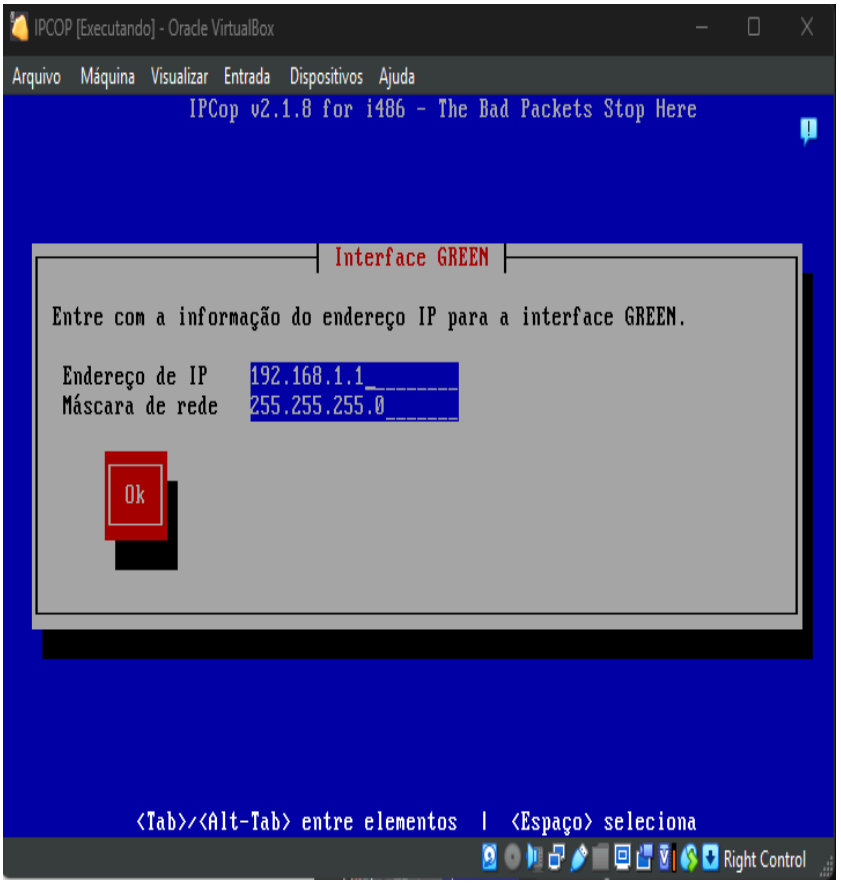
Figura 18 – Instalação de Disco



Fonte: autoria própria, 2024

A tela “Interface *GREEN*” solicitará que sejam digitados o endereço IP e a máscara de rede para a interface *GREEN*, como mostra a Figura 19. Essas configurações são fundamentais para definir a faixa de endereçamento da rede interna e garantir a comunicação adequada entre os dispositivos conectados. Certifique-se de inserir valores válidos e compatíveis com a configuração da sua rede local para evitar conflitos ou problemas de conectividade.

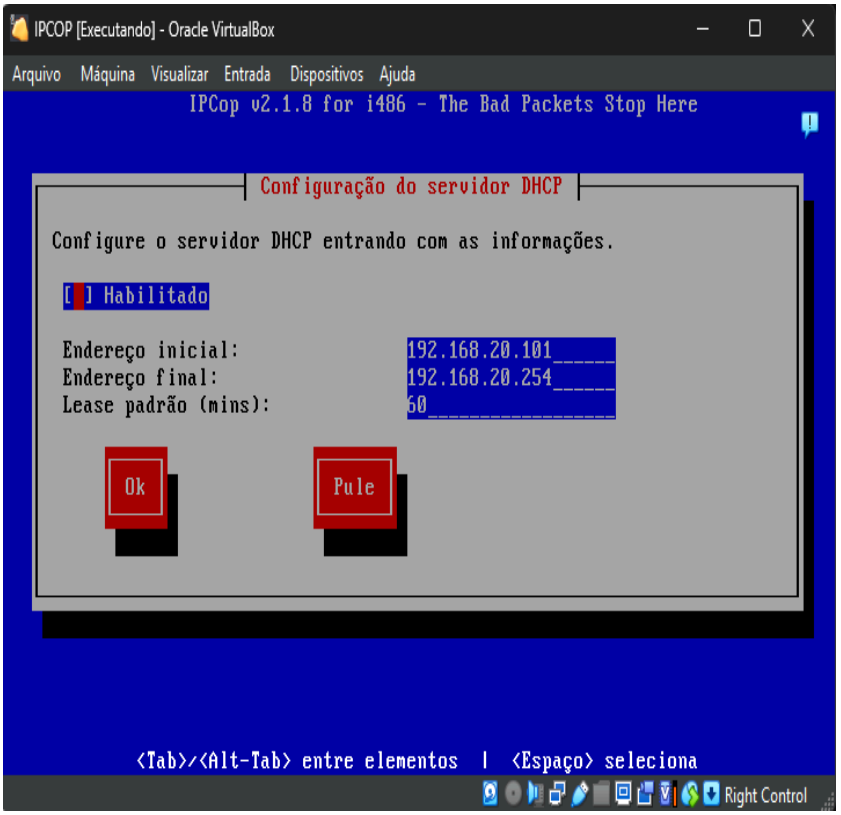
Figura 19 – Interface *GREEN*



Fonte: autoria própria, 2024

A tela “Configuração do servidor DHCP” solicitará que sejam digitados o endereço inicial, o endereço final e o tempo de concessão padrão (em minutos), como mostra a Figura 20. Essas configurações determinam o intervalo de endereços IP que o servidor *Dynamic Host Configuration Protocol* (DHCP) distribuirá automaticamente para os dispositivos na rede, além de especificar o tempo de validade de cada concessão. Certifique-se de definir um intervalo compatível com a faixa de endereços da rede e ajustar o tempo de concessão de acordo com as necessidades operacionais.

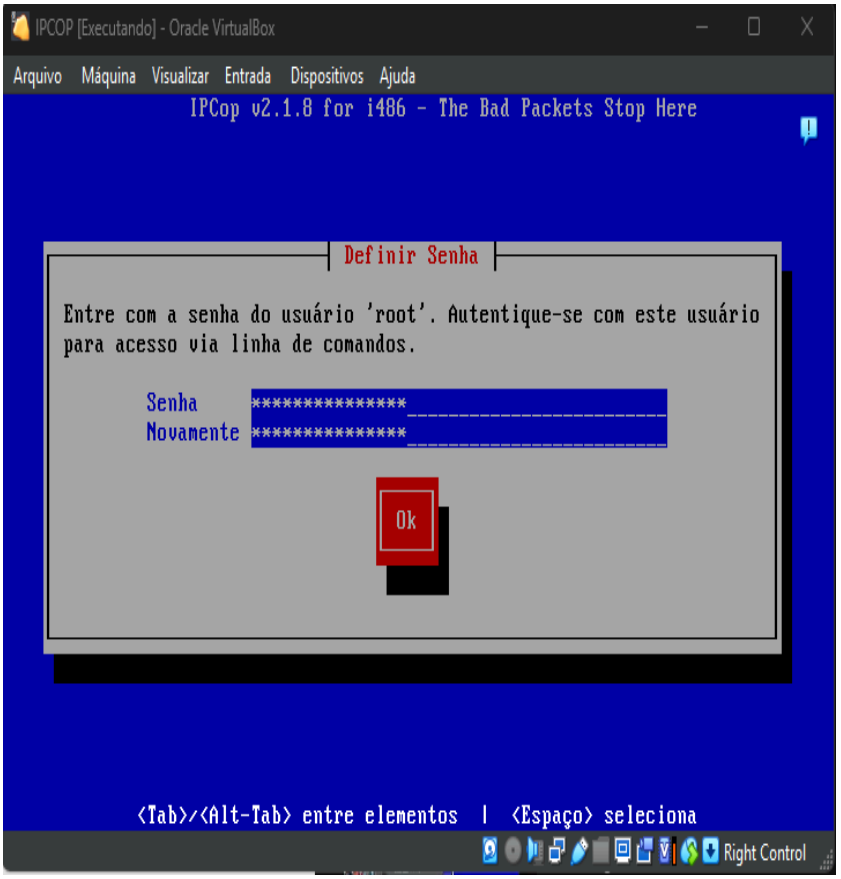
Figura 20 – Configuração do servidor DHCP



Fonte: autoria própria, 2024

A tela “Definir Senha” solicitará que seja digitada uma senha para "*root*", "*admin*" e "*backup*", como mostra a Figura 21. Para evitar o risco de esquecer alguma senha, recomenda-se inserir a mesma senha para todas essas contas. Isso garantirá maior praticidade no gerenciamento, mas lembre-se de escolher uma senha forte e segura para proteger o sistema de acessos não autorizados.

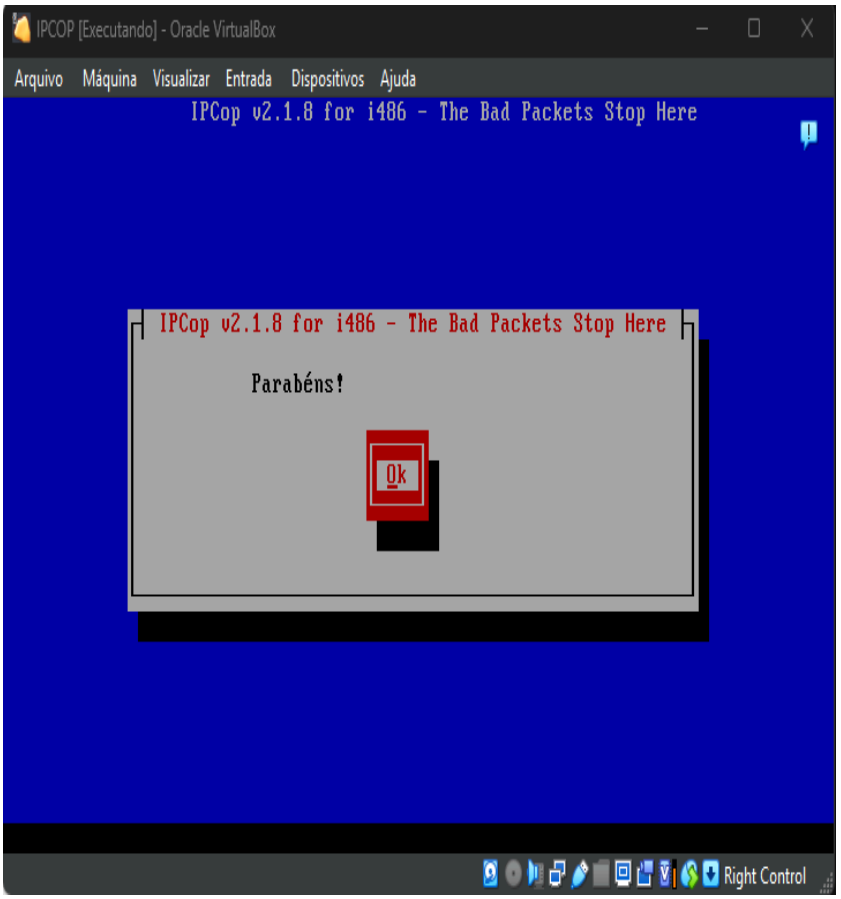
Figura 21 – Definir Senha



Fonte; autoria própria, 2024

A tela “Processo finalizado” mostra que foi finalizado o processo de configuração da interface *GREEN*, como mostra a Figura 22. Isso indica que todas as etapas necessárias para a configuração da interface foram concluídas com sucesso. Agora, a interface *GREEN* está pronta para ser utilizada na rede, permitindo a comunicação entre os dispositivos internos de forma segura e eficiente.

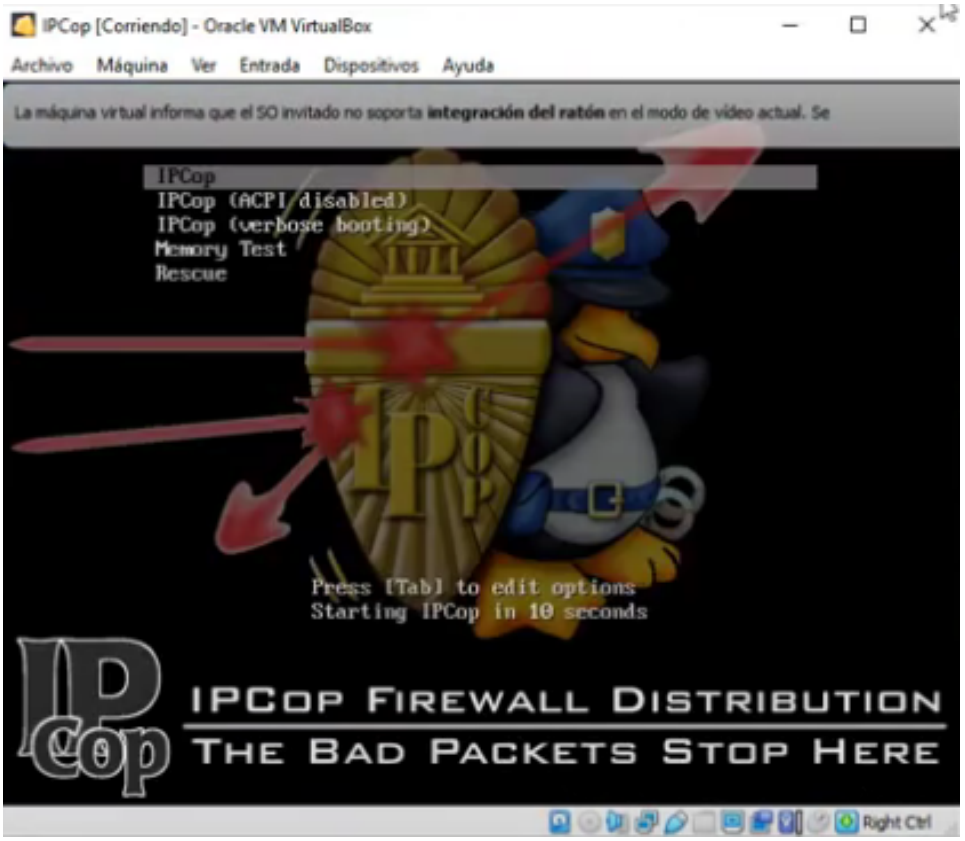
Figura 22 – Processo finalizado



Fonte: autoria própria, 2024

Depois de clicar em “OK”, espere carregar até aparecer a tela da Figura 23. Essa tela indica que o sistema está processando as configurações e, ao ser exibida, confirma que a configuração foi concluída corretamente, permitindo que você avance para as próximas etapas ou comece a utilizar a interface configurada.

Figura 23 – Fechamento do IPCOP



Fonte: autoria própria, 2024

Após a tela de restauração, pode-se fechar a instalação do IPCop e, em seguida, acessar as configurações do sistema. Vá para a aba de rede nas configurações do IPCop e habilite o adaptador 1. Isso é necessário para garantir que o IPCop possa se comunicar com a rede externa e fornecer conectividade à internet.

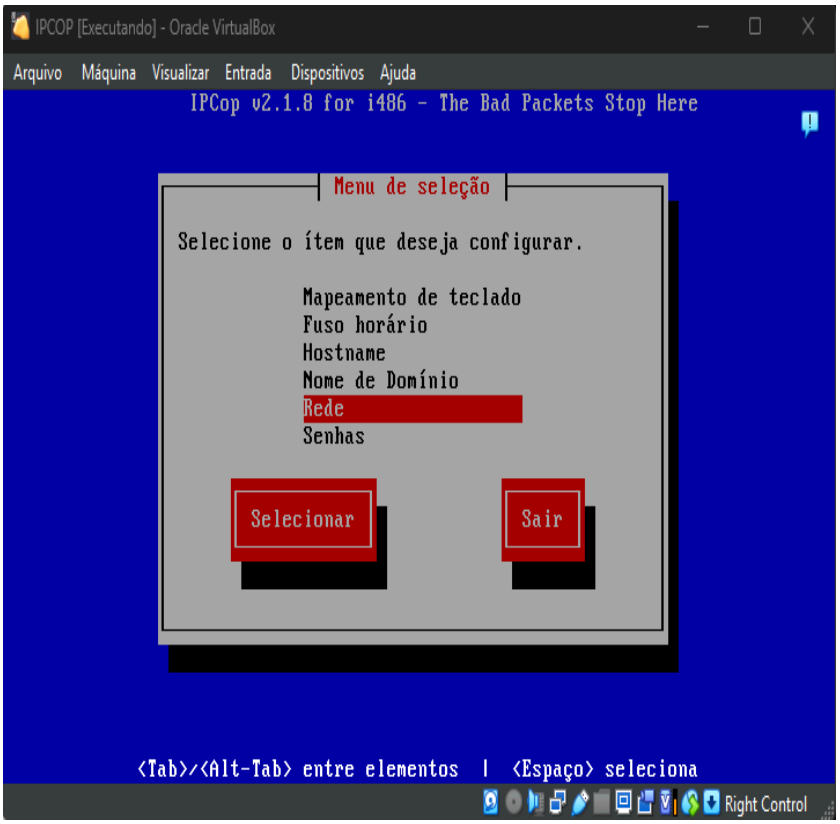
Depois de habilitar o adaptador de rede, reinicie o IPCop. Isso permitirá que o sistema reconheça a interface de rede configurada e o prepare para funcionar corretamente como um *firewall*. O IPCop agora estará pronto para ser utilizado, com as configurações de rede aplicadas e a comunicação de rede funcionando.

Após habilitar o adaptador de rede e reiniciar o IPCop, pode-se ver a tela de login. Quando a tela estiver carregada, continue o processo. O acesso ao sistema requer a autenticação do usuário. Inicialmente, o sistema solicita a inserção do nome de usuário, que, para fins administrativos, é *root*. Em seguida, é solicitada a senha previamente definida durante o processo de instalação.

Depois disso, inicia a linha de comando do IPCop. "Para a configuração inicial do sistema, é necessário utilizar o comando *setup*, seguido da tecla “ENTER”. Esse

procedimento inicia o assistente de configuração, no qual são disponibilizadas opções para o ajuste das configurações adicionais do IPCop, conforme apresentado na Figura 24. Na sequência, deve ser selecionada a opção “Rede” e, posteriormente, a tecla “Selecionar” deve ser pressionada para prosseguir.

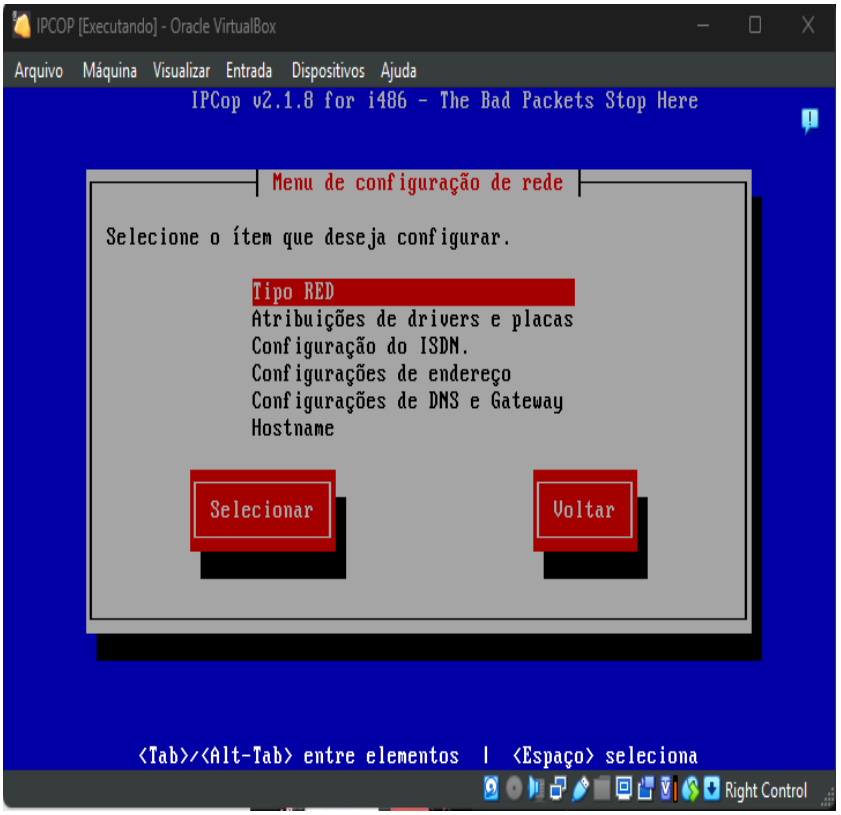
Figura 24 – Menu de Seleção



Fonte: autoria própria, 2024

Em seguida, será mostrada a tela “Menu de configurações de rede” e deve ser selecionado “Tipo *RED*”, como mostra a Figura 25. Essa opção permite configurar as definições da interface RED, que é responsável pela comunicação com a rede externa, garantindo a conectividade com outros sistemas e redes fora do seu ambiente local.

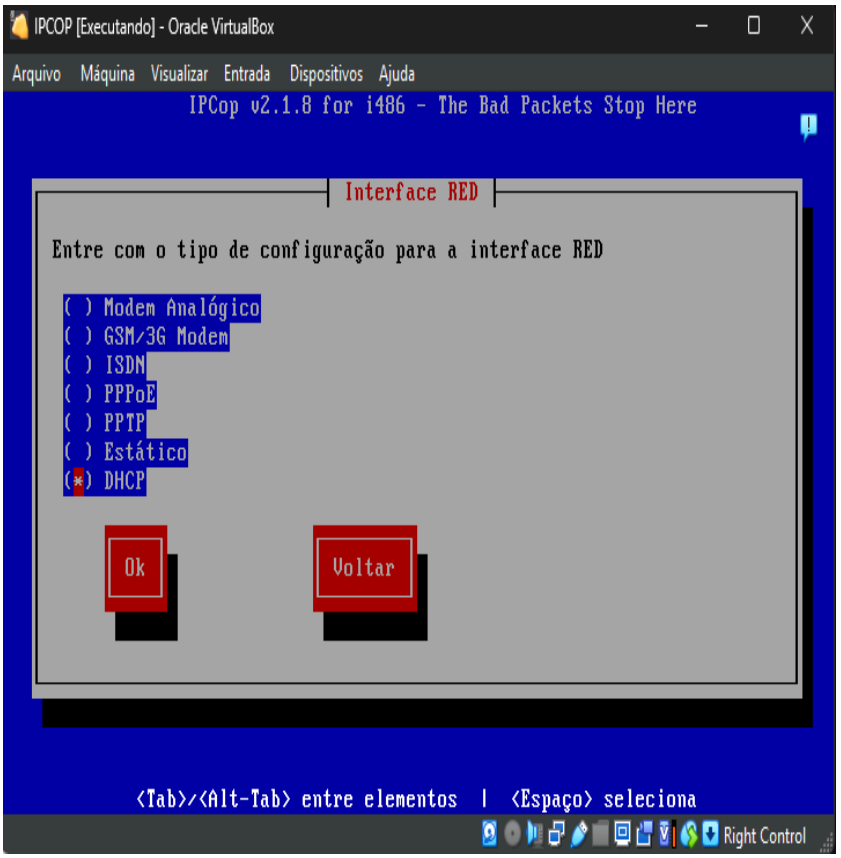
Figura 25 – Menu de configuração de rede



Fonte: autoria própria, 2024

Depois, será apresentada a tela “Interface *RED*” e deve ser selecionado “DHCP” com a tecla “ESPAÇO” e, em seguida, aperte “OK”, como mostra a Figura 26. Selecionando essa opção, o sistema será configurado para receber automaticamente um endereço IP da rede externa, facilitando a conexão com a rede e evitando a necessidade de configuração manual do IP.

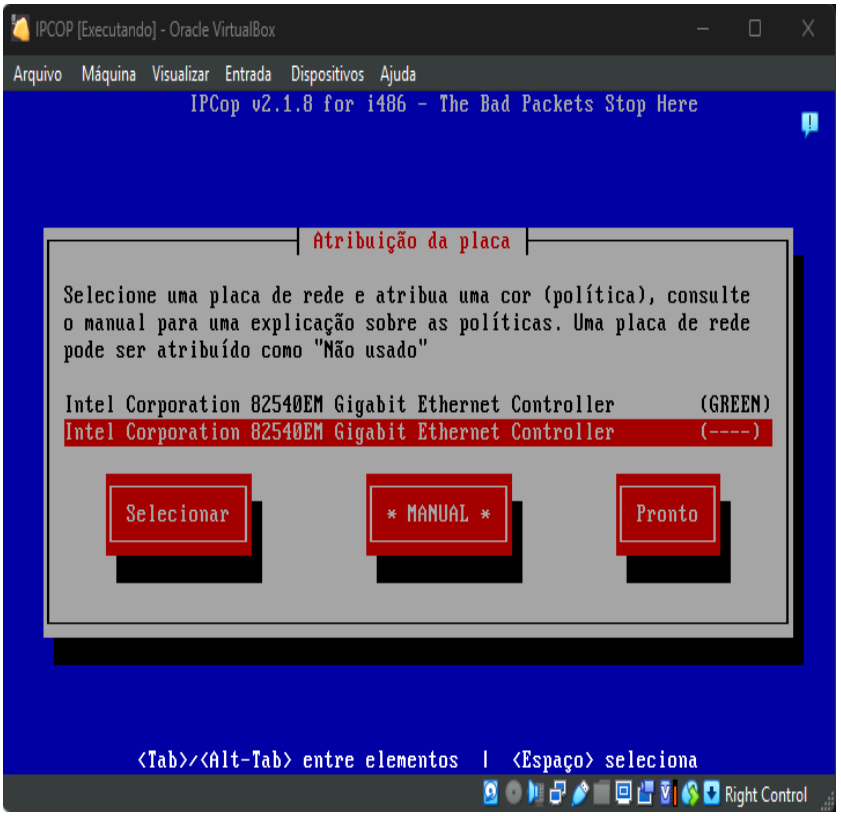
Figura 26 – Interface RED



Fonte: autoria própria, 2024

Na tela “Atribuição de placa”, selecione a opção “*Intel Corporation 82540EM Gigabit Ethernet Controller (----)*” que está vazia, utilizando a tecla “ENTER”, como mostra a Figura 27. Essa ação associará a placa de rede correta ao sistema, permitindo que ela seja configurada adequadamente para a comunicação na rede. Certifique-se de escolher a placa correta para evitar problemas de conectividade.

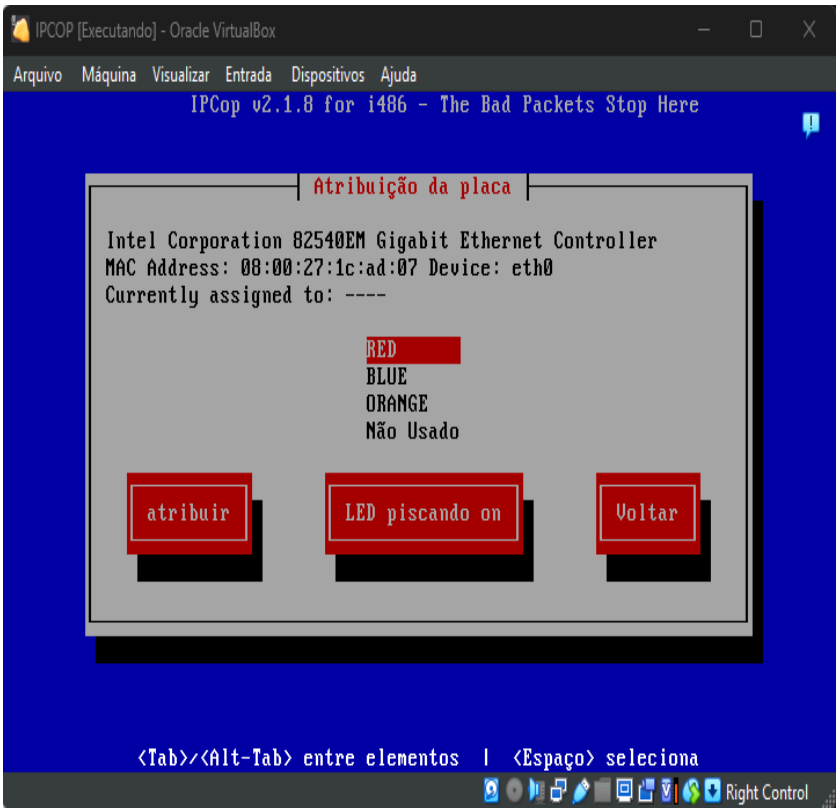
Figura 27 – Atribuição da placa RED



Fonte: autoria própria, 2024

Na tela “Atribuição de placa *RED*”, selecione a opção “*RED*”, como mostra a Figura 28. Isso associará a placa de rede à interface externa, permitindo a configuração da comunicação com a rede externa (internet) ou outras redes fora do seu ambiente local. Certifique-se de que a placa selecionada seja a correta para evitar problemas na conectividade externa.

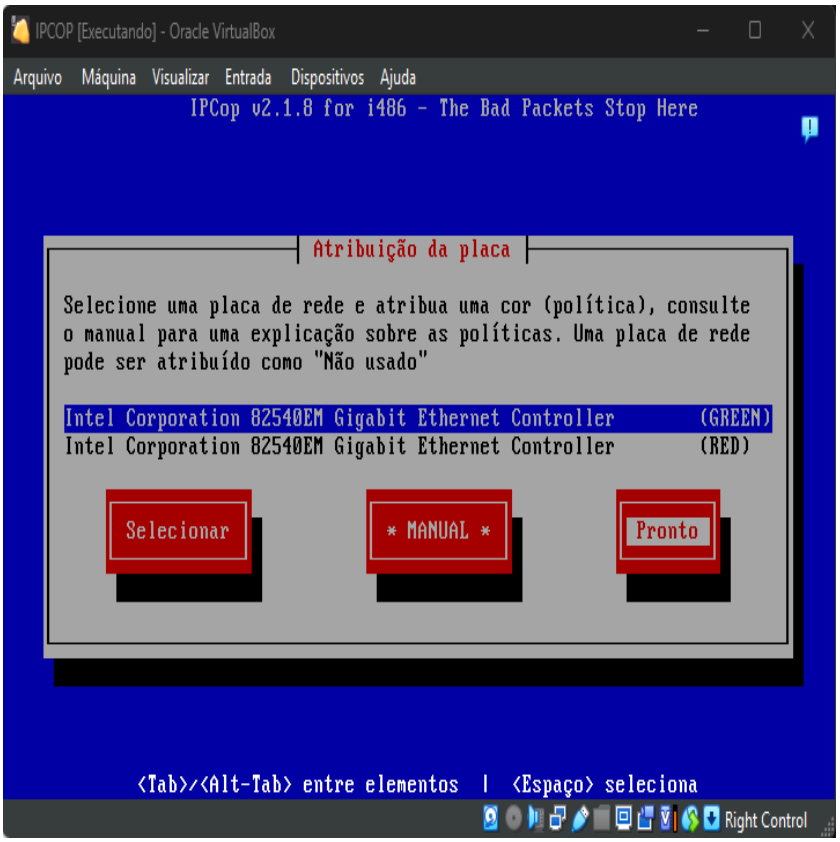
Figura 28 – Atribuição da placa *RED*



Fonte: autoria própria, 2024

Na tela “Atribuição de placa concluída”, selecione a opção “PRONTO”, como mostra a Figura 29. Isso indicará que a configuração da placa foi concluída e que todas as opções necessárias foram selecionadas corretamente. Após essa escolha, o sistema estará pronto para prosseguir com as configurações ou iniciar o funcionamento com a placa atribuída.

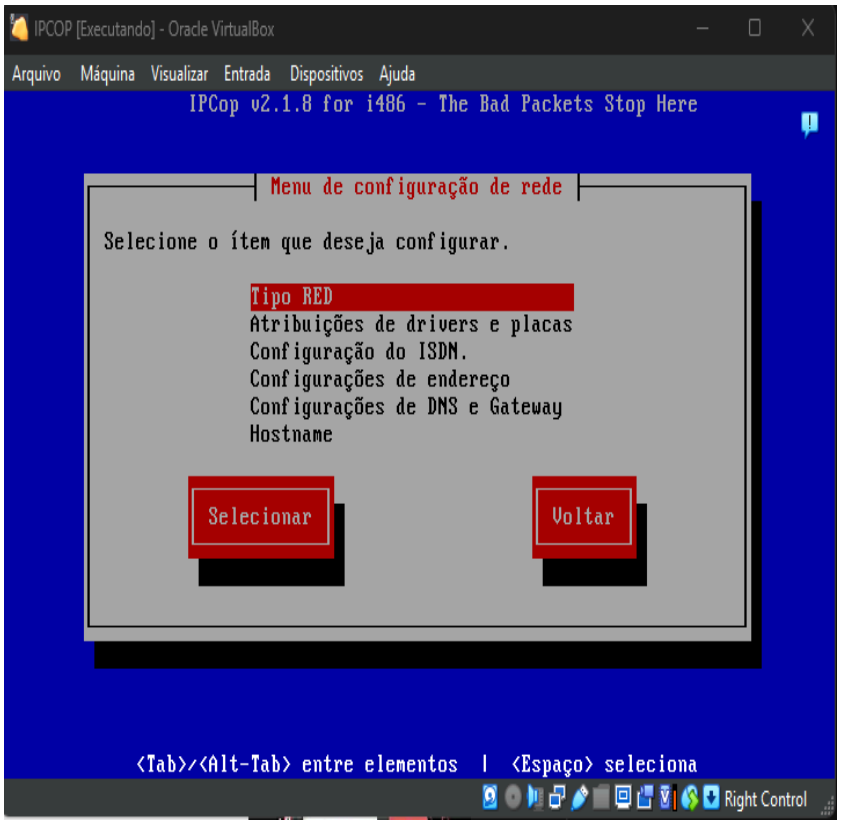
Figura 29 – Atribuição da placa concluída



Fonte: autoria própria, 2024

Na tela “Atribuição de placa”, selecione a opção “Voltar”, como mostra a Figura 30. Essa opção permite retornar à tela anterior para revisar ou ajustar as configurações, caso seja necessário, sem avançar para a próxima etapa.

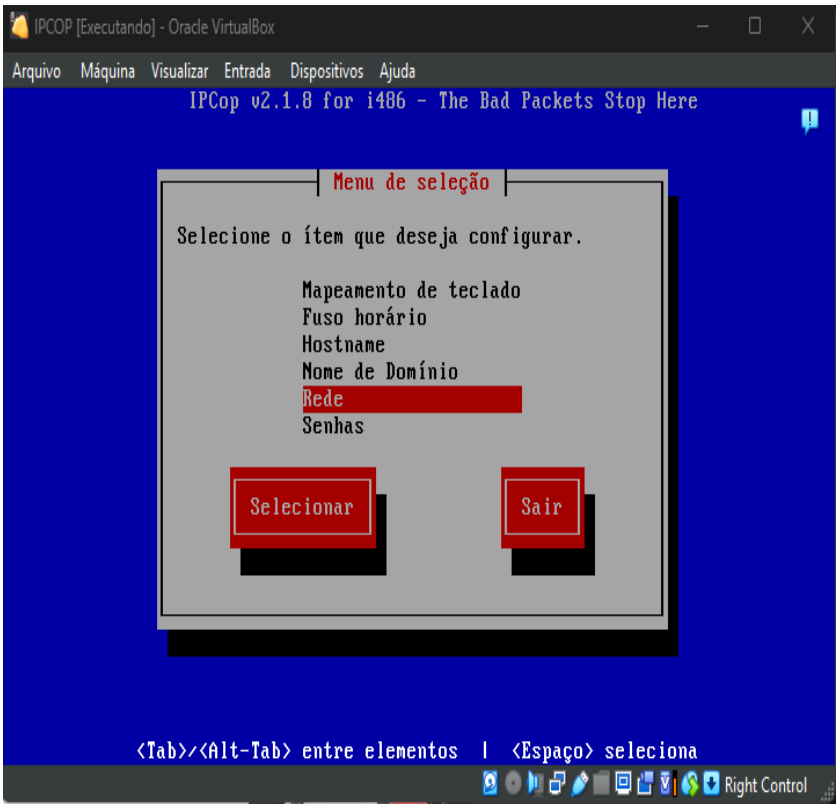
Figura 30 – Menu de configuração de rede



Fonte: autoria própria, 2024

Na tela “Menu de seleção”, selecione a opção “Sair”, como mostra a Figura 31. Essa ação permitirá sair do menu de configurações e finalizar o processo, encerrando a sessão ou retornando ao estado anterior, dependendo do sistema em uso.

Figura 31 – Menu de seleção



Fonte: autoria própria, 2024

Após a etapa “Menu de seleção”, digite no console “init 0” e aperte a tecla “ENTER”. Isso iniciará o processo de desligamento do sistema. Aguarde até que o sistema seja completamente desligado, o que pode levar alguns momentos. Esse comando é utilizado para fazer um desligamento controlado e seguro do sistema operacional.

Agora, a instalação do IPCop foi concluída, assim como todas as configurações realizadas até este momento. O sistema está pronto para ser utilizado, com as interfaces e parâmetros devidamente configurados de acordo com as necessidades da rede.

5 FUNCIONALIDADES DO FIREWALL IPCOP

Todo este capítulo tem sua escrita baseada na referência (IPCop, 2025), que se trata de um documento em inglês, apresentando as funcionalidades do IPCOP.

5.1 Funções da Janela Sistema Home

Para acessar a interface administrativa do IPCop, o usuário precisa abrir um navegador e digitar o endereço IP ou Internet Protocol da interface verde ou o nome do *host*, sempre utilizando a porta segura 8443 (https). Com a versão 2.0.0, o IPCop desativou o redirecionamento das portas 81 e 445, reforçando a obrigatoriedade do uso de conexões criptografadas. Caso necessário, o administrador pode alterar a porta *HyperText Transfer Protocol Secure* (HTTPS) usando a ferramenta *setreservedports* pela linha de comando. Após o login com o usuário *admin* e a senha configurada durante a instalação, o sistema direciona para a página inicial da interface gráfica, onde é possível começar a gerenciar as funções do IPCop, conforme está sendo exibido na Figura 32.

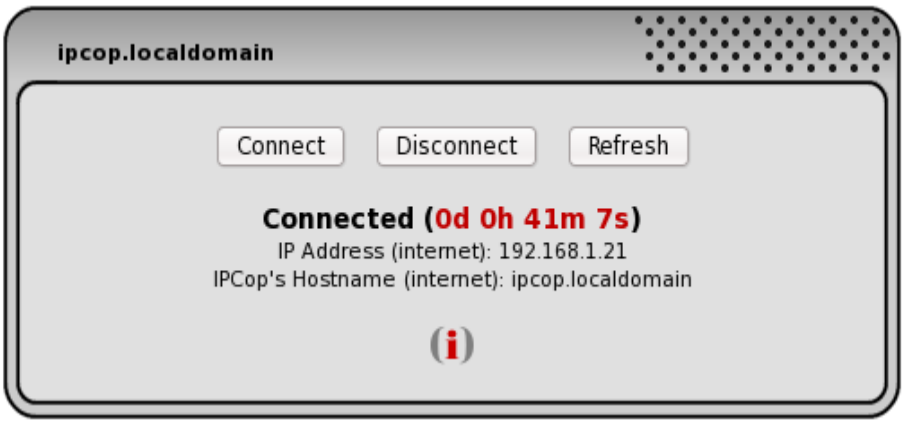
Figura 32 – Janela *Home*

Fonte: IPCop, 2025

A interface administrativa é composta por menus no topo da tela que permitem configurar o sistema, verificar o status da rede, administrar serviços, ajustar regras de firewall e VPNs, além de visualizar os registros de atividade do sistema. No rodapé, o usuário encontra informações úteis como o status da conexão, data e hora atuais, e a versão do IPCop. Também há links rápidos para recursos adicionais do projeto e para o site oficial. A aparência da página inicial pode mudar conforme a configuração da rede, como no caso de conexões via Ethernet RED, onde não é exibido um perfil de conexão.

Outro destaque da interface é o painel de controle da conexão com a Internet, que exibe o status atual e oferece três botões principais: *Connect*, para iniciar uma conexão; *Disconnect*, para encerrá-la; e *Refresh*, que atualiza a página. Abaixo desses botões, é mostrado o perfil de conexão em uso e o estado atual, que pode indicar se está ocioso, tentando discar, conectado ou aguardando atividade para se conectar automaticamente. Quando a conexão está ativa, o tempo é exibido em dias, horas, minutos e segundos, permitindo um controle detalhado por parte do administrador, conforme mostra a Figura 33 e a Figura 34.

Figura 33 – Janela Conexão



Fonte: IPCop, 2025

Figura 34 – Janela Conexão Local

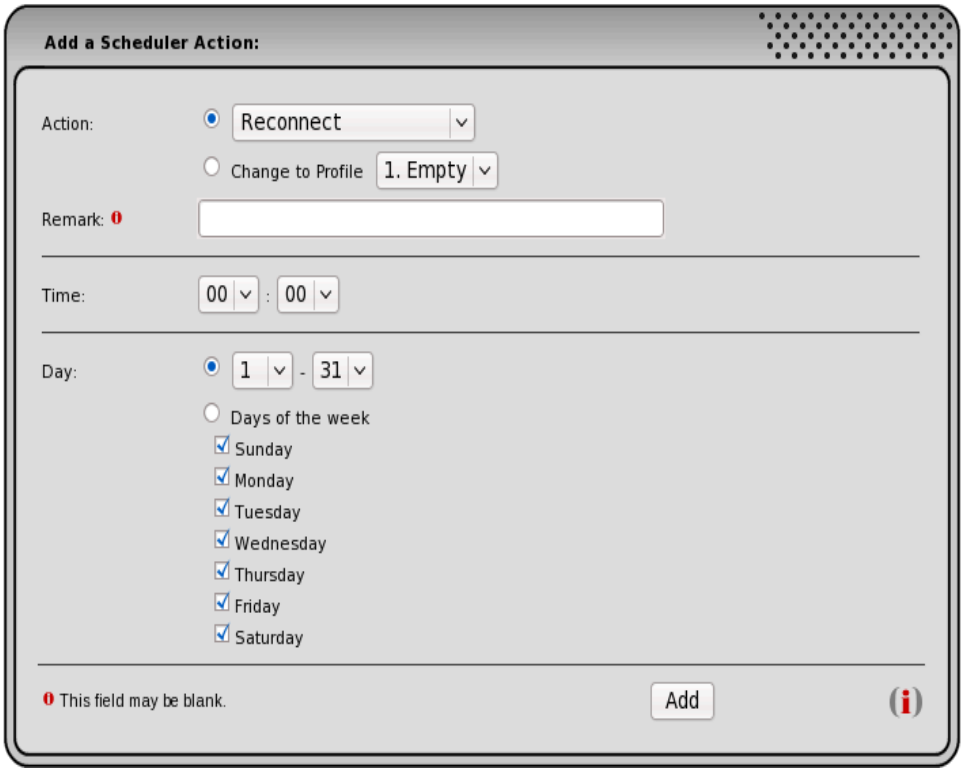
Fonte: IPCop, 2025

Além disso, o IPCop conta com dois tipos de usuários para acesso à interface web: o *admin*, que possui permissão total sobre as configurações, e o *dial*, que está desativado por padrão e permite apenas conectar ou desconectar a Internet. A partir da versão 2.0.0, tornou-se obrigatório fazer autenticação antes de acessar qualquer página da interface, incluindo as iniciais, garantindo maior segurança no gerenciamento do sistema.

5.2 *Scheduler*

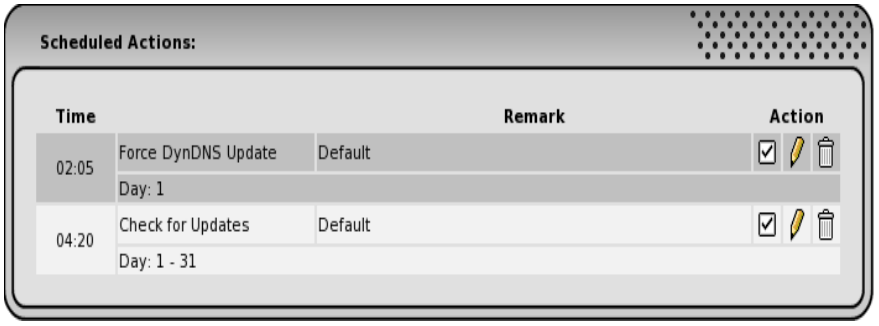
A seção *Scheduler* do IPCop é destinada à programação de eventos automáticos no sistema. Nela, o usuário encontra duas áreas principais: a primeira serve para adicionar ou editar eventos, e a segunda exibe a lista de eventos já programados. Para criar um novo agendamento, basta escolher uma ação, definir o horário e o dia, e clicar no botão Adicionar. Assim que feito, o evento aparece na lista abaixo já ativado e pronto para execução automática conforme a programação, conforme é exibido na Figura 35 e Figura 36.

Figura 35 – Janela *Scheduler*



Fonte: IPCop, 2025

Figura 36 – Janela *Scheduled Actions*



Fonte: IPCop, 2025

Entre as ações disponíveis estão opções como conectar ou desconectar da internet, reiniciar ou desligar o sistema, forçar uma atualização do serviço *Dynamic Domain Name System* (DynDNS), buscar por atualizações ou ainda mudar para um perfil de conexão diferente. Para essa última função, é necessário ter outros perfis previamente configurados na

área de administração do discador. Versões mais recentes do IPCop também permitem agendar ações específicas para VPNs IPsec e OpenVPN, além de verificar atualizações de listas negras usadas pelo filtro de URLs.

Ao adicionar um evento, o administrador pode ainda incluir uma observação descritiva, facilitando a identificação do propósito daquele agendamento. Vale destacar que o sistema já vem com alguns eventos padrão configurados de fábrica, para auxiliar no gerenciamento inicial do IPCop sem necessidade de personalização imediata. Essa flexibilidade torna a função de *Scheduler* uma ferramenta poderosa para automações rotineiras no ambiente de rede.

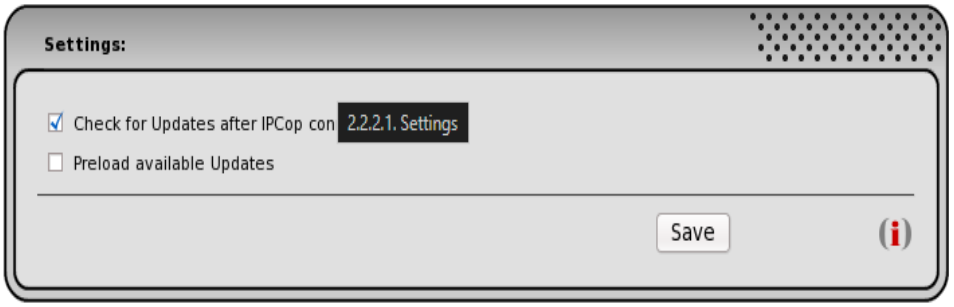
A gestão dos eventos programados é simples: para editar, basta clicar no ícone do lápis amarelo (Figura 36), o que carrega os dados do evento na área de edição acima, permitindo alterações e posterior atualização. Para ativar ou desativar um evento, o administrador clica na caixa de seleção da coluna Ação — o ícone muda para indicar o estado ativo ou inativo. Caso queira remover completamente um evento, é só clicar no ícone da lixeira correspondente.

5.3 *Updates*

A seção *Updates* do IPCop é destinada à manutenção do sistema, permitindo que administradores façam o *download* e a aplicação de atualizações e correções. Essa funcionalidade é essencial para garantir que o sistema esteja sempre protegido contra vulnerabilidades e equipado com melhorias mais recentes. A interface é simples e oferece um acesso rápido às atualizações disponíveis diretamente pela administração web do IPCop.

Logo no início da página, existe uma área chamada *Settings*, onde o administrador pode configurar a verificação automática por novas atualizações. Além disso, é possível habilitar a opção para que o sistema baixe essas atualizações em segundo plano, sem interromper o funcionamento normal da rede. Essa automação facilita a gestão contínua do IPCop e assegura que o ambiente de rede permaneça atualizado com o mínimo de intervenção manual, como mostra a Figura 37.

Figura 37 – *Settings*

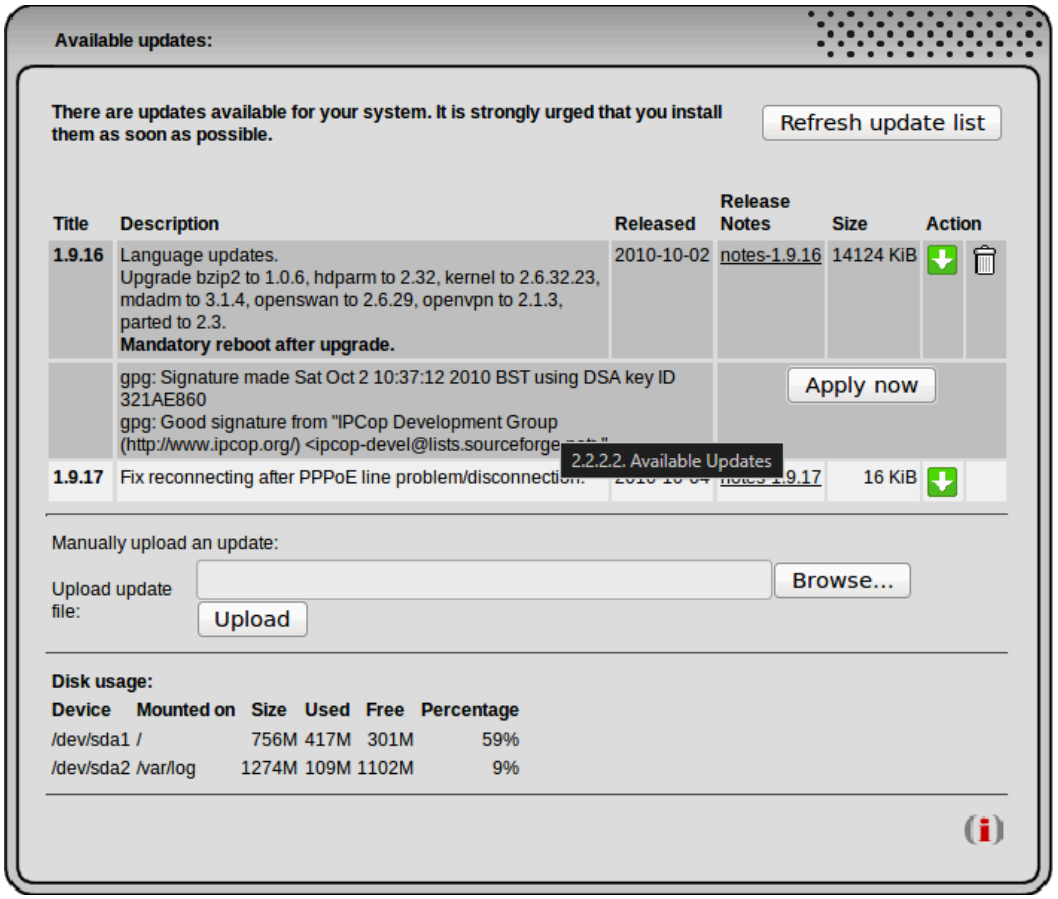


Fonte: IPCop, 2025

Com essas opções, o IPCop oferece mais praticidade e segurança para quem administra redes pequenas ou médias. A possibilidade de programar e baixar atualizações automaticamente ajuda a manter o sistema sempre em conformidade com as últimas versões e correções, reduzindo o risco de falhas e melhorando a performance da solução.

Na seção de atualizações do IPCop, os administradores encontram a opção "*Check for Updates after IPCop connects"*, que controla se o sistema deve buscar por novas atualizações sempre que se conectar à Internet. Caso o usuário queira desativar essa função — também chamada de *"Phone Home"* —, basta desmarcar essa opção. No entanto, para desligá-la completamente, é necessário também desativar ou excluir qualquer evento agendado que esteja configurado para checar por atualizações automaticamente, como mostra a Figura 38.

Figura 38 – *Available Updates*



Fonte: IPCop, 2025

Para quem opta por desabilitar essa verificação automática, é altamente recomendado manter-se informado sobre novas atualizações assinando a lista de e-mails *ipcop-announce*. Isso garante que, mesmo sem a função automática ativa, o administrador não perca avisos importantes sobre melhorias de segurança ou correções críticas do sistema.

Outro recurso disponível é a opção *Preload available Updates*, que permite que o sistema faça o *download* prévio das atualizações assim que forem detectadas, sem aplicá-las imediatamente. Isso facilita a preparação para futuras manutenções, pois os arquivos já estarão armazenados no IPCop, aguardando apenas a autorização do administrador para serem instalados no momento mais conveniente.

Além disso, a página exibe uma lista com todas as atualizações disponíveis (Figura 38), cada uma acompanhada de links que permitem tanto visualizar as notas de lançamento quanto baixar diretamente os pacotes de atualização para o IPCop. Após configurar as preferências, é importante clicar no botão "*Save*" para garantir que as alterações sejam

registradas no sistema.

Quando configurado para isso, o IPCop automaticamente verifica se há novas atualizações disponíveis toda vez que se conecta à Internet. No entanto, o administrador também pode realizar essa verificação manualmente a qualquer momento clicando no botão *Atualizar lista de atualizações*. Se uma nova atualização estiver disponível, ela será exibida na tela com uma breve descrição e um botão para iniciar o download do arquivo necessário.

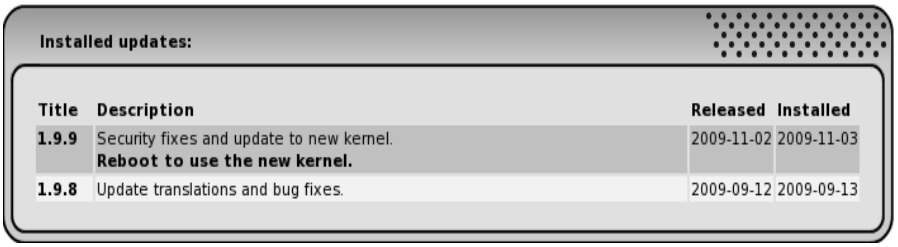
Para baixar a atualização diretamente para o IPCop, basta clicar no ícone de download correspondente. O arquivo, no formato *.tgz.gpg*, será transferido e, após a verificação da assinatura digital, o botão *Aplicar agora* ficará disponível. A partir daí, o administrador pode clicar nesse botão para iniciar a aplicação da atualização de forma automática pelo sistema.

Como alternativa, existe também um método manual para atualizar o IPCop. Neste caso, o arquivo de atualização deve ser baixado primeiro para um computador local, usando um navegador web. O arquivo pode ser obtido na página do projeto no Sourceforge. Uma vez salvo no PC, o próximo passo é usar a seção *Enviar arquivo de atualização* na interface do IPCop para carregar o arquivo para o sistema.

Após selecionar o arquivo com o botão "*Procurar…"* e clicar em "*Enviar"*, o arquivo é transferido para o IPCop. Se o upload for bem-sucedido e a assinatura for validada, o botão "*Aplicar" agora* será exibido, permitindo a instalação da atualização. Dessa forma, o sistema oferece tanto um método direto quanto um processo manual para dar flexibilidade ao administrador.

A seção *Installed Updates* do IPCop exibe uma lista com todas as atualizações que já foram aplicadas ao sistema. Isso permite que o administrador acompanhe facilmente o histórico de correções e melhorias implementadas, garantindo um controle mais rigoroso sobre o estado atual do *firewall,* como mostra a Figura 39.

Figura 39 – *Installed Updates*



Fonte: IPCop, 2025

É importante destacar que o IPCop só aceita a instalação de atualizações oficiais, que são assinadas digitalmente com *GNU Privacy Guard* (GPG). Isso protege o sistema contra a aplicação de arquivos não autorizados ou maliciosos. Além disso, algumas dessas atualizações podem exigir que o IPCop seja reiniciado, por isso é fundamental ler com atenção todas as informações incluídas nas notas de cada patch antes de executar a instalação.

Caso o administrador se depare com o erro “Esta não é uma atualização autorizada”, uma possível causa pode ser que o relógio do sistema esteja com a data incorreta. Isso acontece porque a verificação da assinatura digital considera a data de validade do arquivo, e um relógio desatualizado pode gerar um conflito.

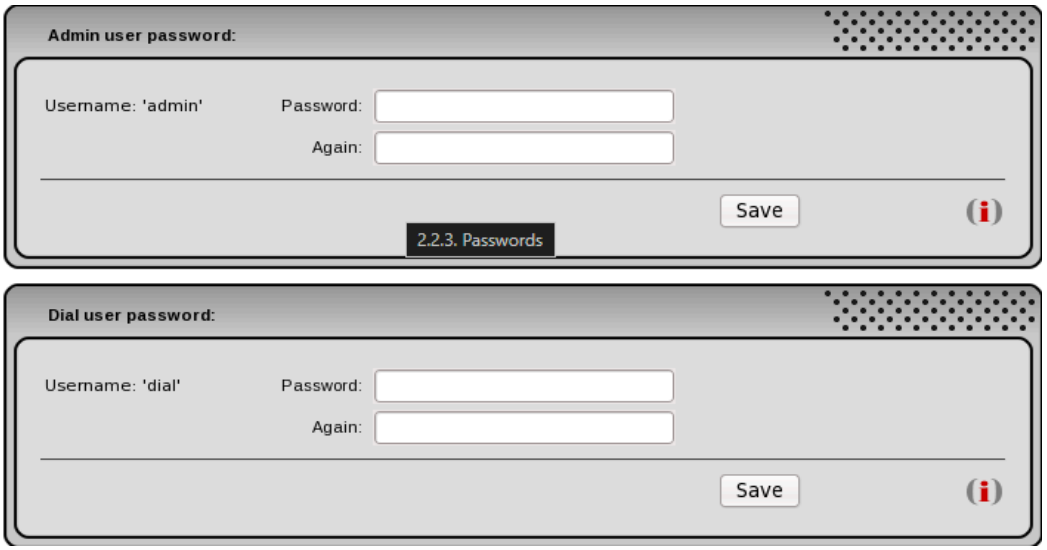
Para resolver esse tipo de problema, recomenda-se verificar o arquivo de log localizado em */var/log/httpd/error_log*. Vale lembrar que o IPCop, por ser frequentemente instalado em hardware mais antigo, pode sofrer com falhas na bateria interna, o que afeta o funcionamento correto do relógio do sistema.

5.4 Passwords

A seção de senhas do IPCop permite que o administrador altere as credenciais dos usuários principais do sistema. Os usuários que podem ter suas senhas atualizadas por essa interface são o *admin*, que possui acesso total às configurações, e o *dial*, que tem permissões restritas, úteis em conexões discadas.

Para modificar a senha de um desses usuários, basta preenchê-la duas vezes nos campos correspondentes e clicar em “*Salvar”*, como mostra na Figura 40. No caso do usuário *dial*, ao definir uma senha, sua conta é automaticamente ativada. Esse usuário pode apenas conectar e desconectar a internet pela interface principal do IPCop, sem permissão para alterar nenhuma configuração sensível.

Figura 40 – Passwords



Fonte: IPCop, 2025

Além dos usuários acessíveis pela interface gráfica, o IPCop também conta com os usuários *root* e *backup*, que exigem um procedimento diferente para alteração de senha. É necessário acessar o console do sistema, fazer login como *root*, e executar o comando "$ setup". A partir daí, é possível selecionar a opção de senhas e alterar a do *root* ou *backup* diretamente.

Todas as senhas definidas no IPCop devem conter pelo menos 6 caracteres, como medida mínima de segurança. Essa exigência ajuda a proteger o sistema contra acessos não autorizados e reforça a importância de utilizar senhas fortes para garantir a integridade e estabilidade do *firewall*.

5.5 *SSH Access*

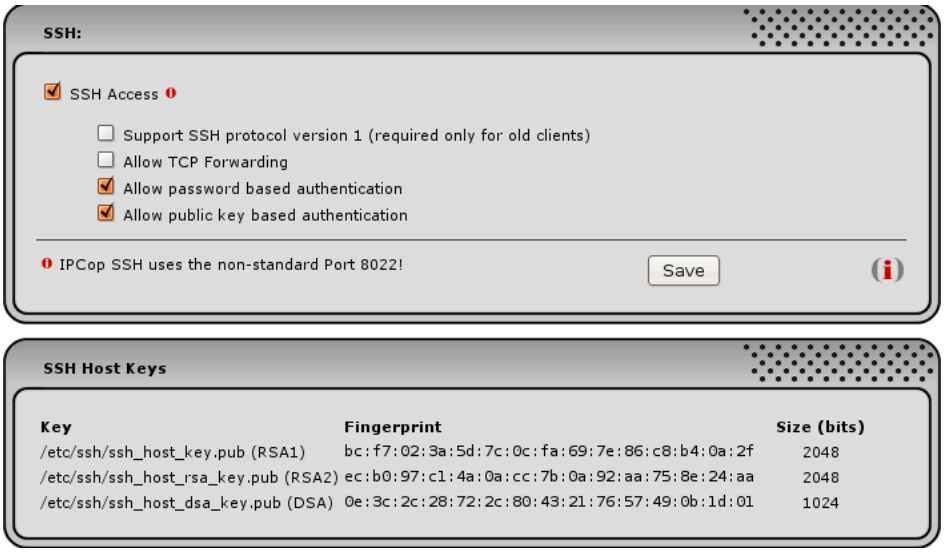
A seção de acesso *Secure Shell* (SSH) do IPCop permite habilitar ou desabilitar a possibilidade de gerenciamento remoto via protocolo SSH. Essa funcionalidade é útil para administradores que precisam acessar o sistema de forma segura, mesmo à distância, mas é desabilitada por padrão por questões de segurança.

Ao marcar a opção correspondente na interface, o acesso remoto por SSH é ativado. A partir dessa página, também é possível configurar diversos parâmetros do serviço SSH, permitindo ajustes finos conforme as necessidades da rede. Entretanto, recomenda-se habilitar essa função apenas temporariamente, enquanto for necessária, e desativá-la logo em seguida.

Para garantir mais segurança, o administrador pode limitar quais redes têm permissão para acessar o IPCop via SSH. Essa restrição pode ser configurada diretamente na seção de configurações do *firewall*, evitando que conexões indesejadas tentem acessar o sistema remotamente.

A prática de ativar o SSH apenas quando necessário e configurar restrições por rede contribui significativamente para a proteção do IPCop. Como o protocolo SSH oferece acesso direto ao sistema, ele deve ser usado com cautela e sempre com medidas adicionais de controle de acesso, como mostra a Figura 41.

Figura 41 – SSH



Fonte: IPCop, 2025

O IPCop permite o acesso remoto por SSH, que pode ser ativado na interface *web*. Por padrão, esse acesso é desabilitado, e a porta utilizada para conexões SSH não é a tradicional 22, mas sim a 8022. Caso esteja utilizando uma aplicação com interface gráfica para se conectar ao IPCop, é essencial informar essa porta alternativa.

Além de ativar o SSH, a interface permite configurar diversas opções de segurança, como a permissão para uso do protocolo SSH versão 1 (altamente desaconselhado por questões de vulnerabilidade), ativar ou não autenticação por senha, e permitir ou bloquear o

redirecionamento de portas *Transmission Control Protocol* (TCP), útil em cenários emergenciais, como acesso remoto a serviços internos sem VPN previamente configurada.

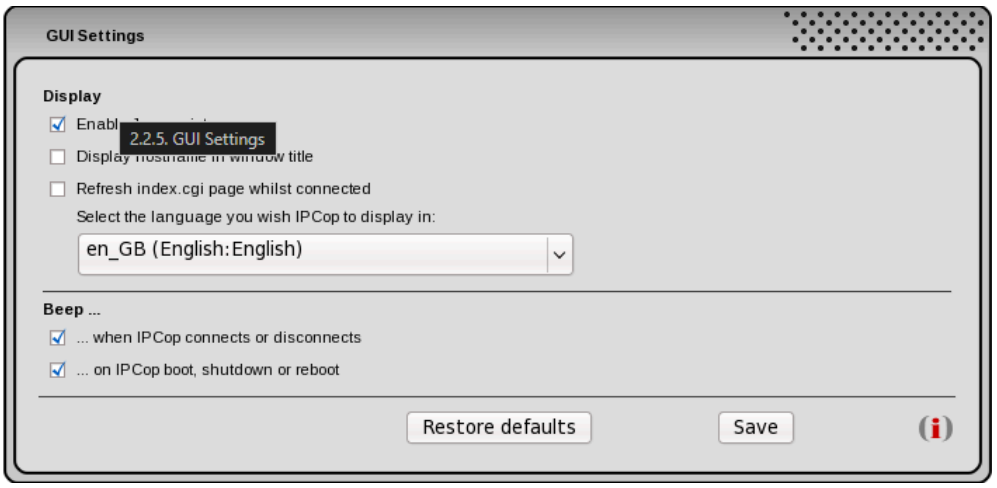
Um exemplo prático envolve a criação de túneis SSH para redirecionar conexões de um serviço interno (como *Telnet*) para sua máquina remota. Isso pode ser feito com o comando SSH utilizando a opção -L para mapear portas locais às portas e endereços internos protegidos pela rede do IPCop. Mesmo sem VPN, esse recurso permite manutenção emergencial.

Adicionalmente, é possível configurar autenticação por chave pública, método mais seguro e recomendado. A seção também exibe as chaves de *host* do SSH utilizadas pelo IPCop, permitindo que o administrador confirme se está conectando à máquina correta ao verificar a impressão digital (*fingerprint*) apresentada na primeira conexão.

5.6 *GUI Settings*

O IPCop permite personalizar a aparência e o comportamento da interface administrativa via navegador. Essas configurações estão disponíveis na seção "GUI Settings" e afetam a experiência visual e funcional do painel. Após realizar alterações, é necessário clicar no botão “Save” para que tenham efeito. Também é possível restaurar os valores padrão com o botão “Restore defaults”, como mostra a Figura 42.

Figura 42 – SSH



Fonte: IPCop, 2025

Entre as opções visuais, o administrador pode ativar o uso de *JavaScript* para uma experiência mais fluida e responsiva. A exibição do nome do host no título da janela pode ser útil ao gerenciar múltiplas instâncias do IPCop. Já a opção de atualização automática da página inicial (index.cgi) a cada 30 segundos permite monitorar em tempo real o status da conexão com a Internet.

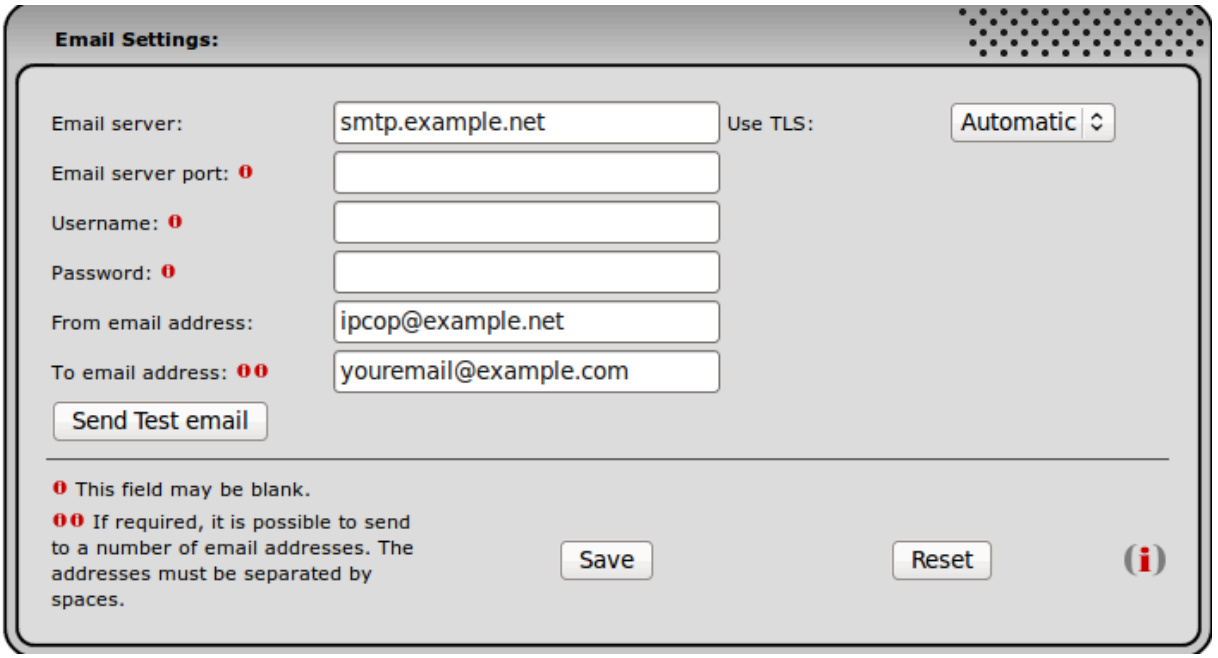
Outro recurso importante é a escolha do idioma da interface. O IPCop suporta atualmente 34 idiomas, mas caso alguma tradução esteja incompleta, as partes faltantes serão exibidas em inglês. O projeto incentiva colaboradores a participar da tradução por meio das equipes dedicadas e da lista de desenvolvedores, permitindo o crescimento contínuo da disponibilidade de idiomas, inclusive durante a instalação do sistema.

Além do visual, há opções sonoras configuráveis. Por padrão, o IPCop emite um som ao conectar-se ou desconectar-se da Internet, bem como ao inicializar ou desligar. Caso o ambiente exija silêncio, como servidores em locais sensíveis, esses sons podem ser desativados facilmente na seção "*Sound*" da mesma página de configurações.

5.7 *Email Settings*

O IPCop pode enviar e-mails automaticamente ao administrador em situações específicas, como alertas por volume de tráfego excedido. Essas configurações são feitas na página "*Email Settings*", onde o envio de e-mails pode ser personalizado de acordo com o servidor *Simple Mail Transfer Protocol* (SMTP) utilizado. Após configurar, é essencial clicar no botão “*Save*” para aplicar as alterações, como mostra a Figura 43.

Figura 43 – SSH



Fonte: IPCop, 2025

O administrador deve informar o endereço do servidor de e-mail (SMTP), como por exemplo “smtp.exemplo.com”. Caso o servidor exija autenticação, há campos opcionais para inserir o nome de usuário e a senha — sendo importante lembrar que espaços ou aspas no campo de senha causam erro. Também é possível definir se a comunicação com o servidor usará TLS, com três opções: “Automático (padrão)”, “Sim” ou “Não”.

Se o servidor de e-mail utilizar uma porta diferente do padrão (geralmente 25, 465 ou 587), pode-se especificá-la no campo apropriado. O endereço de e-mail que será exibido como remetente deve ser preenchido no campo “*From email address*”. Já o(s) destinatário(s) dos alertas devem ser inseridos no campo “*To email address*”. É possível cadastrar múltiplos destinatários, bastando separar os e-mails por espaços.

Por fim, há uma opção para enviar um e-mail de teste, a fim de verificar se as configurações estão corretas. Importante: o teste só poderá ser realizado após salvar as configurações. Este recurso é muito útil para garantir que alertas críticos serão entregues corretamente.

5.8 *Backup Web Page*

A página de Backup do IPCop permite salvar as configurações do sistema, tanto em um disquete quanto em arquivos armazenados no disco rígido ou em uma unidade USB. Esses *backups* podem ser exportados ou restaurados diretamente pela interface web. Após salvar um *backup*, as mensagens de erro e informações do processo serão exibidas na parte inferior da tela, como mostra a Figura 44.

Figura 44 – SSH

Fonte: IPCop, 2025

Na seção "*Backup to Floppy*", é possível gravar a configuração do sistema em um disquete (caso a unidade esteja instalada). A restauração por disquete é feita apenas durante uma nova instalação do IPCop, quando o instalador solicita a presença de um disquete com configuração prévia. Se encontrado e validado, o sistema é restaurado e a instalação é encerrada automaticamente.

A opção "*Backup to Files*" permite criar vários conjuntos de *backup* e escolher o destino, como o *Hard Disk* (HD) do IPCop ou um dispositivo *Universal Serial Bus* (USB). Os

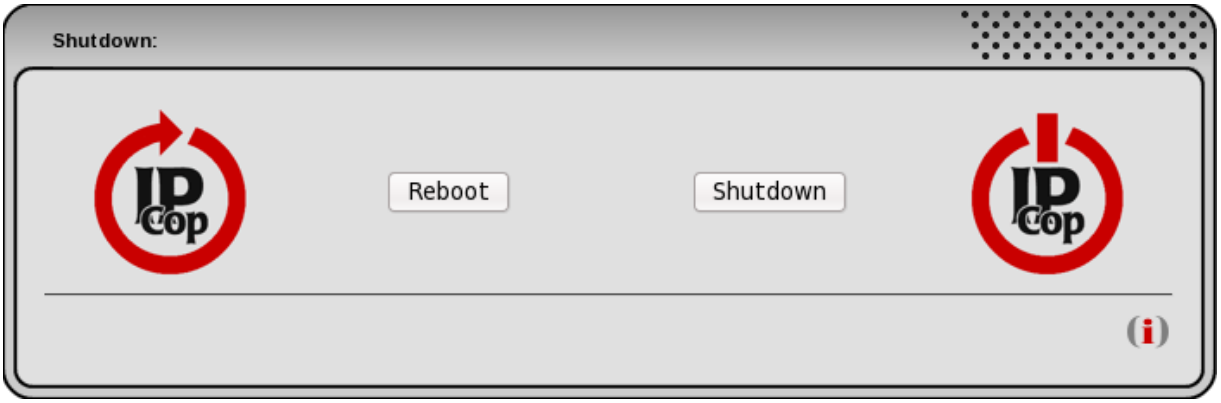
backups são criptografados com uma senha específica de *backup*. Por isso, é importante exportar também a chave de criptografia (*Backup Key*). Essa chave será solicitada caso o sistema precise ser restaurado após falha no disco, ou em uma reinstalação via USB/*HyperText Transfer Protocol* (HTTP)/*File Transfer Protocol* (FTP).

Na seção "*Backup Encryption Key*", deve-se definir uma senha de *backup*, digitá-la na página de *backup* e clicar em "*Export backup key"* para salvar a chave criptografada. Depois, crie um *backup* e exporte o arquivo .dat. Para restauração, ambos os arquivos (chave e .dat) devem estar no dispositivo usado para reinstalação. Se não houver um arquivo .dat sem data, o IPCop restaurará automaticamente o arquivo com a data mais recente.

5.9 *Shutdown Web Page*

A página de desligamento do IPCop permite realizar o desligamento (*Shutdown*) ou a reinicialização (*Reboot*) do sistema por meio de botões simples na interface *web*. Basta clicar na opção desejada para que a ação seja executada imediatamente, como mostra a Figura 45.

Figura 45 – SSH



Fonte: IPCop, 2025

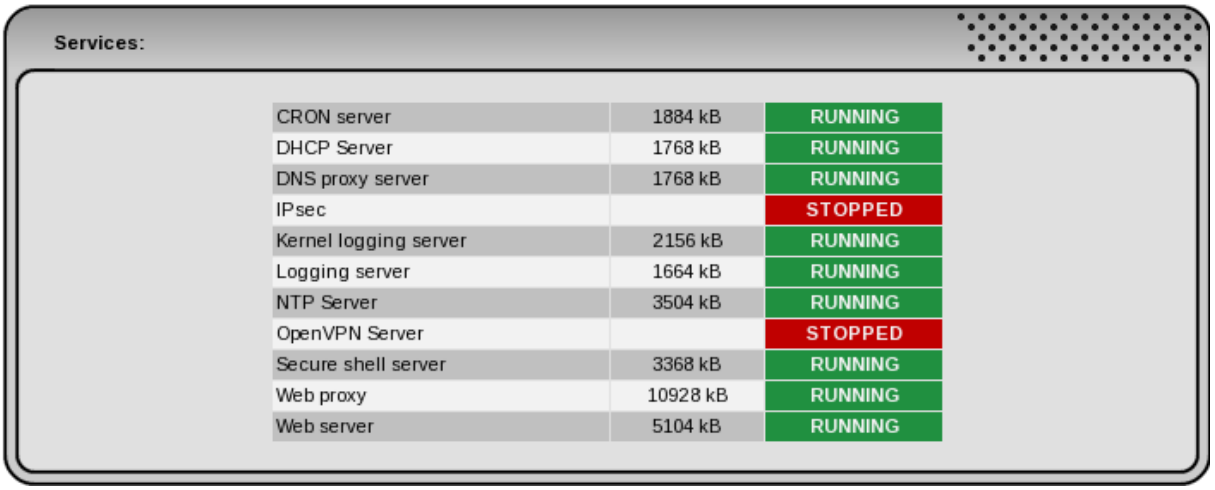
Como dica adicional, se o *hardware* suportar, também é possível desligar o IPCop pressionando o botão físico de energia (*Power*) no equipamento onde ele está instalado.

5.10 *Status Menu*

O menu *Status* do IPCop reúne um conjunto de páginas fundamentais para o acompanhamento do funcionamento do sistema. Por meio dessas interfaces, o administrador pode visualizar dados técnicos, gráficos de desempenho, informações sobre a rede e o tráfego, além de obter uma visão geral sobre os recursos em uso no servidor. Essa centralização facilita a análise rápida e eficaz do ambiente de rede.

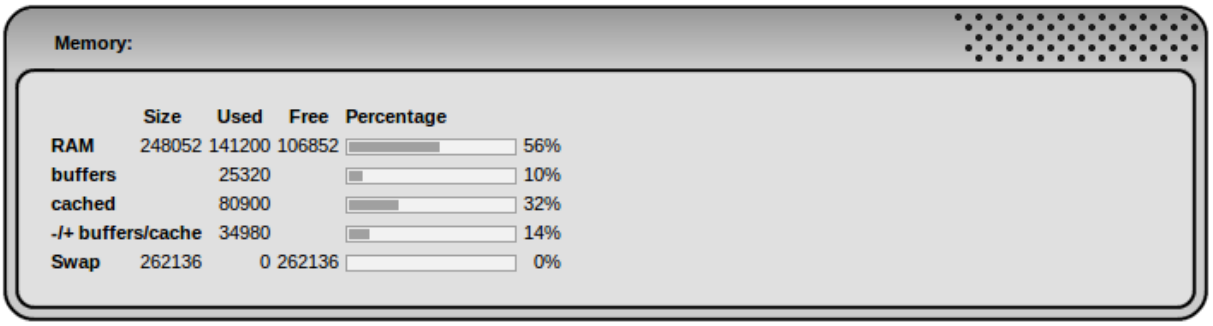
A primeira subpágina, chamada *System Status*, apresenta um painel com os principais indicadores operacionais do IPCop. Entre os itens exibidos estão os serviços ativos, consumo de memória e *swap*, uso de disco rígido e a quantidade de *inodes* disponíveis, como mostra as Figuras 46, 47, 48 e 49. Essas informações ajudam a detectar possíveis gargalos ou falhas no funcionamento do *firewall*.

Figura 46 – *Services*



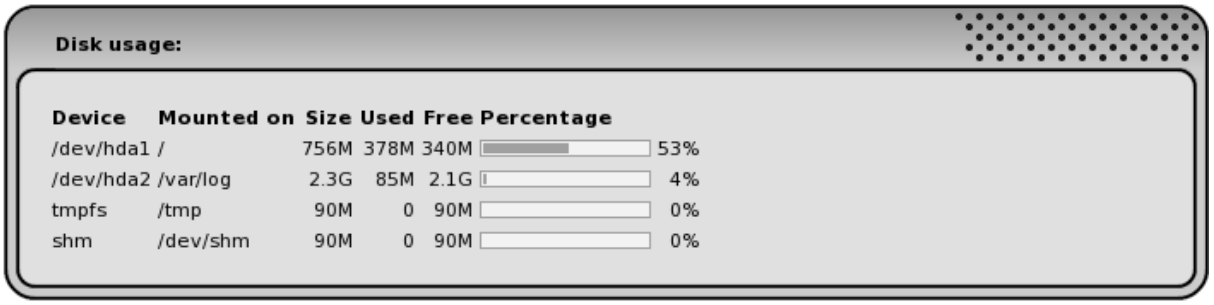
Fonte: IPCop, 2025

Figura 47 – *Memory*



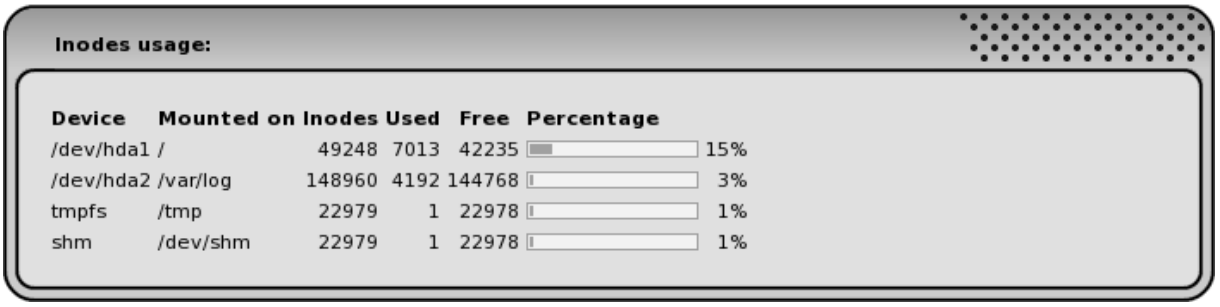
Fonte: IPCop, 2025

Figura 48 – *Disk usage*



Fonte: IPCop, 2025

Figura 49 – *Inodes usage*



Fonte: IPCop, 2025

Ainda na mesma página, o sistema exibe dados sobre a duração de funcionamento contínuo do IPCop (*uptime*), usuários conectados, versão do *kernel* e, quando aplicável, o

status de dispositivos *Redundant Array of Independent Disks* (RAID). Essa variedade de informações técnicas permite ao administrador acompanhar o estado geral do sistema de forma precisa e atualizada.

A subpágina *System Info* oferece um panorama detalhado sobre o hardware. É possível identificar o modelo e frequência do processador, dados sobre o disco rígido, placas de rede, dispositivos conectados via USB e a lista de processos em execução. Além disso, módulos carregados pelo *kernel* também são listados, o que contribui para a resolução de problemas relacionados a drivers e compatibilidades.

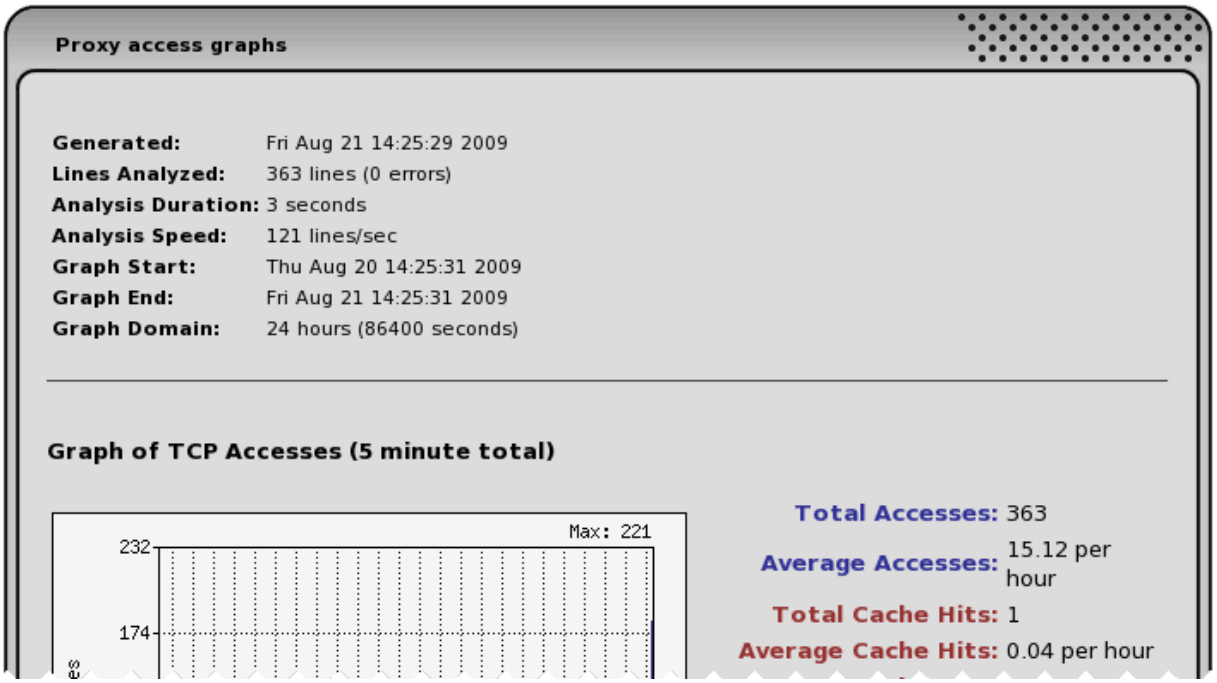
Na seção *Network Status*, o foco está na conectividade. Informações sobre todas as interfaces de rede, configuração de DNS, status do cliente DHCP (quando ativo), e dados de dispositivos *Asymmetric Digital Subscriber Line* (ADSL) podem ser acessados aqui. Também é possível visualizar as tabelas de roteamento e *Address Resolution Protocol* (ARP), essenciais para entender como o tráfego está sendo direcionado.

A área de *System Graphs* fornece representações visuais do desempenho do sistema. Gráficos interativos permitem acompanhar a utilização de *Central Processing Unit* (CPU), memória e disco em diferentes períodos de tempo — como diário, semanal, mensal e anual. Esses gráficos ajudam na identificação de tendências ou de comportamentos anormais no sistema.

A seção *Traffic Graphs* complementa a análise visual, apresentando gráficos que mostram o tráfego de entrada e saída de cada interface de rede. Os dados são organizados por cores de interface (*Green, Red, Blue, Orange*) e também podem ser visualizados por diferentes períodos. É uma ferramenta útil para monitoramento de consumo de banda e identificação de possíveis abusos.

Já em *Proxy Graphs*, os gráficos são gerados a partir dos *logs* do serviço de *proxy Squid*, se este estiver com o registro de dados habilitado. Caso contrário, os gráficos permanecerão vazios. Quando ativos, esses relatórios ajudam a compreender como os usuários estão utilizando o proxy e quais sites estão sendo mais acessados, como mostra a Figura 50.

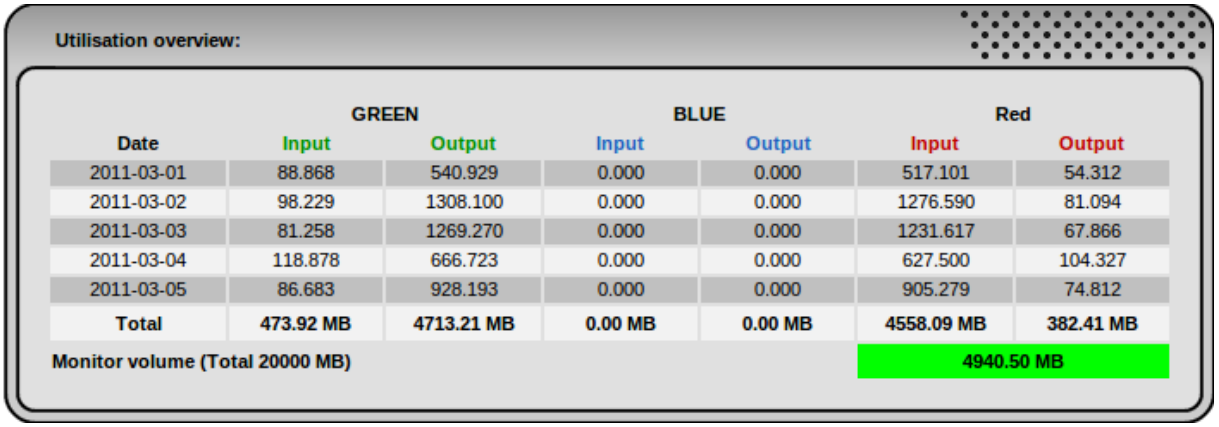
Figura 50 – *Proxy access graphs*



Fonte: IPCop, 2025

A funcionalidade *Traffic Accounting* permite o acompanhamento detalhado do volume de dados trafegado pelas interfaces do IPCop, como mostra a Figura 51. É possível configurar períodos de análise, níveis de alerta e notificações por e-mail. O administrador pode optar por janelas mensais fixas ou períodos contínuos de análise, além de estabelecer limites de uso com alertas visuais codificados por cores.

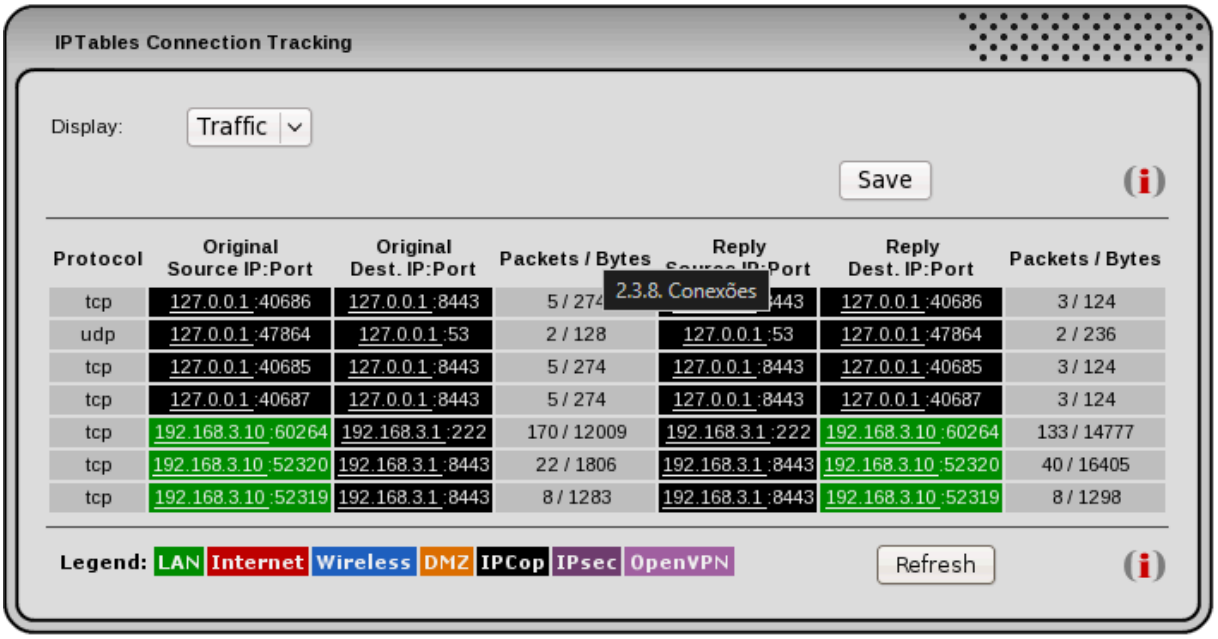
Figura 51 – *Utilisation overview*



Fonte: IPCop, 2025

Na página *Connections*, são listadas as conexões ativas monitoradas pelo sistema. Através do rastreamento de estado do *IPTables*, o IPCop exibe informações sobre o tráfego entre as redes internas e externas, com destaque para os IPs de origem e destino, portas utilizadas e protocolos, como mostra a Figura 52. Essa ferramenta é essencial para monitoramento em tempo real e para investigações de possíveis acessos indevidos.

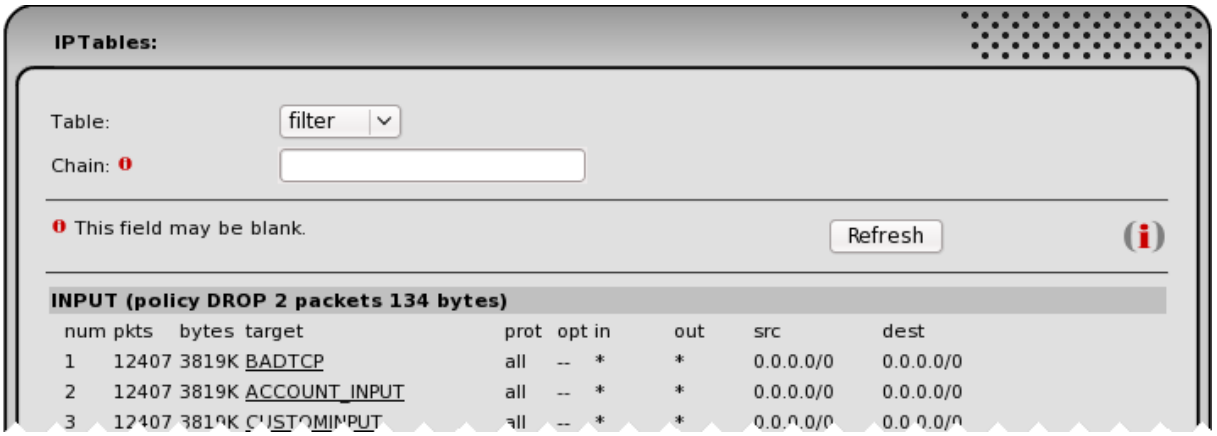
Figura 52 – *IPTables connection tracking*



Fonte: IPCop, 2025

Por fim, a subpágina *IPTables Output* apresenta o conteúdo das tabelas de firewall do sistema. O administrador pode selecionar o tipo de tabela (*filter, nat, mangle, raw*) e especificar uma cadeia para análise detalhada. Essa visualização técnica ajuda na auditoria e verificação das regras de *firewall* configuradas no sistema, garantindo que a segurança esteja de acordo com as políticas definidas, como mostra a Figura 53.

Figura 53 – *IPTables*



Fonte: IPCop, 2025

5.11 *Network Menu*

O menu "Rede" do IPCop reúne páginas administrativas que permitem configurar os métodos de conexão do *firewall* com a Internet. Para acessá-lo, basta clicar na aba "Network" no topo da interface. A partir disso, surgem opções como "*Dialup*", "*Upload*", "*Modem*" e "*Aliases*", cada uma com funcionalidades específicas para gerenciar conexões e dispositivos.

Na seção "*Dialup*", é possível administrar conexões feitas por modem analógico, *Integrated Services Digital Network* (ISDN) ou *Digital Subscriber Line* (DSL). Essa página é dividida em diversas partes, como perfis de conexão, tipo de interface, ajustes de modem e opções de reconexão. Um ponto importante: qualquer alteração só pode ser feita quando o IPCop estiver desconectado da Internet.

Os perfis de discagem são conjuntos de configurações salvos, permitindo que até cinco diferentes sejam criados ou editados. Após configurar um perfil com os dados de conexão necessários, basta salvá-lo e selecioná-lo como ativo para futuras conexões. Há ainda opções para restaurar as configurações anteriores ou renomear os perfis conforme a necessidade.

Na escolha da interface, o usuário define o tipo de porta ou protocolo utilizado, como *Point-to-Point Protocol over Ethernet* (PPPoE) para DSL ou portas seriais para modems analógicos. A velocidade de comunicação entre o computador e o modem também pode ser configurada, o que é essencial para garantir a estabilidade da conexão, especialmente em

sistemas mais antigos.

Outros campos permitem inserir o número de telefone da conexão, ativar o alto-falante do modem, escolher o tipo de discagem (tom ou pulso), configurar o tempo de inatividade (*idle timeout*) e optar por conectar automaticamente ao reiniciar o IPCop. Essas opções oferecem grande flexibilidade para adaptar o comportamento da conexão às necessidades do ambiente.

A aba de reconexão permite escolher entre três modos: manual, persistente ou discagem sob demanda. O modo manual exige que o usuário selecione o botão de conectar sempre que desejar acesso à Internet. Já a conexão persistente mantém o link ativo continuamente e tenta reconectar automaticamente em caso de falha. Por fim, o modo "*Dial on Demand*" conecta automaticamente ao detectar tráfego, útil em redes com uso intermitente.

Para conexões DSL via PPPoE ou USB, configurações adicionais como protocolo, encapsulamento e nomes de serviço podem ser exigidos pelo provedor. Nesses casos, também é necessário preencher os campos *Virtual Path Identifier* (VPI) e *Virtual Channel Identifier* (VCI) com os dados fornecidos pela operadora de Internet.

A parte de autenticação requer o nome de usuário e a senha fornecidos pelo provedor. Os métodos mais comuns são *Password Authentication Protocol* (PAP) e *Challenge Handshake Authentication Protocol* (CHAP), mas, em casos raros, pode-se precisar de um script de login personalizado, que deve ser colocado em um diretório específico do sistema IPCop.

Na aba "*Upload*", o administrador pode enviar *firmwares* e drivers necessários para o funcionamento de determinados modems, como os modelos *Speedtouch* USB, ECI ADSL ou Fritz!DSL. Após o *upload*, alguns arquivos precisam ser extraídos e movidos manualmente para o diretório apropriado, geralmente com comandos via terminal como *root*.

Por fim, a funcionalidade de "*Aliases*" permite adicionar endereços IP adicionais fornecidos pelo provedor. Isso é útil para hospedar diversos serviços acessíveis externamente sob IPs distintos. O administrador pode configurar, ativar, editar ou excluir *aliases* conforme a necessidade, o que amplia a capacidade do IPCop em ambientes com múltiplas aplicações voltadas para a Internet.

5.12 *Services Menu*

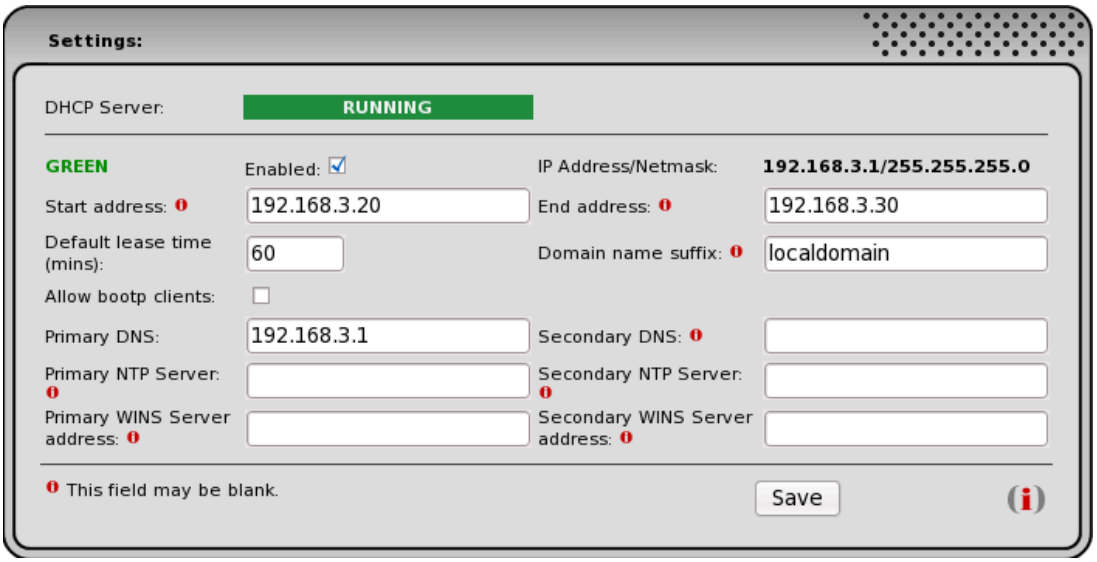
O menu "*Services*" do IPCop oferece uma variedade de serviços adicionais que complementam a função principal do *firewall* de proteger a rede contra acessos indesejados. Esses serviços são especialmente úteis em redes pequenas, onde é comum que um único dispositivo desempenha múltiplas funções, otimizando recursos e simplificando a administração da rede.

Entre os serviços disponíveis, o *proxy* funciona como um servidor intermediário para requisições *web*, melhorando o desempenho e a segurança ao armazenar em *cache* conteúdos acessados com frequência. Isso reduz o consumo de banda e acelera o acesso a sites visitados regularmente, além de permitir o controle do tráfego *web*.

O filtro de URLs é uma ferramenta que bloqueia o acesso a domínios, URLs ou arquivos indesejados, proporcionando um controle mais rígido sobre o que os usuários da rede podem acessar. Essa função é importante para garantir que conteúdos impróprios ou maliciosos não sejam carregados, ajudando a proteger a rede contra ameaças e a manter a produtividade dos usuários.

O servidor DHCP é responsável por distribuir automaticamente endereços IP e outras configurações de rede para os dispositivos conectados, facilitando o gerenciamento dos recursos de IP da rede. Com ele, a configuração de rede dos computadores e outros dispositivos é simplificada, evitando conflitos e erros de configuração manual, como mostra a Figura 54.

Figura 54 – *Settings DHCP Server*



Fonte: IPCop, 2025

O gerenciamento dinâmico de DNS permite que o IPCop atualize automaticamente os registros DNS para dispositivos com endereços IP dinâmicos. Isso é especialmente útil para conexões à Internet que não possuem um IP fixo, mantendo sempre o nome de domínio atualizado e acessível, o que facilita o acesso remoto e a administração da rede.

A edição de *hosts* possibilita que o administrador configure um servidor DNS local, criando entradas personalizadas que facilitam a resolução de nomes internos na rede. Esse recurso é útil para ambientes que precisam de acesso rápido e confiável a servidores internos, evitando depender exclusivamente do DNS externo.

O servidor de tempo sincroniza o relógio dos dispositivos da rede, garantindo que todos tenham a mesma hora correta. Isso é essencial para o registro preciso de eventos em logs, sincronização de processos e funcionamento correto de protocolos que dependem de horários exatos.

A funcionalidade de controle de tráfego, ou *traffic shaping*, permite gerenciar a largura de banda da rede, priorizando determinados tipos de tráfego ou limitando o uso em outras áreas. Com isso, é possível garantir que aplicações críticas tenham prioridade no uso da rede, melhorando a performance geral e evitando congestionamentos.

Em redes maiores, muitos desses serviços são frequentemente delegados a servidores

dedicados, especializados em suas funções. Nesses casos, é recomendável desativar os serviços correspondentes no IPCop para evitar conflitos e otimizar o desempenho do *firewall*, permitindo que ele se concentre em sua função principal.

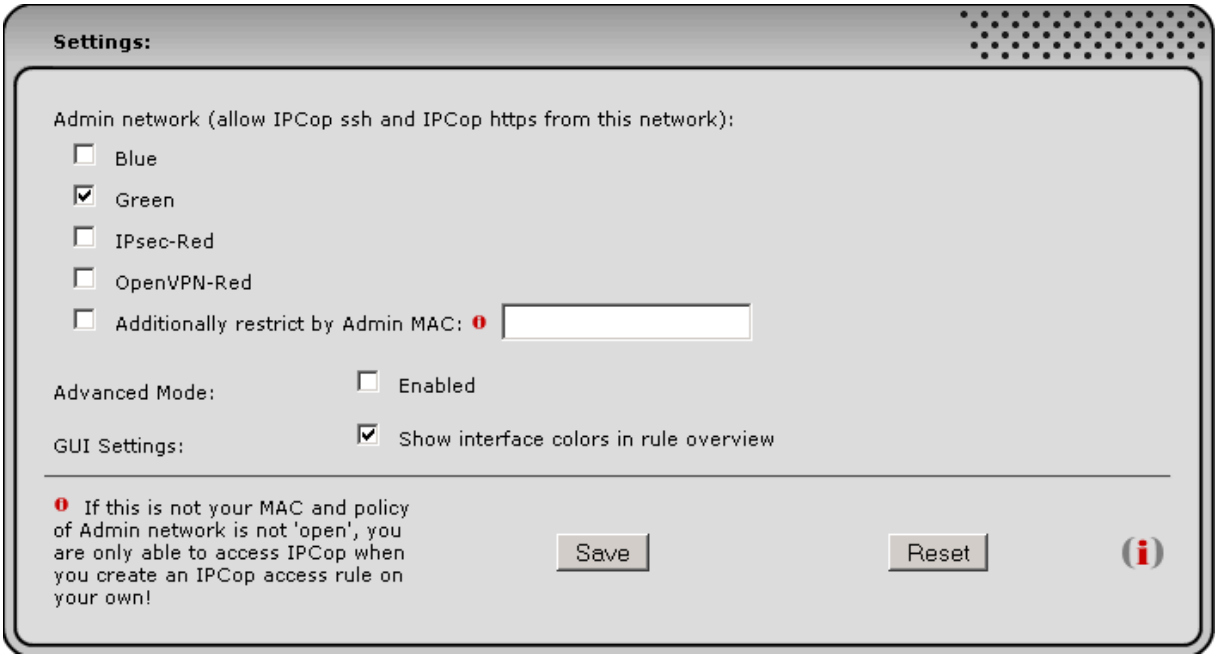
Portanto, o menu "*Services*" do IPCop oferece uma série de recursos valiosos que ampliam as capacidades do *firewall*, especialmente em ambientes menores e menos complexos. A configuração adequada desses serviços pode melhorar significativamente a segurança, a eficiência e o controle da rede, tornando o IPCop uma solução completa para pequenas empresas e redes domésticas.

5.13 *Firewall Menu*

O menu "*Firewall*" do IPCop agrupa algumas das funções centrais do sistema, sendo responsável pelo controle do tráfego que passa pelo *firewall*. É nesse menu que o administrador configura as regras que definem como os dados podem transitar entre as diferentes interfaces de rede, garantindo a segurança e a segmentação adequadas para a estrutura da rede.

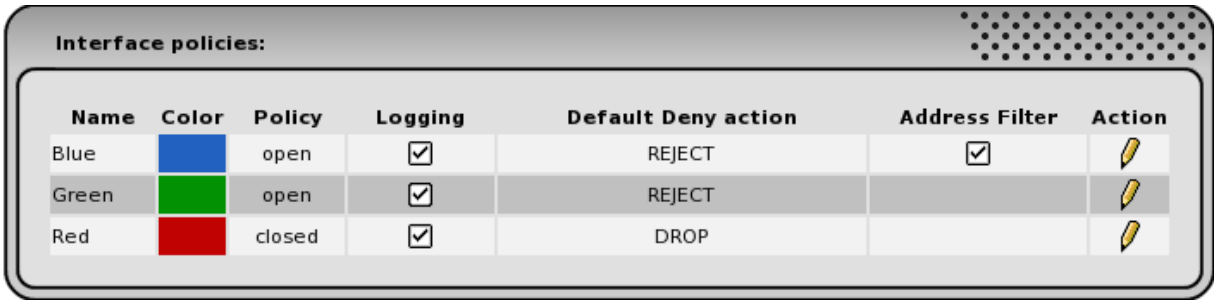
A opção "*Firewall Settings*" permite ajustar configurações básicas do *firewall*, como ativar ou desativar a detecção de pacotes fragmentados, controlar o *logging* de eventos de firewall e definir políticas padrão de entrada e saída para as conexões. Essas definições são importantes para estabelecer o comportamento geral do *firewall* em relação ao tráfego que não é coberto por regras específicas, como mostra as Figuras 55 e 56.

Figura 55 – *Firewall Settings*



Fonte: IPCop, 2025

Figura 56 – *Interface policies*



Fonte: IPCop, 2025

Em "*Address Filter*", o administrador pode bloquear ou permitir o tráfego com base em endereços IP específicos. Esse recurso é útil para permitir ou negar acesso a dispositivos ou redes específicas, proporcionando um controle mais granular sobre quem pode se comunicar dentro ou fora da rede.

A seção "*Services*" refere-se ao gerenciamento de serviços de rede como HTTP, FTP,

SSH, entre outros, permitindo que o administrador controle quais serviços estão disponíveis ou bloqueados. Ao criar regras baseadas em serviços, é possível restringir ou liberar o acesso a aplicações específicas, aumentando a segurança da rede.

Em "*Service Groups*", o administrador pode agrupar serviços semelhantes para facilitar a aplicação de regras de *firewall*. Por exemplo, é possível criar um grupo com todos os serviços relacionados à *web* (HTTP, HTTPS, etc.) e aplicar uma única regra a esse conjunto, tornando o gerenciamento mais simples e eficiente.

A opção "*Addresses*" permite registrar endereços IP ou sub-redes que poderão ser utilizados em regras de *firewall*. Esses registros facilitam a criação de regras, evitando que o administrador precise digitar endereços IP manualmente sempre que for definida uma nova política de acesso.

Em "*Address Groups*", é possível criar grupos de endereços previamente registrados. Assim como com os grupos de serviços, isso facilita a aplicação de regras para múltiplos dispositivos ou redes com características em comum, melhorando a organização e a clareza da configuração do *firewall*.

A seção "*Interfaces*" mostra as interfaces de rede disponíveis no IPCop, como *RED, GREEN, BLUE e ORANGE*, e permite configurá-las conforme as necessidades da rede. O entendimento das interfaces é essencial para a criação de regras que definem o tráfego permitido entre diferentes zonas da rede.

O item "*Firewall Rules*" é onde são definidas as regras que controlam o tráfego entre interfaces, endereços e serviços. Cada regra pode especificar origem, destino, protocolo, porta e ação (permitir ou negar), sendo o componente central para a configuração personalizada da política de segurança da rede.

5.14 *VPNs Menu*

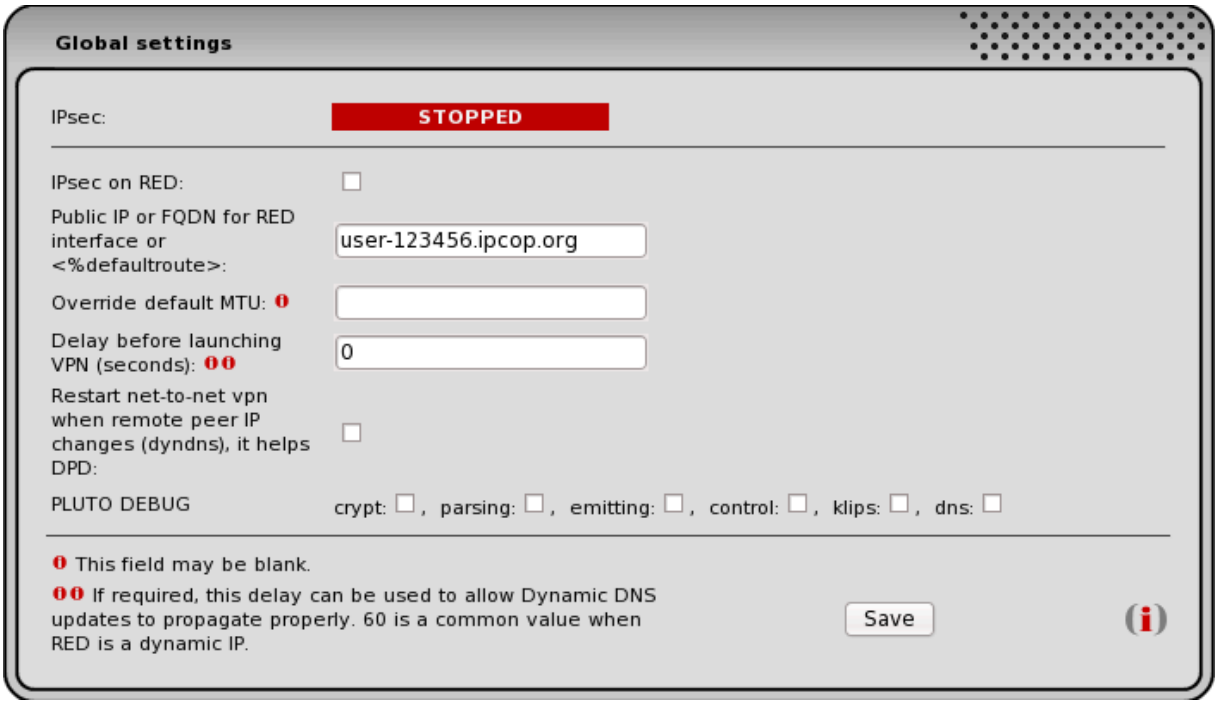
O menu "VPNs" do IPCop reúne as opções responsáveis pela configuração e gerenciamento de redes privadas virtuais (VPNs), que possibilitam a conexão segura entre duas ou mais redes distintas através de uma rede pública, como a Internet. Essa funcionalidade é essencial para empresas ou organizações que desejam integrar filiais ou

permitir o acesso remoto de usuários a partir de diferentes locais, mantendo a segurança e a integridade dos dados trafegados.

Para acessar as opções disponíveis no menu VPNs, o administrador deve selecionar a aba "VPNs" localizada na barra superior da interface *web* do IPCop. Ao clicar nessa aba, será exibido um menu suspenso com as três principais seções disponíveis para configuração de VPNs: IPsec, *OpenVPN* e CA (*Certificate Authorities*). Cada uma dessas opções oferece diferentes formas e níveis de segurança para o estabelecimento das conexões virtuais.

A opção "IPsec" permite a criação e o gerenciamento de túneis VPN baseados no protocolo IPsec (*Internet Protocol Security*), amplamente utilizado para conexões site-to-site entre *firewalls*. Com o IPsec, é possível estabelecer uma ligação criptografada entre redes remotas, garantindo confidencialidade, integridade e autenticação dos dados que circulam entre os pontos conectados, como mostra a Figura 57.

Figura 57 – *Global settings IPsec*

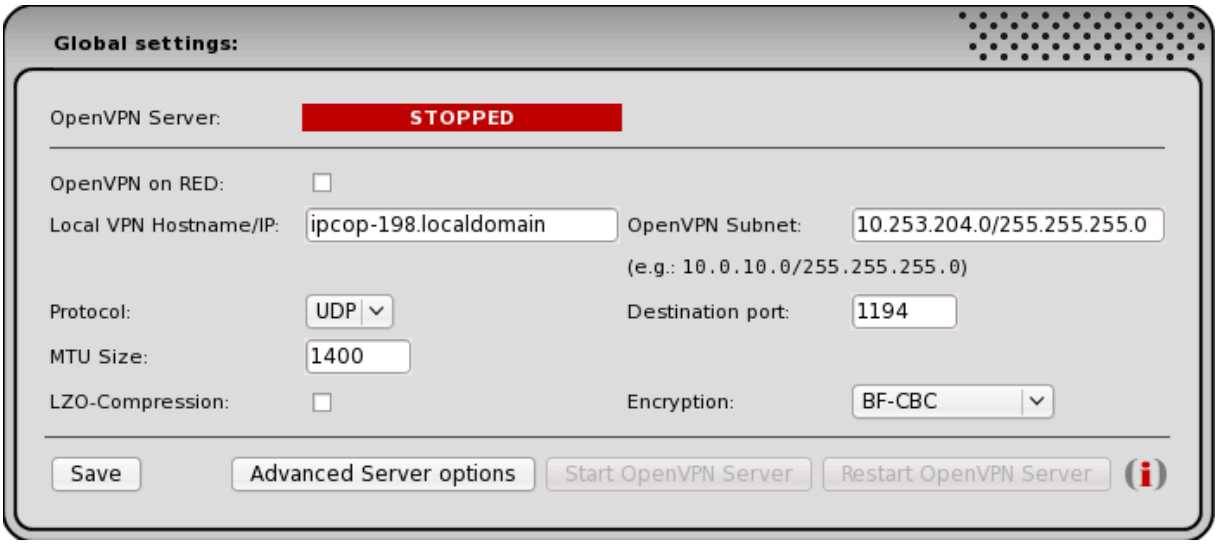


Fonte: IPCop, 2025

Já a opção "*OpenVPN*" oferece suporte a conexões VPN baseadas no protocolo SSL/TLS. Essa alternativa é bastante flexível e ideal para conexões do tipo "*client-to-site*", onde usuários individuais se conectam de forma segura à rede da empresa a partir de locais

remotos. O *OpenVPN* também permite o uso de certificados digitais e autenticação baseada em nome de usuário e senha, proporcionando uma configuração robusta e segura, como mostra a Figura 58.

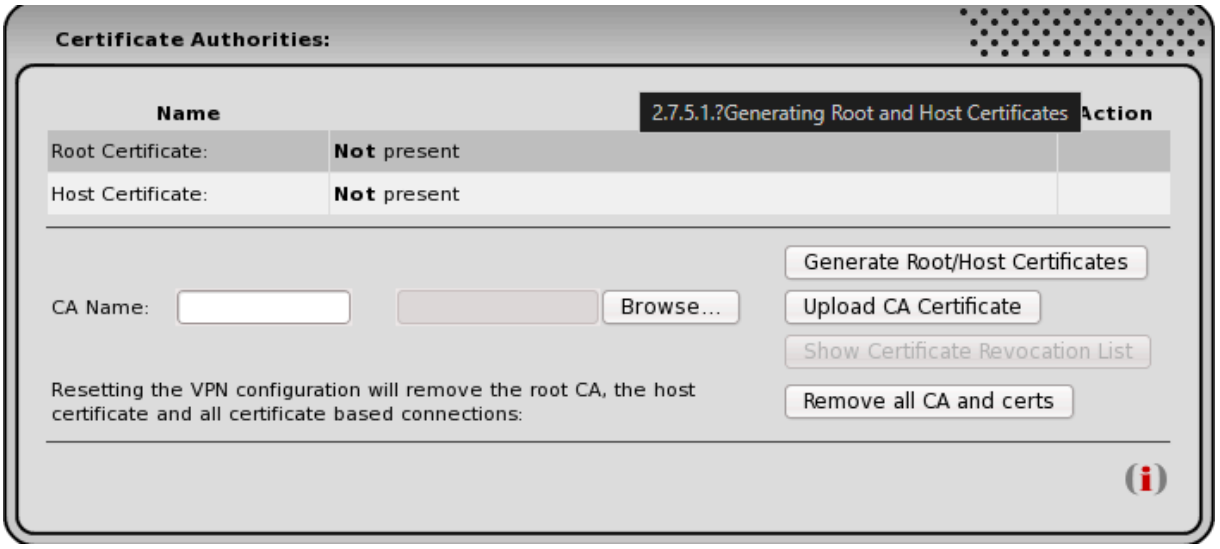
Figura 58 – *Global settings OpenVPN*



Fonte: IPCop, 2025

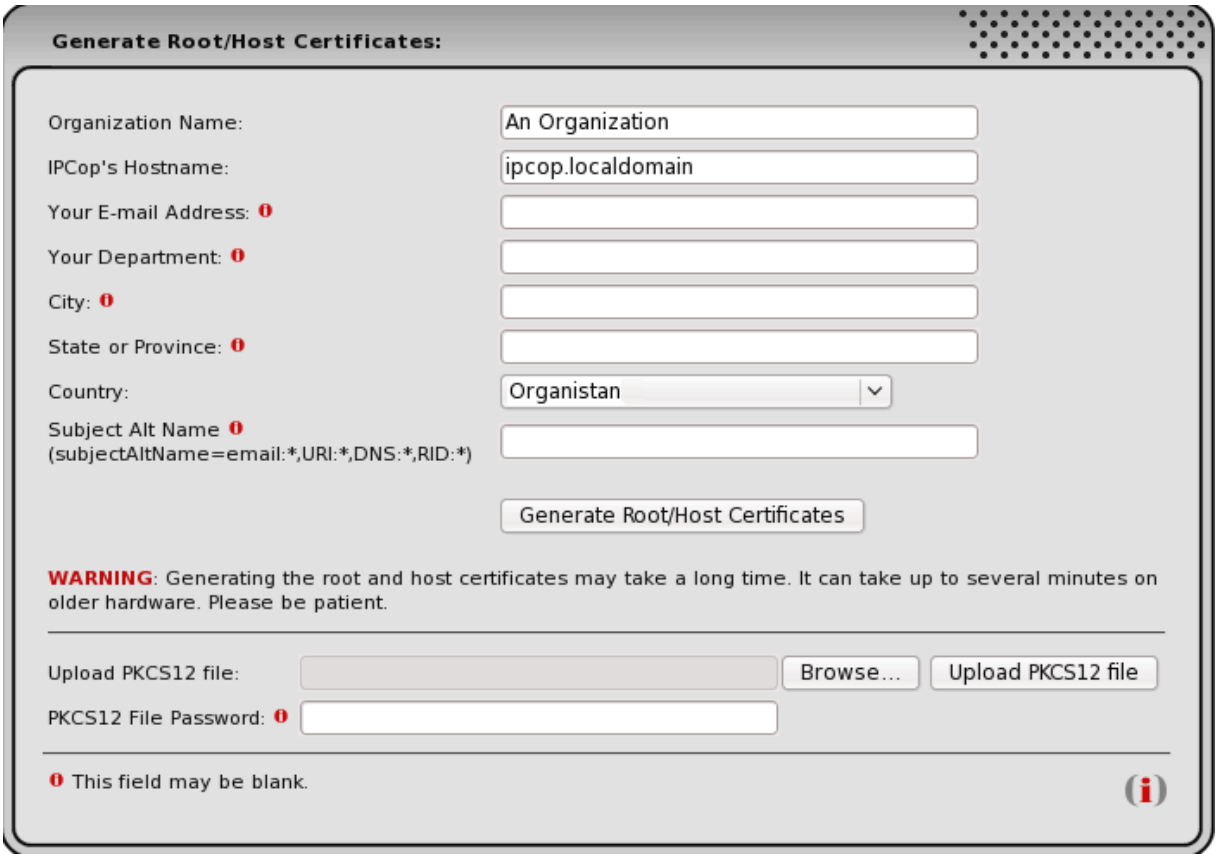
A seção "CA (*Certificate Authorities*)" é responsável pela criação e gerenciamento das autoridades certificadoras utilizadas nas conexões VPN. Por meio dessa funcionalidade, é possível emitir, importar ou revogar certificados digitais utilizados tanto no IPsec quanto no *OpenVPN*, garantindo a autenticidade das partes envolvidas na comunicação e protegendo contra acessos não autorizados, como mostra as Figuras 59, 60 e 61.

Figura 59 – *Certificate Authorities*



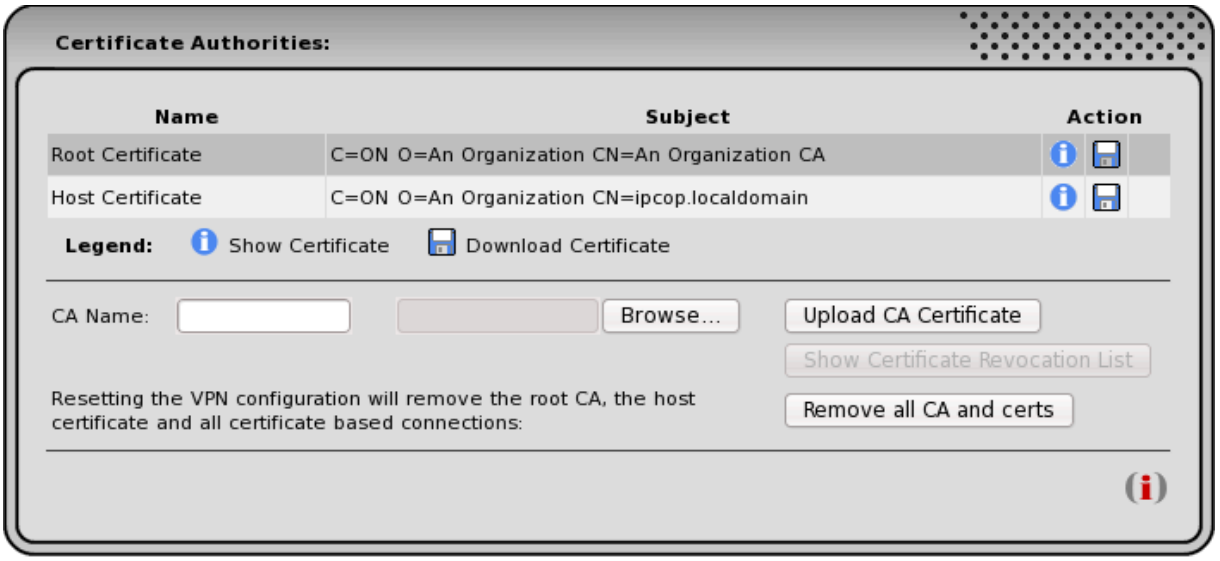
Fonte: IPCop, 2025

Figura 60 – *Generate Root/Host Certificates*



Fonte: IPCop, 2025

Figura 61 – *Certificates Authorities 2*



Fonte: IPCop, 2025

A configuração correta das VPNs no IPCop é fundamental para garantir a proteção das informações transmitidas entre redes remotas, sendo um recurso muito valorizado em ambientes corporativos. Ao permitir conexões criptografadas e autenticadas, o IPCop contribui para que a comunicação entre locais distintos ocorra de maneira segura e eficiente, independentemente da distância geográfica.

Portanto, o menu "VPNs" do IPCop é uma ferramenta poderosa que amplia as capacidades do *firewall*, permitindo não apenas o controle do tráfego interno e externo, mas também a extensão segura da rede local por meio de túneis criptografados. Essa funcionalidade é essencial para atender às demandas de conectividade moderna, sem comprometer a segurança da infraestrutura de rede.

5.15 *Logs Menu*

O menu "*Logs*" do IPCop é uma ferramenta essencial para monitoramento e análise do comportamento da rede e do próprio servidor. Ele oferece acesso detalhado aos registros gerados pelo sistema, permitindo ao administrador acompanhar eventos, identificar falhas e auditar atividades. Para acessar essas funcionalidades, deve-se clicar na aba "*Logs*" localizada

na barra superior da interface do IPCop.

Ao acessar o menu, um submenu suspenso é exibido, contendo as seguintes opções: *Log Settings, Log Summary, Firewall Logs, Proxy Logs, URL Filter Logs e System Logs*. Cada uma dessas páginas fornece informações específicas relacionadas a diferentes aspectos do funcionamento do IPCop, todas com a possibilidade de visualização detalhada e exportação dos dados registrados.

A página "*Log Settings*" permite ajustar como os *logs* serão gerados, armazenados e apresentados. O administrador pode configurar a retenção de *logs*, o nível de detalhamento das informações e escolher filtros para exibir apenas os registros relevantes para sua análise. Esses ajustes tornam a análise mais eficiente e ajudam a manter o desempenho do sistema.

A opção "*Log Summary*" apresenta uma visão geral consolidada dos *logs*, permitindo ao usuário visualizar rapidamente os principais eventos ocorridos em determinado período. Essa função é útil para identificar padrões de comportamento anormal, tentativas de acesso indevido ou falhas recorrentes nos serviços monitorados pelo IPCop.

As "*Firewall Logs*" contém registros de todas as conexões e tentativas de conexão que passaram pelo *firewall*. Essa seção é essencial para auditorias de segurança, pois mostra, por exemplo, quais IPs tentaram acessar a rede interna, quais portas foram utilizadas e se a conexão foi permitida ou bloqueada pelas regras configuradas.

Os "*Proxy Logs*" registram toda a atividade do serviço de *proxy*, incluindo os sites acessados pelos usuários da rede, os horários de acesso e possíveis erros encontrados. Eles são importantes para o controle do uso da internet, ajudando na identificação de comportamentos inadequados ou violações da política de uso da rede.

Na mesma linha, os "*URL Filter Logs*" detalham as tentativas de acesso a domínios bloqueados pelo filtro de URL. Esses registros mostram quais URLs foram barradas, quem tentou acessá-las e quando isso ocorreu. Essa funcionalidade reforça o controle de conteúdo e contribui para a segurança e produtividade dos usuários.

A página "*System Logs*" reúne os registros dos eventos internos do sistema IPCop, como inicializações, atualizações, falhas de hardware, mudanças de configuração e mensagens de erro. É um recurso fundamental para o diagnóstico de problemas técnicos e para garantir o funcionamento estável do *firewall*.

Todas essas sub-páginas compartilham uma interface comum que inclui ferramentas para selecionar os dados de log conforme a data desejada, utilizando menus suspensos de mês e dia. Após selecionar as datas, é necessário clicar no botão "*Update*" para que as informações sejam atualizadas. Também é possível navegar entre os dias usando os botões “<<” e “>>”.

Por fim, a função "*Export*" permite ao administrador baixar os *logs* em formato de texto, nomeado conforme a categoria e a data (ex: *ipcop-firewall-2025-05-21.log*). Isso facilita o armazenamento local, o compartilhamento com outros profissionais ou a inclusão em relatórios e documentações de auditoria. Essa funcionalidade torna o gerenciamento dos registros mais prático e acessível.

5.16 *User Customization*

A seção "*User Customization*" do IPCop oferece ao administrador a possibilidade de adaptar o sistema às necessidades específicas de sua rede. Por meio de arquivos e *scripts* disponíveis no próprio sistema, é possível realizar configurações avançadas que não estão acessíveis diretamente pela interface gráfica. Essas customizações permitem ajustar o comportamento do IPCop de forma mais detalhada, garantindo maior controle sobre seu funcionamento.

Esses arquivos e *scripts* estão organizados em locais específicos do sistema de arquivos do IPCop. Eles foram projetados para facilitar modificações em configurações padrão, automatizar tarefas ou adaptar serviços do sistema para operar de forma diferenciada em ambientes com requisitos especiais. No entanto, é importante ressaltar que essas alterações devem ser feitas com cautela, pois modificações incorretas podem comprometer o desempenho ou a segurança do sistema.

O objetivo principal dessa seção é descrever o propósito de cada um desses arquivos e scripts, além de informar sua localização dentro da estrutura do sistema. Dessa forma, o administrador pode entender melhor como o IPCop funciona "por trás dos panos" e tomar decisões mais informadas ao realizar alterações.

Importante destacar que as personalizações abordadas nesta seção não incluem os *Addons* desenvolvidos pela comunidade. Esses complementos, geralmente disponibilizados de

forma externa ao projeto oficial, oferecem novas funcionalidades ao IPCop, mas não são cobertos por esta documentação. O foco aqui está nas ferramentas nativas que permitem modificar o comportamento do sistema-base.

Para acessar e editar esses arquivos de configuração, é necessário ter privilégios de administrador, ou seja, acesso ao console do IPCop como usuário "*root*". Com esses privilégios, é possível utilizar editores de texto como o "*vi*" para abrir, alterar e salvar os arquivos conforme necessário. Esse nível de acesso garante que apenas usuários autorizados possam realizar mudanças sensíveis no sistema.

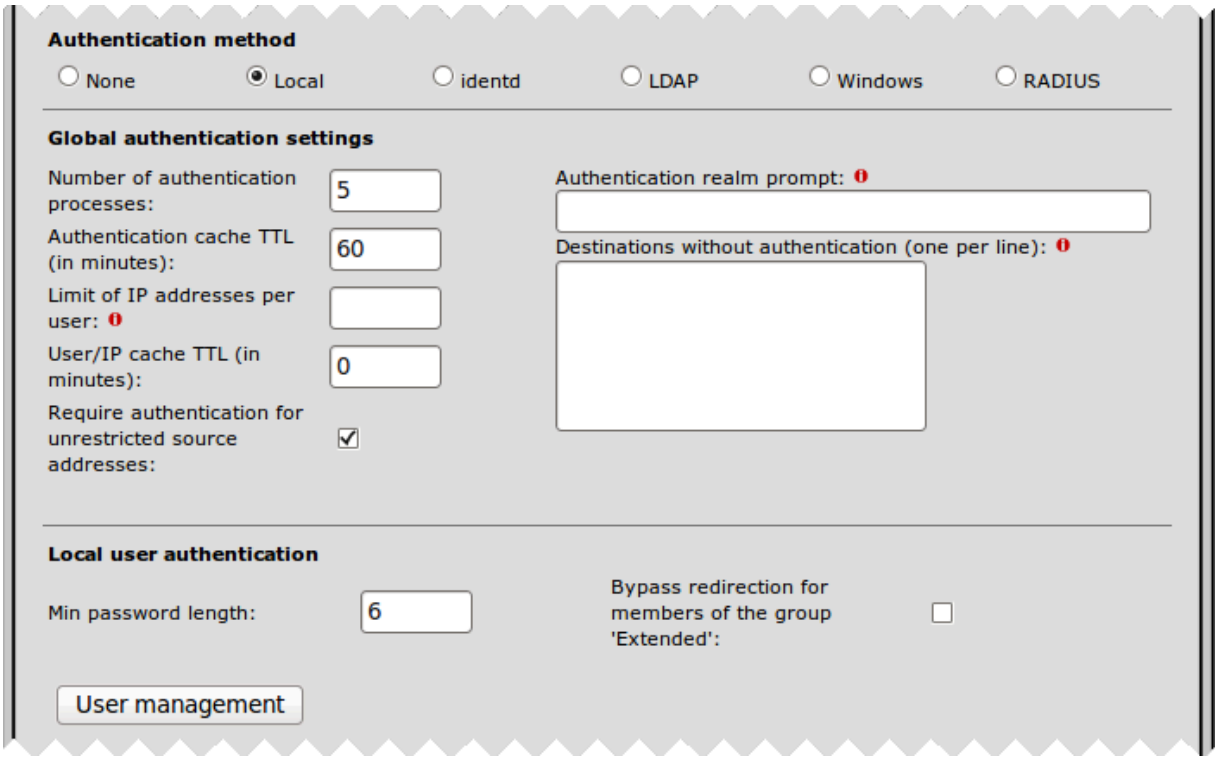
O uso do editor "*vi*", apesar de exigir um certo conhecimento técnico, é comum em sistemas baseados em *Linux*. Ele permite uma edição direta e precisa dos arquivos de configuração, essencial para garantir que as alterações feitas sejam corretamente aplicadas. Por isso, é recomendável que o administrador esteja familiarizado com comandos básicos do vi antes de tentar modificar arquivos do IPCop.

Por fim, a possibilidade de personalizar o IPCop por meio desses arquivos e *scripts* é uma das razões pelas quais ele é uma solução tão flexível para pequenas e médias empresas. Ao permitir ajustes finos no comportamento do sistema, o administrador pode garantir que o *firewall* atenda exatamente às necessidades da rede local, sem depender exclusivamente das opções padrão disponíveis na interface gráfica.

5.17 *Web Proxy Server*

A seção "*Web Proxy Server*" do IPCop oferece uma visão detalhada das opções de autenticação de usuários disponíveis por meio das configurações avançadas do *proxy web*, como mostra a Figura 62. Essas opções são fundamentais para ambientes em que é necessário controlar o acesso à internet com base na identidade do usuário, aumentando a segurança e o controle sobre o uso da rede. O *proxy* funciona como intermediário entre os usuários da rede local e os recursos da internet, permitindo a aplicação de políticas de acesso específicas.

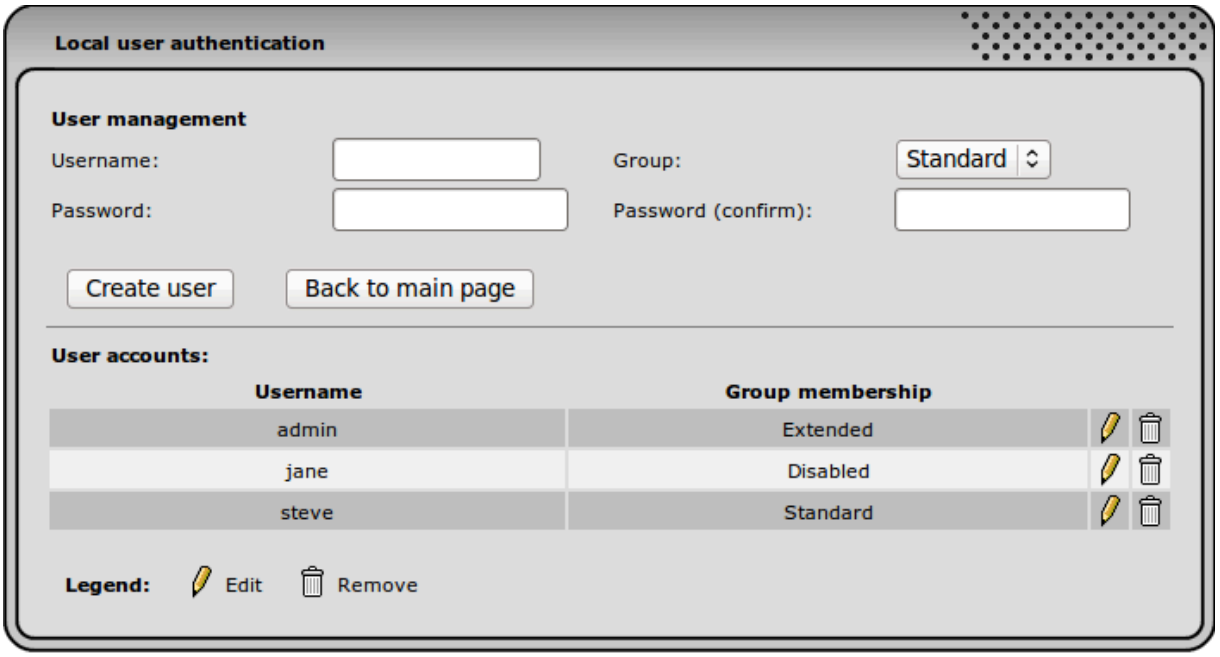
Figura 62 – *Authentication method*



Fonte: IPCop, 2025

Uma das opções de autenticação disponíveis é a “Autenticação Local”. Nesse método, as credenciais dos usuários são armazenadas diretamente no próprio IPCop, e o sistema realiza a verificação localmente. Essa é uma boa escolha para redes pequenas, onde não há servidores externos de autenticação e o gerenciamento centralizado não é necessário. Os administradores podem facilmente adicionar, remover ou editar usuários diretamente pela interface do IPCop, como mostra a Figura 63.

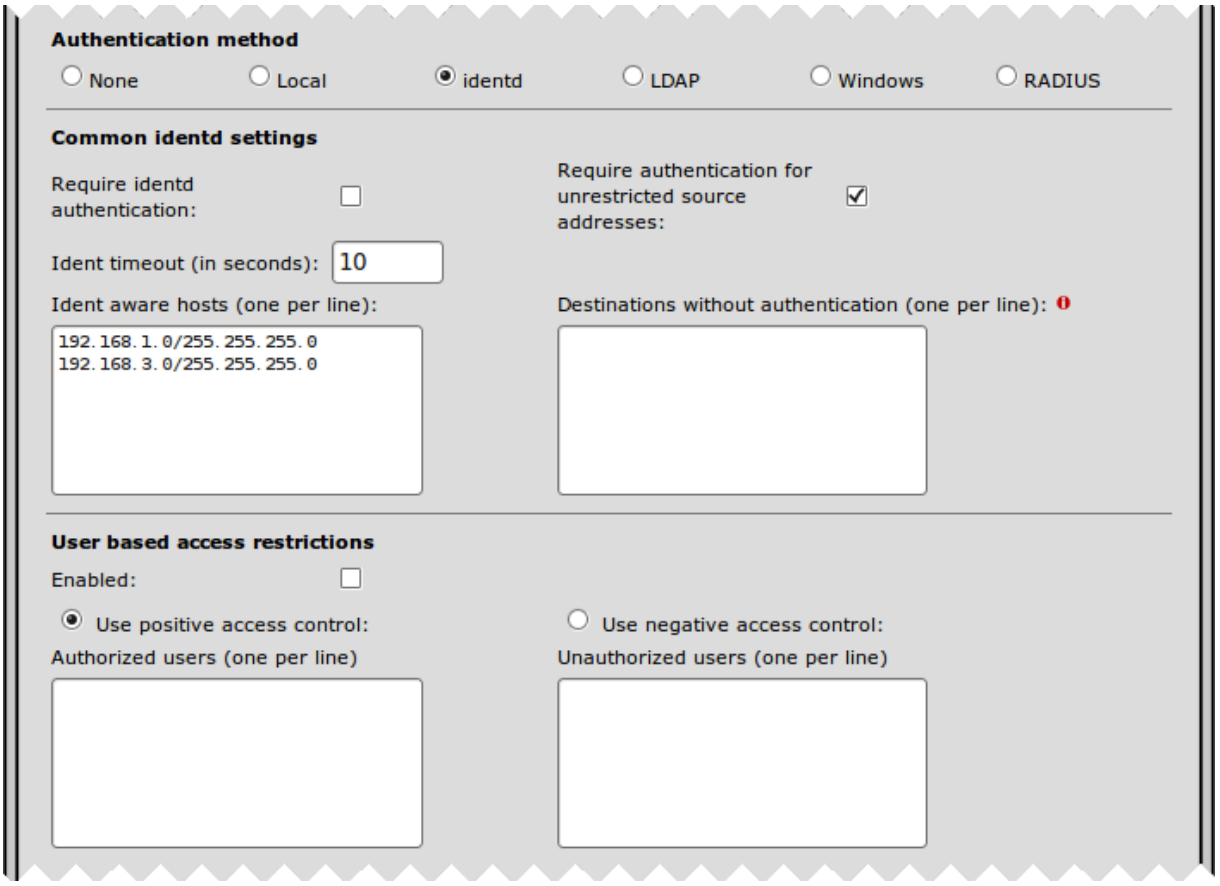
Figura 63 – Local user *authentication*



Fonte: IPCop, 2025

Outro método suportado é a "Autenticação via *identd*", que depende de um serviço rodando nas estações clientes para identificar os usuários, como mostra a Figura 64. O *identd* retorna o nome de usuário associado à conexão, que o *proxy* utiliza para controle de acesso. Esse método exige configuração tanto no lado do servidor quanto nas máquinas dos usuários, o que pode representar um desafio em redes maiores ou heterogêneas.

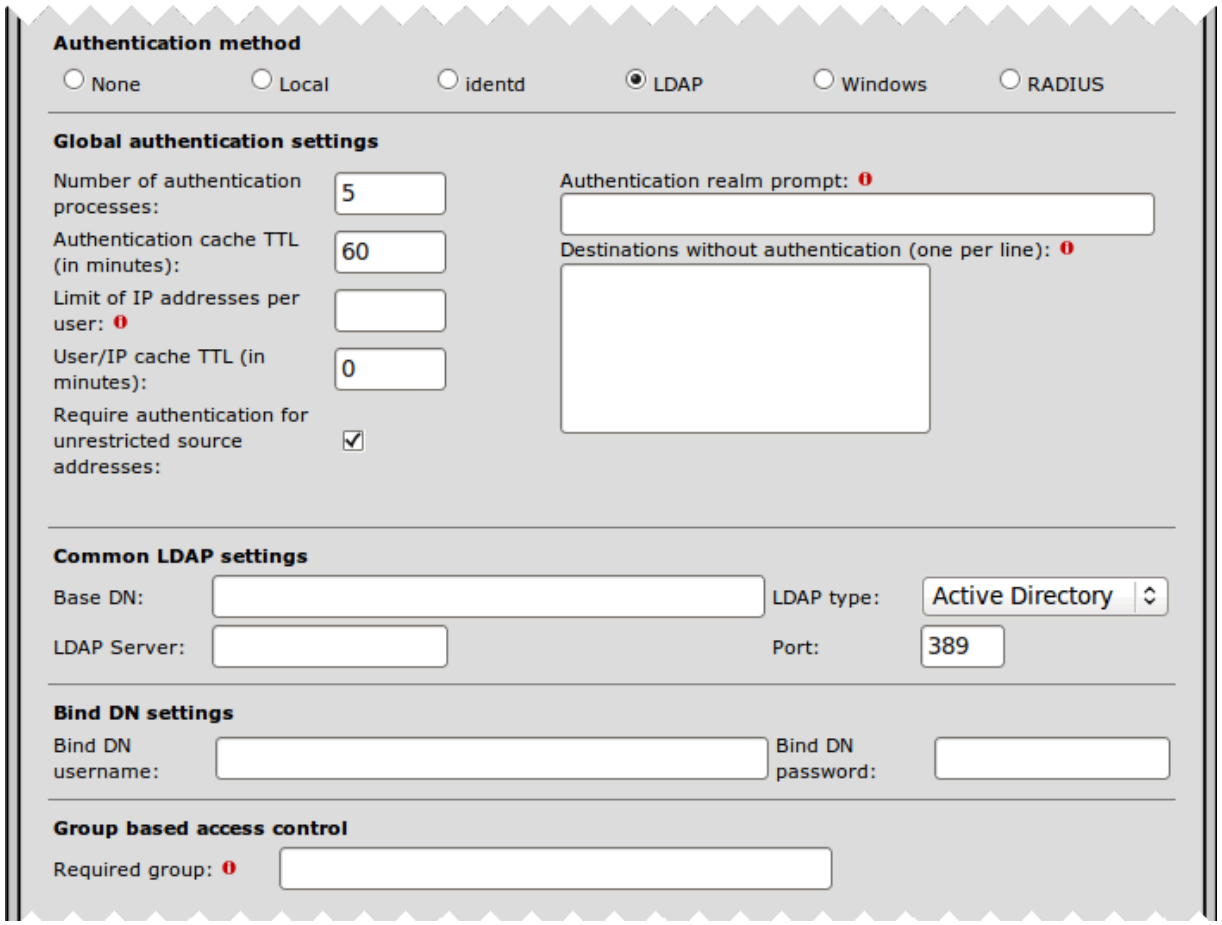
Figura 64 – Identd user *authentication*



Fonte: IPCop, 2025

A “Autenticação via LDAP” é voltada para ambientes que já utilizam diretórios LDAP, como o *Microsoft Active Directory* ou o *OpenLDAP*. Com essa integração, o IPCop pode autenticar os usuários usando as credenciais já existentes na rede corporativa ou escolar, facilitando o gerenciamento centralizado e evitando a duplicação de contas, como mostra a Figura 65. Além disso, permite aplicar regras baseadas em grupos definidos no diretório.

Figura 65 – *LDAP user authentication*

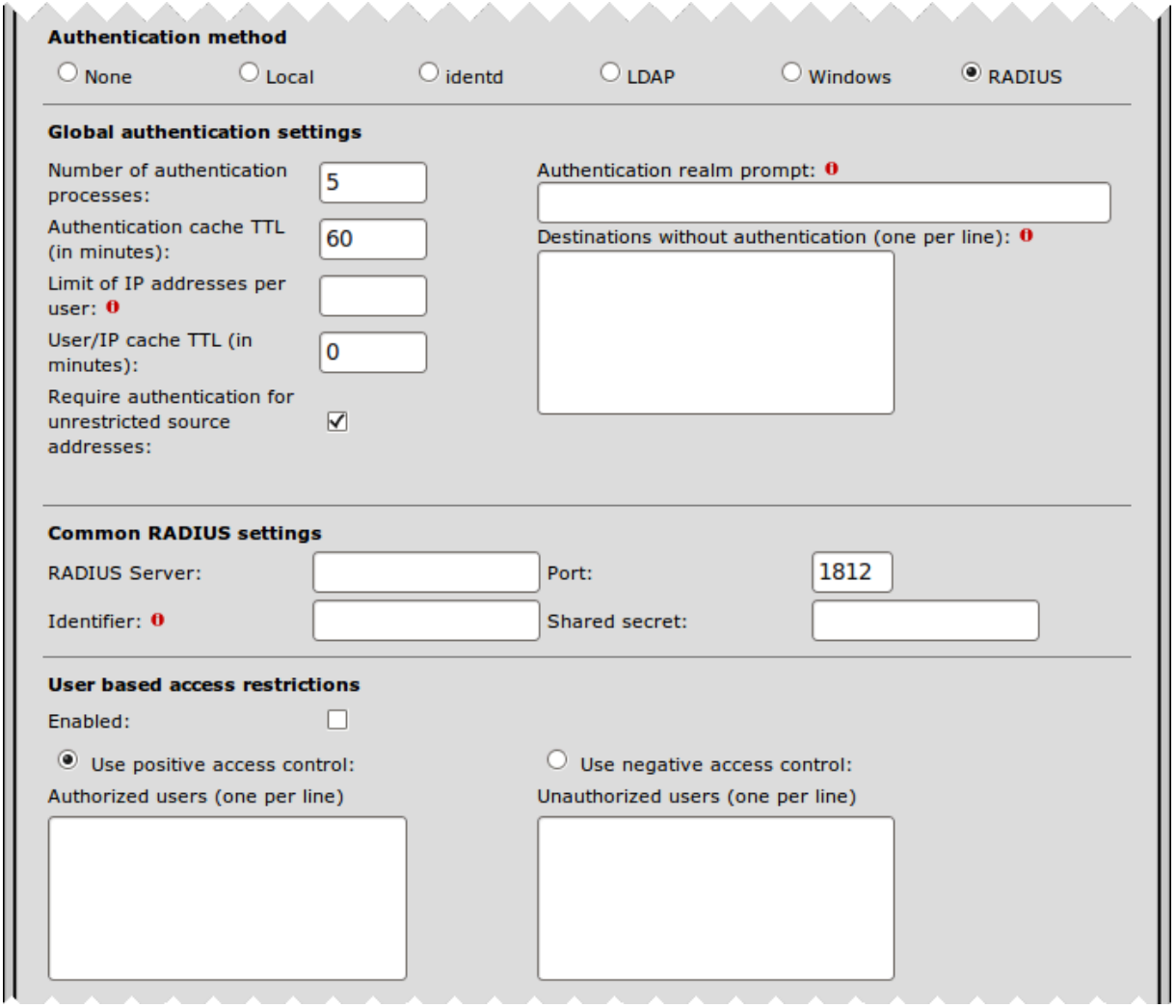


Fonte: IPCop, 2025

A "Autenticação via *Windows*" refere-se à integração com domínios do *Windows*, permitindo que o *proxy* reconheça automaticamente os usuários autenticados na rede. Esse método proporciona uma experiência mais transparente para os usuários, pois elimina a necessidade de digitar novamente credenciais ao acessar a internet. É uma solução eficiente para empresas e escolas com infraestrutura baseada em servidores *Windows*.

A "Autenticação via *RADIUS*" é mais uma opção disponível, permitindo ao IPCop consultar servidores *RADIUS* externos para validar credenciais. Este método é ideal para ambientes que já utilizam *RADIUS* como solução central de autenticação, como universidades e corporações. Com ele, é possível unificar o controle de acesso a diferentes serviços da rede em uma única base de dados de usuários, como mostra a Figura 66.

Figura 65 – *RADIUS user authentication*



Fonte: IPCop, 2025

Além das opções de autenticação, o IPCop oferece as “Extensões de Sala de Aula” (*Classroom Extensions*), voltadas especialmente para instituições de ensino. Essa funcionalidade fornece uma interface administrativa amigável para professores, permitindo que eles controlem facilmente o acesso à internet de seus alunos durante o horário das aulas. Por exemplo, é possível bloquear ou liberar sites temporariamente com poucos cliques.

As “Extensões de Sala de Aula” são especialmente úteis em laboratórios de informática, onde o controle de acesso por parte dos educadores pode influenciar diretamente na disciplina e no foco dos estudantes. Com essa ferramenta, os professores não precisam acessar o sistema principal do IPCop ou ter conhecimento técnico aprofundado, tornando o uso mais acessível e eficiente.

Essas funcionalidades avançadas do servidor *proxy* do IPCop mostram como o sistema pode se adaptar a diferentes ambientes, desde pequenas empresas até grandes instituições de ensino. A diversidade de métodos de autenticação garante flexibilidade para atender às políticas de segurança e gestão de cada rede.

Por fim, a combinação de um servidor *proxy* com autenticação de usuários e ferramentas administrativas torna o IPCop uma solução poderosa para o gerenciamento de acesso à internet. Ele não apenas protege a rede contra acessos indesejados, como também permite criar um ambiente mais controlado, organizado e adaptado às necessidades específicas dos administradores e usuários finais.

6 CONCLUSÃO

Este trabalho buscou responder à seguinte questão de pesquisa: Quais são as funcionalidades e benefícios da customização do IPCop como solução de segurança em redes de pequenas e médias empresas?

O objetivo geral deste trabalho foi explorar as etapas de customização do IPCop em redes de pequenas e médias empresas, abordando desde a configuração básica até as práticas avançadas de segurança.

Além disso, buscou-se analisar as vantagens e limitações do uso do IPCop como solução de *firewall* em ambientes corporativos, destacando como suas funcionalidades podem atender às necessidades específicas de proteção e controle de tráfego de dados em redes empresariais.

Este estudo permitiu concluir que o IPCop é uma solução viável e eficiente para a proteção de redes em pequenas e médias empresas, oferecendo uma ampla gama de recursos de segurança, desde a filtragem de pacotes até o monitoramento do tráfego em tempo real. Sua facilidade de customização e configuração torna-o uma opção acessível, mesmo para administradores com conhecimentos limitados em segurança de redes. Além disso, a flexibilidade do IPCop permite que ele se adapte a diferentes cenários e requisitos, proporcionando um nível de proteção adequado sem a necessidade de investimentos elevados em infraestrutura.

Um dos desafios críticos na customização do IPCop em redes de pequenas e médias empresas é a adaptação dessa solução de *firewall* a ambientes de rede que, muitas vezes, não foram projetados para suportar camadas dinâmicas de segurança. Esse desafio exige não apenas avanços na configuração e integração do IPCop com outras tecnologias, mas também uma abordagem de design voltada para a escalabilidade e manutenção contínua do sistema de segurança. Além disso, destaca-se a importância de políticas claras e práticas éticas na administração do *firewall*, especialmente em ambientes onde a proteção de dados e a integridade das comunicações são essenciais para a continuidade dos negócios e para a minimização de riscos associados a possíveis falhas de segurança.

Conclui-se que a customização do IPCop eleva o nível de segurança às demandas de segurança em redes empresariais de pequeno e médio porte, proporcionando controle sobre o

tráfego de dados, segmentação de rede e monitoramento contínuo. A estrutura modular do sistema permite que recursos adicionais sejam integrados conforme a necessidade, ampliando a capacidade de proteção e adequação a diferentes cenários corporativos.

Uma das dificuldades encontradas foi na busca de material sobre o IPCop e de como realizar implementações.

Para continuidade deste trabalho sugere-se:

- Analisar o desempenho do IPCop como um servidor de VPN em um ambiente simulado de PMEs, medindo a latência e a vazão de dados;
- Realizar diagnósticos de rede usando o IPCop;
- Simular ataques para conferir a eficácia do IPCop.

REFERÊNCIAS

ARIFIN, Viva; FITRIANA, R. Inge. ***Analisis Efektifitas Bandwidth Menggunakan IPCop*** (Studi Kasus: Balai Besar Teknologi Energi). *Jurnal Ilmiah Ilmu Komputer*, v. 1, n. 2, p. 1-9, 2012.

BONAVENTURE, Olivier. ***Computer Networking: Principles, Protocols and Practice.*** S.l.: S.n., 2021. Disponível em: https://www.computer-networking.info/. Acesso em: 10 abr. 2025.

BROOKS, C. ***Practical Cyber Security for SMEs.*** New York: IT Governance Publishing, 2019.

CHECK POINT. ***Check Point Next Generation Firewall (NGFW).*** 2023. Disponível em: https://www.checkpoint.com/products/next-generation-firewall/. Acesso em: 03 set. 2024.

CISCO SYSTEMS. ***Cisco ASA 5500-X Series Next-Generation Firewalls.*** 2023. Disponível em: https://www.cisco.com/. Acesso em: 03 set. 2024.

ENDIAN. ***Endian Firewall Community.*** 2024. Disponível em: https://www.endian.com/community/. Acesso em: 03 set. 2024.

FERREIRA, José; LEMOS, Victor. ***Segurança de Aplicações Web***. 2. ed. São Paulo: Novatec, 2018.

FERREIRA, Ricardo. **Gestão de riscos cibernéticos e continuidade de negócios.** Revista Brasileira de Segurança da Informação, v. 7, n. 2, p. 25–39, 2021.

FOROUZAN, Behrouz A. **Segurança de redes de computadores.** 3. ed. São Paulo: Cengage Learning, 2017.

IPCOP PROJECT. *IPCop v2.1.9* ***Documentation.*** Disponível em: https://www.ipcop.org/docs.html. Acesso em: 05 abr. 2025.

KREMER, J. ***Cybersecurity for Small and Medium-Sized Businesses***. Oxford: Oxford University Press, 2021.

MANIK, Burju; LUBIS, Imran. ***Perbandingan Kinerja IPCop dengan Honeypot dalam Mengamankan Server Linux dari Serangan Hacker.*** *Jurnal Ilmiah Teknologi dan Informasi*, v. 4, n. 2, p. 57-63, 2021.

MENEGUITE, Alexandro. ***Firewall IPCop: instalação, configuração e utilização.*** São Paulo: Érica, 2010.

NORTHCUTT, Stephen; ROSE, Judy Novak. ***Network Intrusion Detection.*** 3. ed. Indianapolis: New Riders, 2020.

OLIVEIRA, Fernanda A.; MARTINS, João P. **Soluções de Firewall para Pequenas e Médias Empresas.** Revista de Tecnologia da Informação, v. 8, n. 1, p. 42-55, 2022.

PALO ALTO NETWORKS. ***PAN-OS Next-Generation Firewall.*** 2024. Disponível em:

https://www.paloaltonetworks.com/. Acesso em: 03 set. 2024.

SHINDER, Thomas W. ***Configuring ISA Server 2000: Building Firewalls for Windows Server 2003, Windows 2000, and Windows NT.*** Indianapolis: Syngress, 2020.

SIMANULLANG, Alexander et al. ***Simulasi Pemanfaatan IPCop sebagai PC Router dalam Jaringan Local (LAN) di Laboratorium FE-UMI.*** *Jurnal Sistem Informasi*, v. 6, n. 1, p. 55-62, 2018.

STALLINGS, William. ***Cryptography and Network Security: Principles and Practice.*** 8. ed. Boston: Pearson, 2021.

TANENBAUM, Andrew S.; FEAMSTER, Nick. **Redes de Computadores.** 6. ed. São Paulo: Pearson, 2021.

ZWICKY, Elizabeth D.; COOPER, Simon; CHAPMAN, D. Brent. ***Building Internet Firewalls.*** 2. ed. Sebastopol: O'Reilly Media, 2021.

PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
GABINETE DO REITOR

Av. Universitária, 1069 • Setor Universitário
Caixa Postal 86 • CEP 74605-010
Goiânia • Goiás • Brasil
Fone: (62) 3946.1000
www.pucgoias.edu.br • reitoria@pucgoias.edu.br

RESOLUÇÃO nº 038/2020 – CEPE

ANEXO I

APÊNDICE ao TCC

Termo de autorização de publicação de produção acadêmica

O estudante Jonas Nunes Resende Filho do Curso de Engenharia da Computação, matrícula 20191003300683, telefone: 62 984053475 e-mail jnresende18@gmail.com, na qualidade de titular dos direitos autorais, em consonância com a Lei nº 9.610/98 (Lei dos Direitos do Autor), autoriza a Pontifícia Universidade Católica de Goiás (PUC Goiás) a disponibilizar o Trabalho de Conclusão de Curso intitulado CUSTOMIZAÇÃO DO IPCOP COMO SOLUÇÃO DE SEGURANÇA EM REDES DE PEQUENAS E MÉDIAS EMPRESAS, gratuitamente, sem ressarcimento dos direitos autorais, por 5 (cinco) anos, conforme permissões do documento, em meio eletrônico, na rede mundial de computadores, no formato especificado (Texto(PDF); Imagem (GIF ou JPEG); Som (WAVE, MPEG, AIFF, SND); Vídeo (MPEG, MWV, AVI, QT); outros, específicos da área; para fins de leitura e/ou impressão pela internet, a título de divulgação da produção científica gerada nos cursos de graduação da PUC Goiás.

Goiânia, 21 de Junho de 2025.

Assinatura do autor: gov.br Documento assinado digitalmente JONAS NUNES RESENDE FILHO Data: 21/06/2025 13:04:39-0300 Verifique em https://validar.iti.gov.br

Nome completo do autor: Jonas Nunes Resende Filho

Assinatura do professor–orientador: gov.br Documento assinado digitalmente SOLANGE DA SILVA Data: 21/06/2025 14:00:42-0300 Verifique em https://validar.iti.gov.br

Nome completo do professor-orientador: Solange da Silva