MANUAL DE ADMINISTRAÇÃO

Versão 1.4

Índice

1. Introdução

Bem vindo e obrigado por optar pelo Netdeep Cop!

1.1. O que é o Netdeep Cop?

O Netdeep Cop é uma solução da Netdeep para otimização e controle do acesso à Internet. A solução oferece recursos de cache e filtros de conteúdo Web, garantindo uma melhor performance da rede, permitindo que os usuários utilizem o serviço de forma eficiente e segura, proporcionando um maior controle minucioso da utilização do serviço de acesso a Web.

O Netdeep Cop é um poderoso Firewall/Proxy baseado no Sistema Operacional Linux e está em constante atualização e testes pela equipe de desenvolvimento da Netdeep, disponibilizando novas facilidades e melhorias. Você pode também participar dando sugestões através do site http://www.netdeep.com.br.

O Netdeep Cop foi desenvolvido a partir do sistema operacional LINUX com um kernel personalizado para este fim. Reunimos as melhores ferramentas disponíveis em software livre, customizadas e otimizadas, e adicionamos, ainda, várias outras ferramentas complementares que fazem do Netdeep Cop um produto rápido para instalar e fácil de configurar.

O Netdeep Cop é uma Distribuição Linux, portanto, não requer nenhum Sistema Operacional e/ou Softwares complementares. É compatível com a grande maioria dos Hardwares disponíveis no mercado e com baixa exigência na configuração da CPU.

Sobre as características de Direitos de Uso veja o apêndice **Licença de Uso** no final deste Manual.

1.2. Principais Características

INSTALAÇÃO:
Instalação rápida (menos de 15 minutos)
Manual de Instalação em Português (Impresso)
Baixa exigência e ampla compatibilidade de Hardware
Baseado em OS/LINUX com Kernel Otimizado
Suporte à DMZ
Suporte à WIRELESS

ADMINISTRAÇÃO:
Administração fácil via WEB/Browser
Manual de Administração em Português (HTML)
Estatísticas e Gráficos de Monitoramento do Acesso Internet
Logs dos Serviços
Backup das configurações

PROTEÇÃO:
FIREWALL baseado em IPTABLES
IDS – Detecção de Intrusos
Proteção DoS, DDoS
Prevenção a ataques repetitivos

CONTROLE:
PROXY/CACHE Avançado Transparente e/ou Autenticado
Filtro de Sites/IP/Black-Lists
Filtro de códigos maliciosos
Permite acesso à CAIXA-Conectividade Social (Sem autenticação de Proxy)

SERVIÇOS:
DHCP Client/Server
PPPoE
Roteamento dinâmico/estático
Redirecionamento de Portas (NAT/PAT)
QoS - Controle de Banda/Tráfego
VPN IPSec e SSL sem limite de túneis
SSH Client
DNS Dinâmico
NTP – Servidor de Tempo
Acelerador de Atualização

E MAIS:
Usuários ilimitados
WebSupport
Updates via Internet

2. Administração e Configuração

2.1. Interface de Administração Web (GUI)

Acessar a interface Netdeep Cop GUI é simples, basta iniciar seu browser(navegador internet) e inserir o Endereço IP da interface GREEN do Netdeep Cop ou o hostname do seu servidor Netdeep Cop, seguido da porta 445 (https/seguro) ou 81(que redireciona a 445), Exemplos: *https://netdeepcop:445* or *https://192.168.10.1:445* ou *http://netdeepcop:81* ou *http://192.168.10.1:81.*

Nota:

O Netdeep Cop é compatível com a maioria dos browsers(navegadores) internet, com suporte https, disponíveis. Em caso de problemas acesse nosso websupport http://www.Netdeep Cop.com.br .

Acesse a interface de administração web do seu Netdeep Cop e comece a explorar as diferentes opções e informações do servidor e veja como é simples e intuitivo administrá-lo e configurá-lo.

A interface de administração possui menu (horizontal) no topo da tela, navegável através de [tab]s, ao clicar em uma opção o submenu correspondente aparecerá com várias opções relacionadas (vertical).

Estes são os principais tópicos da interface de administração:

Na tela inicial ao centro você poderá ver os dados iniciais e *status* de Servidor Netdeep Cop.

Ao acessar um item do ambiente de administração será solicitado uma autenticação, faça *login* com o usuário e senha *admin.*

Os botões [conectar], [desconectar] e [atualizar] estarão disponíveis na tela principal, em caso de conexão PPOE / Discada, para que você possa efetuar sua conexão junto ao seu Provedor*.*

- **Sistema: Submenu de configurações e utilitários do Netdeep Cop.**

- Principal [retorne a página principal de administração]

- Atualizações [atualize seu Servidor Netdeep Cop]

- Senhas [altere as senhas dos usuários admin e de discagem]

- Acesso SSH [permita/bloqueie o acesso remoto SSH ao Servidor Netdeep Cop]

- Cliente SSH [cliente java para acesso ao prompt do Servidor Netdeep Cop]

- Configurações da GUI [altere as configurações da Interface de Administração]

- Cópia de Segurança [faça backup das configurações do Servidor Netdeep Cop]

- Desligar [desligue ou reinicie seu Servidor Netdeep Cop]

- Licença de Uso [registre seu Netdeep Cop]

- Manual de Administração [acesso ao Documentação do programa]

- Créditos [Informações sobre os desenvolvedores do Netdeep Cop)

- **Situação: Submenu de informações detalhadas do Servidor Netdeep Cop.**

- Situação do Sistema [informações de hardware, software e serviços do Servidor]

- Situação da Rede [informações das configurações de rede do Servidor]

- Gráfico do Sistema [Gráfico da situação de CPU/Memória/Disco/Swap do Servidor]

- Gráficos de Tráfego [Gráficos com a situação de tráfego de sua rede]

- Gráficos do Proxy [Gráficos de utilização do Proxy]

- Relatórios Internet [Estatísticas de acesso Internet por usuários e sites]

- Conexões [veja as conexões IP estabelecidas em sua rede]

• Rede: Submenu das configurações de rede (dial-up/PPP/PPPOE).

- Discagem [configurações para conexões discadas]

- Modem DSL [configurações especiais para Modens ADSL]

- Modem Dial [configurações para Modens Dial-Up]

• Serviços: Configuração/Administração dos serviços do Servidor Netdeep Cop.

- Proxy Avançado [configure/administre o Proxy/Cache]

- Filtro de URL [configure/administre o acesso Internet de sua rede]

- Servidor DHCP [habilite/desabilite e configure o Serviço DHCP]

- DNS Dinâmico [configure/administre DNS Dinâmico para sua rede]

- Editar Hosts [crie/altere hosts para sua rede]

- Servidor de Horário [conecte/configure um servidor de tempo]

- Controle de Tráfego [controle/administre o tráfego de sua rede]

- Controle de Banda [controle/administre sua banda Internet]

- Detecção de Intrusos [ative/desative o serviço de detecção de intrusos]

• Firewall: Configuração/Administração de opções de firewall do Netdeep Cop.

- Forwarding de Porta [configure redirecionamentos de portas IP para servidores internos]

- Acesso Externo [configure as portas de acesso externo ao Servidor Netdeep Cop]

- Firewall Avançado [crie/altere regras avançadas de Firewall]

- Configuração de Firewall Avançado [crie/altere regras de serviços avançados de Firewall]

• VPNs: Configuração/Administração de Redes Privadas.

- VPN [administre/configure VPNs para sua rede]

- **Logs: Veja todos os logs do servidor Netdeep Cop.**

- Configuração Log [administre a geração de Logs dos serviços do Netdeep Cop]

- Resumo Log [veja um resumo dos principais serviços do Netdeep Cop]

- Log Filtros URL/Proxy [veja os logs do serviço do Filtro de URL]

- Log Firewall [veja os logs do serviço de Firewall]

- Log IDS [veja os logs do serviço de Detecção de Intrusos]

- Log Sistema [veja os logs principais do Servidor Netdeep Cop]

A Interface de Administração Web na página inicial apresentará informações diferentes, dependendo do modo como o Netdeep Cop foi configurado.

Se sua conexão de Internet é via uma interface Ethernet RED, a interface web não mostrará o nome da conexão corrente, etc.

Nota:

Você não verá uma conexão ativa até que tenha terminado a configuração do servidor do seu Netdeep Cop.

No centro você verá o nome do domínio completo, e informações de sua conexão Internet e de seu Servidor Netdeep Cop.

Botões de Conexão do Modem

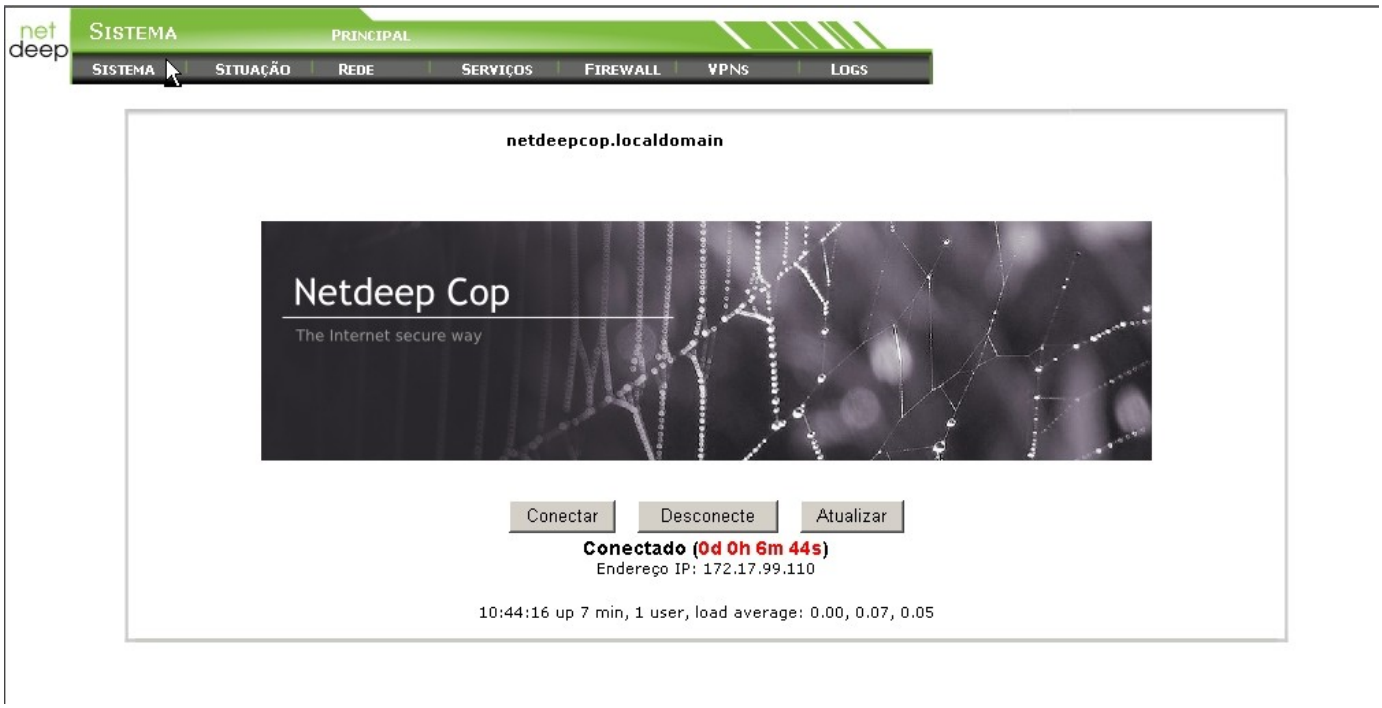
- [Conectar] / [Desconectar] / [Atualizar] – Estes botões servem para forçar a tentativa de conexão/desconexão a Internet.

As conexões a Internet que exijam autenticação devem ser configuradas através das opções do [SubMenu REDE]:

O Status de conexão atual será visível na parte inferior da tela principal

[14:00:40 up 11:22, 0 users, load average: 0.00, 0.00, 0.00]
Esta linha é basicamente a saída do comando Linux **[uptime].**

O Netdeep Cop tem dois usuários web, adicionado ao login do usuário principal. O primeiro é chamado de *admin*. A autenticação deste usuário permite acesso a todos os itens da Interface de Administração Web (GUI). Os outros usuários, chamados dial, podem unicamente usar os botões [Conectar] ou [Desconectar]. Por padrão, usuário dial é desabilitado, para ativá-lo você precisa configurar um password (senha) para ele. Nenhum password (senha) é necessário para ver a página principal da GUI e a página de Downloads. Todos os outros itens pedem o password (senha) do administrador.



2.2. SubMenu Sistema

Selecione o SubMenu Sistema na barra no topo da tela e as seguintes opções aparecerão:

- ***Principal*** *[retorne a página principal de administração]*

- ***Atualizações*** *[atualize seu Servidor Netdeep Cop]*

- ***Senhas*** *[altere as senhas dos usuários admin e de discagem]*

- ***Acesso SSH*** *[permita/bloqueie o acesso remoto SSH ao Servidor Netdeep Cop]*

- ***Cliente SSH*** *[cliente java para acesso ao prompt do Servidor Netdeep Cop]*

- ***Configurações da GUI*** *[altere as configurações da Interface de Administração]*

- ***Cópia de Segurança*** *[faça backup das configurações do Servidor Netdeep Cop]*

- ***Desligar*** *[desligue ou reinicie seu Servidor Netdeep Cop]*

- ***Licença de Uso*** *[registre seu Netdeep Cop]*

- ***Manual de Administração*** *[acesso web a documentação do programa]*

- ***Downloads*** *[kit de utilitários de rede]*

- ***Créditos*** *[Informações sobre os desenvolvedores do Netdeep Cop)*

2.2.1. Atualizações

Esta seção se divide em 3:

1. Mostra seu nível atual das atualizações de Servidor Netdeep Cop.

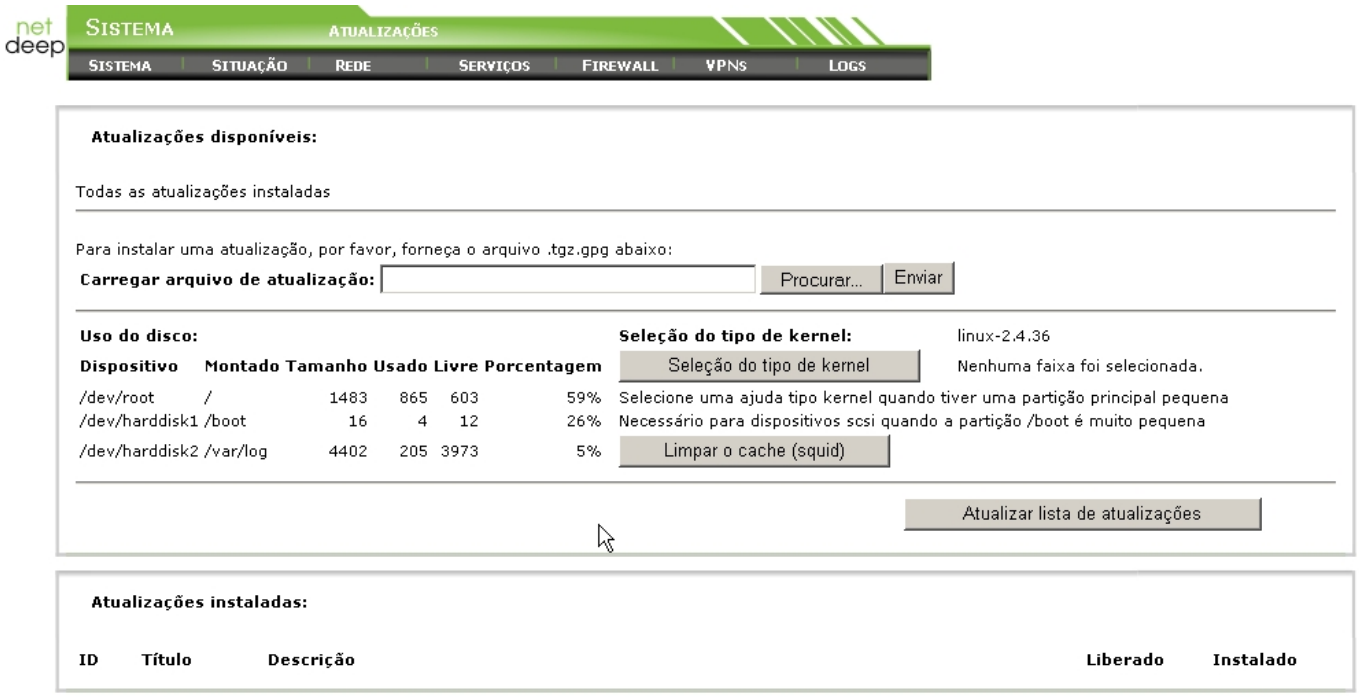
2. Informa sobre as novas atualizações disponíveis.

3. Permite aplicar uma atualização disponível._

Toda vez que você se conecta a Internet, o Netdeep Cop irá checar sobre novas atualizações disponíveis. Você, também, pode clicar na lista de atualizações. Quando uma nova atualização está disponível, você verá a informação na tela com uma pequena descrição e um link para maiores informações. Acesse o link "Info" para ver todas as informações relevantes sobre a atualização.

Executando o download a atualização será baixada em sua máquina (a que está rodando o web browser e não a máquina Netdeep Cop)

Quando o download estiver concluído, use a página de Atualizações para fazer o Upload e aplicar a atualização em seu servidor Netdeep Cop.



Nota

Aplique somente as atualizações oficiais do Netdeep Cop. Algumas atualizações podem re-inicializar o seu servidor Netdeep Cop, então leia todas as informações sobre a atualização antes de aplicá-la.

2.2.2. Senhas

O SubMenu Senhas da GUI permite mudar os passwords (senha) do *admin* e/ou do usuário *dial*. Para alterar insira o password (senha) desejado do Usuário que você deseja atualizar e clique em [salvar].

Ative o usuário Dial se necessário. Este usuário especial possui a habilidade de usar os botões na página principal do Netdeep Cop, mas não pode alterar outros itens da GUI do Netdeep Cop. Use

esse artifício se você tem uma Conexão Internet que exija autenticação.

2.2.3. Acesso SSH

O SubMenu SSH da GUI permite decidir se o acesso remoto SSH ao servidor Netdeep Cop está ou não disponível.

Ative colocando um check na caixa do acesso remoto SSH.

É também possível configurar muitos parâmetros SSH *daemon* através deste item. A opção SSH é desabilitada por padrão e pode ser habilitada apenas quando necessário e desabilitada ao final.

Similar às portas HTTP e HTTPS para a máquina Netdeep Cop que foram mudados para as portas 81 e 1445, a porta SSH na máquina Netdeep Cop foi mudado para 222. Se você está usando um aplicativo GUI para acessar a sua máquina Netdeep Cop, lembre-se de especificar a porta 222. Se você está usando o SSH, comando scp ou sftp, a sintaxe para especificar as portas fora do padrão é diferente para cada comando.

Partindo do ponto de que sua máquina Netdeep Cop está no endereço IP 192.168.254.1, o comando será:

SSH

$ **ssh -p 222 root@192.168.254.1**

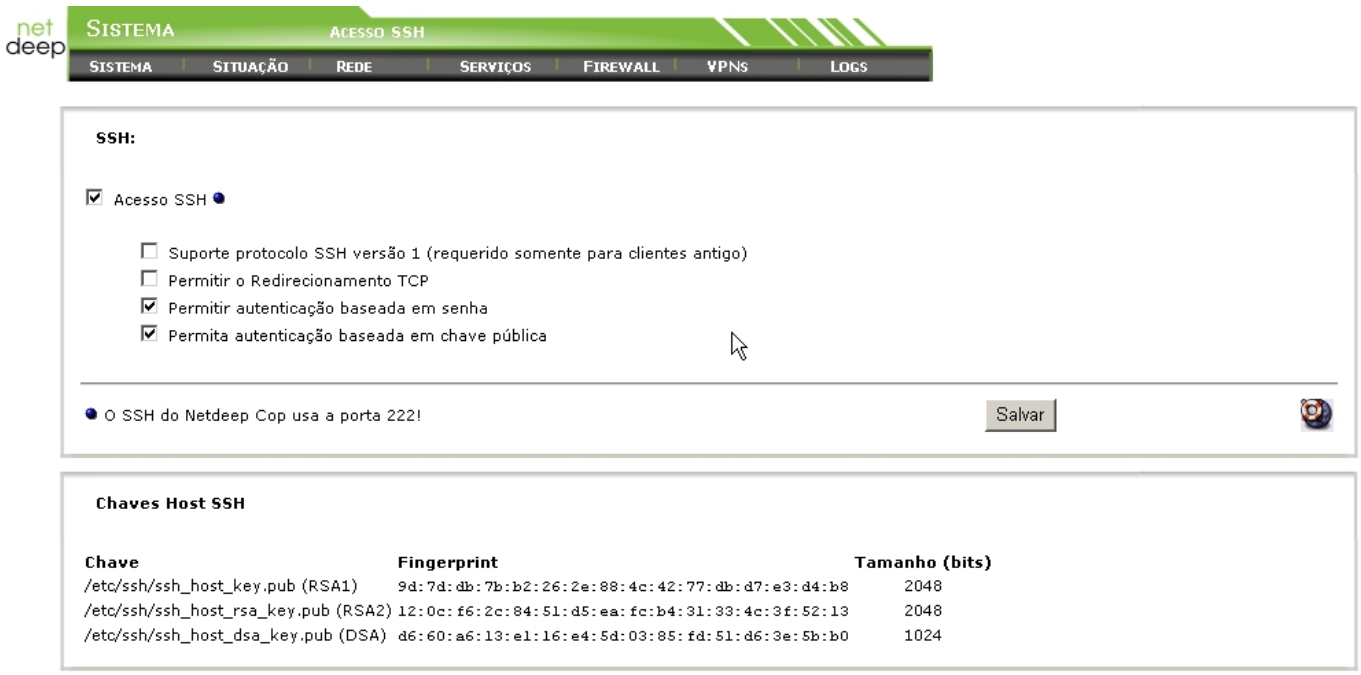
SCP

$ **scp -P 222 [arquivos] root@192.168.254.1:**

SFTP

$ **sftp -o port=222 root@192.168.254.1**

Use as páginas de ajuda de cada comando para adquirir uma explicação mais completa.



2.2.4. Cliente SSH

Configure as opções do Cliente SSH:

Este cliente web SSH permite acessar através de uma interface Java o *prompt* do Servidor Netdeep Cop e até outros Hosts que possuam acesso remoto. É necessário que sua máquina possua o Java instalado.

Configure, então, as cores, versão de Suporte SSH, compressão, etc.

Para acessar o cliente web SSH clique em [iniciar cliente].

2.2.5. Configurações da GUI

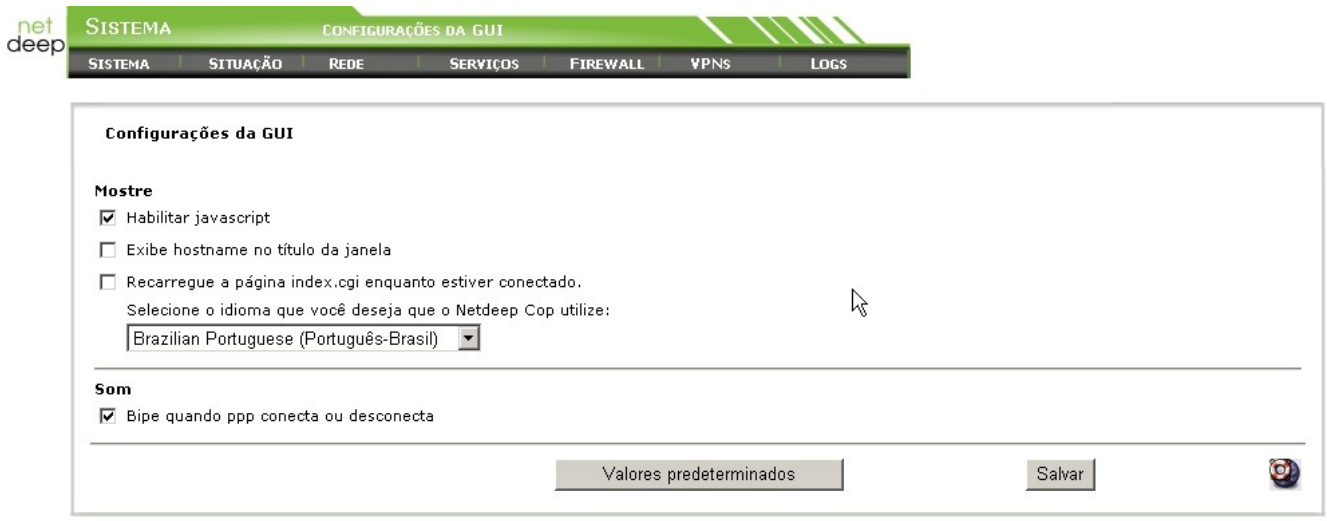
Nesta página você configura como as páginas da GUI do Netdeep Cop funcionam e aparecem.

Habilitar Javascript: A Interface de Administração Web (GUI) do Netdeep Cop usa extensivamente o JavaScript para prover uma visão melhorada. No entanto, alguns browsers (navegadores) não funcionam corretamente com JavaScript. Se este botão não for clicado, vários menus *dropdown* serão desabilitados e suas escolhas aparecerão no topo de qualquer página.

Exibir hostname: Este item mostrará o hostname do Netdeep Cop no topo de cada página. Se você mantém mais de uma máquina Netdeep Cop, isto será vantajoso, sendo que você será capaz de dizer em que máquina seu browser (navegador) está atualmente.

Selecione o Idioma: que você desejar para a exibição do Netdeep Cop.

O Netdeep Cop está planejando disponibilizar mais idiomas. Quando novos idiomas estiverem disponíveis, você poderá fazer o download de uma nova língua e se desejar, e ativá-la através da GUI.



2.2.6. Cópia de Segurança

Há dois meios de fazer o backup do Netdeep Cop e três jeitos de restaurá-lo.

Você pode criar um disquete de restauração ou criar arquivos de restauração.

1. Ao criar um disquete de backup, a informação salva é limitada porque seu tamanho é de 1.44 Mb. Mas este é, no entanto, o backup usado quando o Netdeep Cop é restaurado da mídia (disquete), durante a instalação do Netdeep Cop, será pedido um disquete para fazer a restauração. Todas as configurações salvas no disquete serão restauradas e a instalação será completada.

2. Quando se cria o backup de arquivos, o Netdeep Cop cria dois arquivos, um arquivo *tar.gz* e um arquivo *.dat*. Também cria uma chave de backup única que será usada para criptografar_todos os arquivos *tar.gz*. Enquanto o arquivo *.dat* é criptografado, a criptogragia é usada para "assinar" o arquivo *.dat* para que não seja acidentalmente restaurado numa máquina Netdeep Cop diferente. Uma vez que essa chave seja criada, apenas arquivos *.dat* específicos podem ser usados em uma restauração.

Para uma proteção backup/restauração completa, todos os métodos devem ser usados.

Se você precisa reinstalar o Netdeep Cop use o disquete de backup, se você o tiver, durante a o processo de instalação para restaurar as configurações antigas. Então importe o arquivo .tar.gz para a nova máquina Netdeep Cop e restaure todas as configurações e logs.

2.2.6.1. Backup em Arquivos

Ao clicar no botão [criar], o Netdeep Cop irá gerar uma chave de backup, se uma já não foi previamente criada, e criar os dois arquivos backup. Se esta é a primeira vez que você está criando arquivos de backup, o texto que está no botão [Importar *.tar.gz*] irá mudar para [Importar *.dat*.]. Isto indica que no futuro apenas arquivos *.dat* serão importados. Em seguida exporte ambos arquivos para o computador em que você está rodando o seu browser (navegador) clicando nos seus links [Exportar].

Se você deseja fazer a restauração de um arquivo backup, selecione um dos Backups listados na janela Backup Sets. Ou importe um arquivo *.dat* salvo por outra máquina.

2.2.6.2. Backup em Disquete

O meio mais fácil de restaurar sua configuração é reinstalar o Netdeep Cop do CD-ROM. Durante o

processo de instalação, você será questionado se possui um disquete backup com uma configuração do Netdeep Cop. Se você deseja restaurar sua configuração através de um disquete de backup, coloque o disquete no drive e selecione o botão [Restaurar]. Sua configuração será restaurada e a instalação será concluída.

Após completar a instalação, você pode usar o SubMenu de Backup para importar um arquivo *.tar.gz* não assinado e restaurar a partir dele, adquirindo todos os logs perdidos, etc.

AVISO

O Netdeep Cop não grava em disquetes com formato DOS. Para usar os disquetes para o Netdeep Cop, você precisará formatá-lo no Linux.O comando para fazê-lo é:

*# **fdformat /dev/fd0***

*Se você possui outra máquina Linux, use-a para formatar o disquete. Ou use o acesso/cliente SSH ou Putty para fazer o login como root no Netdeep Cop e execute este comando. Antes de executar o comando **fdformat** insira o disquete no drive.*

2.2.6.3. Configuração do Backup

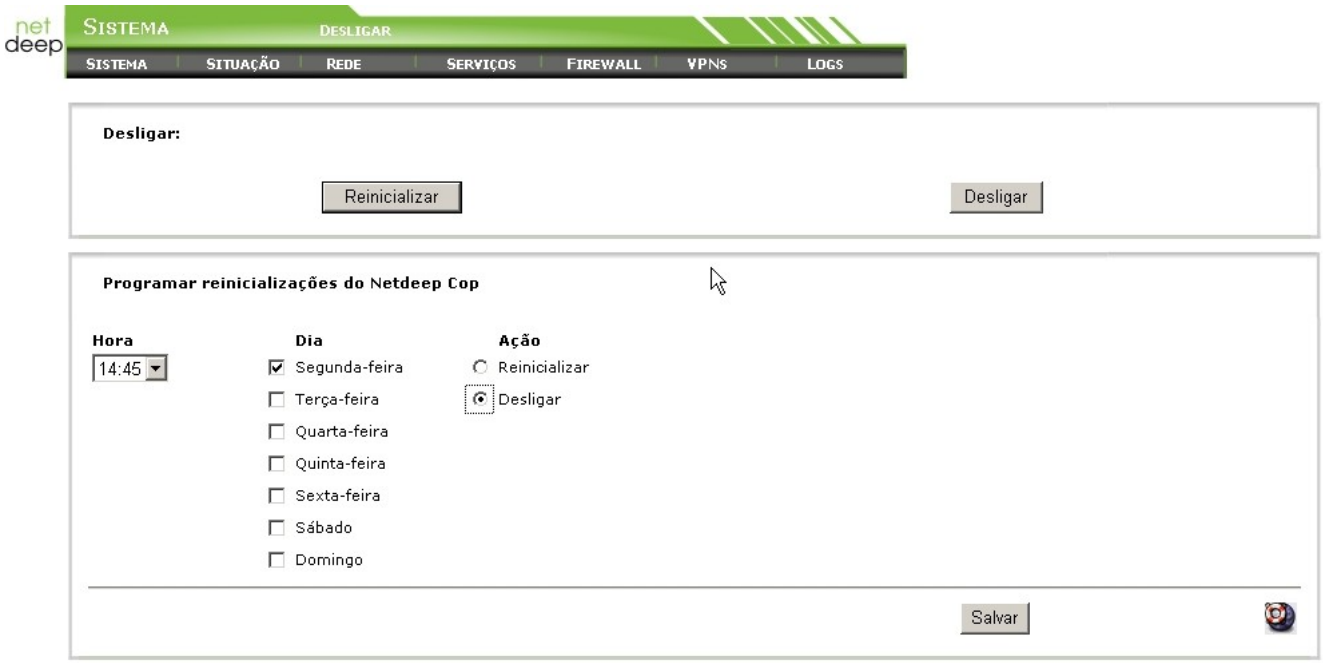
Coloque o disquete no drive e clique no botão [Cópia de segurança para o disquete]. Sua configuração será passada para o disquete e será verificada.

2.2.6.4. Informação

Todas mensagens produzidas durante o backup aparecerão nesta página.

2.2.7. Desligar

Esta página permite você Desligar ou Re-Iniciar o Servidor Netdeep Cop. Simplesmente clique no botão da opção que você quer e pronto.



2.2.8. Licença de Uso

Esta página permite você registrar e ativar sua Licença de Uso do Netdeep Cop.

Somente a partir da ativação você terá acesso completo à todas as funcionalidades do Servidor Netdeep Cop.

Clique no botão [Registrar] e preencha os dados. A equipe Netdeep Cop lhe enviará por email a chave para ativar sua Licença.

2.2.9. Manual de Administração

Para facilitar a administração do Netdeep Cop, disponibilizamos o Manual de Administração do Netdeep Cop em arquivo PDF.

2.3. SubMenu Situação

2.3.1. Situação do Sistema

Estas páginas apresentam um conjunto de informações se referindo à situação atual do seu servidor Netdeep Cop:

. Serviços: Exibição de quais serviços estão rodando no momento.

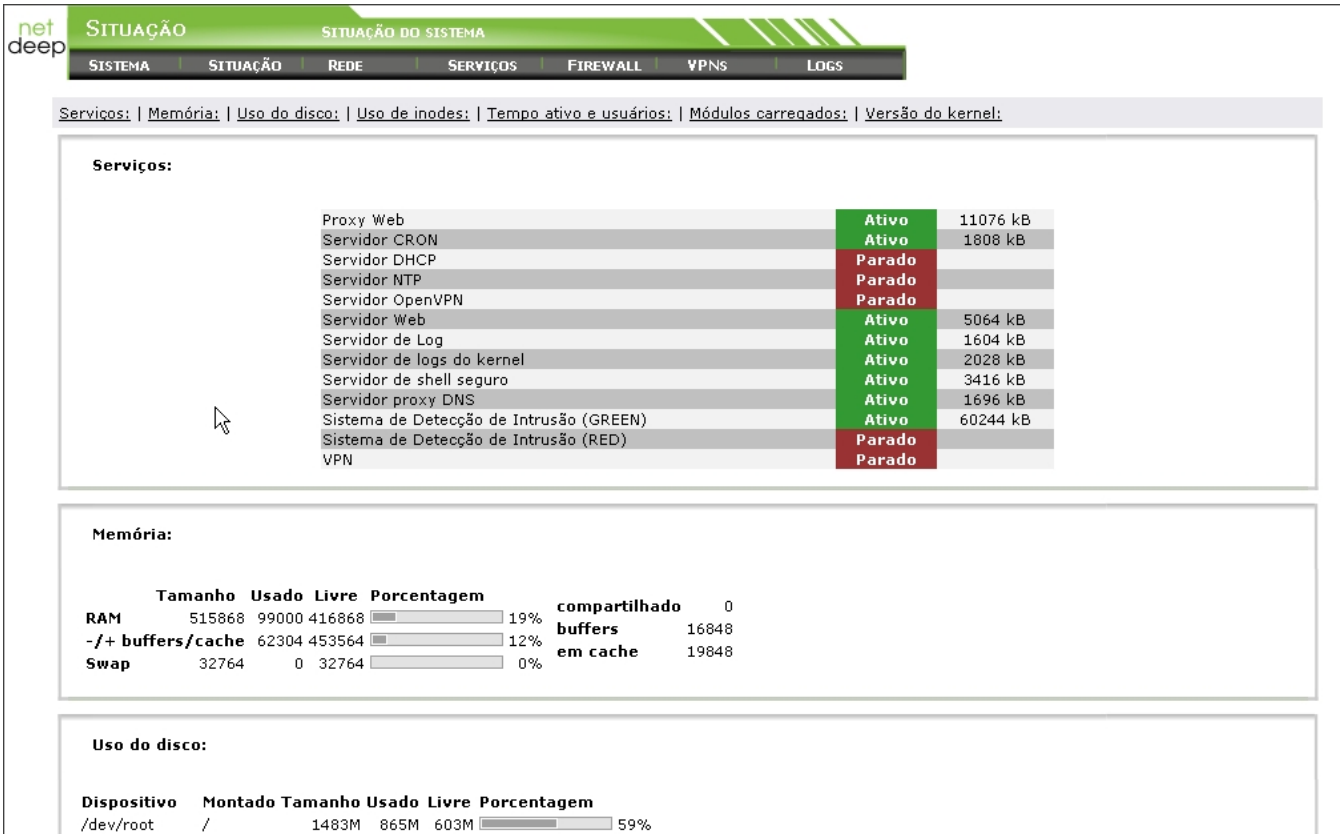
. Memória: Exibe a memória/swapfile em uso no seu servidor Netdeep Cop.

. Uso do Disco: Exibe a quantidade total/usada do espaço do disco rígido no seu Netdeep Cop.

. Tempo ativo e Usuários: Exibe o output do comando **uptime** e informação dos usuários ativos no momento, no servidor Netdeep Cop.

. Módulos: Exibe todos os módulos carregados no momento e em uso pelo kernel.

. Versão Kernel: Exibe informações do próprio Kernel do Netdeep Cop.



2.3.2. Situação da Rede

Esta Página apresenta a Situação da Rede, envolvendo interfaces e protocolos

. Interfaces: Esta seção mostra a informação em todos as interfaces (placas) de rede. Isto inclui PPP, IPSec, Loopback, etc.

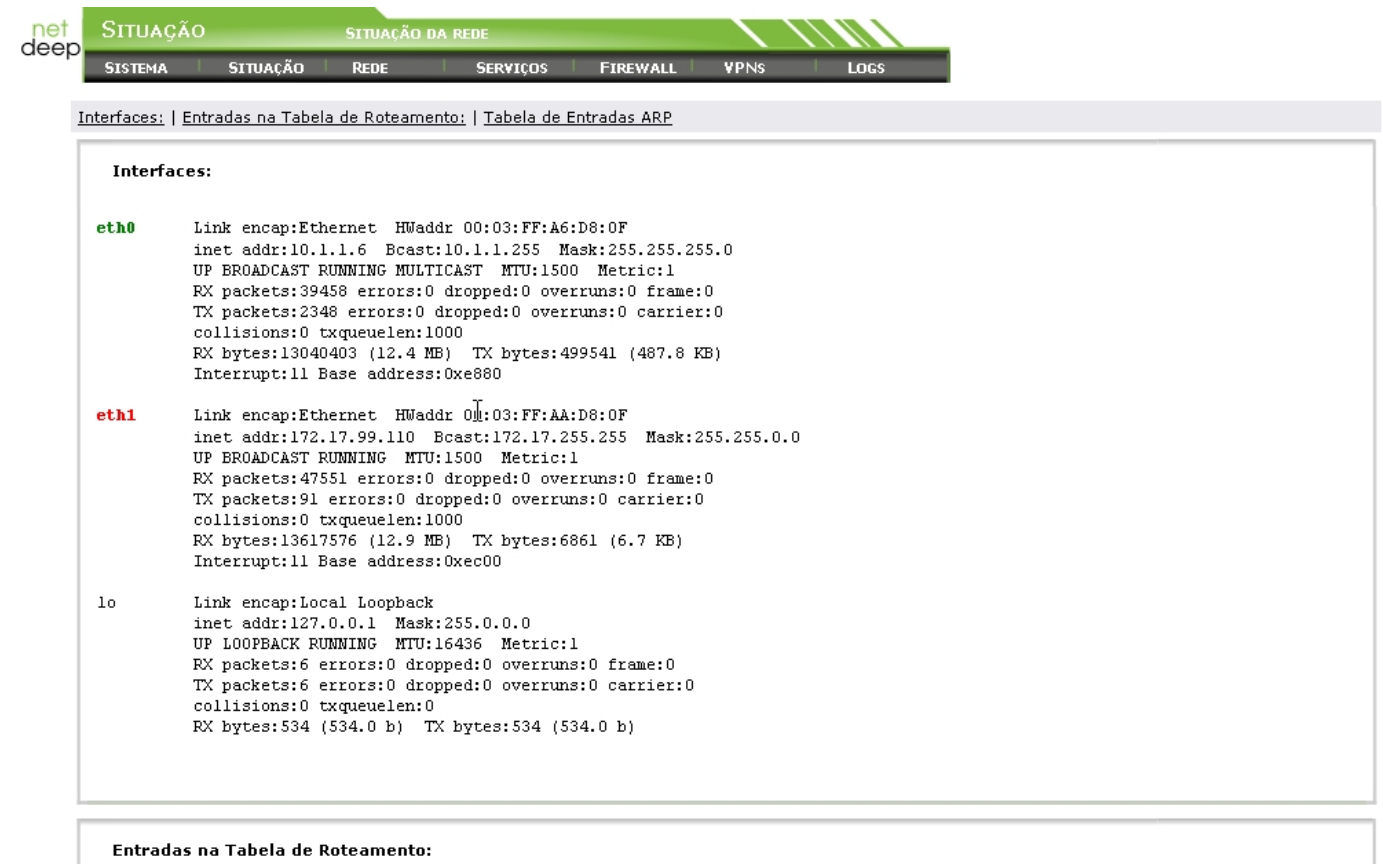
. Leases Dinâmicas: Exibe o conteúdo do arquivo /var/state/dhcp/dhcpd.leases se o DHCP está ativo. As leases dinâmicas correntes, ou seja os endereços IP distribuídos automaticamente pelo Serviço de DHCP, estão listadas com hostnames (se disponíveis) e com datas de validade. As leases que validaram são registradas.

Nota

Esta seção será visível apenas se o DHCP estiver habilitado. Leia a seção sobre o Servidor DHCP para maiores detalhes.

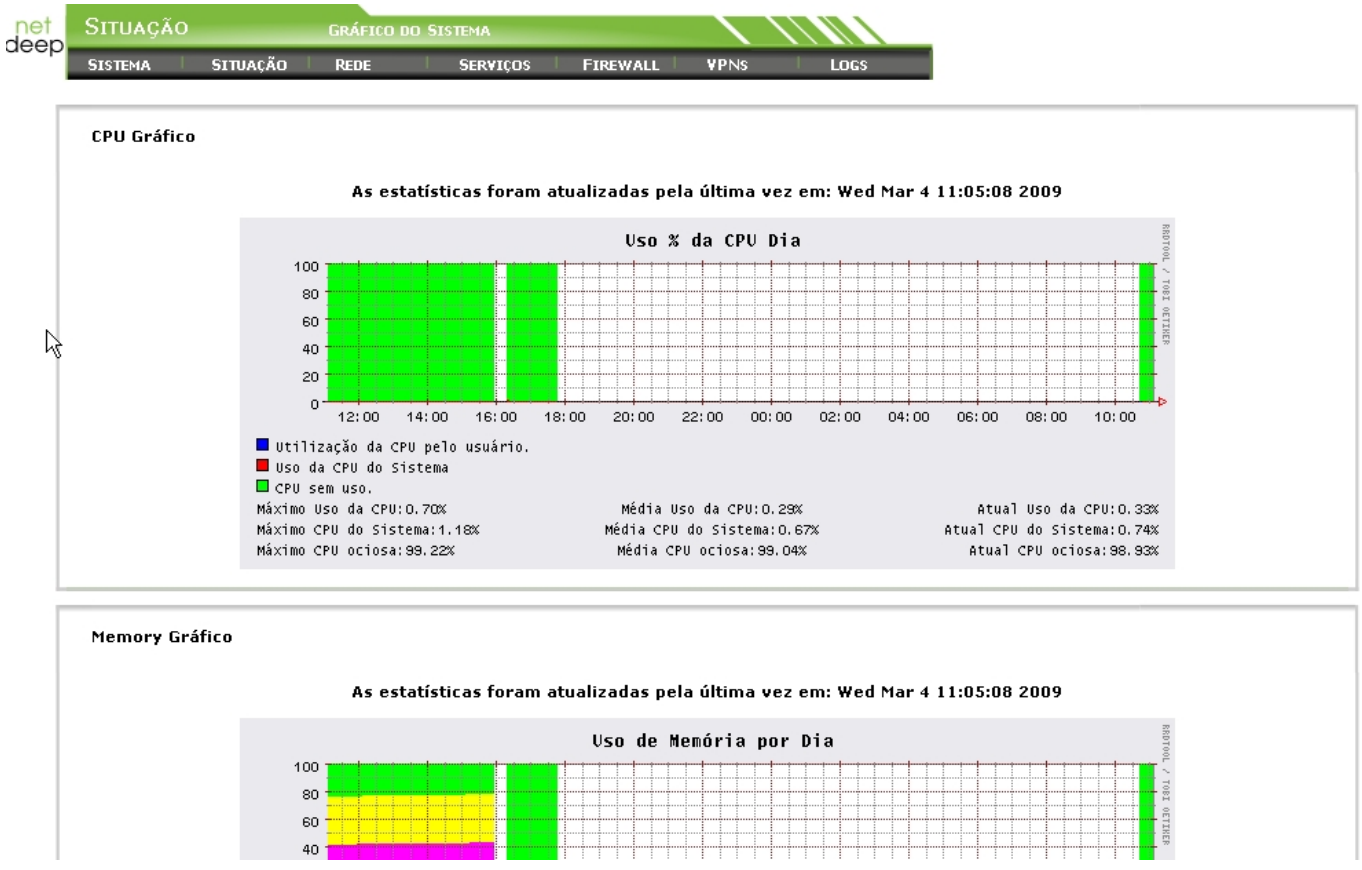
. Entradas da Tabela de Roteamento

. Entrada da Tabela ARP



2.3.3. Gráficos do Sistema

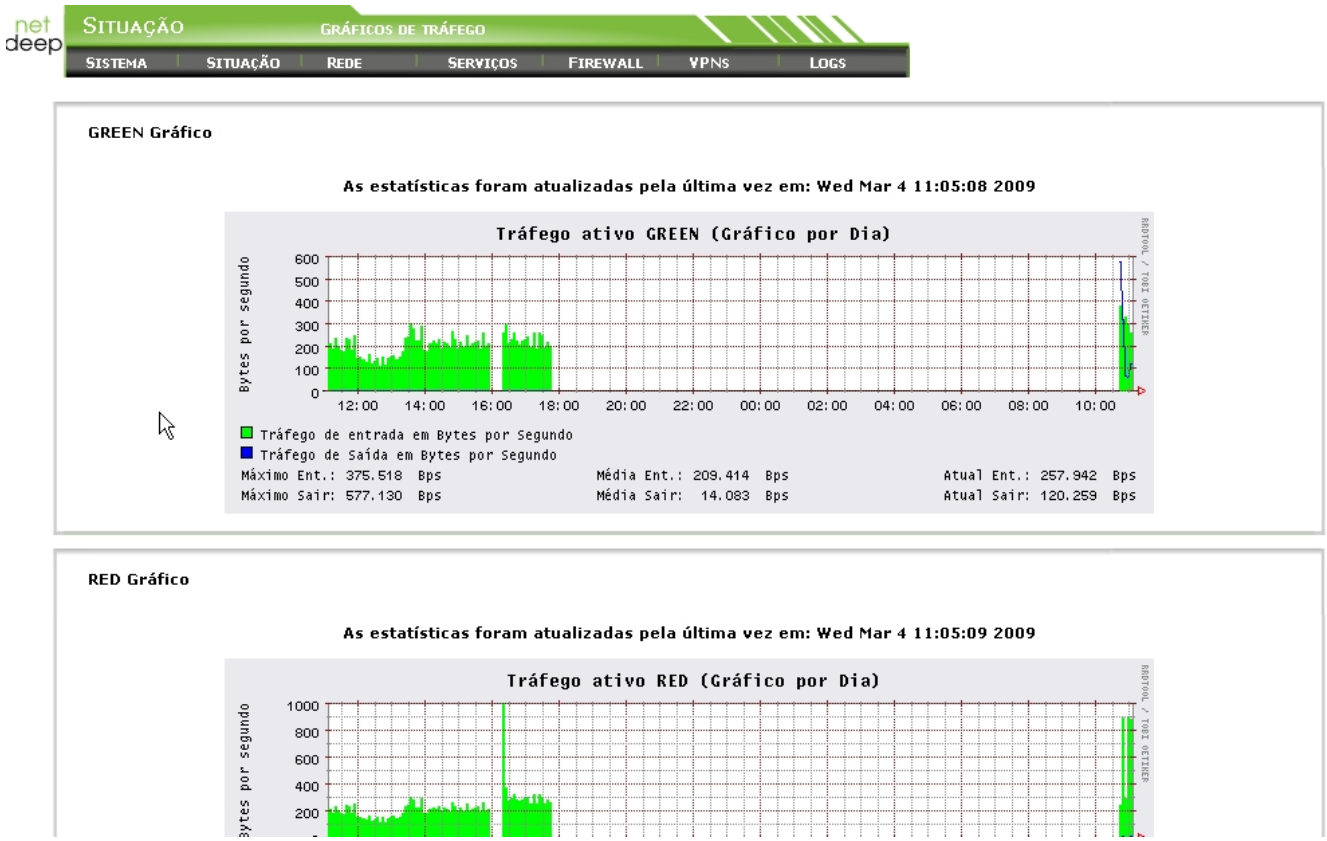
Clique nos quatro gráficos (CPU, Memória, Swap e Disco) para ver os gráficos de uso por Dia, Semana, Mês e Ano.



2.3.4. Gráficos do Tráfego

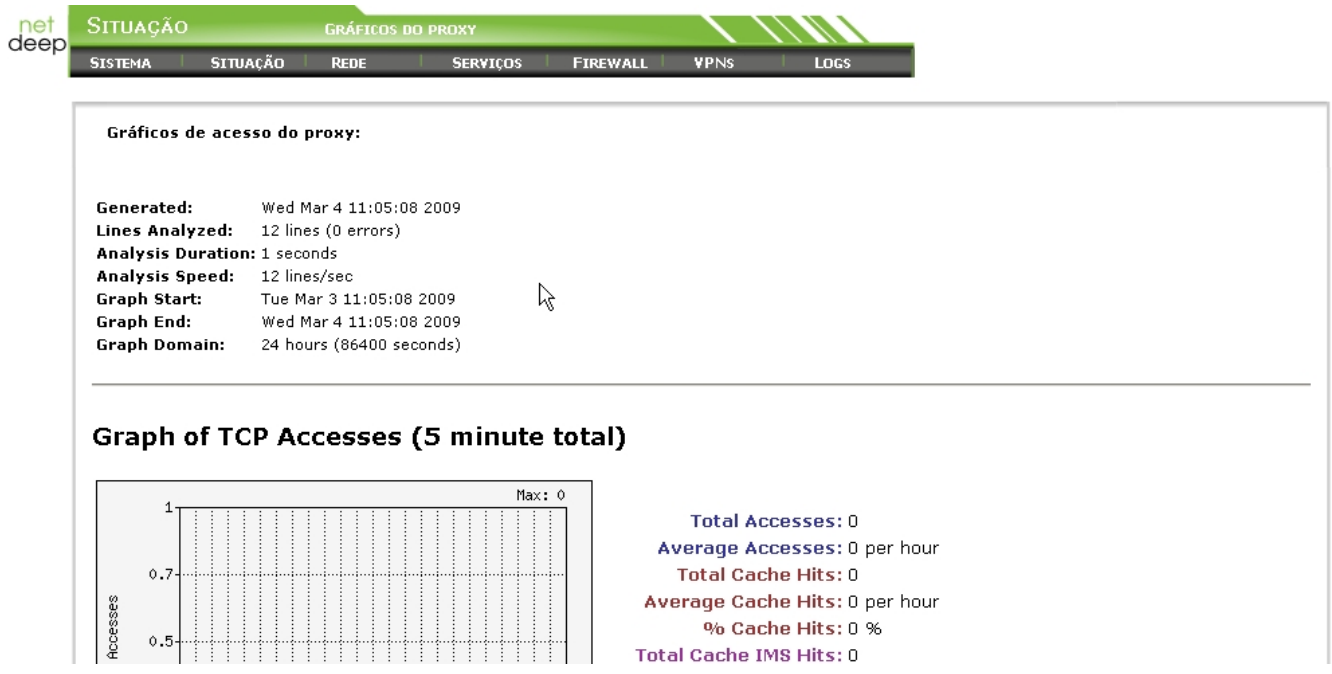
Esta página fornece um gráfico do tráfego de entrada e saída do Netdeep Cop.

Clique em um dos gráficos para mostrar mais detalhes da interface: por Dia, Semana, Mês e Ano.



2.3.5. Gráficos Proxy

Esta página mostra o tráfego do serviço de Proxy do Netdeep Cop. Esta informação é útil para verificar se o Cachê do Proxy está do tamanho correto.

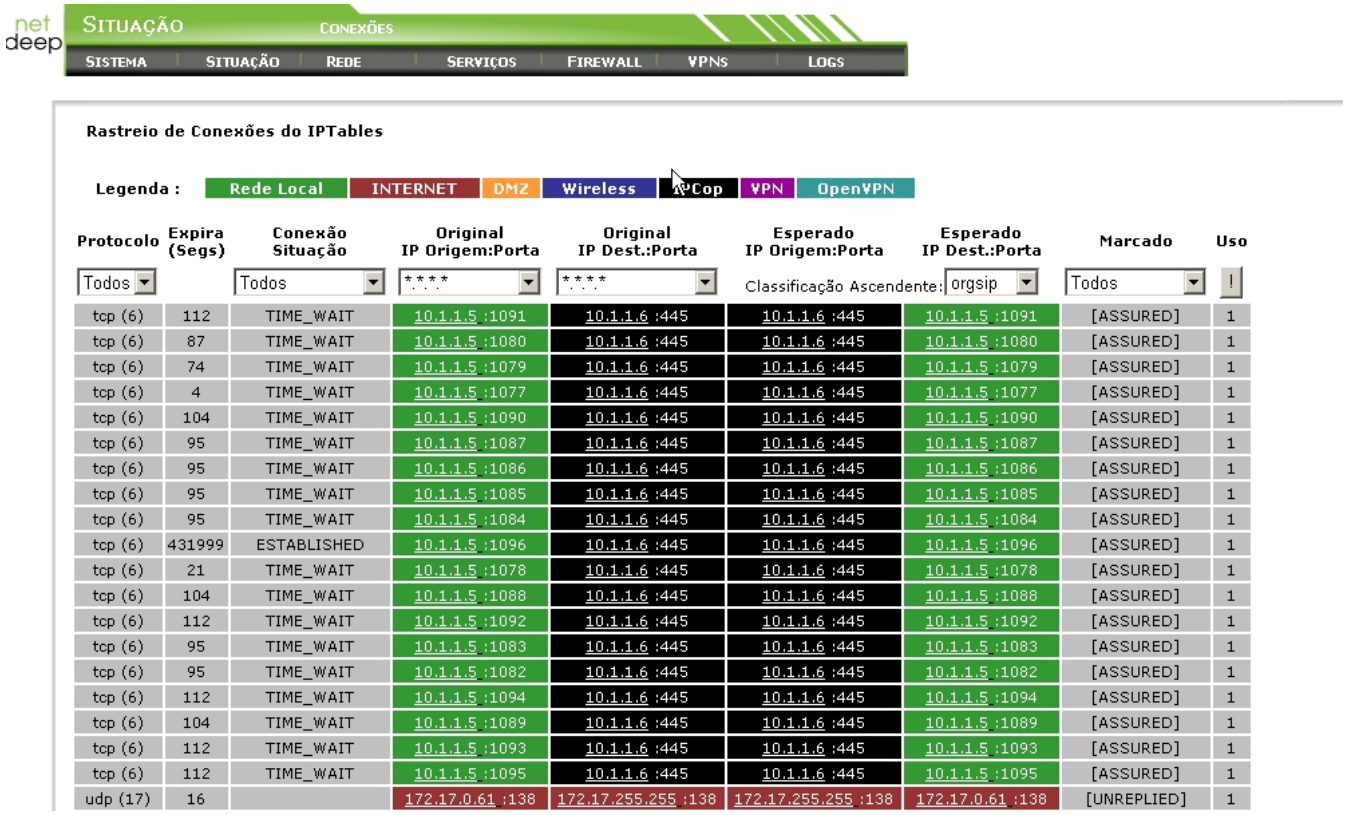


2.3.7. Conexões

O Netdeep Cop usa o firewall Netfilter para manter um firewall estável. O Firewall mantém o rastro de todas as conexões ***de*** e ***para*** os endereços IP das redes GREEN, BLUE e ORANGE, baseada em fonte e destinação de endereços IP e portas, como também o estado da própria conexão. Após a conexão estar estabilizada, envolvendo máquinas protegidas, apenas pacotes consistentes com o estado de conexão corrente são permitidos através do firewall do Netdeep Cop.

A janela Rastreio de Conexões do IPTables mostra as conexões do IPTables. Os pontos finais da Conexão são codificados com cores em sua localidade na rede. O código das cores está no topo da página. Informações ou conexões aparecem na próxima página. Cada conexão ***de*** ou ***para*** suas rede é mostrada.

Clique em um endereço IP para a visão reversa do DNS.



2.4. SubMenu de Rede

2.4.1. Discagem

Esta subseção do DialUp é dividida em 5 seções diferentes que podem ser configuradas e são aplicáveis apenas se você está acessando a Internet usando um modem analógico, um dispositivo ISDN ou uma conexão DSL autenticada.

Note: Você não pode selecionar ou modificar um perfil enquanto o Netdeep Cop está *online*, ou conectando para ficar *online* no modo "Dial on Demand". Antes de usar esta página, vá à página principal da GUI e se a linha de *status* mostrar ***Conectado*** ou Dial-on-Demand em espera, clique no botão [Desconectar] e retorne a configuração.

Após fazer as configurações ou selecionar o Perfil, lembre-se de retornar à pagina principal da GUI e clique no botão [Conectar], para que o Netdeep Cop fique *online* novamente.

Perfis: Esta seção oferece as opções de nomear e fazer a configuração de novos Perfis de DialUp (máximo de cinco), ou renomear Perfis que já existem e mudar seus parâmetros.

Selecione um Perfil a ser criado ou modificado da lista. Preencha ou mude os parâmetros do perfil e clique no botão [Salvar]. Para selecionar o Perfil que será usado em conexões futuras, use a lista para fazer sua escolha e clique no botão [Selecionar]. Use o botão [Restaurar], enquanto edita o Perfil, para retornar a configuração anterior.

Conexão: Esta seção oferece as seguintes possibilidades:

1. Selecione a Interface apropriada para seu dispositivo de conexão da Internet. Pode ser tanto uma porta_de comunicação serial (COM1 - COM4) usado mais para modems e ISDN cards, ou PPPoE no qual é usado mais para conexões DSL.

2. Selecione o modelo adequado para o padrão do modem. Isto irá decidir quão rápido a informação será passada de e para seu dispositivo de conexão. Com sistemas ou modems de computadores antigos, você pode achar necessário usar um dos baixos classificadores de dados para estabelecer comunicações eficazes de modelo/modem. Em caso de PPPOE aparecerão as configurações pertinentes.

3. Coloque o Número correto para discagem da Conexão de Internet. Se a conexão é via a interface PPPoE, há chances de você deixar este em branco.

4. Selecione o speaker do Modem ligado ou desligado. Quando os speakers estão ligados você pode ouvir o andamento da conexão e pode ser útil para perceber algum problema. Esta opção é útil somente se você está utilizando um modem analógico.

5. Selecione o modo Dialing. Use a discagem Tone ao menos que sua conexão de telefone reconheça apenas discagem a Pulso. Discagem a Pulso é bem mais lenta que discagem Tone.

6. Insira seu Maximum retries preferido. Isto decidirá a frequência em que o Netdeep Cop tenta se conectar a Internet após a conexão ter falhado.

7. Insira seu timeout inativo (expiração por ociosidade). Este decidirá como o Netdeep Cop lida com sua conexão de Internet quando nada está sendo de fato enviado ou recebido via a conexão. O número que você colocar aqui indica ao Netdeep Cop quanto tempo ele deve esperar após qualquer atividade na Internet antes que o link do modem seja desconectado. Se você programá-lo em 0, o Netdeep Cop uma vez conectado, não desconectará automaticamente da Internet.

8. O checkbox Persistent Connection (reconectar persistente) é usado para instruir o Netdeep Cop a manter o modem conectado em todos os momentos, mesmo quando não há atividade na Internet. Este modo tende a conectar a Internet toda vez que o link falhar por qualquer motivo, como tempo acabado no ISP ou queda do link do modem . Use este modo com cautela. Se a conexão tem o custo baseado no tempo de uso, você provavelmente não vai querer usar esta opção. No entanto, se você possui um serviço ilimitado no seu ISP, você pode querer usar esta opção para manter o link conectado o máximo possível. Note que no modo persistente, o Netdeep Cop para de conectar quando ultrapassa o número de fracassos consecutivos estabelecidos em Maximum Retries (número máximo de tentativas). Neste caso você terá de usar o botão [Dial] na página principal da GUI.

9. Dial on Demand (discagem por demanda) é disponibilizado ao clicar no checkbox. Note que após autorizar o Dial on Demand, você ainda tem que clicar no botão [Conectar] na página principal antes do Netdeep Cop começar a conectar automaticamente quando detectar a atividade de Internet. A opção Dial on Demand não está disponível para conexões PPPoE.

10. A opção de Dial on Demand para DNS determina se o Netdeep Cop irá ou não conectar automaticamente quando os requisitos do DNS são detectados. Normalmente pode ser o que você quer que aconteça.

11. Connect on Restart (conectar ao reiniciar) fará com que o Netdeep Cop seja conectado após iniciar, se o Dial on Demand não for selecionado. Você provavelmente vai querer colocar essa opção como ativa se você está usando o Dial on Demand. Isto porque a combinação das configurações irá automaticamente programar o sistema Netdeep Cop no Dial on Demand em modo de espera cada vez que o Netdeep Cop for trocado ou reiniciado.

12. ISP Requires Carriage Return (o ISP requer retorno da portadora). Alguns ISPs pedem ao modem quem mande um carriage return para sinalizar que o envio de informações terminou. Se seu ISP requer isso, deixe isto checado. O padrão é checado.

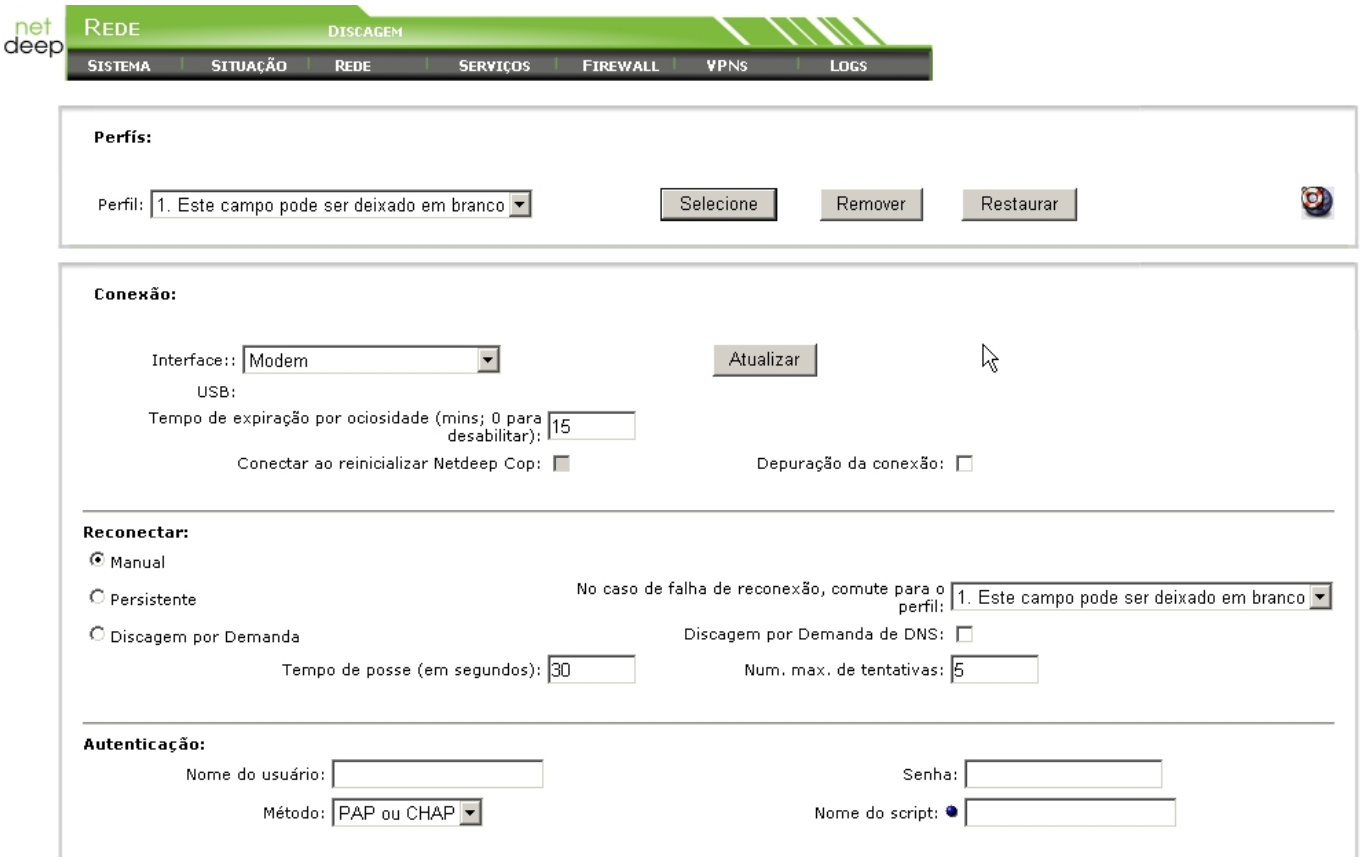
Settings PPPoE adicionais – Se ambos PPPoE ou USB ADSL estão habilitados, estão disponíveis as opções de configuração adicional.

Aqui você pode inserir os parâmetros adicionais sobre o serviço de nomes (DNS), que alguns ISP exigem. Se seu ISP não os exige, ou se não oferece nenhum, você pode deixar ambos campos em branco. Seu ISP irá lhe fornecer dois itens, VPI E VCI, você precisará inserir se estiver usando uma conexão USB ADSL.

Autenticação. Username and Password são o nome do usuário e o password que seu ISP deveria ter fornecido a você quando abriu sua conta com eles. Há vários meios no qual ISPs usam este nome usuário e password para fazer o login em seus sistemas. Os métodos mais comuns são PAP ou CHAP.

Se seu ISP usa texto para o texto do login, escolha um padrão de script login. A outra opção de script está sendo fornecida para pessoas que possuem ISPs com necessidades especiais. Se você precisa disto, você precisa fazer o login na caixa do Netdeep Cop e criar um arquivo em */etc/ppp*. Este nome de arquivo (sem o componente /etc/ppp) deve ser inserido na caixa do nome do Script. O arquivo possui um par 'expect send' separado por um tab. *USERNAME* será substituído pelo nome do usuário e *PASSWORD* pelo password. Examine o arquivo demonloginscript no */etc/ppp*, e o use como um exemplo do que deve ser feito neste arquivo.

DNS. Selecione automaticamente se seu ISP suporta o servidor automático de configuração DNS, como normalmente é o caso. A alternativa é deixar Automatico não marcado e colocar os Endereços IP nas caixas dos DNS Primários e Secundários. Estes Endereços IP geralmente serão providos pelo seu ISP aonde forem necessários.



2.4.2. Modem DSL

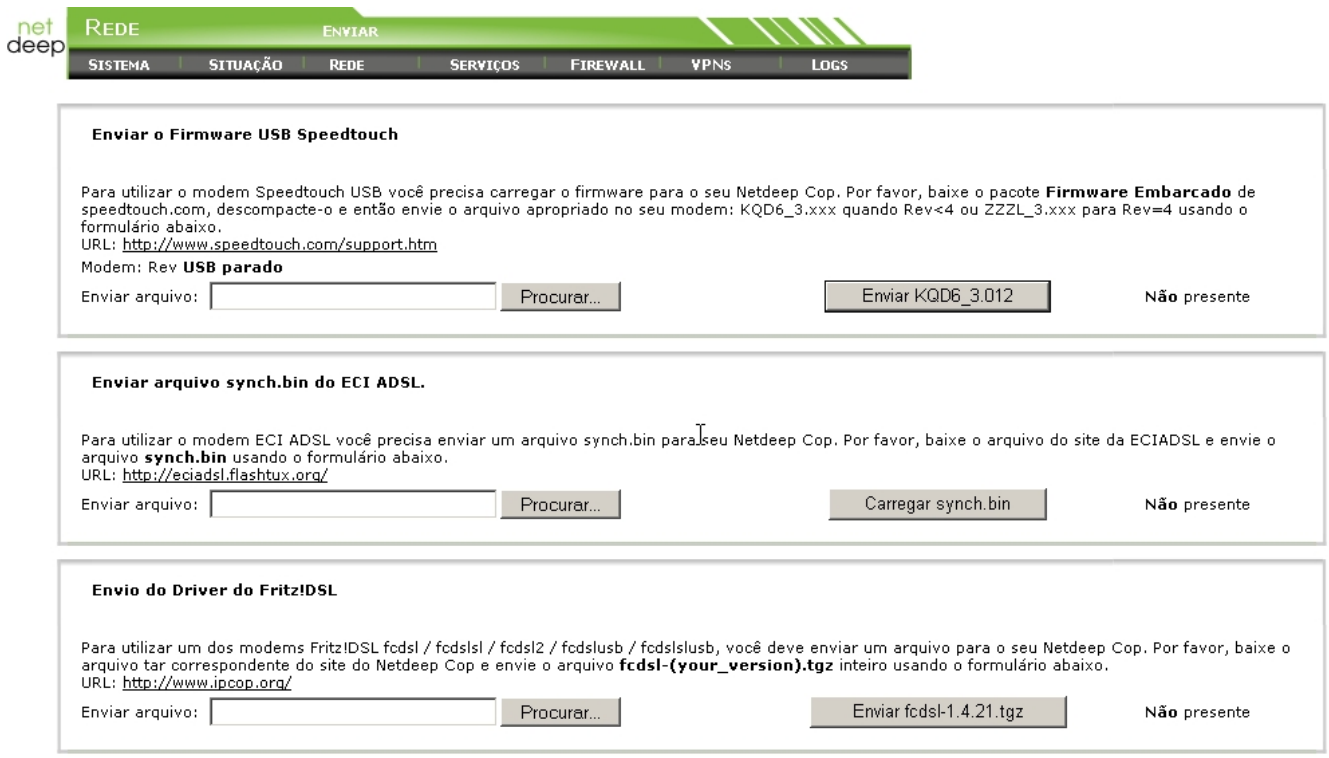
Use esta página para fazer o download dos arquivos necessário para dar suporte aos vários modems no desktop da sua máquina e então faça o upload no seu Netdeep Cop.

Upload Speedtouch USB Firmware. Use esta seção para fazer o upload do arquivo *mgmt.o* para o Netdeep Cop - O USB ADSL não funcionará antes que isto seja feito. Use o link específico para ir ao site, resgistre e faça o download do arquivo no desktop da máquina. Então selecione o arquivo do desktop e aperte o botão upload para transferir ao Netdeep Cop. Uma vez que o upload foi feito com sucesso, você pode usar o USB ADSL.

Upload ECI ADSL Arquivo *Synch.bin*. Use esta seção para fazer o upload do arquivo *sync.bin* para o Netdeep Cop - ECI ADSL não irá funcionar antes que isso seja feito. Use o link específico para ir no site e fazer o download do arquivo em seu desktop. E então escolha o arquivo no seu desktop e pressione o botão upload para transferí-lo ao Netdeep Cop. Uma vez que o upload foi efetuado com sucesso, você pode usar o ECI ADSL.

Upload Fritz!DSL Driver. Use esta seção para fazer o upload do arquivo *fcdsl.o* ao Netdeep Cop - Fritz!DSL não irá funcionar até que isso seja feito. Use este link específico para ir ao site e fazer o download do arquivo no seu desktop.

Então escolha o arquivo do seu desktop, e pressione o botão upload para transferí-lo ao Netdeep Cop. Uma vez que o upload foi feito com sucesso, você pode usar o Fritz!DSL.



2.4.3. Modem DIAL

Configuração do Modem. Serve apenas se você for conectar a internet com um modem analógico. O padrão de configuração que aparece no GUI são compatíveis com a maioria dos modems analógicos.

No entanto se, você está tendo problemas ao se conectar, compare estes parâmetros com os demais sugeridos no manual do modem que você está usando. Qualquer um ou todos esses parametros podem ser deixados em branco.

Init – A Inicialização padrão string usado pela maioria dos modems Hayes-compatible já está disponível para você nesta área. Mas, se o seu modem pedir um parâmetro diferente, então mude-o.

Hangup - O Hang up padrão string usado pela maioria dos modems Hayes-compatible já está disponível para você nesta área. Mas, se o seu modem pedir um parâmetro diferente, então mude-o.

Configure os Parâmetros do PPP / Upload do Driver do Modem

Speaker on (auto falante ligado) – O padrão Speaker no string usado pela maioria dos modems Hayes-compatible já está disponível para você nesta área. Mas, se o seu modem pedir um parâmetro diferente, então mude-o.

Speaker off (auto falante desligado) – O padrão Speaker-off string usado pela maioria dos modems Hayes-compatible já está disponível para você nesta área. Mas, se o seu modem pedir um parâmetro diferente, então mude-o.

Tone Dial (discagem de tom) - O padrão Tone Dial string usado pela maioria dos modems Hayes-compatible já está disponível para você nesta área. Se seu modem e linha telefônica podem

agüentar o Tone Dial e você está aguardando problemas de conexão, então tenha a certeza de que este string é apropriado para o seu modem.

Pulse Dial (discagem de pulso)– O padrão Pulse Dial string usado pela maioria dos modems Hayes-compatible já está disponível para você nesta área. Você não deveria precisar mudá-lo, mas se seu serviço de telephone não suporta o Tone Dialing então você precisa se certificar se esse é o string apropriado para a sua conexão.

O único item esta área que não deve ficar em branco é a do Connect Timeout (tempo de expiração de conexão). Ela diz ao Netdeep Cop o tanto de tempo permitido para o modem a iniciar a conexão. Após essa quantidade de segundos terminar sem uma resposta apropriada ou um recebimento de fim, o Netdeep Cop desistirá e tentará a conexão novamente. O padrão deve trabalhar bem mas se você perceber que a conexão está caindo no meio de uma sequência de negociação (ligue o auto falante e fique atento à conexão) então você deve aumentar esse parâmetro aos poucos até que a conexão tenha sucesso.

Parâmetros do Modem

2.5. SubMenu de Serviços

O Netdeep Cop oferece uma variedade de ferramentas e serviços para administrar e controlar o acesso Internet na sua rede. São eles:

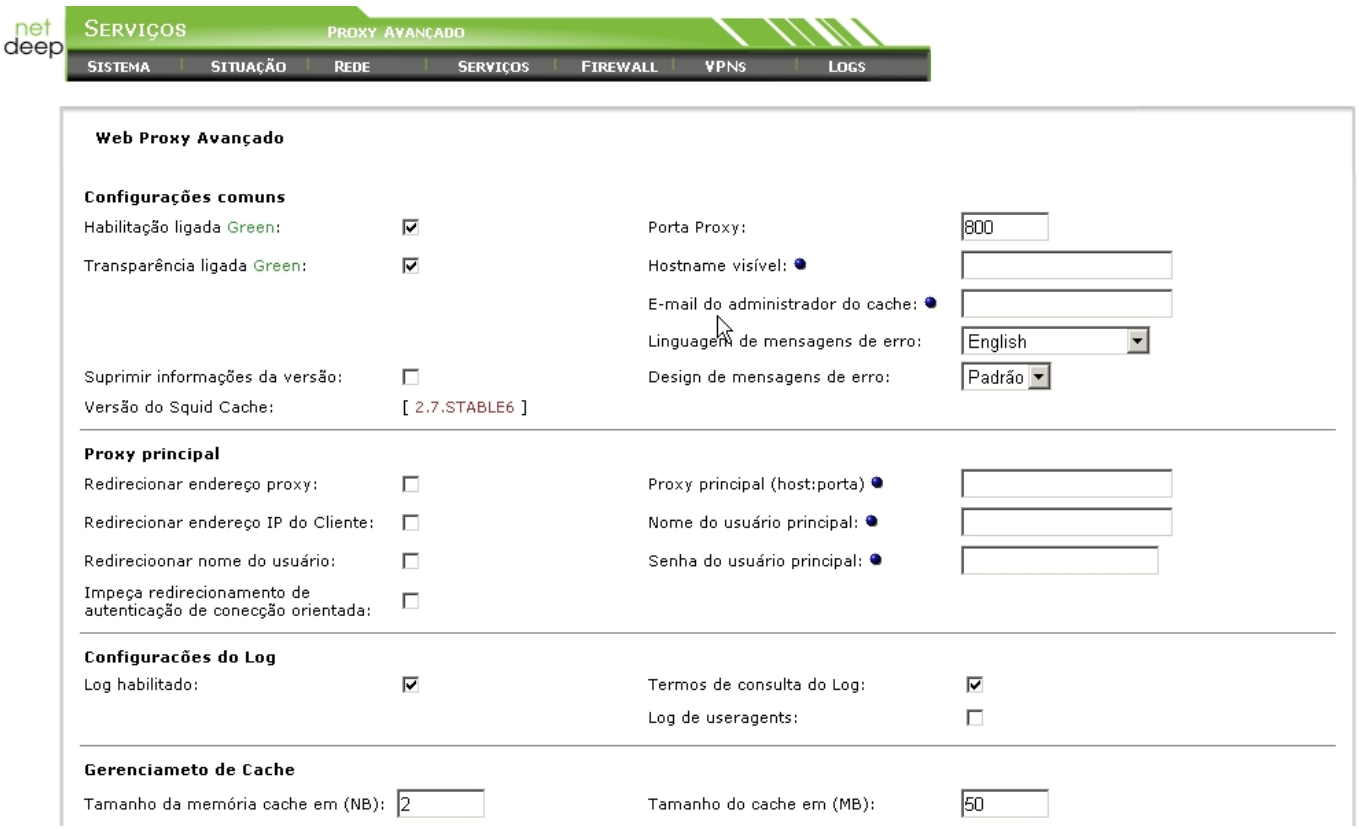
- ***Proxy Avançado***
- ***Filtro de URL***
- ***Acelerador de Atualização***
- ***Servidor DHCP***
- ***DNS Dinâmico***
- ***Editar Hosts***
- ***Servidor de Horário (NTP)***
- ***Controle de Tráfego***

- ***Detecção de Intrusos (IDS)***

Aqui estão as principais ferramentas para controle do acesso Internet em sua rede.

Pode ser que em sua rede alguns desses serviços já sejam providos por servidores e devem ser desabilitados no Netdeep Cop, como é o caso, por exemplo, do Servidor DHCP.

2.5.1. Proxy Avançado



O serviço de *Proxy* é um programa que faz pedidos das páginas *web* para todas as máquinas de sua rede. O servidor *Proxy* irá fazer o *cache* das páginas que foram acessadas na *web*, então se 3 máquinas requerem a mesma página apenas uma transferência da Internet é realmente requerida. Se sua organização possui um número de *websites* usados em comum, estes podem ser salvos nos acessos da Internet.

Normalmente você precisa configurar os *browsers* (navegadores) usados na sua rede para utilizar o servidor *Proxy* para acessar a Internet.

Você deve colocar o nome/endereço de *Proxy* do Servidor Netdeep Cop e a porta configurada na caixa ***Porta do Proxy***, padrão 800. Esta configuração permite aos *browsers* (navegadores) a usar o *proxy*, se eles desejarem. Também, é possível rodar o *proxy* em um modo "transparente". Neste caso, os browsers (navegadores) não precisam de uma configuração especial e o Firewall redireciona automaticamente todo o tráfico na porta 80 (porta padrão http) para o servidor *proxy*.

Você pode escolher se quer os requisitos do *proxy* na rede GREEN (interna) e/ou na rede BLUE (wireless). Marque apenas as caixas relevantes.

Se você escolher ***proxy habilitado*** então você também pode ter o acesso ao *log* pelas caixas marcadas na caixa ***Log Habilitado***. Os acessos feitos através do *proxy* podem ser vistos ao colocar as escolhas no *Logs de Filtros URL* do **menu *Logs***. E no menu *Arquivamento* no **menu Logs.**

Se seu ISP (provedor) pede para usar seu *cache* para o acesso web então você deve especificar o *hostname* e a porta na caixa ***Upstream proxy (proxy principal)***. Se o *proxy* do seu ISP (provedor) pede um nome usuário e uma senha, insira-os nas caixas do ***Upstream username (usuário principal)*** e ***Upstream password (senha do usuário principal)***.

Gerenciamento do Cache. Pode escolher quanto espaço de disco deve ser usado para o *cache* das páginas web nesta seção. Você, também, pode colocar o tamanho do menor objeto que pode ser feito o *cache*, o que normalmente é 0, e o maior é 4096KB. Por razões de privacidade, o *proxy* não fará o cache das páginas recebidas através de https, ou outras páginas aonde o nome usuário e senha são submetidos através de URL.

No item [Não faça cache ...] adicione os domínios que não farão cache, por ex.: domínios da empresa, etc.

Controle de acesso baseado na rede:

Subnets permitidas: Colocar as subnets com permissão de acesso, por default (padrão) a rede interna já é inserida pelo Netdeep Cop, ex.: 192.168.1.0/255.255.255.0.

Endereços IP/MAC ADDRESS sem restrição:

Colocar os endereços IP(ou MAC-Address) dos Servidores da Rede e das máquinas que não terão restrição de acesso à Internet. Se você optou por usar servidor DHCP em sua rede então use endereços IP fora do range do DHCP.

Endereços IP/MAC ADDRESS banidos:

Colocar os endereços IP(ou MAC-Address) das máquinas que não estão autorizadas para acesso externo (Internet). Se você optou por usar servidor DHCP em sua rede então use endereços IP fora do range do DHCP.

Restrições de tempo: Mantenha os valores padrões ou defina os dias da semana e horários para permitir/negar acesso à Internet.

Limites de Transferência. O *proxy* também pode ser usado para controlar como os usuários acessam a web. O único controle acessível através da interface da web é o tamanho máximo de informação recebida e enviada pela web. Você pode usá-lo para prevenir que seus usuários façam *download* de arquivos grandes e tornem lento o acesso à Internet para todos os demais. Programe este para 0 (padrão) para remover todas as restrições.

Filtro MIME:

Habilite este item para realizar filtros baseados em MIME.

Web Browser:

Habilite e selecione, se necessário, os browsers (navegadores) que serão permitidos para acessar a Internet.

Privacidade:

Use este item para configurar Falso UserAgent para sites externos.

Filtro de URL (Filtro de URL). O Netdeep Cop disponibiliza uma importante ferramenta para controle e administração do acesso Internet pelos usuários de sua rede. Este é um item opcional, clique em [Habilitado] para o serviço e acesse a página **Filtro de URL** para as demais configurações. Recomendamos habilitá-lo para a utilização de filtros de sites.

Método de autenticação. O *proxy* também pode ser usado para controlar quais usuários podem acessar a web. Opte por Nenhum, Local, LDAP, Windows ou Radius. A opção **Local** permitirá que você cadastre e administre seus usuários no próprio Servidor Netdeep Cop, enquanto as demais opções (**LDAP, Windows ou Radius**) utilizará outro servidor de sua rede para prover autenticação aos usuários.

Atenção: para utilizar autenticação, a opção Transparência Ligada deve estar desabilitada.

Para que um usuário altere sua própria senha (no caso de autenticação Local), utilize este caminho: http:[IP do Netdeep Cop]:81/senha/

Após as alterações pressione nos botões ***[Salvar]*** e ***[Salvar e Reiniciar]***.

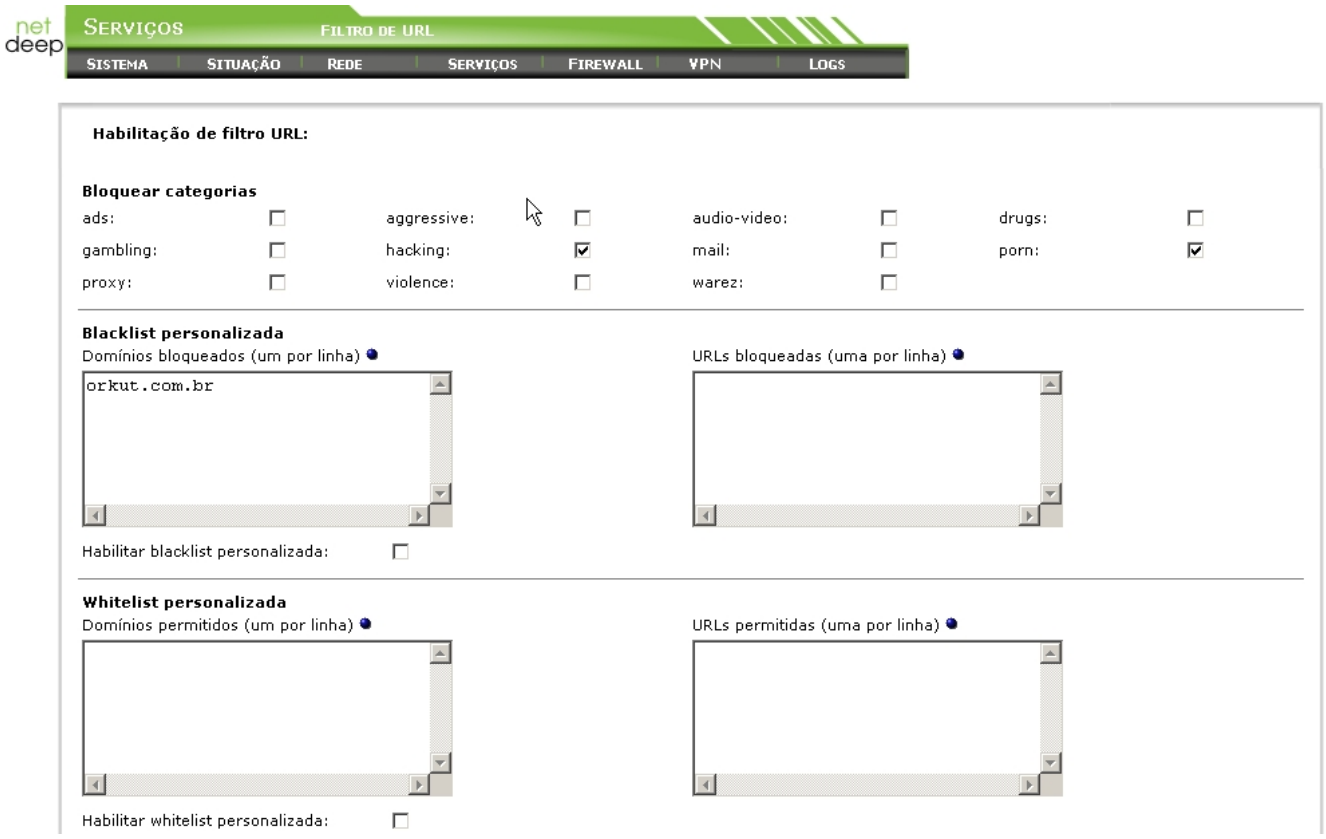
Você pode apagar todo o *cache* de páginas web clicando no botão ***[Limpar o Cache]***.

Aviso

O Cache pode tomar muito espaço no seu disco rígido. Se você usa um cachê grande, então considere um disco rígido maior na configuração de seu Servidor Netdeep Cop.

Quanto maior o cache que você escolhe, maior memória é necessária para o servidor proxy para administrar o cache. Se você está rodando Netdeep Cop em máquina de memória pequena, não escolha um cache grande.

2.5.2. Filtro de URL



O serviço Filtro de URL possibilita uma série de controles (filtros) sobre o acesso Internet em sua rede. Este é um item opcional e para funcionar tem que ser habilitado na página do **Proxy Avançado**.

2.5.2.1. Habilitação dos Filtros

Bloquear Categorias:

O primeiro filtro do Filtro de URL é baseado em Blacklists disponíveis na Internet, cuja atualização veremos mais adiante, e são divididas em categorias que você pode escolher clicando nas caixas correspontes.

Blacklist / Whitelist personalizada:

Você pode restringir e/ou permiter o acesso à páginas Internet que sobreporão às Blacklists do subitem anterior. O bloqueio ou a permissão pode ser por domínio ou por URL (caminho específico) e deve ser adicionadas uma por linha.

Lista personalizada de expressões:

Outra forma de controle é o filtro por palavras e/ou expressões contidas na URL e/ou conteúdo do site. Este filtro se sobrepõem aos anteriores e deve ser usado com cuidado para evitar bloqueios indevidos.

Você pode ainda usar uma lista personalizada clicando na caixa [habilitar lista de expressões personalizadas].

Bloqueio por extensão de arquivos:

Para evitar que os usuários de sua rede acessem arquivos (*downloads*) com extensões específicas, você pode usar este filtro que bloqueio os arquivos **executáveis**, de **áudio/vídeo** e **compactados.** Para habilitar clique nas caixas desejadas.

Redirecionar arquivo local:

Em caso de erro por bloqueio você pode personalizar uma página HTML que será exibida para o usuário durante o bloqueio de acesso. Para usar implementar esta página personalizada, clique em [Habilitar] e configure o local do arquivo.

Controle de Tempo de Acesso:

Neste subitem você pode [Definir tempo de acesso] e/ou [Definir cotas por usuário]. Com este filtro você pode controlar o acesso à sites por tempo/usuário/hosts/redes e pode controlar uma quantidade de bytes por usuário/tempo/hosts/redes.

Configuração de Páginas Bloqueadas:

Configure neste subitem o retorno de erro para os usuários ao acessarem páginas bloqueadas. Ex. Página com DNS error, Redirecionar para uma página da web específica, Adicionar uma página personalizada de erro, Usar ou alterar o texto da página padrão, etc.

Configurações Avançadas:

Neste subitem você pode configurar detalhes da geração de Logs e funcionamento de alguns bloqueios.

Salvar e Reiniciar:

Todas as alterações do Filtro de URL requerem que sejam salvas e reiniciadas. Use os botões, portanto, de [Salvar] e [Salvar e Reiniciar] o serviço. Não é necessário reiniciar o Servidor Netdeep Cop.

2.5.2.2. Manutenção dos Filtros

Atualização de Blacklist:

Caso você opte por adicionar uma nova Blacklist personalizada de sites a serem bloqueados, neste subitem você pode fazer o upload e atualizar sua Blacklist.

Atualização automática de Blacklist:

Para maior tranqüilidade na administração de seu Servidor Netdeep Cop, você pode agendar e definir a fonte de atualização de suas Blacklists, neste subitem. O padrão é a SquidGuard.

Editor de Blacklist:

Esta ferramenta permite que você edite o arquivo de Backlist e faça alterações conforme suas necessidades.

Configurar Backup e Restore do Filtro de URL e Blacklist:

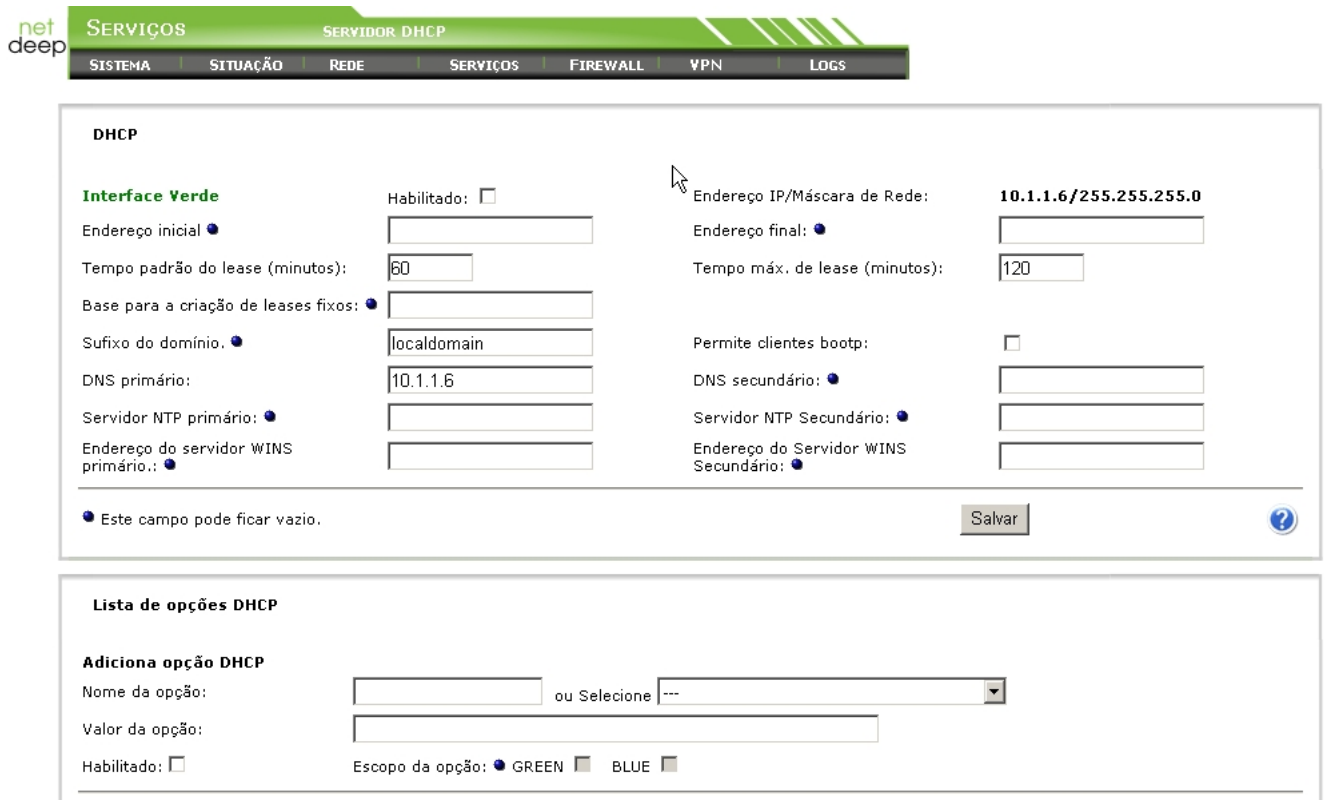
Neste subitem você pode gerar um Backup das configurações do Filtro de URL, fazer copiar backup e restaurar quando necessário a partir de sua máquina. Este é um procedimento altamente recomendável.

2.5.3. Servidor DHCP

DHCP (Dynamic Host Configuration Protocol) lhe permite controlar a configuração de rede de todos os seus PCs a partir do Servidor Netdeep Cop. Quando um PC se conecta à sua rede, irá receber um endereço IP e as configurações de DNS e WINS serão programadas no Netdeep Cop automaticamente. Para usar este adicional, os PCs precisam ser programados para obter a configuração de rede automaticamente.

Você pode escolher se quer ter este serviço em sua rede GREEN (interna) e/ou na rede BLUE (Wireless). Basta clicar na caixa.

Para uma explicação mais detalhada do DHCP você acessar: http://www.dhcp.org



2.5.3.1. Parâmetros do Servidor DHCP

Configure os parâmetros do DHCP a seguir:

Endereço IP Inicial (opcional). Você pode especificar o mais baixo e mais alto endereço IP que o servidor irá distribuir para os PCs. O padrão para se distribuir os endereços está na subnet que você estabeleceu quando instalou o Netdeep Cop. Se você tem máquinas na sua rede que não usam o DHCP e tem seus endereços IP configurados manualmente, você deve acertar os endereços inicial e final para que o servidor não distribua nenhum desses IPs manuais,.

Você deve ter certeza de que qualquer endereço listado na seção do ***Fixed Lease (leases fixos atuais)*** também estejam fora desta área.

Endereço IP Final (opcional). Especifique o endereço IP mais alto que será distribuído.

O **DNS Primário** especifica o que o servidor DHCP informará aos seus clientes como seu servidor de DNS Primário. Devido ao fato do Netdeep Cop rodar um proxy DNS, você provavelmente irá querer deixar o padrão, para que o DNS Primário seja o endereço IP do Servidor Netdeep Cop. Se você possui seu próprio servidor de DNS, então mencione-o aqui.

DNS Secundário. Você também pode especificar um segundo servidor DNS no qual será usado, se o primeiro não está disponível. Este pode ser outro servidor DNS da sua rede ou do seu ISP (provedor).

Lease time (tempo do lease) Padrão. Este pode ser deixado no seu valor padrão ao menos que você precise especificar seu próprio valor. O *lease time* padrão é o tempo de intervalo de validade para os endereços IP. Antes do *lease time* de um endereço expirar, seus computadores

irão pedir uma renovação do seu *lease*, ou seja, do seu o endereço IP atual. Se os parâmetros do DHCP foram mudados, quando houver um pedido de renovação, as mudanças serão reproduzidas. Em geral, os *leases* são renovados pelo servidor.

Tempo máximo do lease. Isto pode ser deixado no valor padrão, ao menos que você queira especificar seu próprio valor. O tempo máximo do lease é a duração de intervalo no qual o servidor sempre irá honrar os pedidos dos clientes para renovar seus endereços IP. Após o tempo máximo de *lease*, os endereços IP podem ser mudados pelo servidor. Se a dinâmica de extensão do endereço IP for mudada, o servidor irá distribuir um novo endereço IP.

O **Sufixo do nome Domínio** (opcional). Defina o nome domínio que o servidor DHCP passará para os clientes. Se qualquer *hostname* não resolver, o cliente tentará novamente após anexar o nome especificado no *hostname* original. Muitos servidores DHCP do ISP (provedor) estabelecem o nome domínio para sua rede e informam aos clientes para colocarem www como padrão de *homepage* no *browser* (navegador). "www" não é um domínio totalmente qualificado. Mas seu computador irá anexar o sufixo do domínio fornecido pelo DHCP do ISP para isto, criando um FQDN para o servidor da web. Se você não quer que seus usuários tenham que esquecer endereços como www, estabeleça o sufixo do domínio idêntico ao seu servidor DHCP do ISP.

Servidor WINS (opcional). Se você está rodando uma rede Windows e possui um Serviço de Nomes Windows (WINS) você pode colocar o endereço IP nesta caixa. O DHCP passará este endereço para todos os hosts quando eles adquirirem os parâmetros da rede.

Pressione [Salvar] para efetivar as mudanças.

2.5.3.2. Adicione um *fixed lease* novo

Se você possui uma máquina que você gostaria de modificar os endereços IP através do servidor DHCP mas quer que eles recebam sempre os mesmos endereços IP, você pode pedir ao servidor DHCP para que aponte um IP fixo baseado no *Mac Address* da placa de rede da máquina.

Isto é diferente de configurar endereços IP manuais. Essas máquinas irão contatar o servidor DHCP para obter seu IP e irão pegar o que for configurado para elas.

Você pode especificar os seguintes parâmetros de *fixed lease*:

MAC Address: Os seis *octet/byte colon* separarão o *MAC address* da máquina que irá dar a elas o *fixed lease*.

AVISO

O formato do *MAC address* é xx:xx:xx:xx:xx:xx, não xx-xx-xx-xx-xx-xx, como algumas máquinas mostram, ex.: 00:e5:b0:00:02:d2.

O **Endereço IP** é o estático *lease* que o servidor DHCP sempre distribuirá para o *MAC address* associado. Não use um endereço IP da extensâo dinâmica do DHCP.

O **próximo endereço** (opcional). Algumas máquinas na sua rede podem ser clientes ***(thin clients)*** que precisam carregar um arquivo iniciador de um servidor de sua rede. Aqui você pode especificar o servidor, se necessário.

Nome do Arquivo (opcional). Especifique o arquivo inicializador para esta máquina.

Root Path (opcional) Se arquivo inicializador não está no diretório padrão, especifique o caminho completo para ele.

Habilitado. Clique nesta caixa para informar ao servidor DHCP para distribuir este *lease* estático. Se a entrada não está habilitada, será arquivado nos arquivos do Netdeep Cop, mas o servidor DHCP não irá emitir este *lease*.

2.5.3.3. *Fixed Leases* Correntes

Esta seção mostra os *fixed leases* correntes e permite editá-las ou deletá-las.

Para editar um *lease* que já existe, clique no ícone lápis. Os valores serão mostrados na página. Faça as modificações necessárias e pressione [Salvar].

Para remover algum *profile* existente, clique no ícone da lixeira. O *lease* será removido.

2.5.3.4. *Dynamic leases* correntes

Se o DHCP é habilitado, esta seção lista os *dynamic leases* que existem no arquivo /var/state/dhcp/dhcpd.leases. O endereço IP, *MAC Address*, *hostname* (se estiver disponível) e o tempo de validade do *lease* de cada registro será mostrado, classificados por endereço IP.

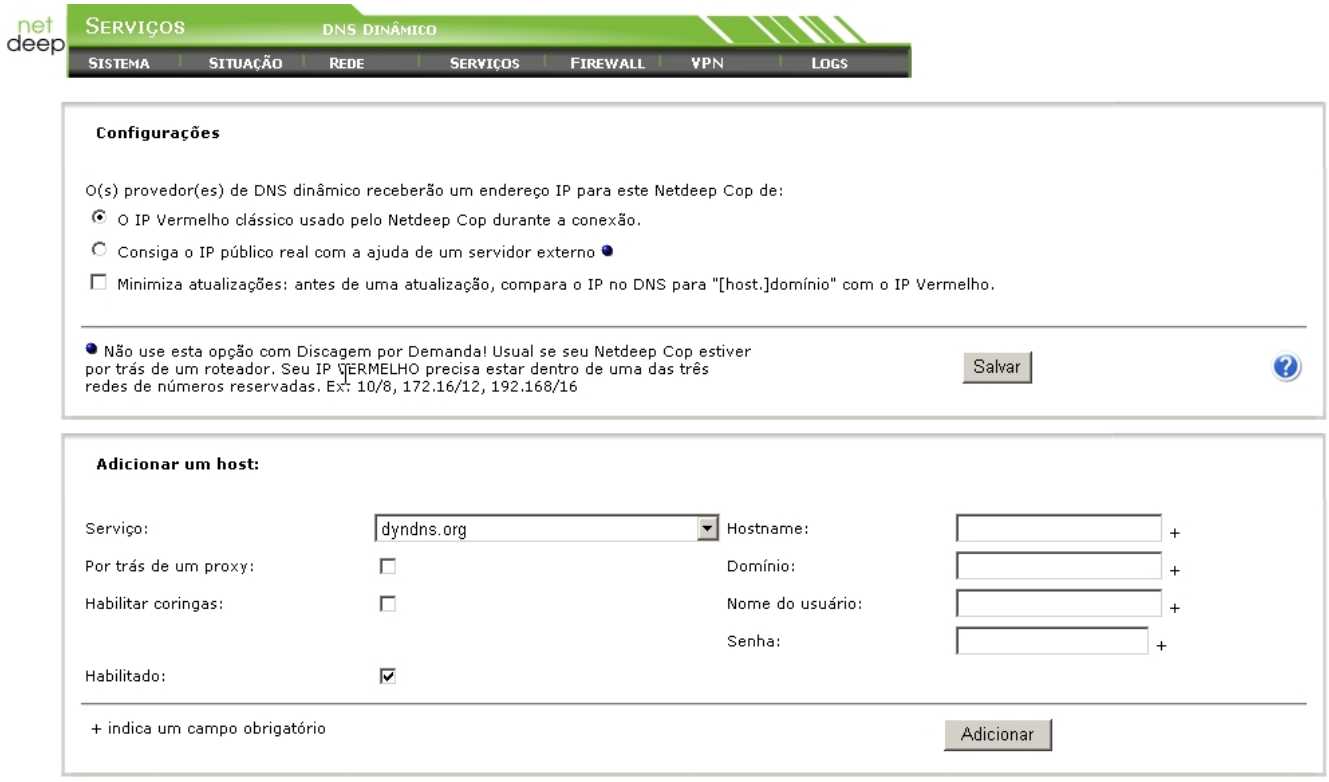
É fácil copiar e colar um *MAC Address* daqui para a seção de *fixed lease*, se desejar. Os tempos de *lease* que já validaram estão fechados.

2.5.3.5. Mensagens Erradas

Se um problema for encontrado nos dados inseridos, uma mesangem de erro aparecerá no topo da página após você pressionar o botão [Salvar].

2.5.4. DNS Dinâmico

DNS Dinâmico (DYNDNS) lhe permite tornar seu servidor disponível na Internet mesmo que não tenha um endereço IP da Internet fixo. Para usar o DYNDNS, você precisa primeiramente registrar um subdomínio com um provedor DYNDNS. E toda vez que seu servidor se conectar a Internet e um endereço IP for dado pelo seu ISP (provedor), este endereço será informado ao servidor DYNDNS. Quando uma máquina cliente deseja conectar-se ao seu servidor, este irá resolver o endereço indo ao servidor DYNDNS, o qual dará o ultimo valor (endereço IP). Se este está atualizado então o cliente conseguirá conectar ao seu servidor (se as regras do seu Firewall permitirem isso). O Netdeep Cop se mantém de forma mais fácil quando seus endereços DYNDNS são atualizados automaticamente por muitos provedores DYNDNS.



2.5.4.1. Adicionar um Host

Configure os parâmetros a seguir do DYNDNS:

O **Serviço** escolhe um provedor DYNDNS *dropdown*. Você deve estar registrado no provedor DYNDNS escolhido.

Por trás de um proxy Esta caixa marcada deve ser marcada apenas se você está usando um serviço no-ip.com e seu Netdeep Cop está atrás de um proxy. Esta caixa é ignorada por outros serviços.

Habilitar coringas permite que você tenha subdomínios no seu hostname DNS dinâmico apontando para o mesmo IP do seu hostname (ex.: com a caixa marcada habilitada,

www.netdeepcop.dyndns.org apontará para o mesmo IP do Netdeep Cop.dyndns.org). Esta caixa marcada

é sem utilidade sem o serviço no-ip.com, eles permitem apenas ativar ou desativar de seu website.

Hostname insira o hostname que você registrou no seu provedor DYNDNS.

Domínio insira o domínio que você registrou no seu provedor DYNDNS.

Nome do Usuário / Senha insira o nome do usuário e a senha que você registrou no seu provedor DYNDNS.

Habilitado se este item não estiver marcado, o Netdeep Cop não poderá fará as atualizações das informações no servidor DYNDNS. Isto reterá as informações para que você possa reabilitar a atualização do DYNDNS sem re-colocar as informações.

2.5.4.2. Hosts Atuais

Nesta seção você pode visualizar as entradas DYNDNS que você configurou.

Para editar uma entrada clique em seu ícone lápis. Faça suas mudanças e clique no botão [Salvar].

Você também pode fazer a atualização do **Por trás de um proxy**, usando coringas e habilitar a caixa marcada diretamente da listas de entradas dos hosts atuais.

2.5.4.3. Forçando a Atualização Manual

Você pode forçar o Netdeep Cop a atualizar a informação manualmente pressionando o [**Forçar Atualização]**. No entanto, só ocorrerá a atualização quando o endereço IP for realmente mudado, pois os provedores dinâmicos de serviço DNS não lidam com atualizações que não provocam mudanças. Se a entrada host foi habilitada, seu endereço será atualizado automaticamente cada vez que o IP for alterado.

2.5.5. Editar Hosts

Adicionalmente às entradas de DNS cache da Internet, o DNS proxy no Netdeep Cop permite inserir os hosts (nomes) dos endereços IP locais que você deseje manter manualmente. Estes podem ser colocados para máquinas locais ou máquinas da Internet.

2.5.5.1. Adicionar um host

Para adicionar um host (nome de uma máquina) insira os dados:

IP de Origem (endereço IP da máquina/host).

Nome do Host (hostname).

Nome do Domínio (opcional), se o domínio não é o hostname, insira-o aqui.

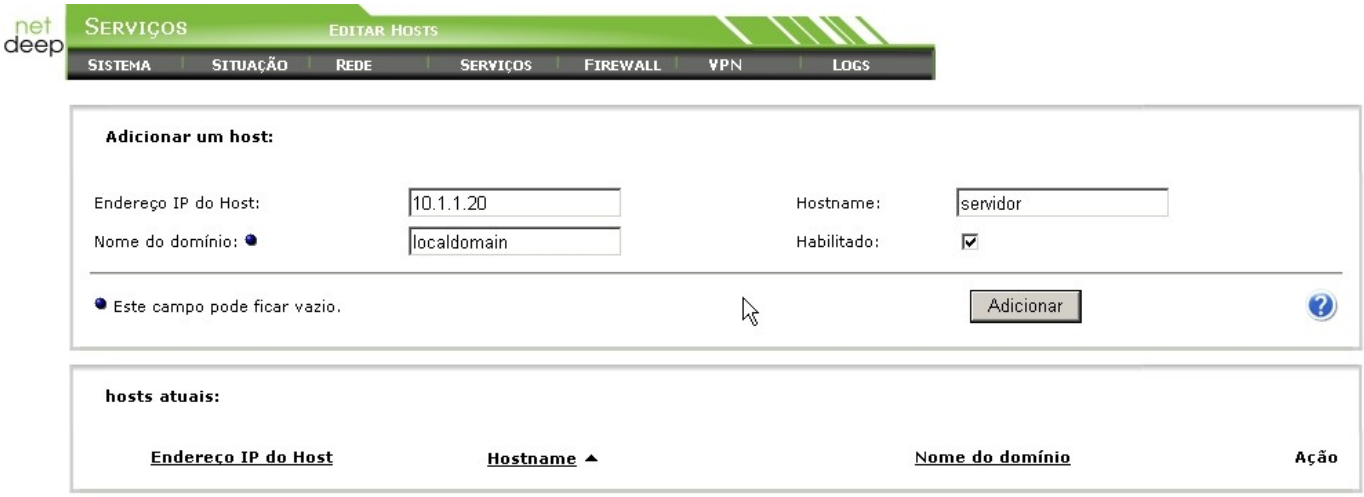
Clique em [Habilitado] e pressione [Adicionar], para que a entrada seja salva.

2.5.5.2. Hosts Atuais

Nesta seção você pode visualizar as entradas DNS configuradas.

Para editar uma entrada clique no ícone Lápis. Faça suas mudanças e clique no botão [Salvar].

Para deletar uma entrada clique no ícone Lixeira.



2.5.6. Servidor de Horário (NTP)

O Netdeep Cop pode ser configurado para obter o tempo de um conhecido *timeserver* preciso na Internet e disponibilizar este tempo (horário) para que as máquinas de sua rede obtenham um horário atualizado e sincronizado com o Servidor Netdeep Cop. Esta é uma excelente maneira de manter todas as máquinas de sua rede com horário atualizado e sincronizado.

Para configurar o sistema de tempo, certifique-se de que a caixa [Obtenha ...] está clicada e coloque o nome completo do *timeserver* que você quer usar na caixa do Sevidor NTP Primário (Ex. ntp.ansp.br). Se você quiser, também pode colocar um Servidor NTP Secundário. E pode prover o serviço de tempo para o resto de sua rede clicando na caixa [Fornece hora ...].

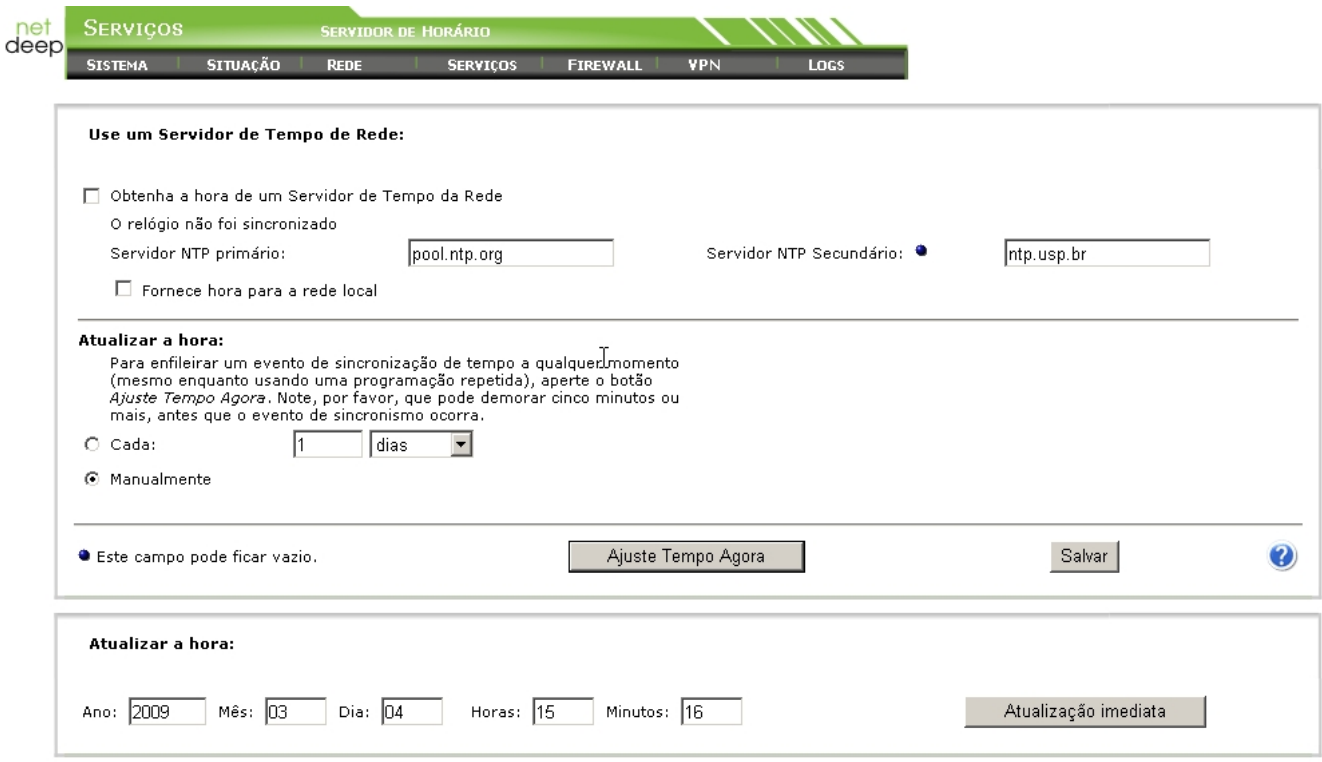
Você pode escolher fazer a atualização de hora no seu Netdeep Cop periodicamente, por exemplo, a cada hora, ou fazer a atualização quando desejar, clicando no [Ajuste tempo ...].

Para salvar sua configuração clique no botão [Salvar].

Se você não sabe como usar um servidor de tempo da Internet, você pode colocar a hora manualmente e clicar no botão [Atualização Imediata].

Nota

O Netdeep Cop pode agir como um servidor de tempo na sua rede, por isso, para mantê-lo atualizado use o ajuste automático de tempo periódico. O relógio do Netdeep Cop se mantém sincronizado mesmo que ele não esteja conectado permanentemente a Internet.



2.5.7. Controle de Tráfego

O Controle de Tráfego permite que você crie prioridades de tráfego IP através do seu Firewall. Este item é Opcional.

O Netdeep Cop usa *WonderShaper* para executá-lo. O WonderShaper foi criado para diminuir a latência PING assegurando que interaja com o tráfego, como o SSH reage enquanto está fazendo o dowload ou upload no Link de acesso Internet.

Muitos ISPs (provedores) usam velocidades padrões de *download*, não como latência. Para maximizar a velocidade do *download*, eles configuram seu equipamento para suportar banda larga no tráfego. Quando o tráfego interativo está misturado nessas bandas largas, sua latência aumenta muito, como *packets ACK* devem esperar na fila até que eles cheguem a você. O Netdeep Cop dá importância e prioriza seu tráfego do jeito que você quiser. Isto é feito quando você especifica o tráfego em prioridades de categoria Alto, Médio e Baixo, O tráfego *Ping* sempre tem a maior prioridade – permitindo que você tenha uma conexão rápida, mesmo enquanto faz *downloads* em massa.

Para usar o Controle de Tráfego no Netdeep Cop:

1. Use sites conhecidos por serem rápidos para estimar sua velocidade máxima de *upload* e *download*. Preencha as velocidades nas caixas correspondentes na parte dos Parâmetros.

2. Autorize o Controle de Tráfego clicando a caixa de autorização.

3. Identifique quais serviços serão usados atrás do seu Firewall.

4. E então classifique-os em 3 níveis de prioridade. Por exemplo:

   a. Tráfego interativo como SSH (port 22) e VOIP (Voice Over IP) vão no grupo de maior prioridade.

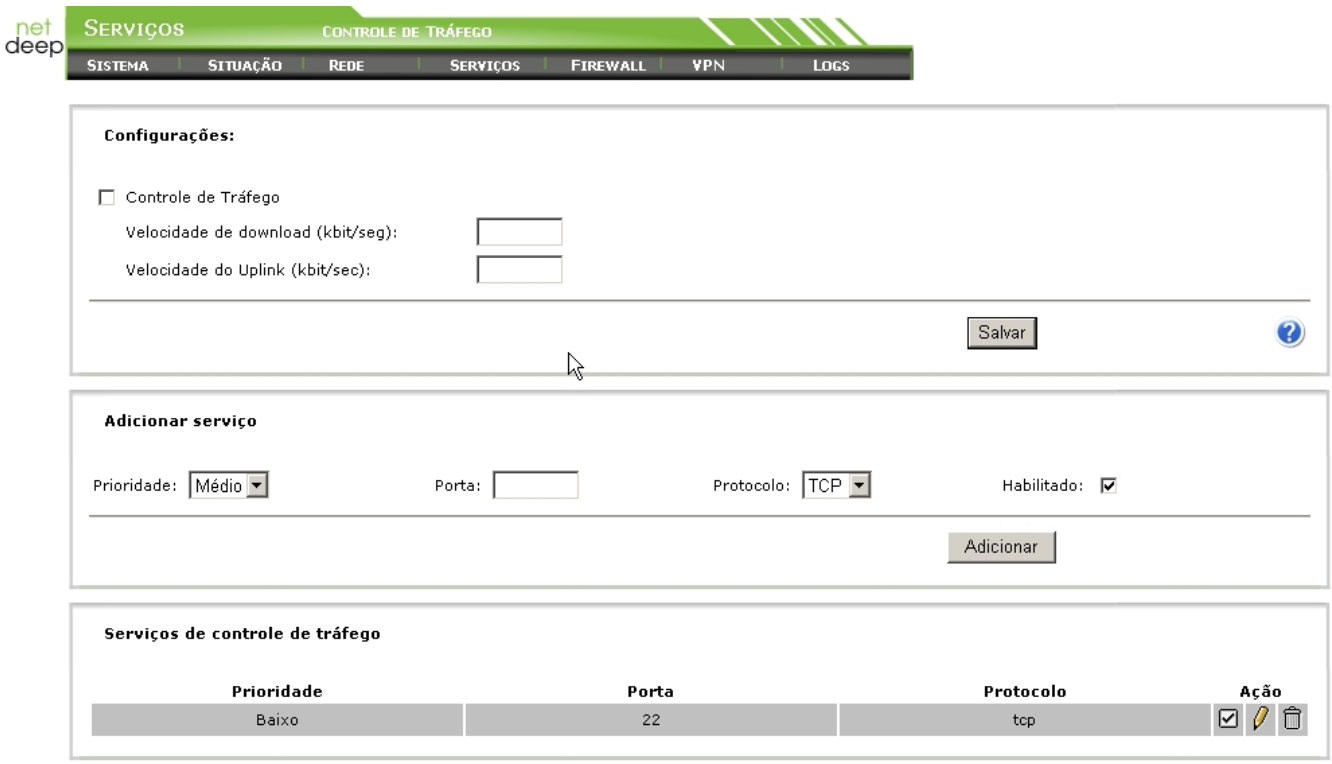
   b. Sua navegação normal de tráfego de comunicação como a web (port 80) e streaming

video/audio no grupo de prioridade média.

c. Coloque seu tráfico de volume como as transferências de arquivo *P2P* no grupo de baixo tráfego.

5. Crie uma lista de serviços e prioridades usando a seção Adicionar Serviço.

Os serviços acima são apenas exemplos do potencial de configuração do Controle de Tráfego. Dependendo do seu uso, você irá querer, sem dúvida, reajustar suas escolhas de prioridades (Alto, Médio e Baixo).

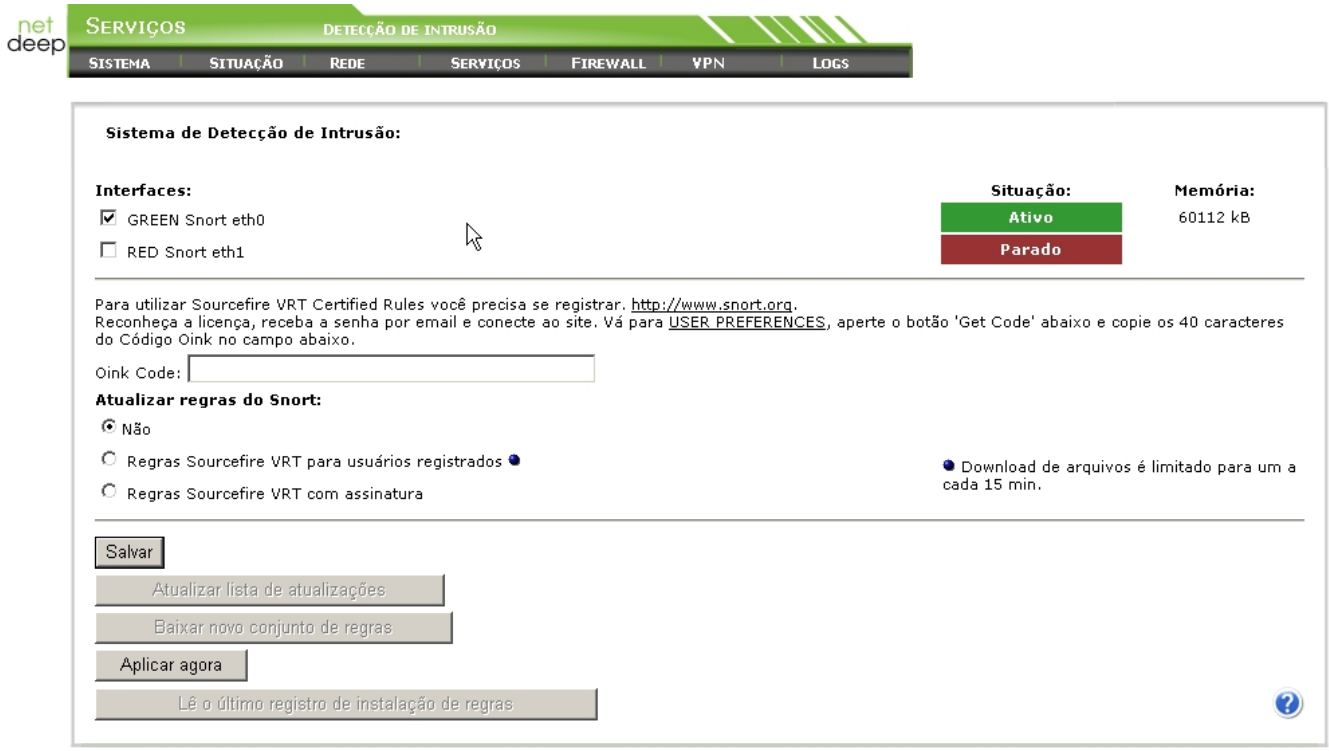


2.5.8. Detecção de Intrusos

O Netdeep Cop possui um poderoso sistema de detector de intrusos, baseado no Snort, o qual analisa o conteúdo dos pacotes recebidos pelo Firewall e procura por assinaturas conhecidas ou atividades maliciosas.

O Netdeep Cop pode monitorar os pacotes nas interfaces RED, GREEN e BLUE. Apenas assinale as caixas relevantes e clique no botão [Salvar].

Quanto mais ataques são descobertos, mais as regras usadas pelo Snort para reconhecê-los serão atualizadas. Para fazer o *download* da ultima versão, clique no botão [Baixar ...] para o novo regulador ser atualizado e iniciado.



2.6. SubMenu do Firewall

2.6.1. Redirecionamento de Porta (Port Forwarding)

Esta subseção lhe permite configurar os redirecionamentos de porta para o Netdeep Cop. Isto é 100% opcional, então você pode seguramente ignorar esta seção se não quiser utilizar este adicional.

2.6.1.1. Visão Geral do Redirecionamento de Porta

O Firewall previnem requisições externas de acesso aos sistemas protegidos (rede GREEN). No entanto, algumas vezes esta é uma situação muito severa. Por exemplo, se você está rodando um servidor web e há uma solicitação para aquele servidor por usuários externos, ela será bloqueada devido ao padrão. Isto significa que apenas os usuários da rede interna podem usar o servidor. Esta situação não é normal para servidores de web. A maioria das pessoas querem que os de fora tenham acesso ao servidor. E é aí onde o *Port Forwarding* entra em cena.

O *Port Forwarding* (redirecionamento de porta) é um serviço que permite acesso externo (de fora) à sistemas da rede interna.

Para configurar um redirecionamento de porta é necessário saber qual ou quais as portas são requisitadas pelo sistema/host que você pretende permitir o acesso externo.

De posse das informações das portas, você pode inserir as informações no GUI do Netdeep Cop.

A lista TCP/UDP lhe permite escolher qual protocolo será seguido. A maioria dos servidores regulares usam TCP. Alguns servidores de *games* e *chats* usam UDP, DNS usa TCP e UDP. Se o protocolo não é especificado neste documento do servidor, então provavelmente seja TCP.

As portas mais comuns são:

- 80 para servidores web- 20 para servidores FTP

- 53 para servidores de DNS
- 25 e 110 para servidores de mail, etc.

Se você desejar, você pode especificar o limite de portas. Para especificar o limite, use ":" entre os dois números de porta, o menor número vem primeiro.

O *Destination IP* (Porta Destino) é o endereço IP interno do servidor (por exemplo, você pode querer que seu servidor da web no IP 192.168.0.3).

O *Source IP* ou Apelido IP (Porta Origem) é o endereço IP (RED) externo que será afetado. O Netdeep Cop tem capacidade de controlar mais de um endereço IP (RED). Se você tem apenas IP RED externo, então escolha o IP Padrão.

2.6.1.2. Redirecionamento de Porta e Acesso Externo

O Acesso Externo *NÃO* afeta as redes GREEN ou ORANGE. Não há permissão para abrir as portas do Netdeep Cop, nem para as redes GREEN ou ORANGE .

Para possibilitar um acesso externo, no campo *Source IP* (IP ou Rede de Origem), ou rede (branco para "TODOS"):'

Este é o campo que controla o acesso externo – se você deixá-lo em BRANCO, seu *port forwarding* será aberto para TODOS OS ENDEREÇOS DA INTERNET. Uma forma alternativa é colocar um endereço ou rede da Internet que vai acessar o sistema/host.

Se você tiver mais de um endereço IP externo, ele aparecerá na tabela, e poderá ser usado para entrada do *port forwarding*.

Outras itens para notar:

- Nós suportamos o protocolo GRE.

- Você pode ter limites e *wildcards port*. Os *wildcards* (meta-caracteres/coringas) válidos são:

- * no qual traduzem para 1-65535

- 85 -* no qual traduzem para 85-65535

- *-500 no qual traduzem para 1-500

- Caracteres válidos de separação de limite de porta são ":" ou "-". Note que "–" será modificado para ":" mesmo que seja exibido como um "-" na tela.

- Você precisa inserir apenas a primeira porta origem e o destino será completado.

- Você pode editar uma configuração clicando no ícone do *Yellow Pencil* na coluna de Ação e até que você pressione o botão [Atualizar], nada será mudado e nada será perdido.

- Quando você está editando uma configuração, você a vê sublinhada em amarelo.

- Para deletar uma configuração, clique no ícone da Lixeira à direita da coluna de Ação.

- As variações de Portas não podem sobrepor uma a outra.

• Portas individuais não podem ser colocadas no meio de uma variação. Ex.: se você já tem 2000-3000 estabelecidos e tenta adicionar/configurar a porta 2500, isto produzirá um erro. Você não pode usar a mesma porta em várias máquinas/host.

• Portas reservadas: no endereço IP RED principal (IP PADRÃO) algumas portas são reservadas para que o Netdeep Cop faça sua administração. São elas: 67, 68, 81, 222, e 445.

• Quando você edita um *port forwarding*, haverá uma caixa extra entitulada *'Override external access to ALL' (permite acesso externo para todos)*. Ela é usada como um meio fácil e sujo de abrir uma porta para TODOS os endereços da Internet para testar ou qualquer outra razão qualquer.

• Se você tem um *port fowarding* como acessos externos múltiplos, quando você deleta todos os acessos externos, a porta se torna aberta para TODOS os endereços, então seja cuidadoso com isto.

• Há um atalho para Autorizar ou Não o *port forwarding* ou acesso externo. Clique no ícone "Habilitador" (a caixa está na coluna de Ação) para uma entrada em particular que você queira autorizar ou não. O ícone muda para uma caixa vazia quando não está autorizado. Clique na caixa para autorizá-lo novamente. Note que quando você não autoriza o *port forwarding*, todos os acessos externos associados são desabilitados e quando você autoriza o *port fowarding*, todos os acessos internos associados são autorizados.

2.6.2. Acesso Externo

Nesta página você pode configurar os parâmetros de Acesso Externo à máquina Netdeep Cop. E é 100% opcional, então você pode seguramente ignorar esta seção se não quiser fazer uso deste adicional.

Este item não afeta em nada o acesso às redes Green, Blue ou Orange, que são controlados pela seção anterior *Redirecionamento de Porta.*

• Se você deseja manter sua máquina Netdeep Cop isolada, deve especificar a porta TCP 445 / https. Se você tem acesso ssh autorizado, você também pode autorizar a porta TCP 222 / ssh.

• As opções TCP/UDP permite que você escolha qual protocolo será seguido. A maioria dos servidores regulares usam TCP.

• Se o protocolo não é especificado na documentação do servidor, então provavelmente seja TCP.

O IP de Origem é o endereço IP de uma máquina externa que você dá permissão para acessar seu firewall. Você pode deixá-lo em branco, o que permite qualquer endereço IP conectar. Apesar de perigoso, ele é util se você quiser administrar sua máquina de qualquer lugar do mundo. No entanto, se você pode limitar os endereços IP para manutenção. Os endereços IP das máquinas ou redes que são permitidos os acessos, devem ser listados nesta caixa.

• A Porta de Destino é a porta externa que é permitido o acesso, ex.: 445.

• O item do IP Destino permite que você escolha qual IP RED será afetado por esta regra. O Netdeep Cop tem a capacidade de controlar mais de um endereço IP RED (externo). Se você possui apenas um endereço IP RED, então escolha o IP Padrão.

Uma vez que você tenha colocado todas as informações, clique na caixa [Habilitado] e pressione [Adicionar]. Isto irá mover a régua para a próxima seção, e listá-la como ativa.

• Veja a lista de Regras Atuais que estão ativas. Para remover uma, clique na "Lixeira". Para editar uma, clique no "Yellow Pencil" (lápis).

• Para autorizar ou não uma regra, clique no ícone "Habilitar" (na coluna de Ação) para a entrada em particular que você queira autorizar ou não. O ícone muda para vazio quando não está autorizado. Clique na caixa para autorizá-la novamente.

2.6.3. DMZ (REDE ORANGE)

Esta seção permite que você configure regras de DMZ para o Netdeep Cop. Este item é 100% opcional, então você pode seguramente ignorar esta seção se não quiser fazer uso deste adicional.

Está página é visível apenas se você instalou e configurou placas/interfaces para as redes ORANGE ou BLUE.

Uma DMZ ou Demilitarized Zone (Zona ORANGE) é usada como um ponto de semi-seguro entre a Zona RED externa e a Zona GREEN interna. Na zona GREEN estão todas as suas máquinas internas. Na Zona RED é o âmbito da Internet. A DMZ permite implementar servidores sem que

haja a permissão de acesso interno (GREEN), mas com acesso pela Zona RED.

Por exemplo, suponha que sua rede tenha um servidor de web. Certamente você quer que os clientes externos (aqueles da Zona RED) possam acessá-lo. Mas suponha que você também quer que seu servidor web seja capaz de enviar ordens sobre clientes aos usuários da Zona GREEN. Isto não funcionaria em uma configuração tradicional de Firewall, porque o pedido para acessar a Zona GREEN estaria partindo de fora da Zona GEEN. Você certamente não quer dar a todos os seus clientes externos acesso direto às máquinas do lado GREEN. Então como isso pode funcionar? Usando a DMZ e as regras DMZ.

As regras DMZ dão às máquinas da Zona ORANGE (DMZ) acesso limitado para certas portas para as máquinas GREEN. Os servidores (as máquinas da Zona ORANGE) são mais susceptíveis à ataques de hacker porque precisam ter regras flexíveis relativas a Zona RED. A permissão de acessos limitados do ORANGE para o GREEN ajudarão a prevenir acessos não autorizados as àreas restritas que poderiam comprometer seu servidor.

A lista TCP/UDP permite escolher qual protocolo será seguido. A maioria dos servidores usam TCP. Alguns servidores de games e chats usam UDP. Se o protocolo não é especificado na documentação do servidor, então normalmente é TCP. Use o protocolo para especificar na página *Port Forwarding*.

A **Rede de Origem** é um menu que mostra as redes internas disponíveis na máquina.

O **IP Origem** é o endereço IP da máquina que você deseja dar permissão para acessar seus servidores internos.

A **Rede Destino** é um menu que mostra as redes externas disponíveis na máquina.

O **IP Destino** é o endereço IP da máquina da Zona GREEN ou BLUE que irá receber a requisição / pedido.

A **Porta Destino** é a porta da máquina que estará escutando o pedido.

Uma vez que você tenha inserido todas as informações, clique na caixa [Habilitar] e pressione [Adicionar]. Isto moverá a régua para a próxima seção, e irá listá-la como ativa.

As listas de regras atuais mostra as regras que estão em vigor. Para remover basta um clique na "Lixeira". Para editar um clique no "Yellow Pencil" (lápis).

Para habilitar ou desabilitar uma regra – clique no ícone [Habilitar] (na caixa da coluna de Ação) para a entrada que você queira habilitar ou desabilitar. O ícone muda para uma caixa vazia quando a regra é desabilitada. Clique na caixa para habilitar novamente.

2.6.4. Wireless (REDE BLUE)

Esta subseção permite que você configure o acesso à rede Wireless (BLUE) do Servidor Netdeep Cop.

Este comando é 100% opcional, então você pode seguramente ignorar esta seção se não quiser fazer uso deste adicional. Esta página será visível apenas se você instalou e configurou a placa wireless da interface BLUE.

Na seção dos Parâmetros você insere os dados do Wireless Access Point no Endereço IP ou no endereço MAC, ou uma máquina da rede BLUE que você pode conectar a Internet através do Netdeep Cop.

Se você quer acessar a rede GREEN a partir da rede BLUE, você deve abrir uma regra (página de Regras DMZ) ou use uma VPN.

Uma vez que você tenha inserido toda a informação, clique na caixa [Habilita] pressione [Adicionar[. Isto irá mover a régua para a próxima seção e listá-la como ativa.

Veja o status e controle as regras que estão em vigor. Para remover uma, clique na Lixeira. Para editar uma, clique no "Yellow Pencil".

Para autorizar ou não uma regra – clique no ícone [Habilita] (na caixa a direita) para um entrada que você queira autorizar ou não. O ícone muda para uma caixa vazia quando a regra não está autorizada. Clique na caixa para autorizá-la novamente.

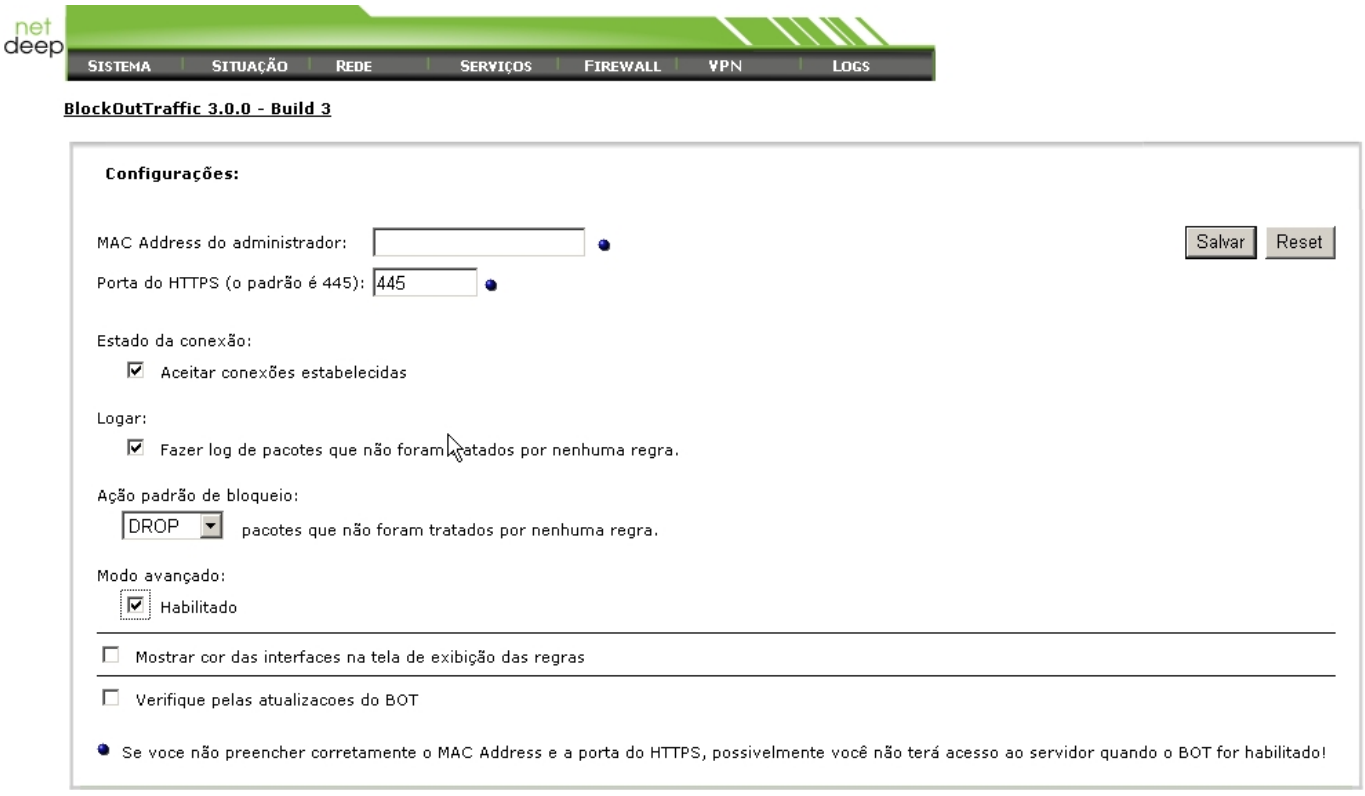
O Netdeep Cop é compatível com interfaces (placas) wireless da marca ORINOCO. Eventualmente algumas interfaces wireless podem requerer informações e apoio técnico do fabricante, para funcionar adequadamente no Servidor Netdeep Cop.

2.6.5. Bloqueio de tráfego de saída e Config. de Firewall Avançado

Esta seção permite que você configure regras especiais de Firewall para o Netdeep Cop. Este item é 100% opcional, então você pode seguramente ignorar esta seção se não quiser fazer uso deste adicional.

O Netdeep Cop já possui os dispositivos de segurança de Firewall que normalmente são necessários em uma rede. No entanto, você pode adicionar regras específicas e adicionais ao Firewall através destas seções.

Para utilizar esta seção é necessário domínio sobre regras IPTABLES. Use estas seções com cuidado, para evitar problemas no funcionamento de seu Servidor Netdeep Cop.

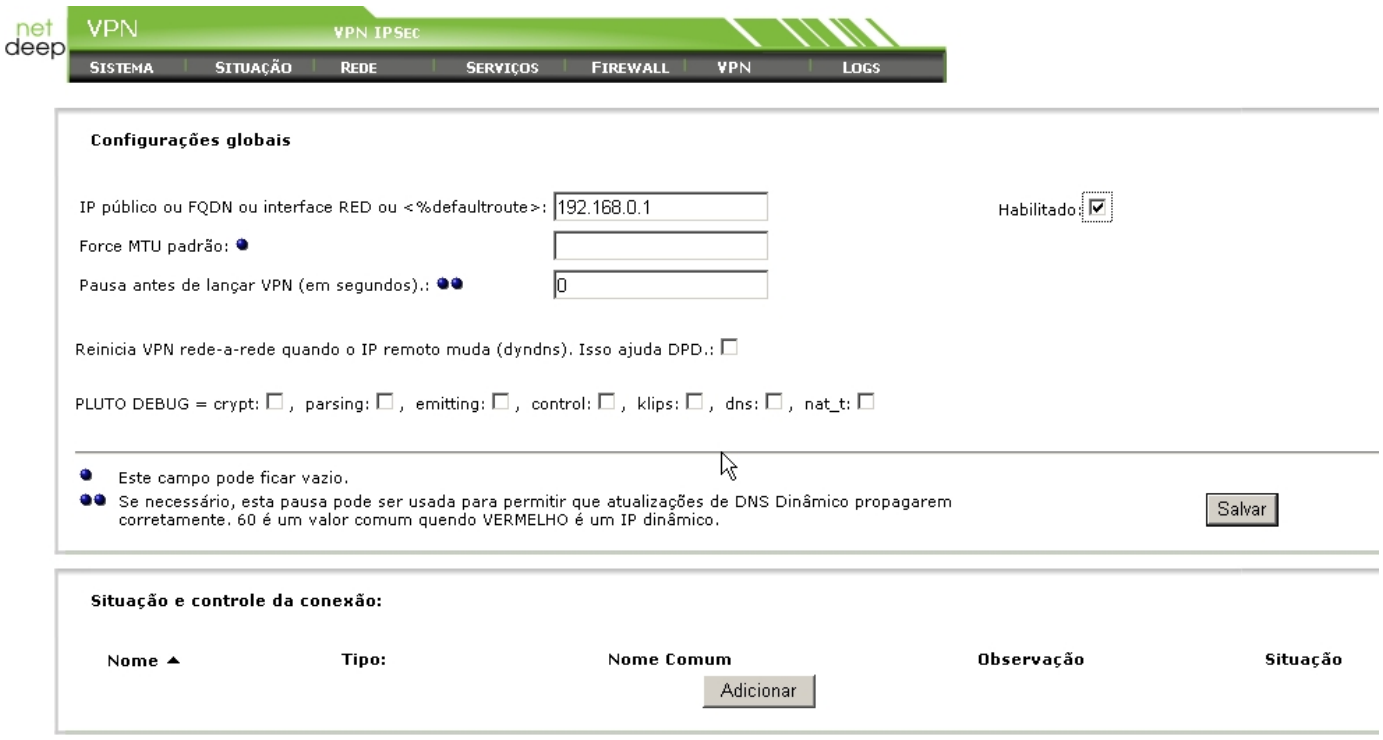


2.7. SubMenu de VPNs

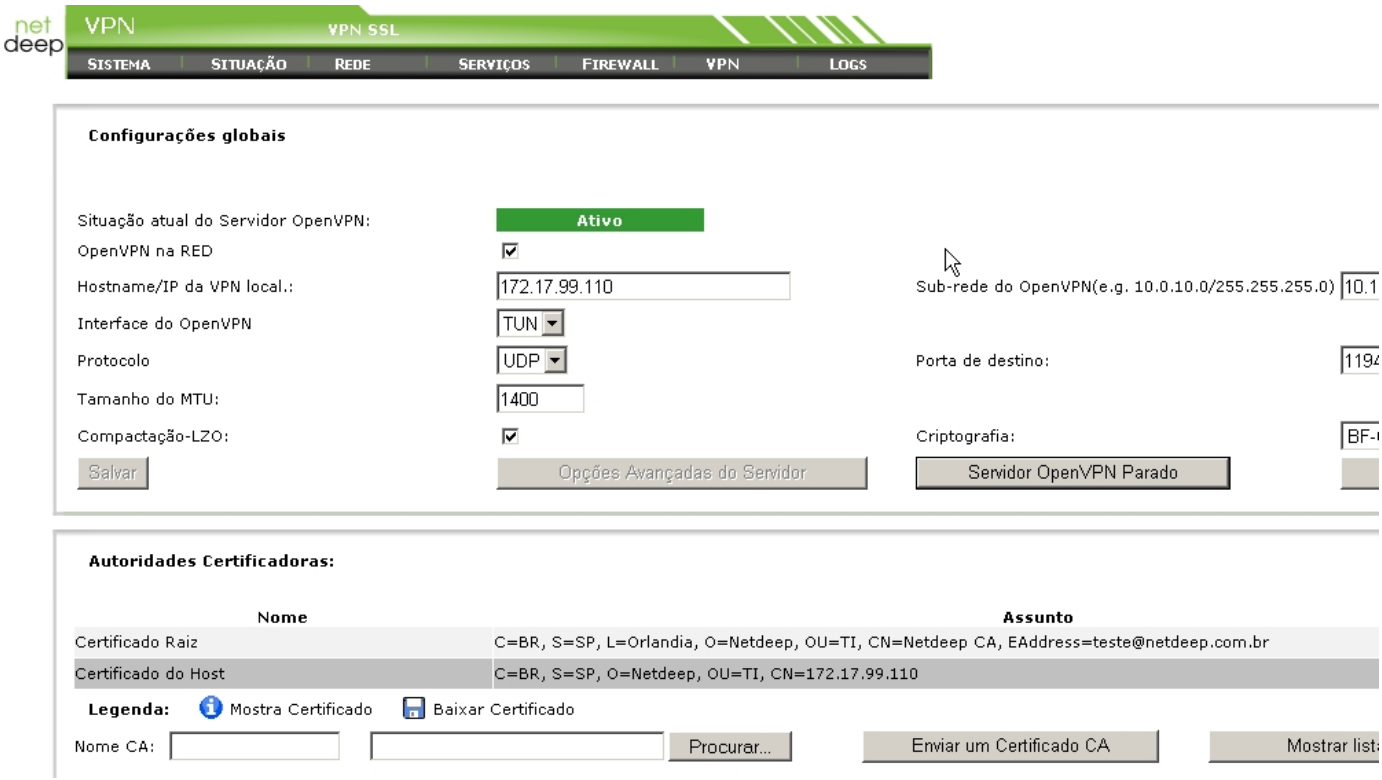
2.7.1. Virtual Private Networks (VPNs)

O Netdeep Cop pode facilmente estabelecer VPNs (Redes Privadas) entre outros servidores Netdeep Cop, usando túneis IPSec e SSL. Para este tópico temos uma documentação adicional sobre o mesmo. Está disponível gratuitamente em nosso site: http://www.netdeep.com.br

VPN IPSec



VPN SSL



2.8. SubMenu de Logs

2.8.1. Introdução

Os Logs consistem em cinco ou seis sub-páginas – Configuração do Logs, Resumo de Logs, Logs do Proxy/Filtro de URL, Logs do Firewall, Logs do IDS(se ativo) e Logs do Sistema.

Estes podem ser parametrizados e as informações podem ser exibidas por Mês ou Dia.

Cada vez que você seleciona uma nova combinação, você também deve clicar no botão [Update] para que as informações dos Logs sejam atualizadas. Quando você seleciona uma sub-página a informação de Logs aparecerá com a data atual.

Os botões permitem a navegação de visualização das informações.

O botão [Exportar] faz o download em arquivo *text-format (log.dat)*, contendo a informação da atual página de Logs do servidor Netdeep Cop, para seu computador.

Dependendo de como seu computador estiver configurado, ao pressionar o botão [Exportar] iniciará o download do arquivo, mostrando o conteúdo do *log.dat* na sua janela browser (navegador), ou abrindo o arquivo em um editor de texto. Você pode, também, salvar o *log.dat* em um arquivo text-format, se desejar.

2.8.2. Configuração do Log

Nesta página você configura os parâmetros de visualização, resumo e registro dos Logs.

2.8.3. Resumo do Log

Nesta página você pode visualizar, atualizar e exportar os Logs gerados pelo Netdeep Cop.

2.8.4. Logs do Proxy / Filtro URL

Esta página lhe dá a possibilidade de ver os LOGS gerados pelo Cache do Proxy no Netdeep Cop.

O Proxy fica inativo após a primeira instalação do Netdeep Cop, e pode ser ativado e desativado pelo administrador no SubMenu (***Serviços > Proxy Avançado***).

Nota

*Este item aparecerá apenas se você tiver ativado o **Serviços > Proxy Avançado**.*

Devido ao grande número de informações a ser processado, a página do Proxy pode levar algum tempo para aparecer após sua seleção inicial ou atualização.

Existem várias informações nesta página para você visualizar os aspectos e detalhes do funcionamento do Serviço de Proxy de seu Netdeep Cop.

2.8.5. Logs do Firewall

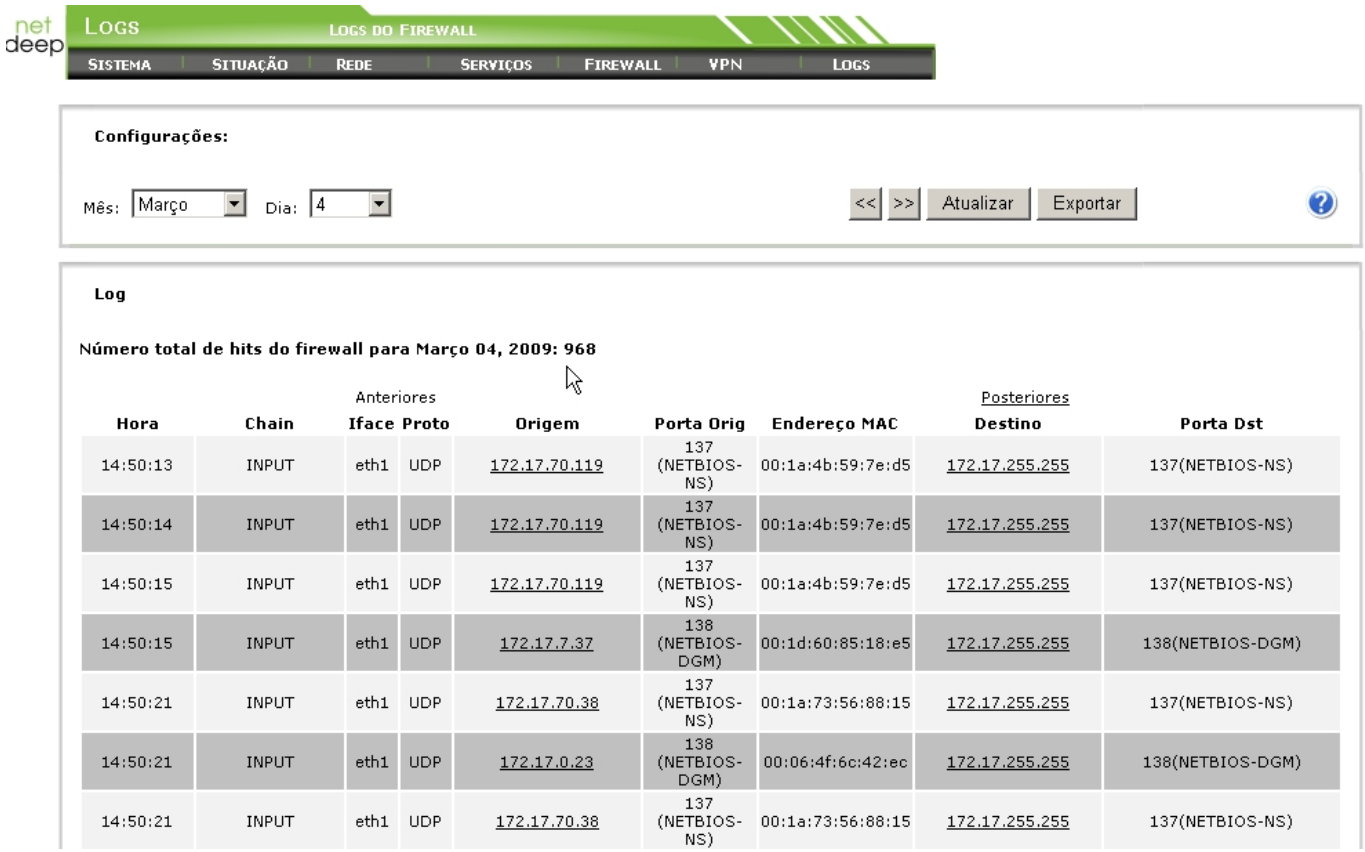
Esta página mostra os pacotes que foram bloqueados pelo Firewall do Netdeep Cop

Nota

Nem todos os pacotes negados são hostis de crackers querendo acessar sua máquina. Pacotes bloqueados acontecem, muitas vezes, devido a causas desconhecidas e podem ser ignoradas seguramente. Em meio a estes pode haver pacotes bloqueados naturalmente pelas tentativas de conexões a uma porta "ident/auth" (113).

Use os controles da página para navegar e visualizar as informações.

Você pode obter informações sobre os endereços IP listados, clicando em um deles. O Netdeep Cop efetua uma busca no DNS e relata qualquer informação disponível sobre seu registro e domínio.



2.8.6. Log do Intrusion Detection System (IDS)

Esta página mostra incidentes detectados pelo Netdeep Cop Intrusion Detection System (IDS). O serviço IDS é inativo após a primeira instalação do Netdeep Cop, e pode ser ativada (e desativada) pelo administrador. (Serviços > IDS Intrusion Detection).

Use os controles da página para navegar, visualizar e exportar as informações.

Você pode obter informações sobre os endereços IP listados, clicando em um deles. O Netdeep Cop efetua uma busca no DNS e relata qualquer informação disponível sobre seu registro e domínio.

2.8.7. Logs do Sistema

Esta página permite que você veja os Logs do sistema e outros.

Use os controles da página para navegar, visualizar e exportar as informações.

Existem onze categorias diferentes para você selecionar:

- **Netdeep Cop** (padrão) – eventos gerais do Netdeep Cop

- **RED** – mostra o tráfego da interface externa (Internet) e pode ser uma fonte muito útil para

solucionar problemas, como situações de falhas ao conectar.

- **DNS** – mostra um log de atividade para *dnsmasq* do domínio.

- **Servidor DHCP** – mostra um log de atividades para o Servidor DHCP do Netdeep Cop.

- **SSH** – provê um registro de usuários que fizeram o log in e log out no Servidor Netdeep Cop através de uma interface SSH.

- **NTP** – mostra um log de atividades do servidor de tempo *ntpd*.

- **CRON** – provê um registro de atividades agendadas no *cron daemon*.

- **Login/Logout** - provê um registro de usuários que fizeram o *log in* e o *log out* no Netdeep Cop. Isto inclui *logins* locais e através da interface SSH.

- **Kernel** – é um registro da atividade Kernel do Netdeep Cop.

- **IPSec** – é um registro da atividade do IPSec – gerado pelo módulo de VPN do Netdeep Cop.

- **Update Transcript (atualizar transcrições)** – é um log de resultados de qualquer atualização aplicada no Servidor Netdeep Cop através da janela Sistema > Atualizações.

2.8.8. Arquivamento

Esta página provê uma estatística detalhada do uso da Internet pelo usuários e é uma das ferramentas mais valiosas para controle do acesso dos usuários do Netdeep Cop.

As tabelas estatísticas (diárias, semanais e mensais) mostram os sites mais acessados, os sites acessadas por cada usuário, etc.

Se for implementado o acesso autenticado à Internet, conforme veremos nas configurações do Proxy/Filtro de URL, as informações serão apresentadas por nome de usuário, caso contrário serão apresentadas por endereço IP.