Fedora - Dicas

- FIREWALLD - UTILIZAÇÃO
- Alterar o endereço IP em um servidor Fedora

FIREWALLD - UTILIZAÇÃO

Este tutorial tem como objetivo demonstrar um funcionamento básico para liberar e bloquear portas no firewall do Fedora.

O Firewall do Fedora Server

O Fedora Server utiliza o Firewalld para gerenciar o filtro de pacotes baseado em iptables. Esse firewall possui algumas regras padrão e trabalha com o conceito de zonas onde a liberação de serviços é feito dentro delas.

A tabela abaixo demonstra como está configurado o firewall da rede após a instalação do sistema operacional:

Regra	**Comportamento**
INPUT	Liberado apenas o acesso a porta 22(TCP) e conexões do tipo RELATED,ESTABLISHED.
FORWARD	Aceita apenas conexões do tipo RELATED,ESTABLISHED.
OUTPUT	Não possui restrições.

Zonas

O firewalld gerencia um grupo de regras conhecido como zonas. As zonas definem o tipo de tráfego que será permitido baseado no nível de confiança da rede onde o seu servidor está conectado. Cada zona está atrelada a uma interface de rede existente no servidor.

O comando abaixo lista as zonas existentes:

```
firewall-cmd --get-zones
```

Abaixo são mostradas as zonas existentes no firewalld em ordem de nível de confiança:

Zona	**Descrição**
drop	Todos os pacotes são descartados.
block	Todos os pacotes são rejeitados.
public	Rede que você não conhece, pública.

external	Rede externa onde o servidor com o firewalld funciona como um
gateway	para a rede interna. É configurada com mascaramento para manter a privacidade da rede interna.
internal	É a parte interna da rede. Equipamentos nessa rede possuem um nível maior de confiança e serviços adicionais estão disponíveis.
dmz	São equipamentos isolados, ou seja, que não devem possuir acesso a sua rede. Apenas algumas conexões de entrada para esses equipamentos são permitidas.
work	Equipamentos de trabalho com liberação de serviços adicionais.
home	Equipamentos de casa. São dispositivos mais conhecidos e confiáveis e que possuem liberação para um pouco mais de serviços que a zona work.
trusted	Equipamentos de confiança. Praticamente todos os serviços estão disponíveis para os equipamentos nesta zona.

Listar as regras existentes

O comando abaixo lista todas as regras existentes no serviço firewalld:

```
firewall-cmd --list-all
```

Se desejar listar apenas as regras de uma determinada zona utilize a opção –zone:

```
firewall-cmd –zone=public --list-all
```

Liberar portas de entrada

Para modificar as regras de entrada do firewall do Fedora, utilizamos o comando firewall-cmd.

No exemplo abaixo é demonstrado como liberar as portas 80(TCP) e 443(TCP) para acesso da rede pública, de forma permanente, para um servidor HTTP através da linha de comando:

```
firewall-cmd --permanent --zone=public --add-port=80/tcp
firewall-cmd --permanent --zone=public --add-port=443/tcp
firewall-cmd --set-default-zone=public
firewall-cmd --reload
```

onde:

--permanent	Adiciona a regra de forma permanente, ou seja, após reiniciar o filtro as regras permanecerão. Se for omitida esta opção as regras são válidas até o firewalld ser reiniciado.
--zone=public	É a zona pública não confiável. São endereços que você não conhece mas podem ser autorizados caso a caso.
--add-port=80/tcp	Informação da porta e protocolo que serão adicionados na zona public.
--reload	Recarrega as regras mantendo o estado das conexões.
--set-default-zone=public	Define a zona public como a padrão a ser utilizada.

Liberando um host ou uma rede

Abaixo é demonstrado como liberar o acesso total ao servidor para a rede cuja origem é 192.168.1.0/24:

```
firewall-cmd --permanent --zone=public --add-source=127.0.0.1/8
firewall-cmd --reload
```

--permanent	Adiciona a regra de forma permanente, ou seja, após reiniciar o filtro as regras permanecerão. Se for omitida esta opção as regras são válidas até o firewalld ser reiniciado.
--zone=public	É a zona pública não confiável. São endereços que você não conhece mas podem ser autorizados caso a caso.
--add-source=192.168.1.0/24	Informação da rede ou host que serão adicionados na zona public.
--reload	Recarrega as regras mantendo o estado das conexões.

Configurando o firewalld para agir como NAT

Para essa função faz-se necessário ter pelo menos 2 interfaces de rede no servidor, uma que faça a conexão com a rede pública e outra a rede interna.

No exemplo abaixo, a interface eth0 está conectada na rede pública e a eth1 na rede interna:

```
firewall-cmd --permanent –zone=internal –add-interface=eth1
firewall-cmd –permanent –zone=public -add-masquerade
firewall-cmd --reload
```

--permanent	Adiciona a regra de forma permanente, ou seja, após reiniciar o filtro as regras permanecerão. Se for omitida esta opção as regras são válidas até o firewalld ser reiniciado.
--zone=public --zone=internal	Selecionamos a zona public para fazer o mascaramento e a internal para informar a rede interna.
--add-masquerade	Adiciona o mascaramento na zona selecionada.
--reload	Recarrega as regras mantendo o estado das conexões.

Configurando o firewalld para Port Forward

Para redirecionar portas da rede externa para um endereço da rede interna, utilize os comandos abaixo:

```
firewall-cmd --permanent --zone=public –add-forward-
port=port=443: proto=tcp: toport=443: toaddr=192. 168. 1. 11
firewall-cmd --reload
```

--permanent	Adiciona a regra de forma permanente, ou seja, após reiniciar o filtro as regras permanecerão. Se for omitida esta opção as regras são válidas até o firewalld ser reiniciado.
--zone=public	É a zona pública não confiável. São endereços que você não conhece mas podem ser autorizados caso a caso.
--add-forward-port=	Ativa a regra para o port forward.
port=443	Porta de origem.
proto=tcp	Protocolo de origem.
toport=443	Porta de destino.
toaddr=192.168.1.11	IP de destino na rede interna.
--reload	Recarrega as regras mantendo o estado das conexões.

Contato

Monsta Tecnologia Ltda

Site: http://www.monsta.com.br

Downloads: http://www.monsta.com.br/download.html

E-mail: contato@monsta.com.br

Alterar o endereço IP em um servidor Fedora

Este tutorial passo a passo irá guiá-lo no processo de alteração do endereço IP em um servidor Linux Fedora. Aprenda a configurar um endereço IP estático ou dinâmico para garantir a conectividade de rede ideal para o seu servidor.

Configurar o IP do servidor

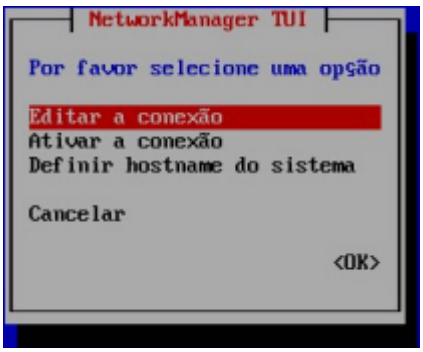
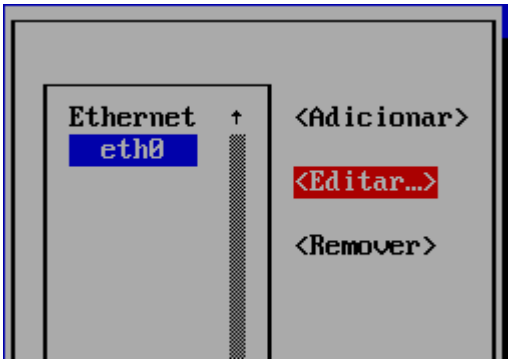
Entre com as credenciais de root em seu servidor. Uma vez logado, instale o programa para gerenciar interfaces de rede:

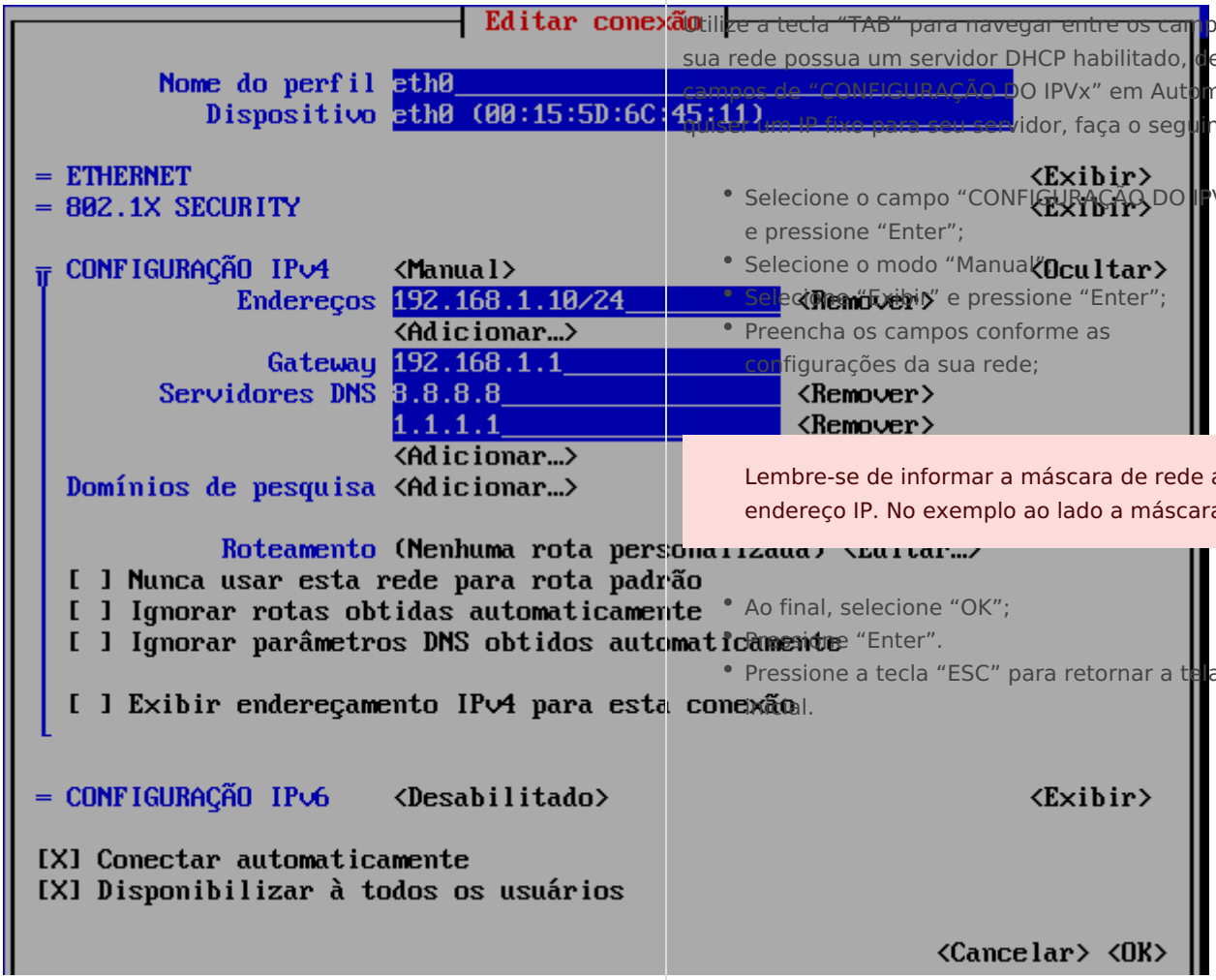
```
dnf install -y NetworkManager-tui
```

Depois de instalado, execute o gerenciador:

```
nmtui
```

Siga a sequência abaixo para editar as configurações de rede:

	• Selecione “Editar a conexão”; • Pressione “Enter”.
	• Selecione sua conexão de rede; • Selecione “Editar”.

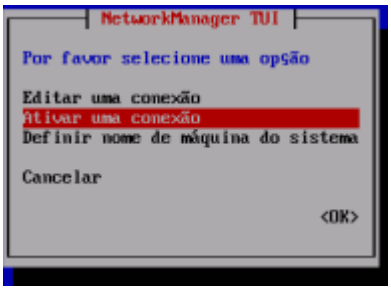


Utilize a tecla “TAB” para navegar entre os campos. Caso sua rede possua um servidor DHCP habilitado, deixe os campos de “CONFIGURAÇÃO DO IPVx” em Automático. Se quiser um IP fixo para seu servidor, faça o seguinte:

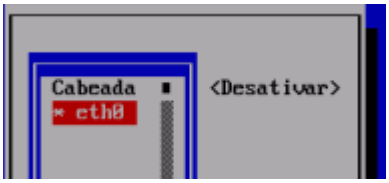
- Selecione o campo “CONFIGURAÇÃO DO IPVx” e pressione “Enter”;
- Selecione o modo “Manual”;
- Selecione “Exibir” e pressione “Enter”;
- Preencha os campos conforme as configurações da sua rede;

Lembre-se de informar a máscara de rede após o endereço IP. No exemplo ao lado a máscara é /24.

- Ao final, selecione “OK”;
- Pressione “Enter”.
- Pressione a tecla “ESC” para retornar a tela inicial.



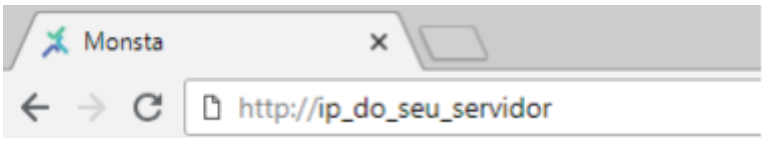
- Selecione “Ativar uma conexão” e pressione “Enter”.



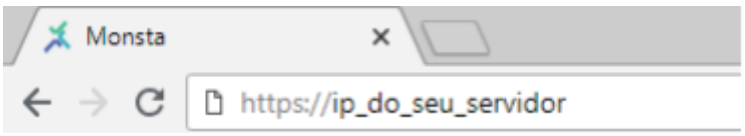
- Selecione a placa de rede que teve seu IP alterado e pressione “Enter” para desativá-la;
- Em seguida, pressione “Enter” novamente para ativá-la.
- Pressione “ESC” até sair do programa e retornar ao prompt de comando.

Acessar o Monsta

Após configurar o endereço IP do servidor, abra um navegador de internet e acesse:



ou



A tela de login do Monsta será apresentada. Para efetuar o login, utilize suas credencias.

Regras de Firewall (Opcional)

Se a sua rede possui um firewall que controla os acessos à internet, libere os seguintes hosts e portas:

> Host a.ntp.br e 2.fedora.pool.ntp.org
> Host mind.monsta.com.br na porta 443/TCP
> Host mind.monsta.com.br na porta 80/TCP

As portas acima para mind.monsta.com.br e www.monsta.com.br permitem:

-> Backup automático das configurações.
-> Restauração do backup em caso de alguma falha.
-> Envio de notificações por E-mail, SMS e Telegram.
-> Checagem do estado da comunicação entre o Monsta instalado em seu servidor e o a Nuvem do Monsta. Com isso é possível receber alertas em caso de paradas inesperadas do serviço de monitoramento, tal como o desligamento impróprio do servidor ou falha no link de internet.
-> Autenticação das Chaves de Licenciamento.
-> Verificar e atualizar a versão do sistema.

Dica

Utilize este tutorial para configurar regras do seu firewall caso sua instalação do Fedora tenha instalado o sistema FirewallD:

Firewalld - Utilização

Contato

Monsta Tecnologia Ltda

Site: http://www.monsta.com.br

Downloads: http://www.monsta.com.br/download.html

E-mail: contato@monsta.com.br