

Tutorial Pfsense

Instalação e Configurações Básicas

Aires Santos, Caíque Cabral, Jéssica Silva, Juliana Farias, Luiz Henrique Menezes e Oscar Junior

Março de 2013

Tutorial desenvolvido como requisito parcial para aprovação na disciplina de Redes de Computadores II (Prof. Rafael Reale) do Curso Téc. em Informática, Modalidade Subsequente, do Instituto Federal da Bahia – Campus Valença.

Esse tutorial explica detalhadamente a instalação do software PFSENSE, destinado a servidores firewall. O processo descrito é aplicado a uma máquina virtual, mas também pode ser realizado em um servidor real.

Antes de iniciarmos nosso tutorial, vamos esclarecer alguns conceitos básicos para a futura implementação do nosso servidor Pfsense:

O que é firewall?

Firewall pode ser definido como uma barreira de proteção, que controla o tráfego de dados entre seu computador e a Internet(ou entre a rede onde seu computador está instalado e a Internet). Seu objetivo é permitir somente a transmissão e a recepção de dados autorizados. Existem firewalls baseados na combinação de hardware e software e firewalls baseados somente em software. Este último é o tipo recomendado ao uso doméstico e também é o mais comum.



Explicando de maneira mais precisa, o firewall é um mecanismo que atua como "defesa" de um computador ou de uma rede, controlando o acesso ao sistema por meio de regras e a filtragem de dados. A vantagem do uso de firewalls em redes, é que somente um computador pode atuar como firewall, não sendo necessário instalá-lo em cada máquina conectada.

Firewall em forma de softwares

Aplicações com a função de firewall já são parte integrante de qualquer sistema operacional moderno, garantindo a segurança do seu PC desde o momento em que ele é ligado pela primeira vez. Os firewalls trabalham usando regras de segurança, fazendo com que pacotes de dados que estejam dentro das regras sejam aprovados, enquanto todos os outros nunca chegam ao destino final.

Outra medida muito usada são os filtros por portas e aplicativos. Com eles, o firewall pode determinar, exatamente, quais programas do seu computador podem ter acesso ao link de internet ou não. As portas de comunicação também podem ser controladas da mesma forma, permitindo que as portas mais "visadas" pelos malware sejam bloqueadas definitivamente.

Firewall como hardware

Os firewalls em forma de hardware são equipamentos específicos para este fim e são mais comumente usados em aplicações empresariais. A vantagem de usar equipamentos desse tipo é que o hardware é dedicado em vez de compartilhar recursos com outros aplicativos. Dessa forma, o firewall pode ser capaz de tratar mais requisições e aplicar os filtros de maneira mais ágil.

Filtragem de pacotes

O firewall que trabalha na filtragem de pacotes é muito utilizado em redes pequenas ou de porte médio. Por meio de um conjunto de regras estabelecidas, esse tipo de firewall determina que endereços IPs e dados possam estabelecer comunicação e/ou transmitir/receber dados. Alguns sistemas ou serviços podem ser liberados completamente (por exemplo, o serviço de e-mail da rede), enquanto outros são bloqueados por padrão, por terem riscos elevados (como softwares de mensagens instantâneas, tal como o ICQ). O grande problema desse tipo de firewall, é que as regras aplicadas podem ser muito complexas e causar perda de desempenho da rede ou não ser eficaz o suficiente.

Este tipo se restringe a trabalhar nas camadas TCP/IP, decidindo quais pacotes de dados podem passar e quais não. Tais escolhas são regras baseadas nas informações endereço IP remoto, endereço IP do destinatário, além da porta TCP usada.

Quando devidamente configurado, esse tipo de firewall permite que somente "computadores conhecidos troquem determinadas informações entre si e tenham acesso a determinados recursos". Um firewall assim, também é capaz de analisar informações sobre a conexão e notar alterações suspeitas, além de ter a capacidade de analisar o conteúdo dos pacotes, o que permite um controle ainda maior do que pode ou não ser acessível.

Firewall de aplicação

Firewalls de controle de aplicação (exemplos de aplicação: SMTP, FTP, HTTP, etc.) são instalados geralmente em computadores servidores e são conhecidos como Proxy. Este tipo não permite comunicação direta entre a rede e a Internet. Tudo deve passar pelo firewall, que atua como um intermediador. O Proxy efetua a comunicação entre ambos os lados por meio da avaliação do número da sessão TCP dos pacotes.

Este tipo de firewall é mais complexo, porém muito seguro, pois todas as aplicações precisam de um Proxy. Caso não haja, a aplicação simplesmente não funciona. Em casos assim, uma solução é criar um "Proxy genérico", através de uma configuração que informa que determinadas aplicações usarão certas portas. Essa tarefa só é bem realizada por administradores de rede ou profissionais de comunicação qualificados.

O firewall de aplicação permite um acompanhamento mais preciso do tráfego entre a rede e a Internet (ou entre a rede e outra rede). É possível, inclusive, contar com recursos de log e ferramentas de auditoria. Tais características deixam claro que este tipo de firewall é voltado a redes de porte médio ou grande e que sua configuração exige certa experiência no assunto.



O que é Pfsense?

O Pfsense é um dos mais conhecidos e provavelmente mais rico, em recursos, entre os sistemas para appliance pré-configurado, pronto amigável, amistoso e facilitado uso por interface Web de uma versão customizada do FreeBSD que oferece inúmeros recursos, focado para ambiente de roteamento e firewalling, bem como segurança de networking, com excelente solução para VPN, entre outros diversos recursos. É um projeto descendente do famoso m0n0wall, e que provavelmente, você já ouviu falar. Ao lado do (mais específico) FreeNAS, e recentemente colocado por Patrick Tracanelli na FUG o artigo sobre oAskoziaPBX, são os principais e grandes projetos derivados do m0n0wall.

O Pfsense chegou a um nível de desenvolvimento que não há muito mais o que fazer o que integrar, a não ser manter a atualização e estabilidade, além de melhoria dos recursos atuais. Talvez o único recurso que o Pfsense não integre – por opção dos criadores do Projeto – é um IPS (Intrusion Prevention System). O resto, de controle de banda avançado, à VPN, passando por Captive Portal, autenticação RADIUS, etc., é rico em recursos.



O que é squid?

O **Squid** é um servidor proxy que suporta HTTP, HTTPS, FTP e outros. Ele reduz a utilização da conexão e melhora os tempos de resposta fazendo cache de requisições freqüentes de páginas web numa rede de computadores. Ele pode também ser usado como um Proxy reverso.

O Squid foi escrito originalmente para rodar em sistema operacional tipo Unix, mas ele também funciona em sistemas Windows desde sua versão.

Servidor Proxy

No cache são armazenados os objetos da Internet (ex. dados de páginas web) disponíveis via protocolo HTTP, FTP e Gopher num sistema mais próximo ao do cliente. Os navegadores podem então usar o Squid local como um servidor Proxy HTTP, reduzindo o tempo de acesso aos objetos e reduzindo a utilização da conexão. Isto é muito usado por provedores no mundo todo para melhorar a velocidade de navegação para seus clientes e também em LAN que compartilham a mesma conexão à Internet. Ele pode fornecer anonimato e segurança dado ser um intermediário no acesso aos objetos. No entanto a sua utilização pode gerar preocupações a respeito da privacidade, pois o Squid é capaz de armazenar registros sobre os acessos, incluindo URLs acedidas, a data e hora exatas, e quem acedeu.

A aplicação cliente (ex. navegador) deverá especificar explicitamente o servidor Proxy que quer utilizar (típico para os clientes de provedores), ou poderá utilizar um Proxy transparente, em que todos os pedidos HTTP para fora, são interceptados pelo Squid e todas as respostas são armazenadas em cache, dessa forma não sendo necessário configurar o navegador.

Squid tem algumas funcionalidades que permitem tornar as conexões anônimas, tais como desabilitar ou alterar campos específicos do cabeçalho dos pedidos HTTP do cliente. Se isto é feito e como, é controlado pela pessoa que administra a máquina que corre o Squid. As pessoas que requisitam páginas numa rede que usa Squid de forma transparente podem não saber que esta informação está a ser registrada.

O que é Captive Portal?

Captive portal é um programa de computador responsável por controlar e gerenciar o acesso a Internet em redes públicas, de forma "automatizada". Ao digitar o endereço de qualquer site no navegador o usuário é interceptado pelo sistema do *Captive Portal* e redirecionado para uma interface que solicita a autenticação.

É importante lembrar que não existe uma fórmula ou receita pronta que indique passo-a-passo como o PfSense deve ser configurado. Pois, tudo depende da necessidade da aplicação do mesmo. Neste caso, estaremos, inicialmente, demonstrando a criação da máquina virtual, depois a instalação do PfSense na máquina criada e, em seguida, mostrando de maneira simples algumas configurações básicas para proteção de uma rede.

Requisitos:

A seguir descreve os requisitos mínimos de hardware para Pfsense 1.2.x. Observe os requisitos mínimos não são adequados para todos os ambientes.

CPU - Pentium 100 MHz

RAM - 128 MB

Requisitos específicos para plataformas individuais seguir.

Live CD

CD-ROM

USB flash drive ou disquete para armazenar arquivo de configuração

Instalação no disco rígido

CD-ROM para instalação inicial

GB de um disco rígido

Incorporado

512 MB cartão Compact Flash

porta de série para o console

A ISO do Pfsense pode ser baixada gratuitamente aqui:

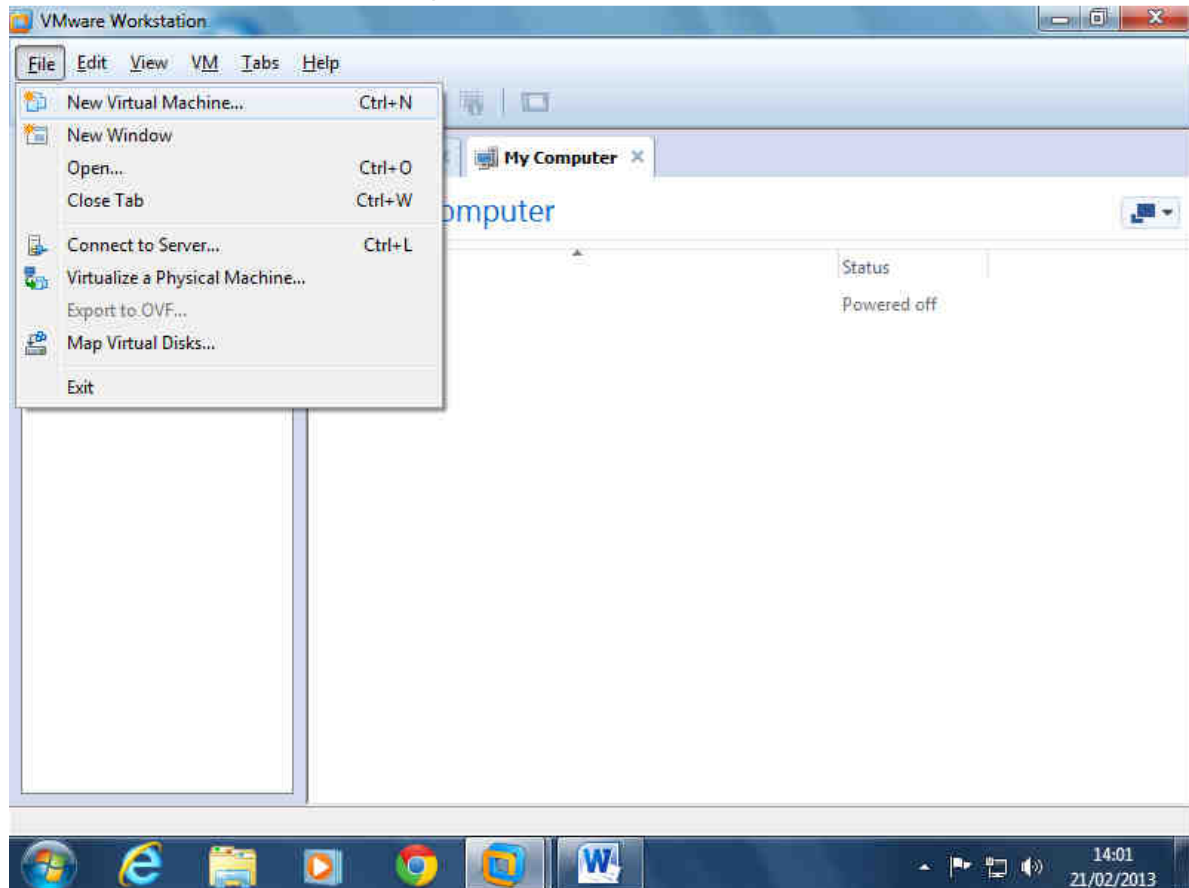
<http://www.pfsense.org/mirror.php?section=downloads>

Tutorial de instalação do Pfsense

Configuração da Máquina Virtual

Para instalar o servidor do Pfsense utilizaremos uma máquina virtual, ela simula através de um software um outro computador dentro do sistema operacional presente na máquina real, essa técnica se chama *virtualização* e utilizaremos o *VMware Workstation para tal*.

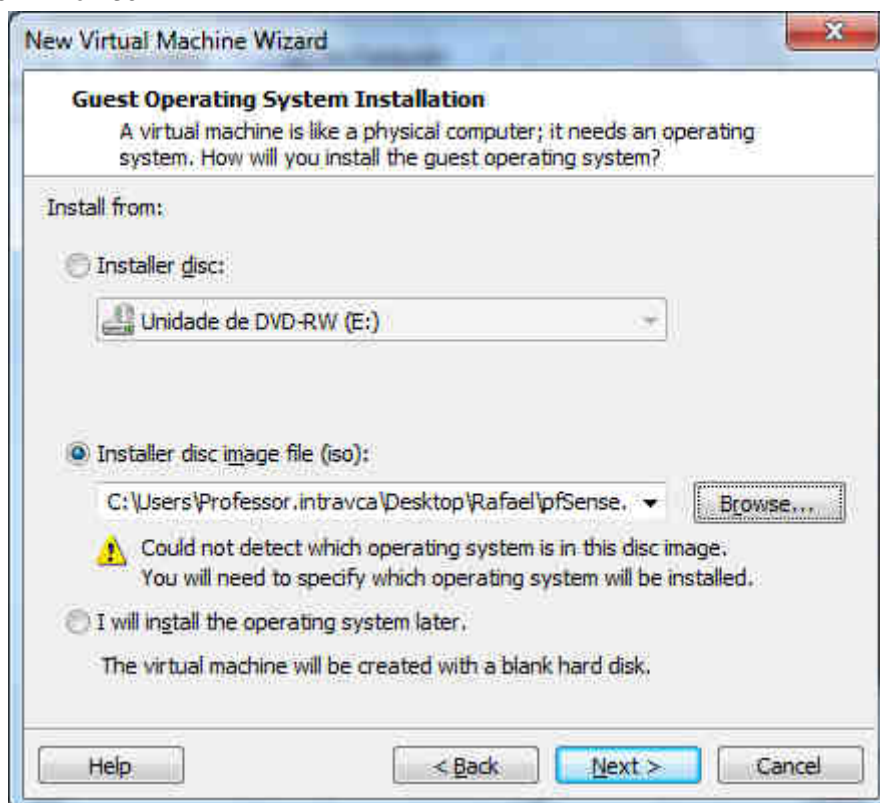
1- No VMware criaremos uma nova maquina virtual na aba *File > New Virtual Machine*



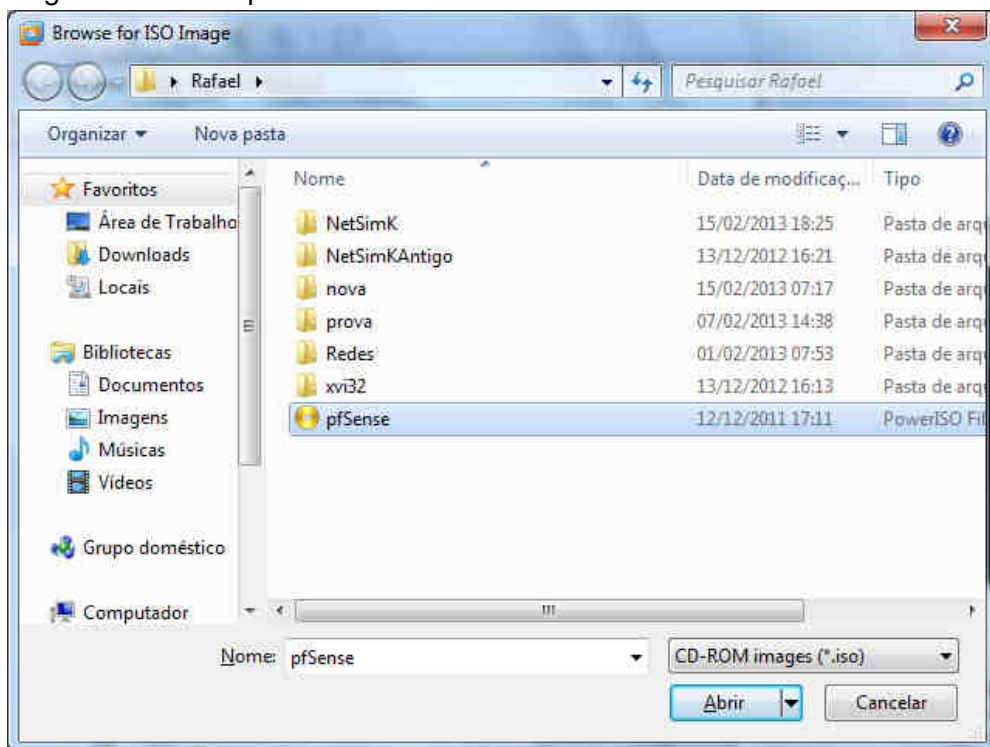
2- Na janela que aparecerá, deixe marcada a opção *Typical (recommended)* e clique em *Next*



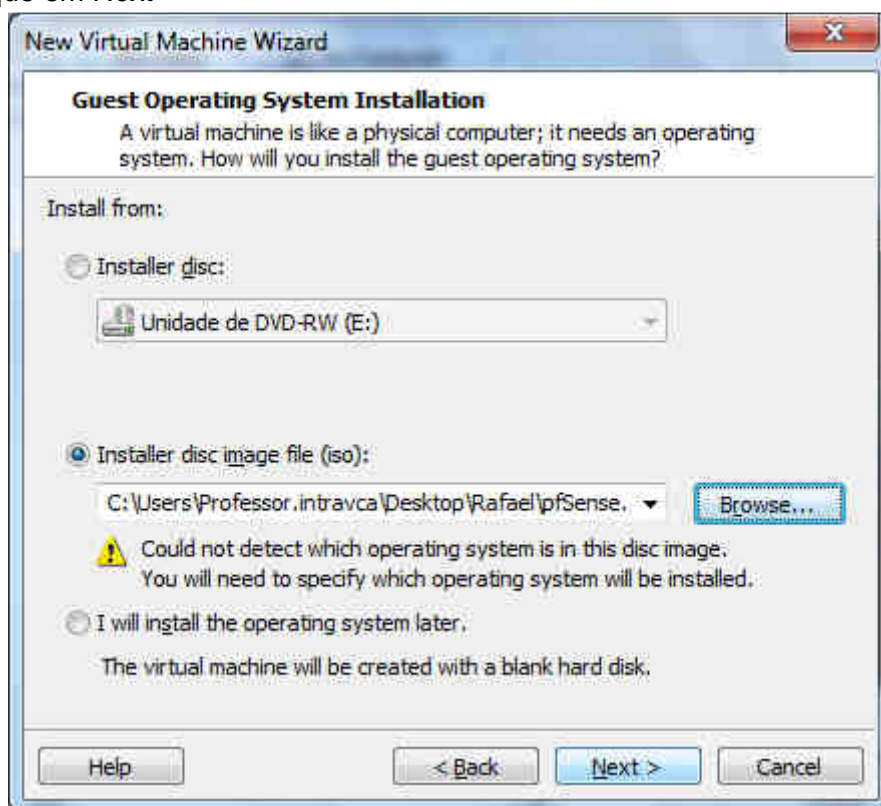
3- Na janela abaixo, caso a imagem do PfSense seja esteja gravada no CD escolha a opção *Installer disc* e insira o CD no seu drive, mas como não é o nosso caso escolheremos a ISO que foi baixada no site do pfSense clicando em *Browse*



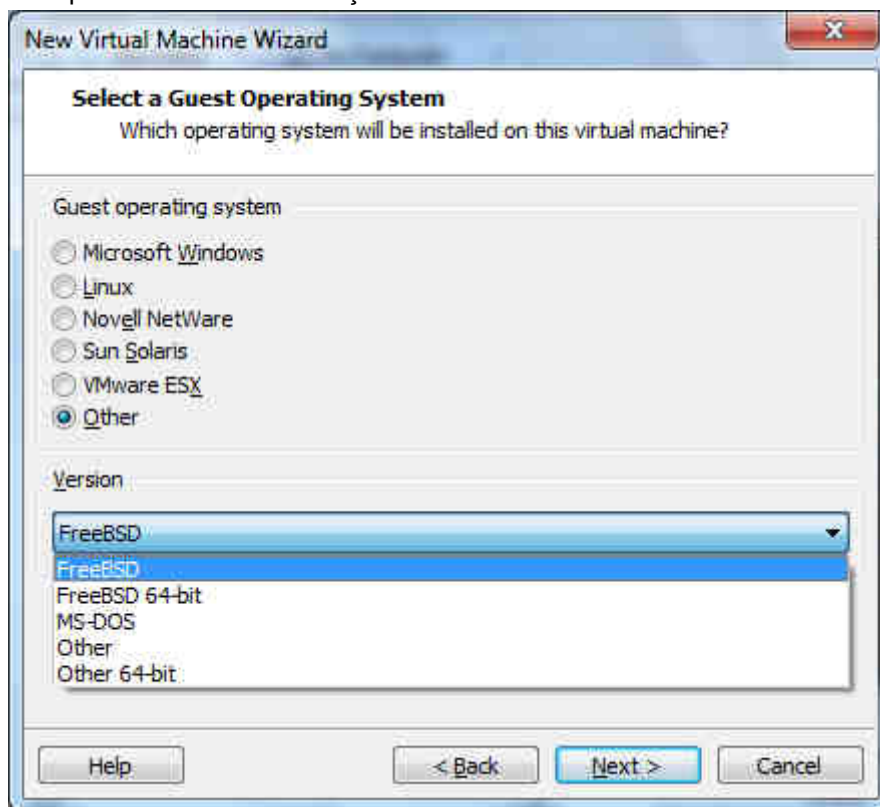
4- Encontre a imagem salva e clique em *Abrir*



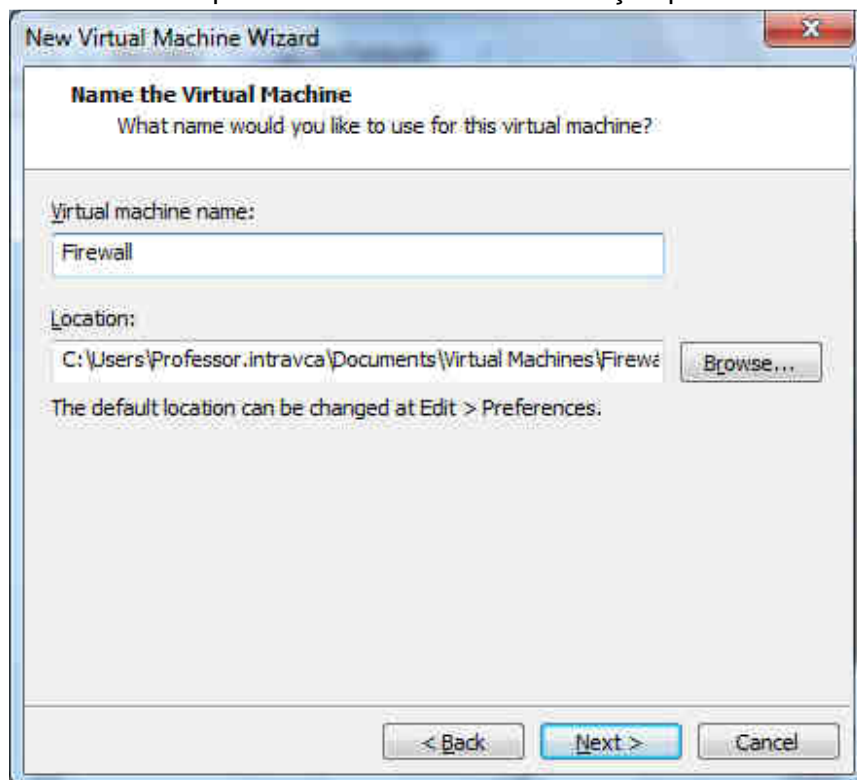
5- Em seguida clique em *Next*



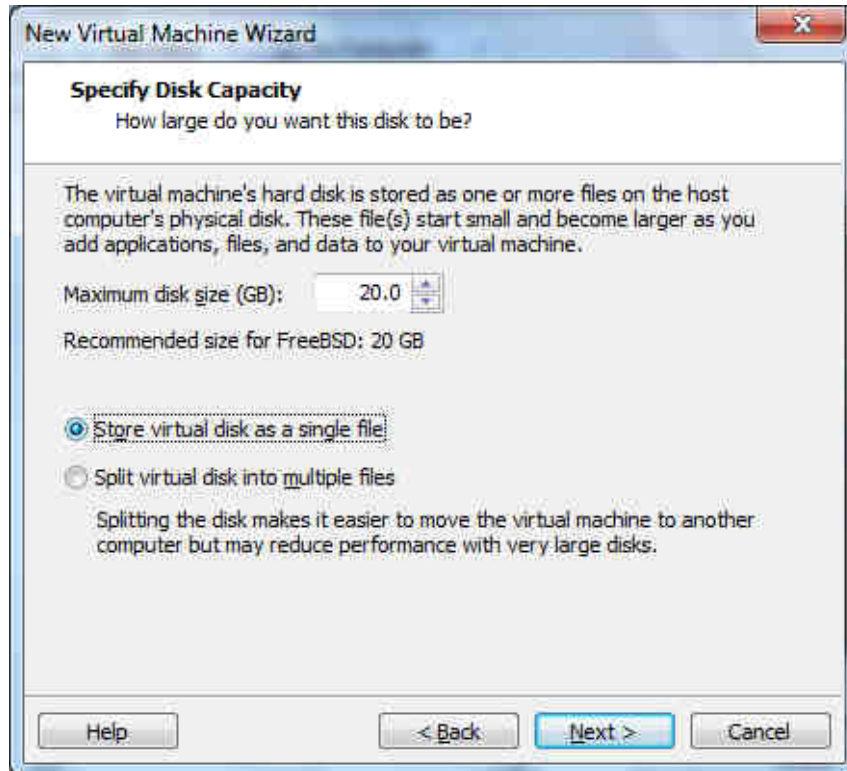
6- Essa janela pergunta qual sistema operacional você está instalando. Clique em *Other* e abaixo selecione FreeBSD. *O pfSense é uma distribuição do FreeBSD



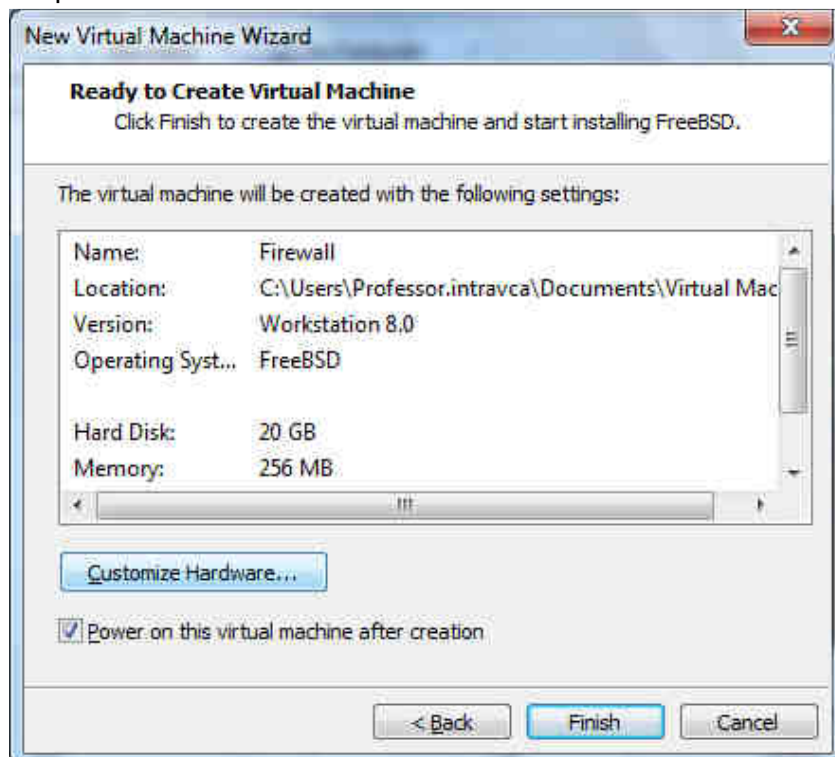
7- Aqui escolha o nome da sua maquina virtual e o local de instalação pode deixar o local padrão.



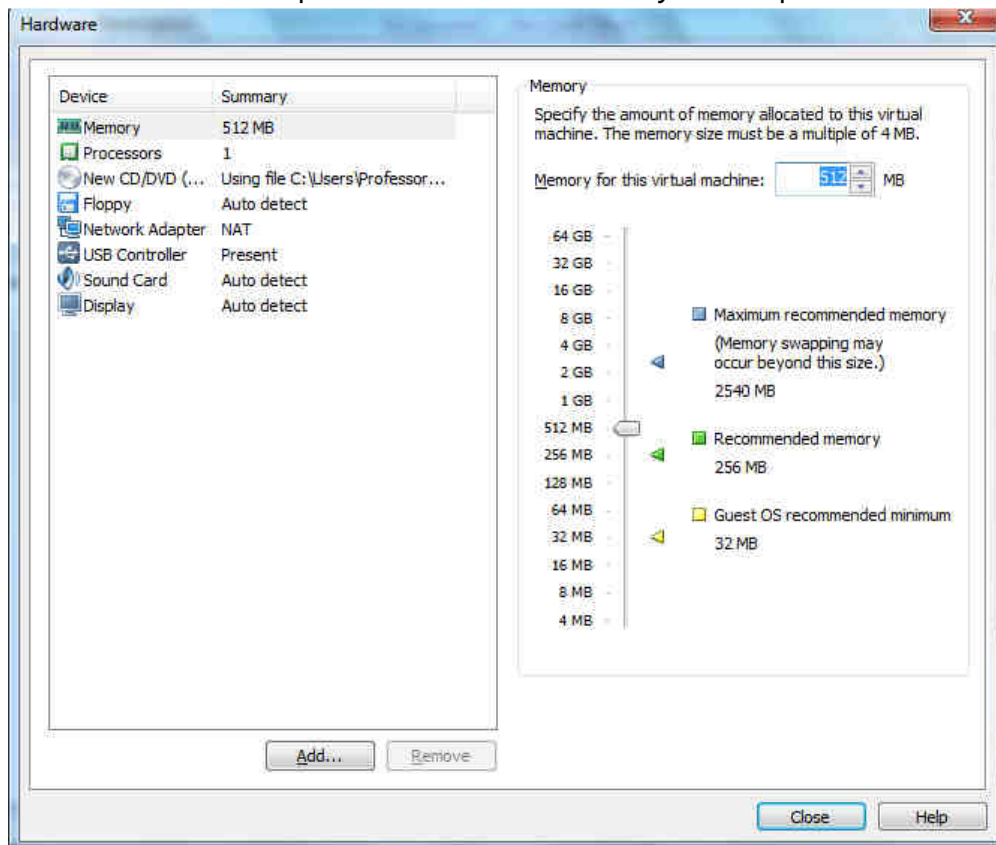
8- Aqui se escolhe o tamanho do HD da maquina virtual. Como não é necessário muito espaço para a instalação do sistema operacional, destinamos apenas 20GB. Deixe a opção *Store virtual disk as a single file* marcada e clique em *Next*.



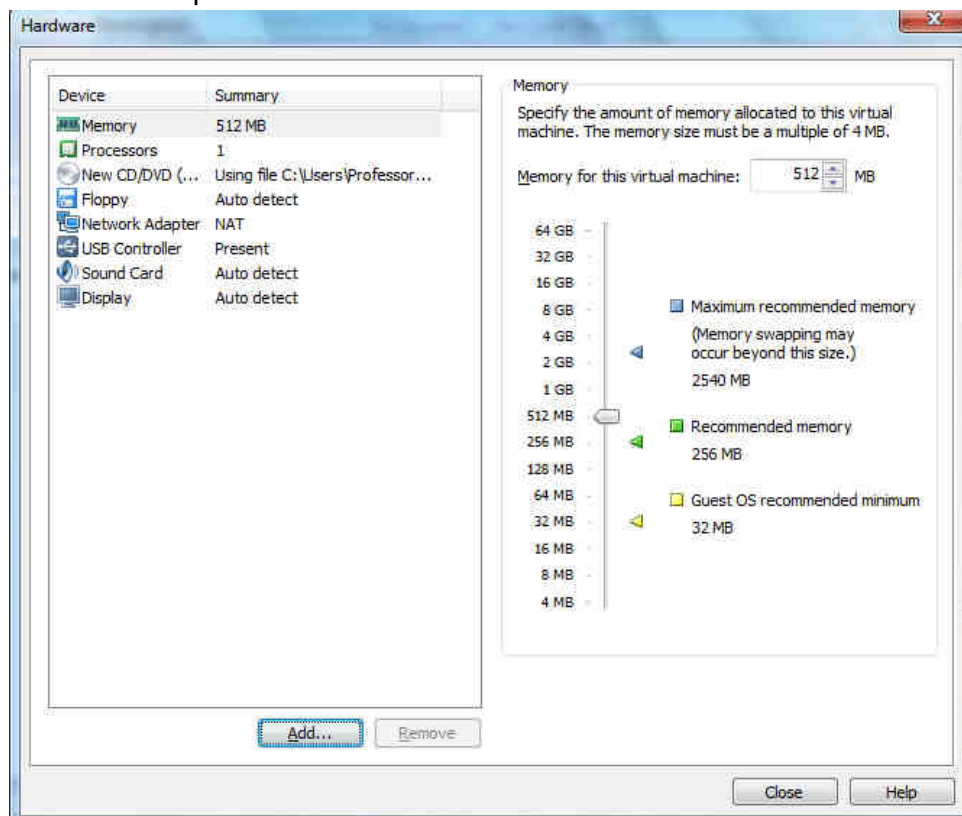
9- Na próxima janela clique em *Customize Hardware*



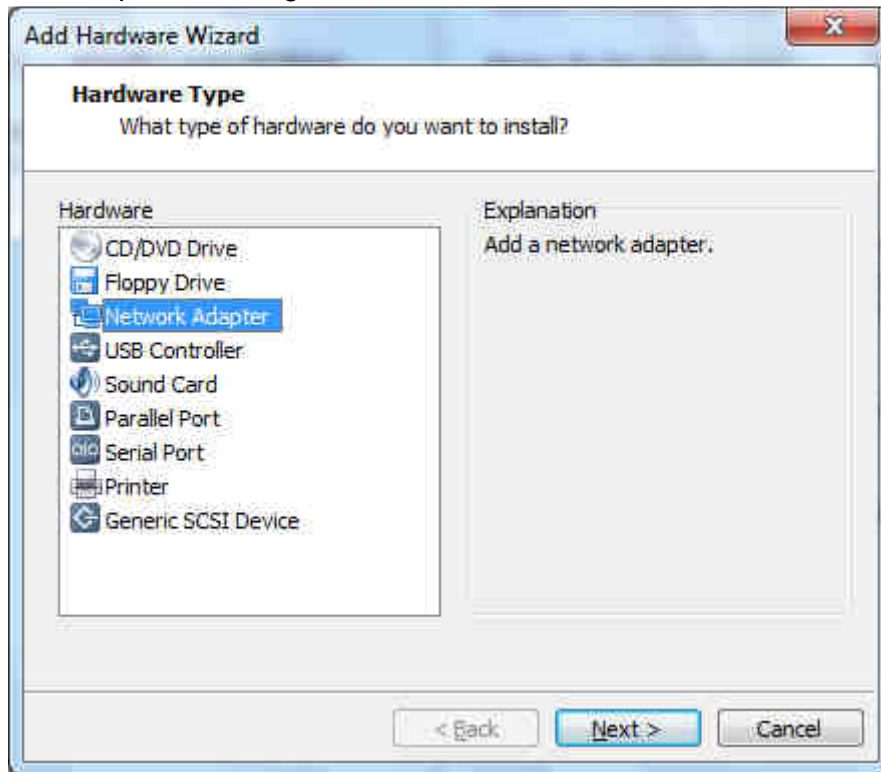
10-Aumente a memória RAM da Máquina virtual: Na aba *Memory* deslize para 512MB



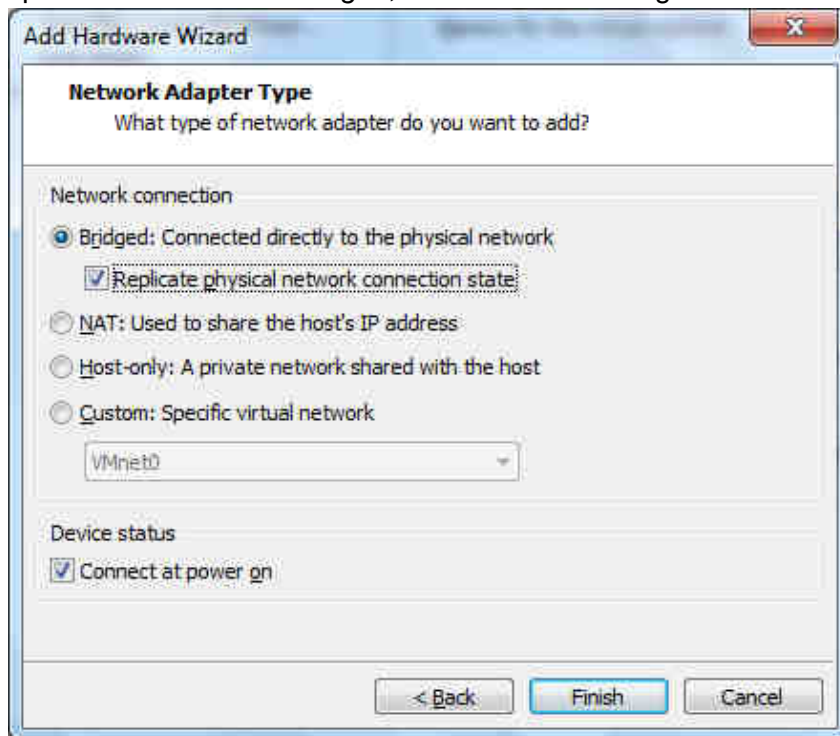
11- Agora adicione mais uma placa de rede clicando em *Add*



12- Clique em *Network Adapter* e em seguida em *Next*

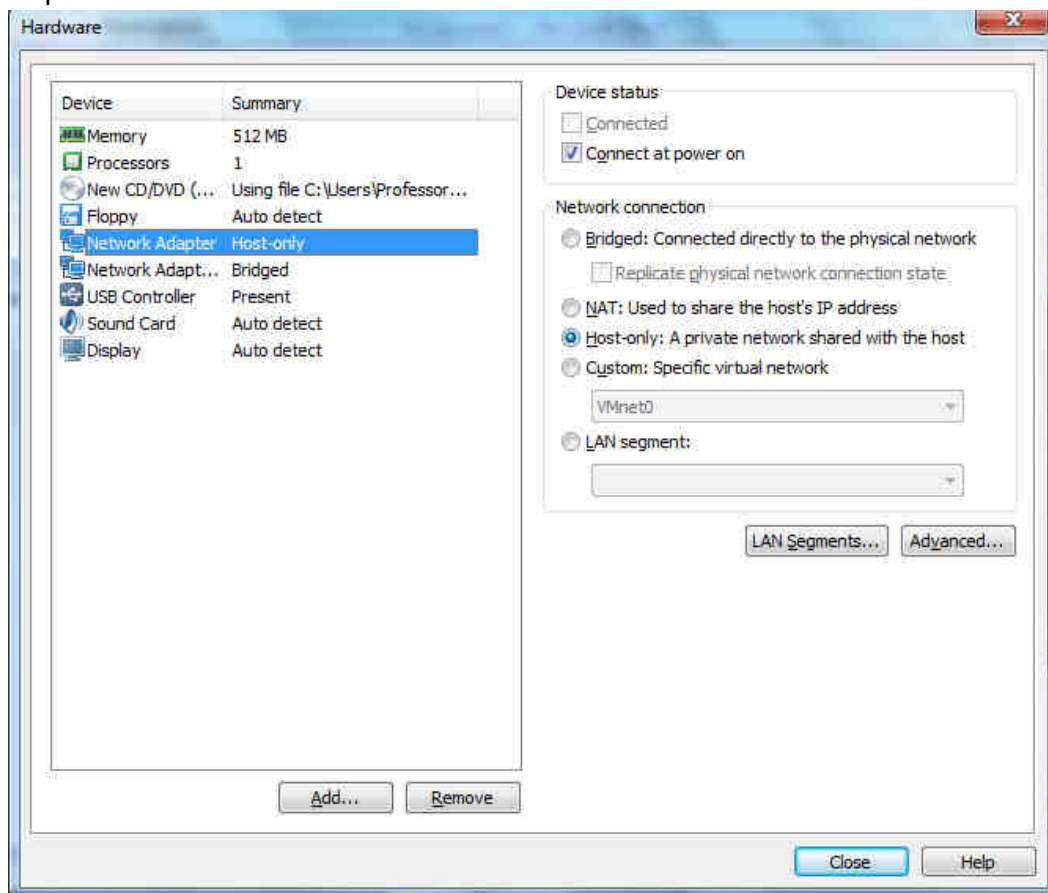


13- Configure a nova placa de rede como *Bridged*, como mostra a imagem abaixo:

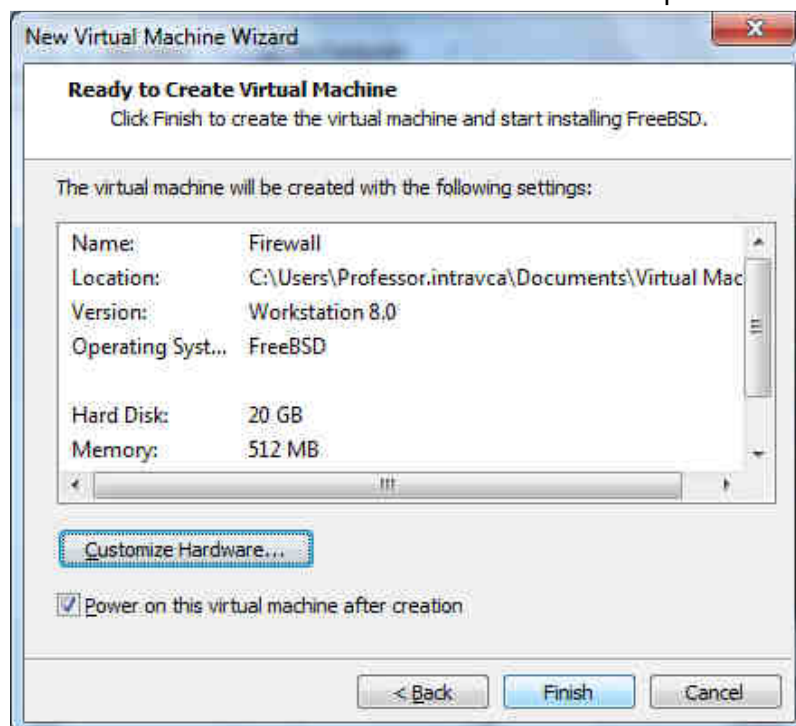


14- Agora a maquina virtual possui 2 placas de rede, a recém-criada e configurada como Bridged e a que já existia por padrão do pfSense. Dê um clique na placa que já existia e configure-a como *Host Only* como mostra a imagem abaixo:

Em seguida clique em *Close*

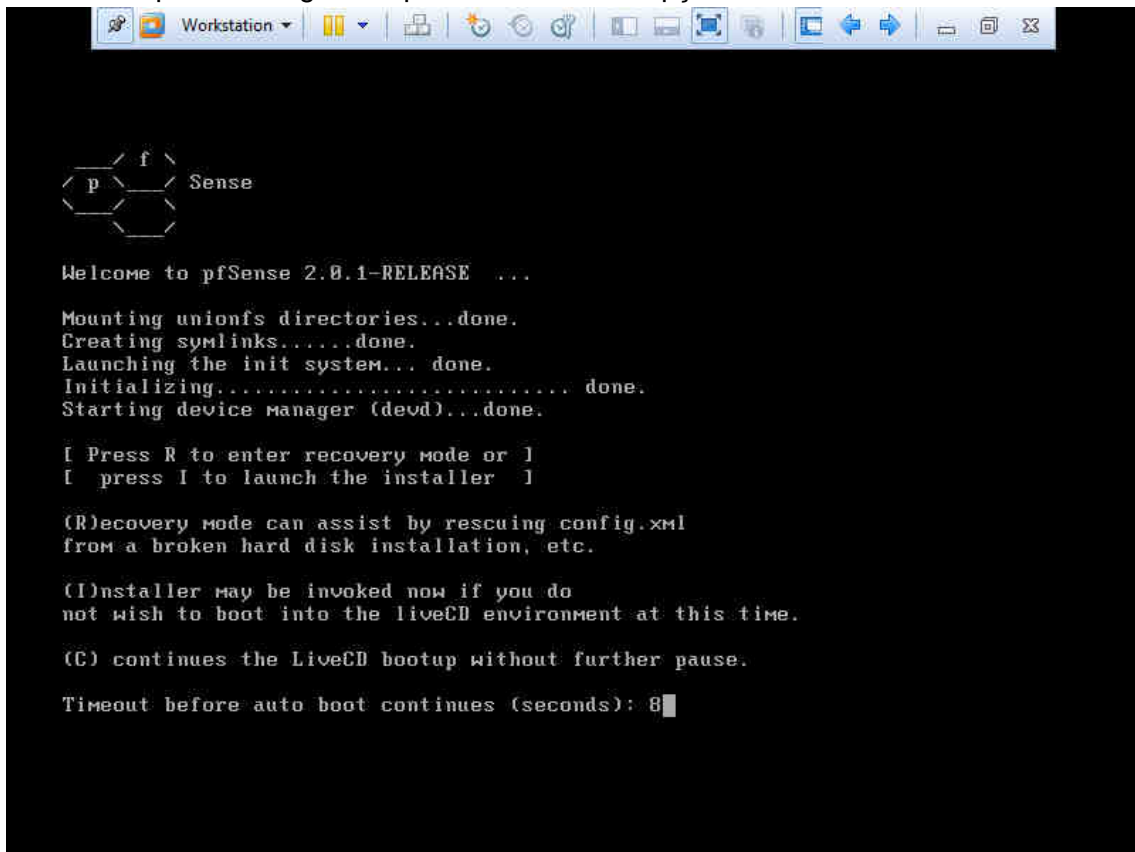


15- Mantenha a opção *Power on this virtual machine after create* one clique em *Finish*

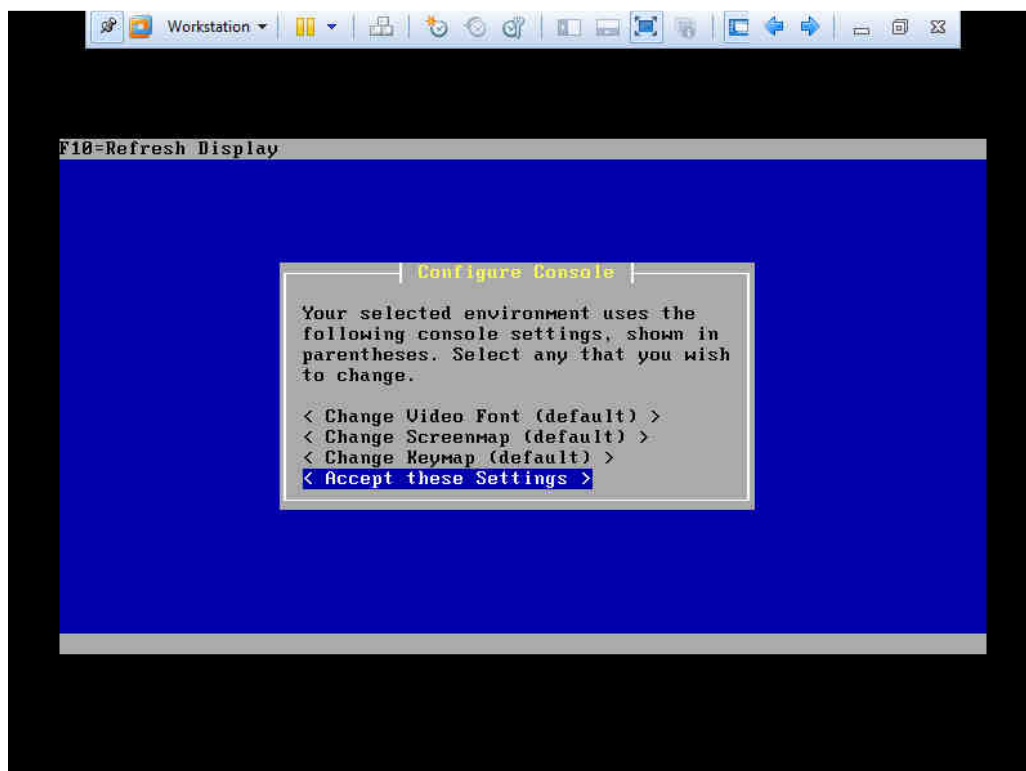


Instalação

16- A maquina virtual será iniciada. Essa é a tela inicial de instalação do PfSense, para instalar digite " i" .
Atenção: Você tem apenas 8 segundos para escolher sua opção.

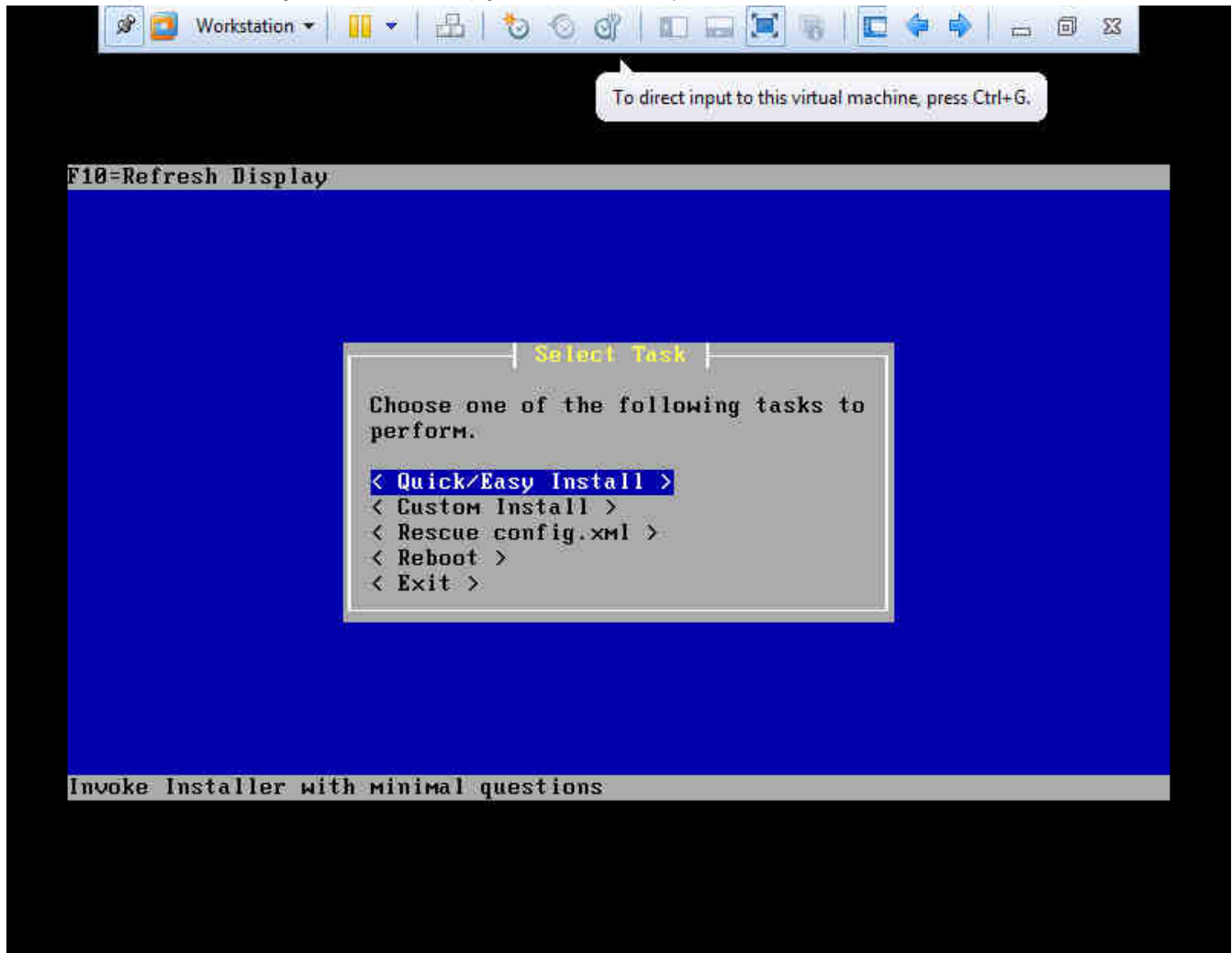


17- Neste campo escolha a opção Accept these settings para aceitar as configurações padrões. Porque agente não quer mudar o vídeo nem o teclado.



17- Após isso escolha uma das opções abaixo para instalar o Pfsense. A primeira opção "Quick/Easy Install", instala de maneira fácil e rápida. A opção "Custom Install" instala de maneira personalizada, "Rescue config. xml" recupera as configurações de uma outra instalação. "Reboot" reinicia, "Exit" sai da tela de configuração.

Para esse tipo de instalação escolha a opção: 'Quick/Easy Install'.

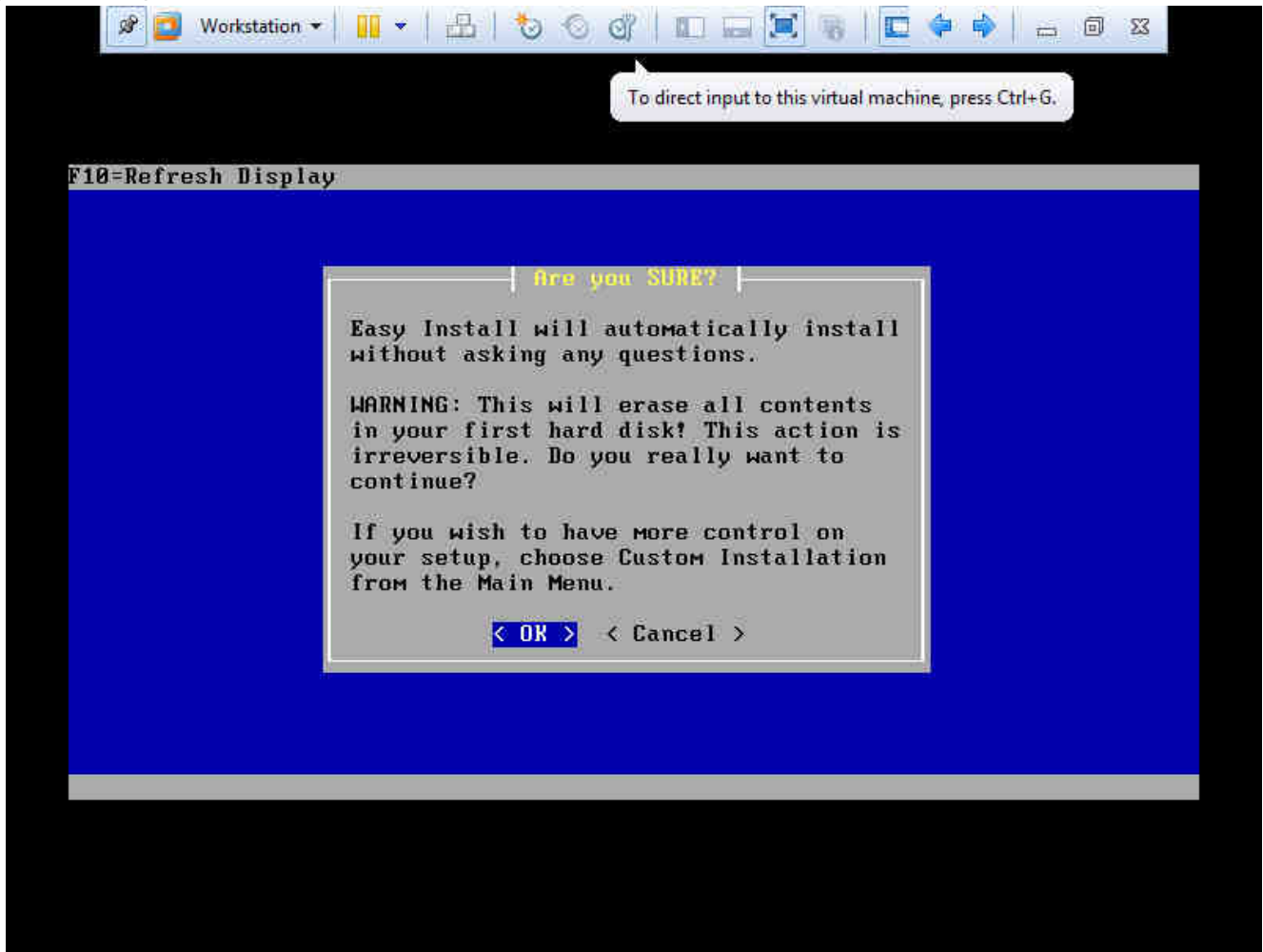


18- Em seguida, aparece uma tela de confirmação com a seguinte mensagem:

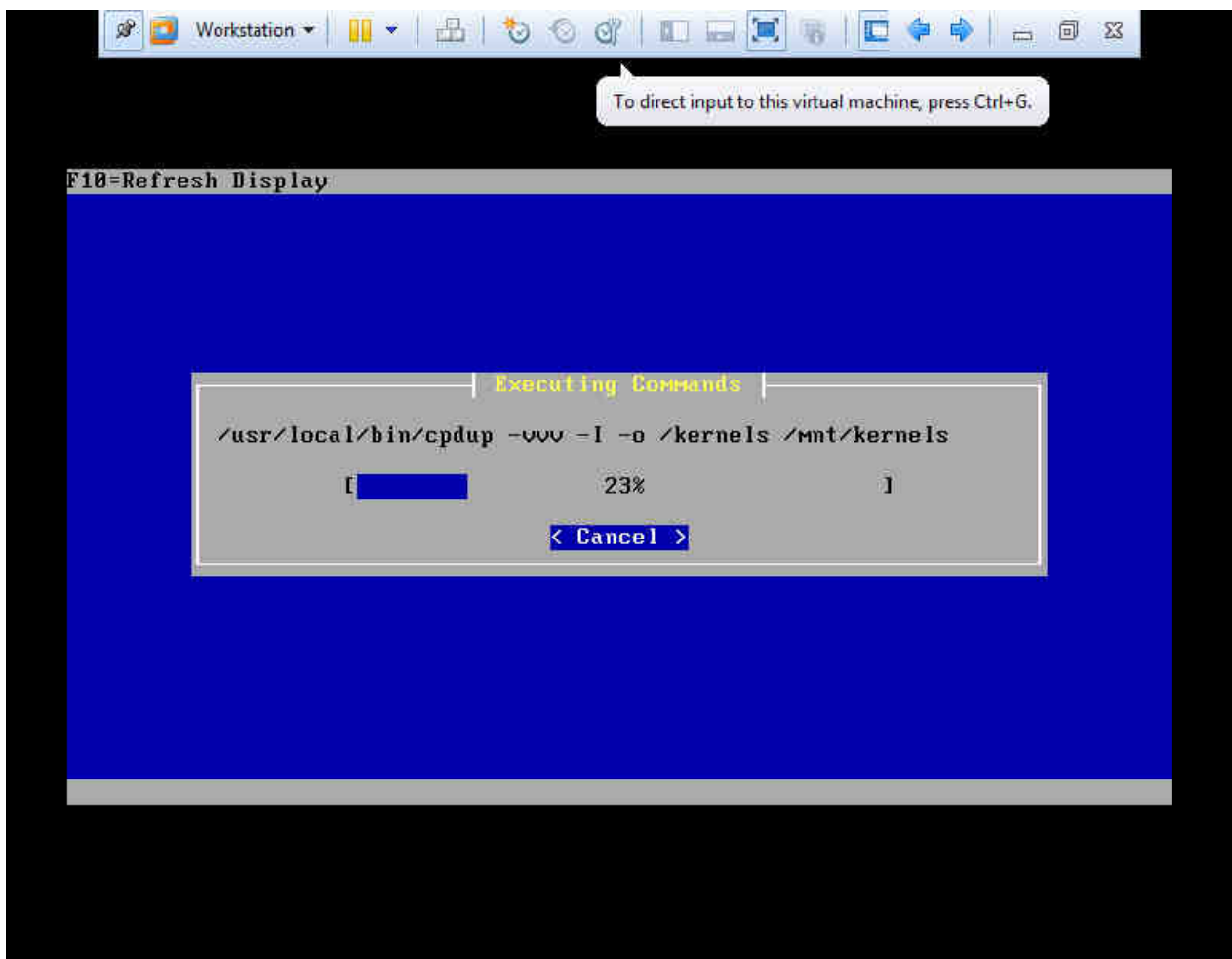
Aviso: Esta instalação irá apagar todo o conteúdo em seu disco rígido! Esta ação é irreversível, tem certeza que deseja continuar?

Caso a instalação seja pelo Vmware não apagará as informações em seu HD. Mas se a instalação for na máquina real, certifique-se de fazer um backup dos seus arquivos.

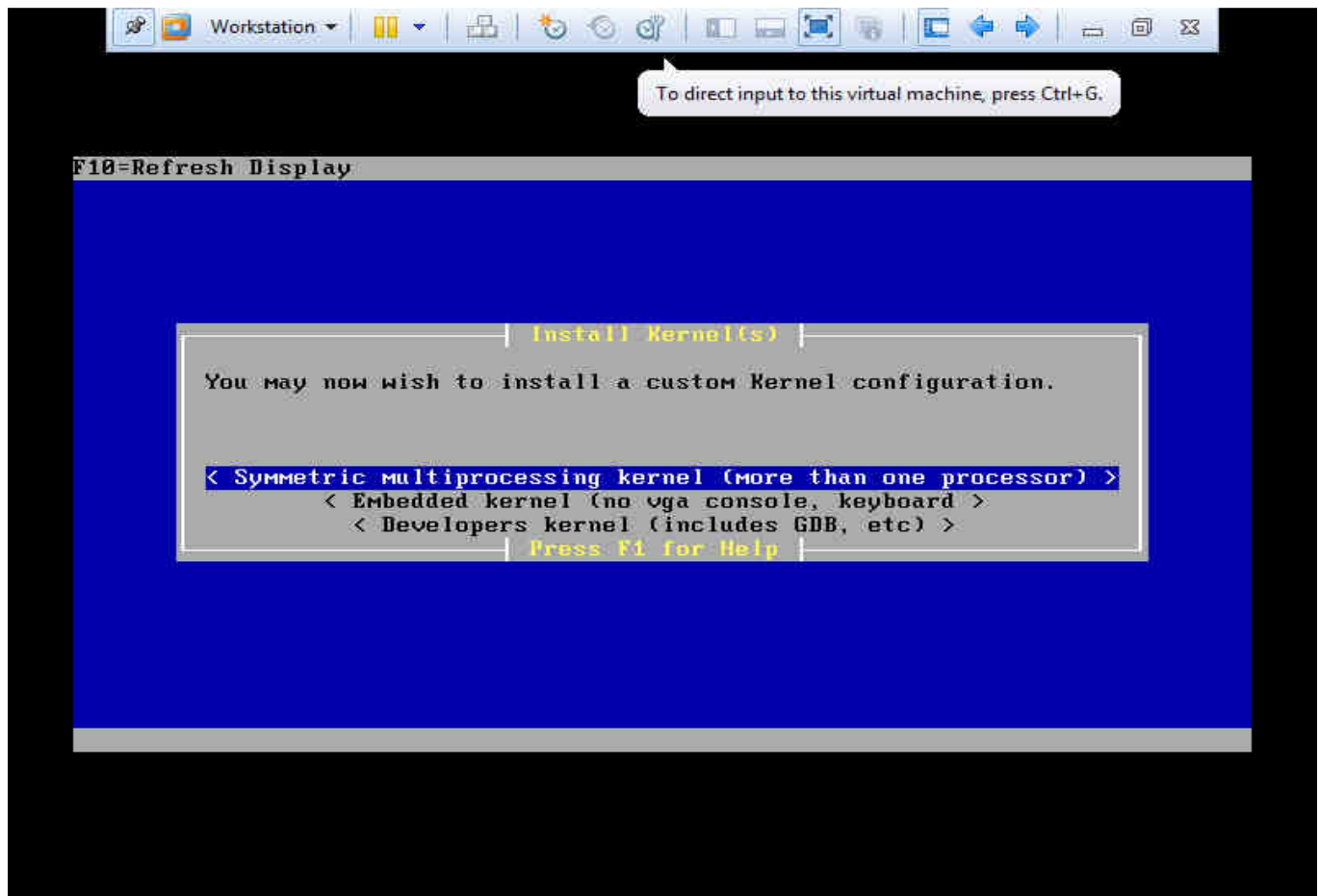
Após isso clique em "OK".



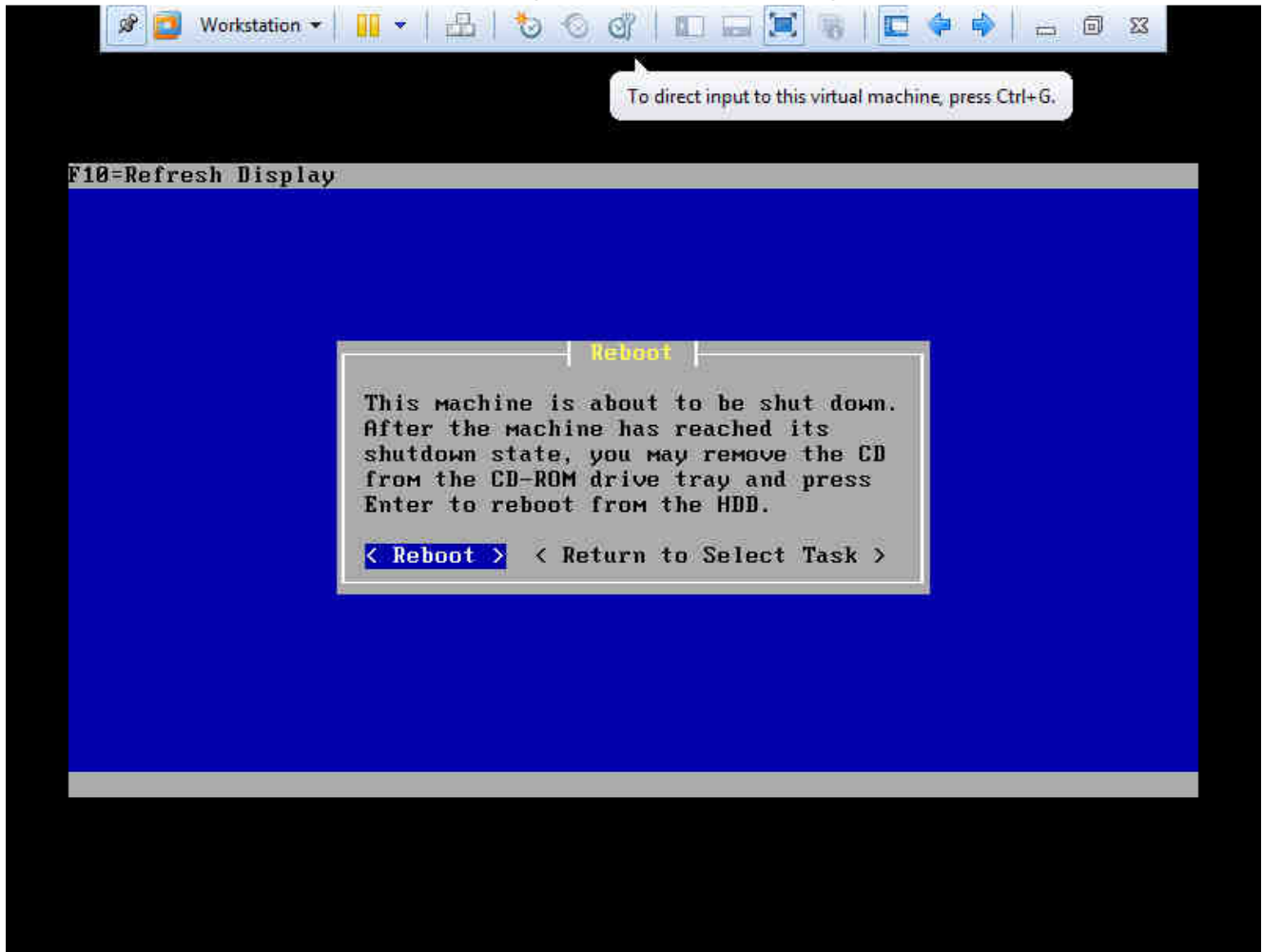
19- Em seguida aguarde o término da instalação.



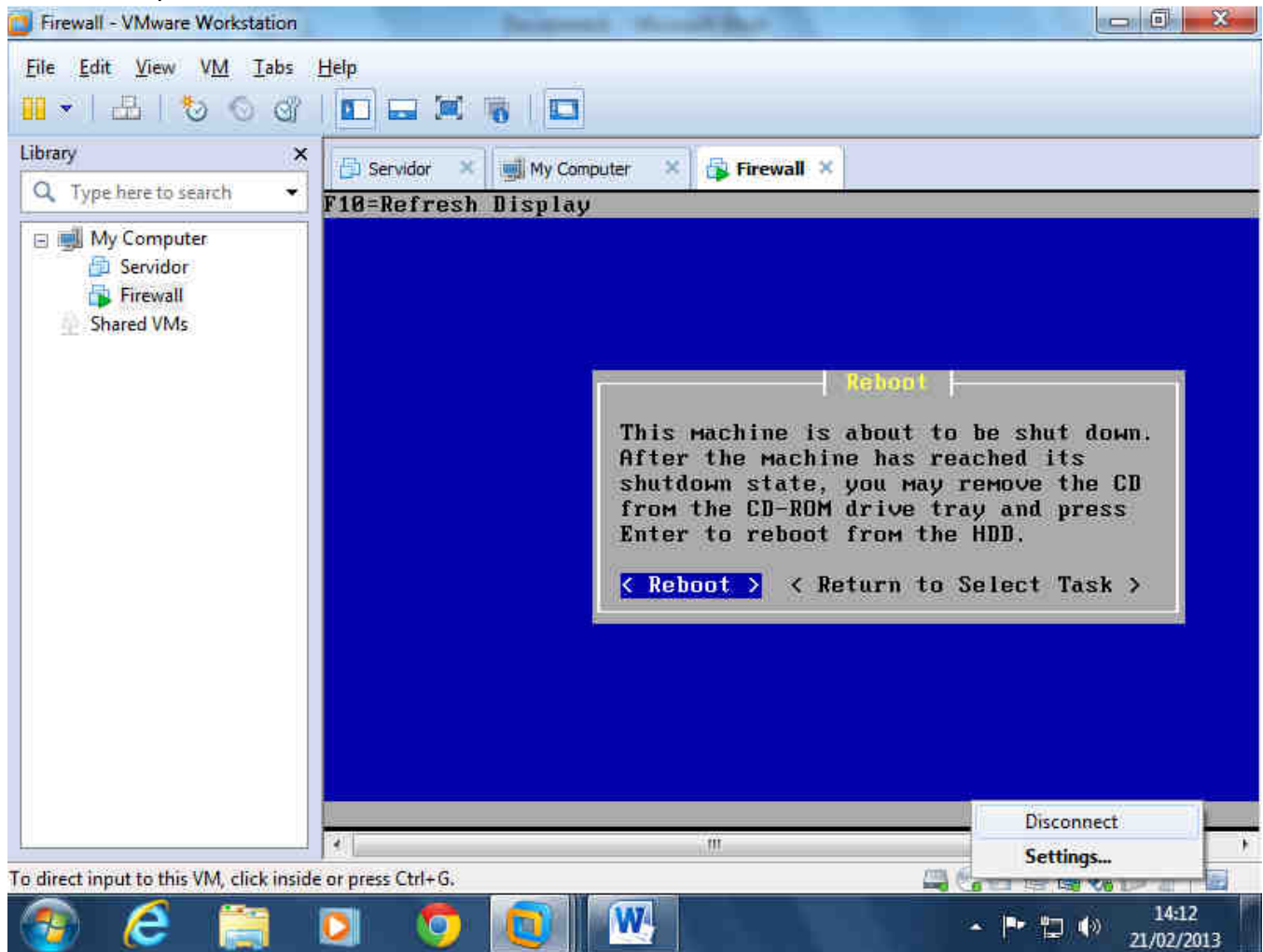
20- Na tela de Install Kernel(s) selecione: "Symmetric multiprocessing kernel (more than one processor)" pressione: "Enter". A segunda opção serve para instalar o kernel do sistema operacional em dispositivos que não possuem saída de vídeo ou entrada para teclado. A terceira opção é para desenvolvedores que desejam fazer alterações no código.



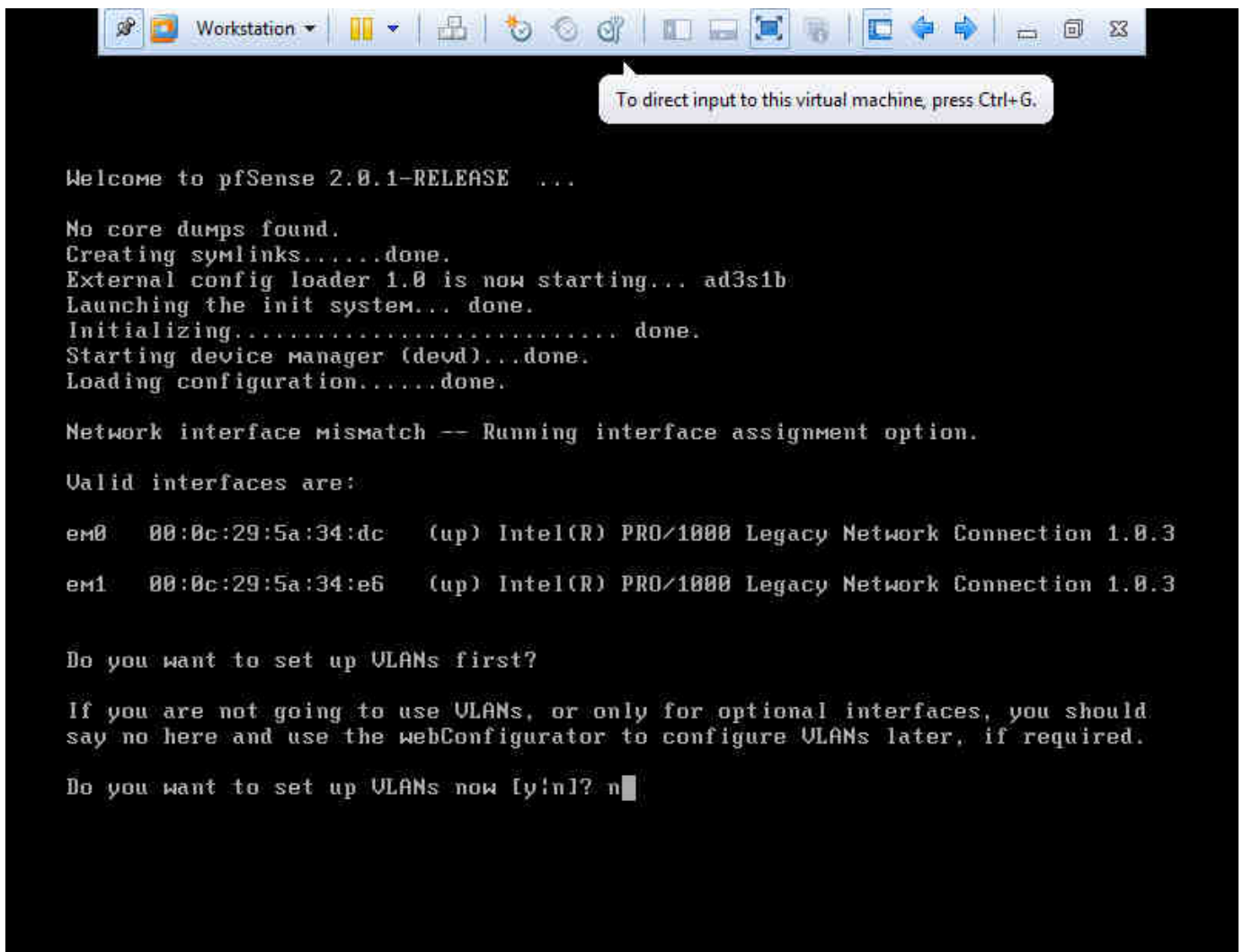
21- Na tela abaixo avisa que sua máquina vai reiniciar, mas antes você terá que retirar o cd e depois clicar em Reboot. Como estamos instalando pelo Vmware, teremos que desconectar virtualmente.



22- Para isso clique no cd, no rodapé do VMware e clique em desconectar. Em seguida volte a tela do VMware e clique em “Reboot”.



23- Essa é a tela inicial de configuração do PfSense. Nessa tela mostra as placas de rede instaladas, sendo elas (em0 e em1). E faz a seguinte pergunta ao usuário:“Você gostaria de configurar as redes virtuais locais agora?” (y;n). Nesse caso, digitaremos “n”.



```
Workstation
To direct input to this virtual machine, press Ctrl+G.

Welcome to pfSense 2.0.1-RELEASE ...

No core dumps found.
Creating symlinks.....done.
External config loader 1.0 is now starting... ad3s1b
Launching the init system... done.
Initializing..... done.
Starting device manager (devd)...done.
Loading configuration.....done.

Network interface mismatch -- Running interface assignment option.

Valid interfaces are:

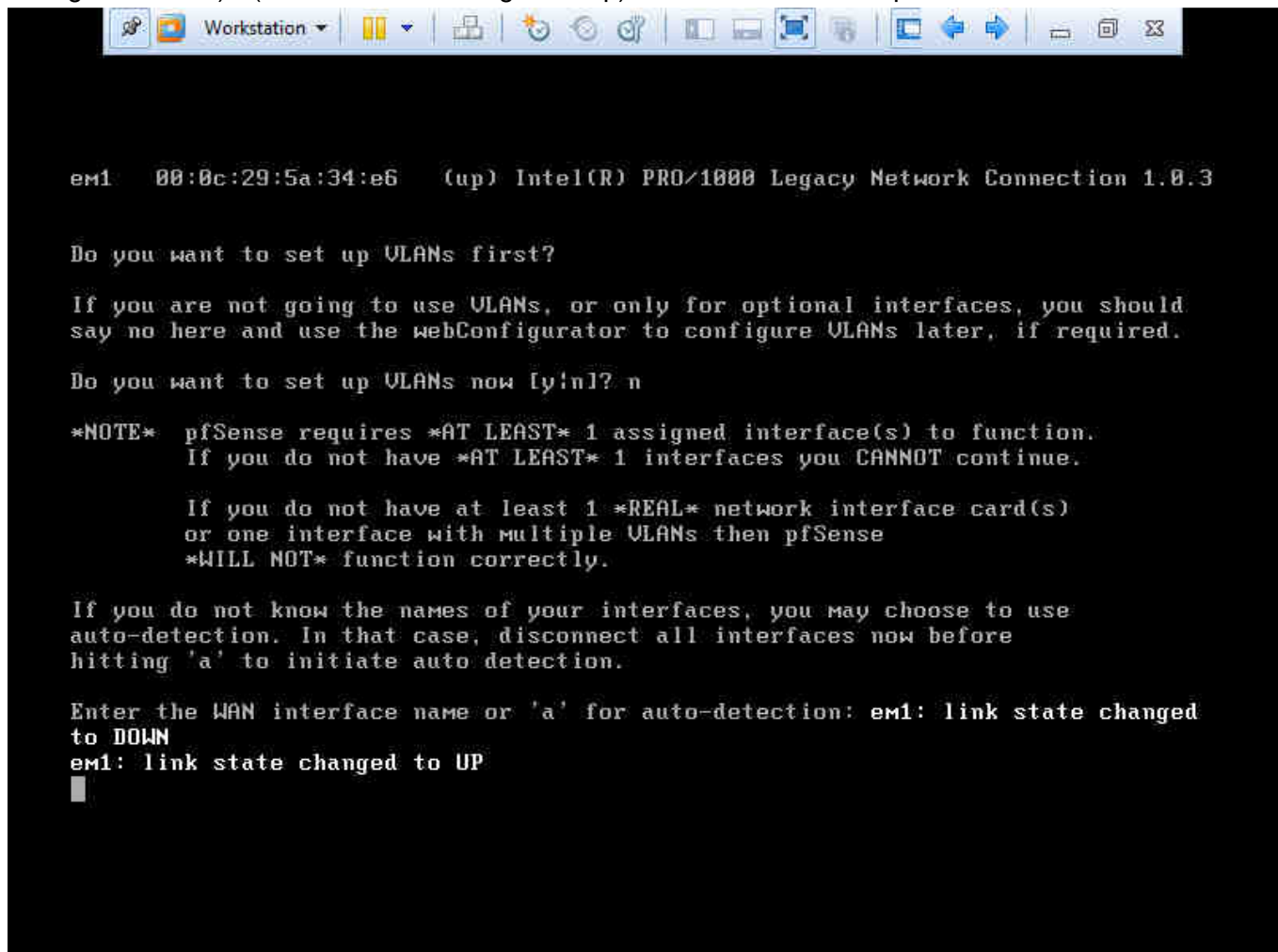
em0    00:0c:29:5a:34:dc    (up) Intel(R) PRO/1000 Legacy Network Connection 1.0.3
em1    00:0c:29:5a:34:e6    (up) Intel(R) PRO/1000 Legacy Network Connection 1.0.3

Do you want to set up VLANs first?

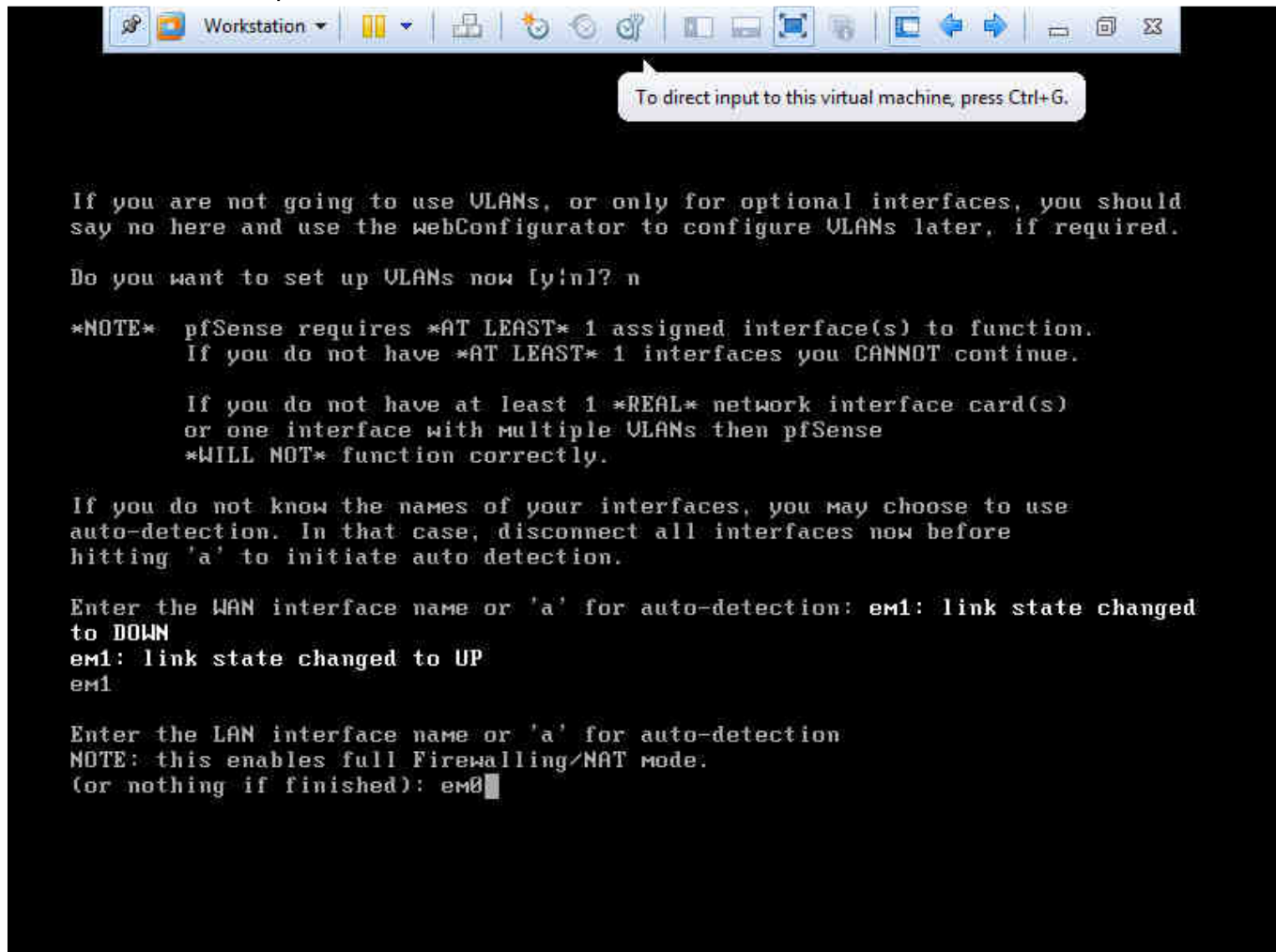
If you are not going to use VLANs, or only for optional interfaces, you should
say no here and use the webConfigurator to configure VLANs later, if required.

Do you want to set up VLANs now [y;n]? n
```

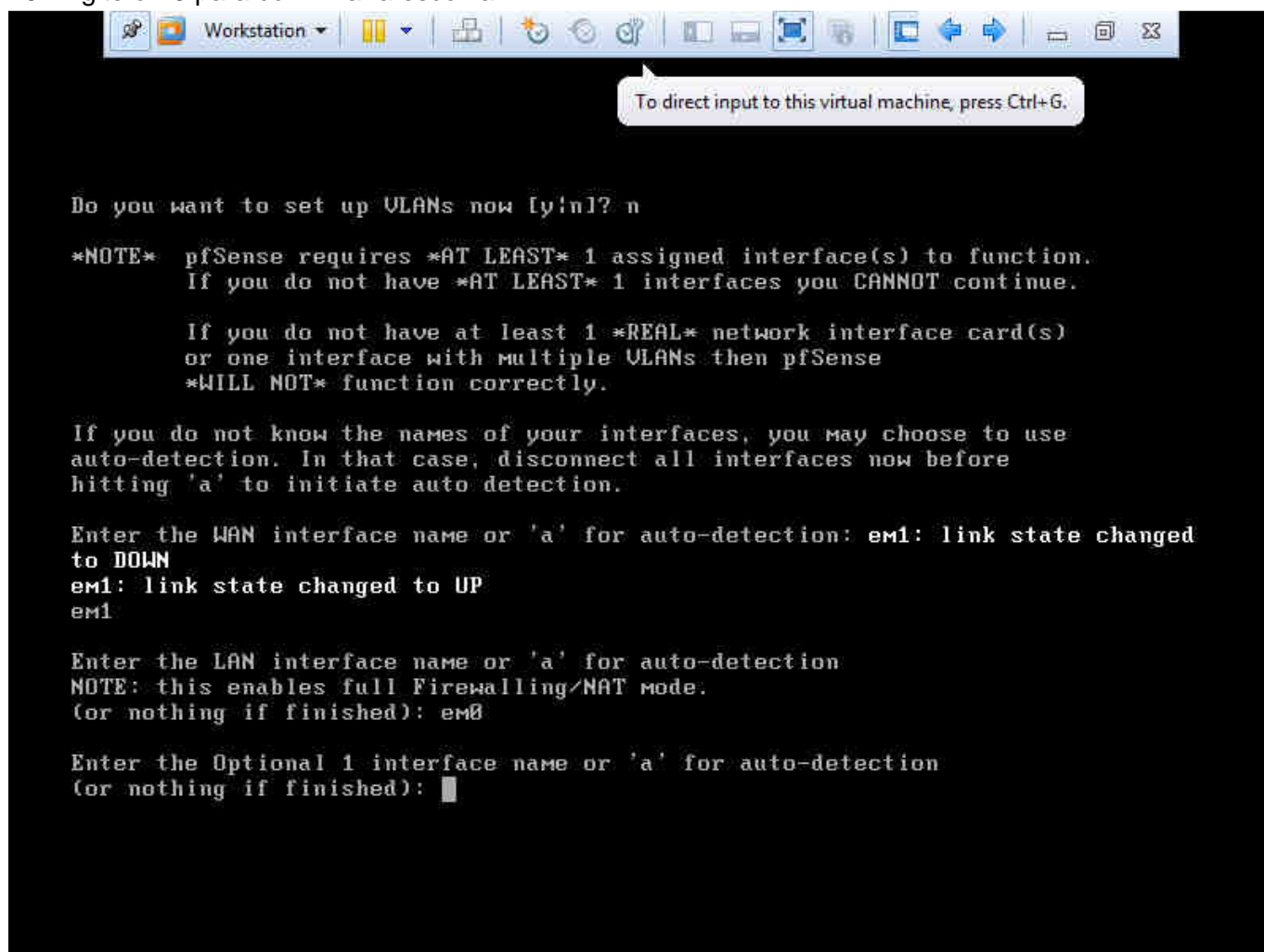
24- Em seguida vamos desconectar o cabo da conexão com a internet e conectar para identificar a WAN. Para isso clique no rodapé do Vmware com o botão direito no ícone de rede da bridge. E clique em “desconectar” e logo em seguida “conectar”. Vai aparecer a seguinte mensagem na tela: - (em1: link state changed to down) - (em1:link state changed to Up). Neste nosso caso a placa WAN é **em1**.



25- Pronto, já identificamos quem é a nossa placa WAN, digite **em1** na tela para confirmar. Como só temos duas placas a outra será a LAN. Neste caso **em0**.



26- Digite **em0** para confirmar a escolha.

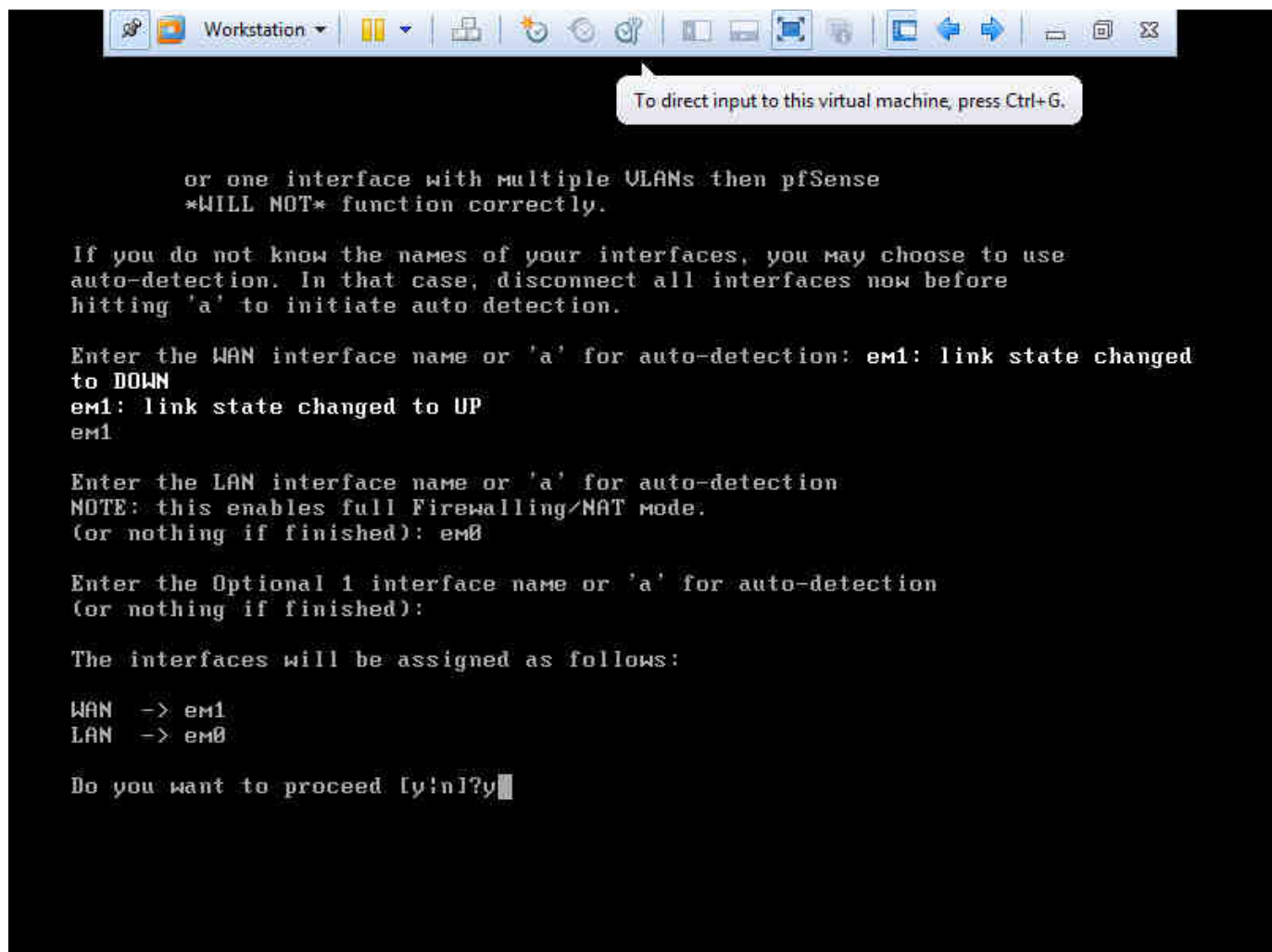


27- Em seguida irá aparecer na tela as configurações das placas. Sendo elas:

Wan -> em1

LAN-> em0

Depois aparece uma mensagem de confirmação, digite "y" , caso suas placas estejam configuradas corretamente.



```
or one interface with multiple VLANs then pfSense
*WILL NOT* function correctly.

If you do not know the names of your interfaces, you may choose to use
auto-detection. In that case, disconnect all interfaces now before
hitting 'a' to initiate auto detection.

Enter the WAN interface name or 'a' for auto-detection: em1: link state changed
to DOWN
em1: link state changed to UP
em1

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(or nothing if finished): em0

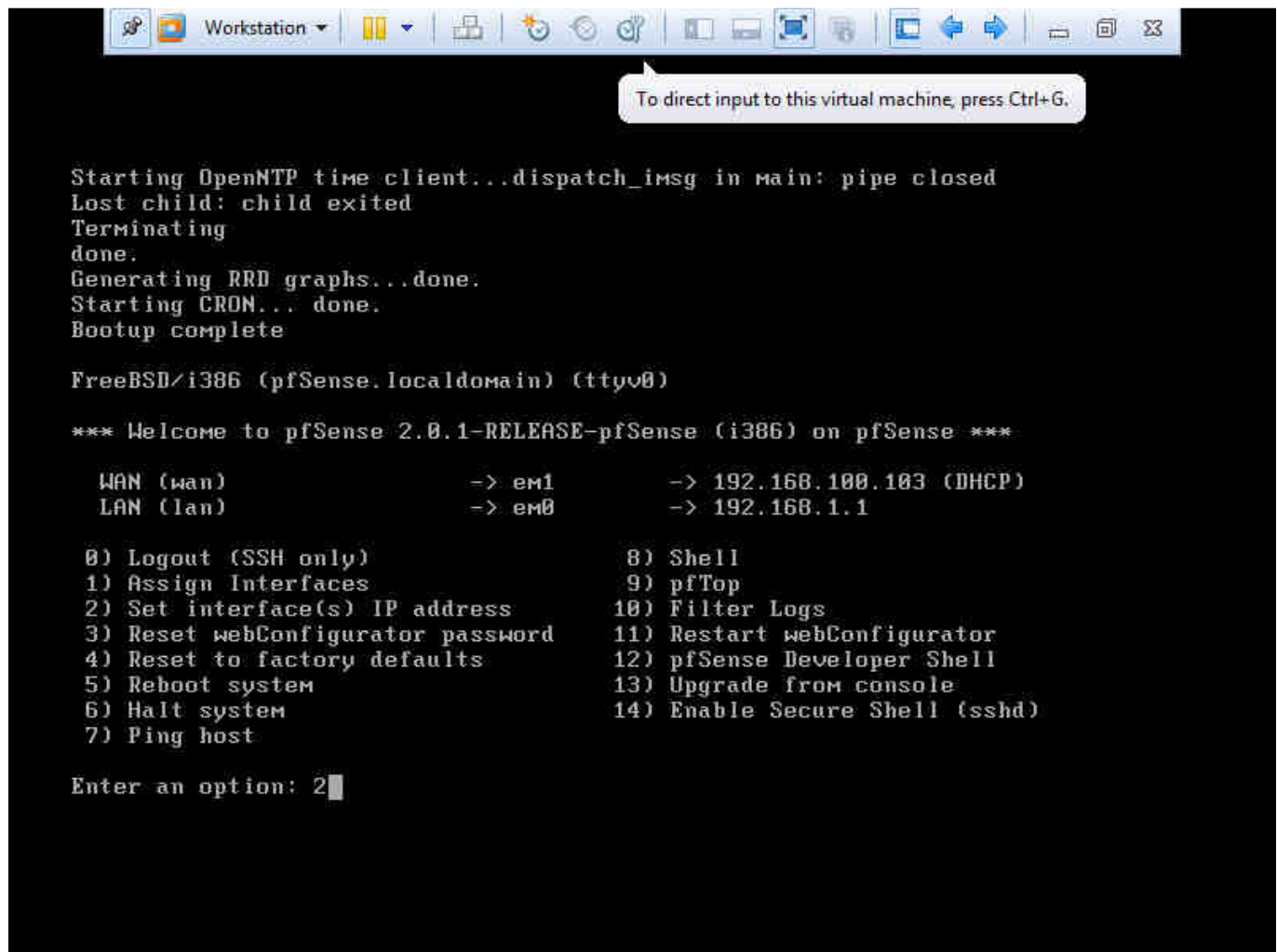
Enter the Optional 1 interface name or 'a' for auto-detection
(or nothing if finished):

The interfaces will be assigned as follows:

WAN -> em1
LAN -> em0

Do you want to proceed [y:n]?y
```

28- Nessa tela iremos alterar o endereço Ip da Lan. Digite sua opção. Nesse caso é "2".



```
Starting OpenNTP time client...dispatch_imsg in main: pipe closed
Lost child: child exited
Terminating
done.
Generating RRD graphs...done.
Starting CRON... done.
Bootup complete

FreeBSD/i386 (pfSense.localdomain) (ttyv0)

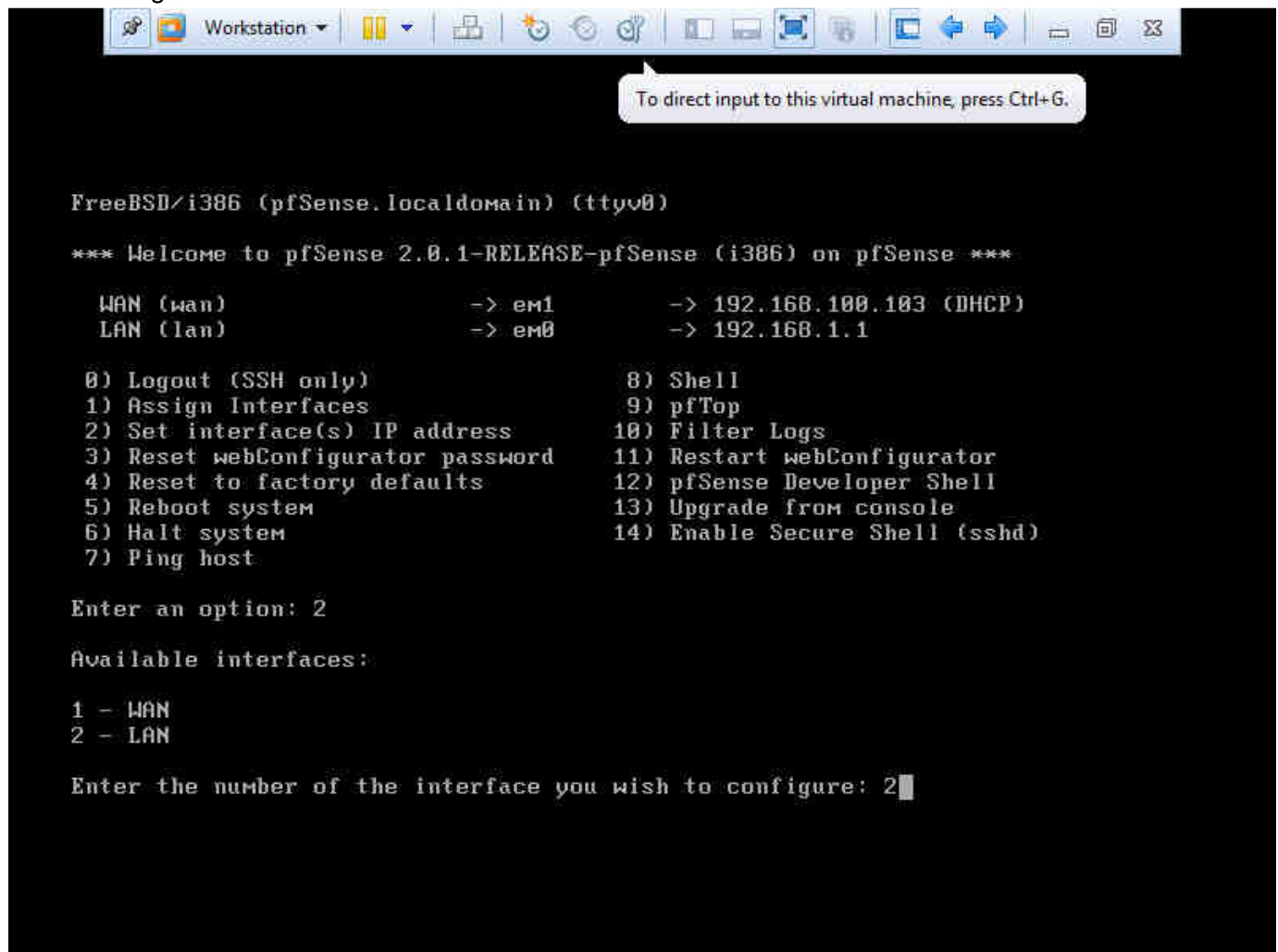
*** Welcome to pfSense 2.0.1-RELEASE-pfSense (i386) on pfSense ***

WAN (wan)          -> em1          -> 192.168.100.103 (DHCP)
LAN (lan)           -> em0          -> 192.168.1.1

0) Logout (SSH only)      8) Shell
1) Assign Interfaces      9) pfTop
2) Set interface(s) IP address 10) Filter Logs
3) Reset webConfigurator password 11) Restart webConfigurator
4) Reset to factory defaults 12) pfSense Developer Shell
5) Reboot system         13) Upgrade from console
6) Halt system           14) Enable Secure Shell (sshd)
7) Ping host

Enter an option: 2
```

29- Como iremos alterar o ip da Lan, digite o número “2” novamente, caso fosse da WAN seria “1”, como mostra a seguir:



The screenshot shows a virtual machine window titled "Workstation" with a toolbar at the top. A tooltip above the console area reads: "To direct input to this virtual machine, press Ctrl+G." The console output is as follows:

```
FreeBSD/i386 (pfSense.localdomain) (ttyv0)

*** Welcome to pfSense 2.0.1-RELEASE-pfSense (i386) on pfSense ***

WAN (wan)          -> em1          -> 192.168.100.103 (DHCP)
LAN (lan)           -> em0          -> 192.168.1.1

0) Logout (SSH only)      8) Shell
1) Assign Interfaces      9) pfTop
2) Set interface(s) IP address 10) Filter Logs
3) Reset webConfigurator password 11) Restart webConfigurator
4) Reset to factory defaults 12) pfSense Developer Shell
5) Reboot system          13) Upgrade from console
6) Halt system            14) Enable Secure Shell (sshd)
7) Ping host

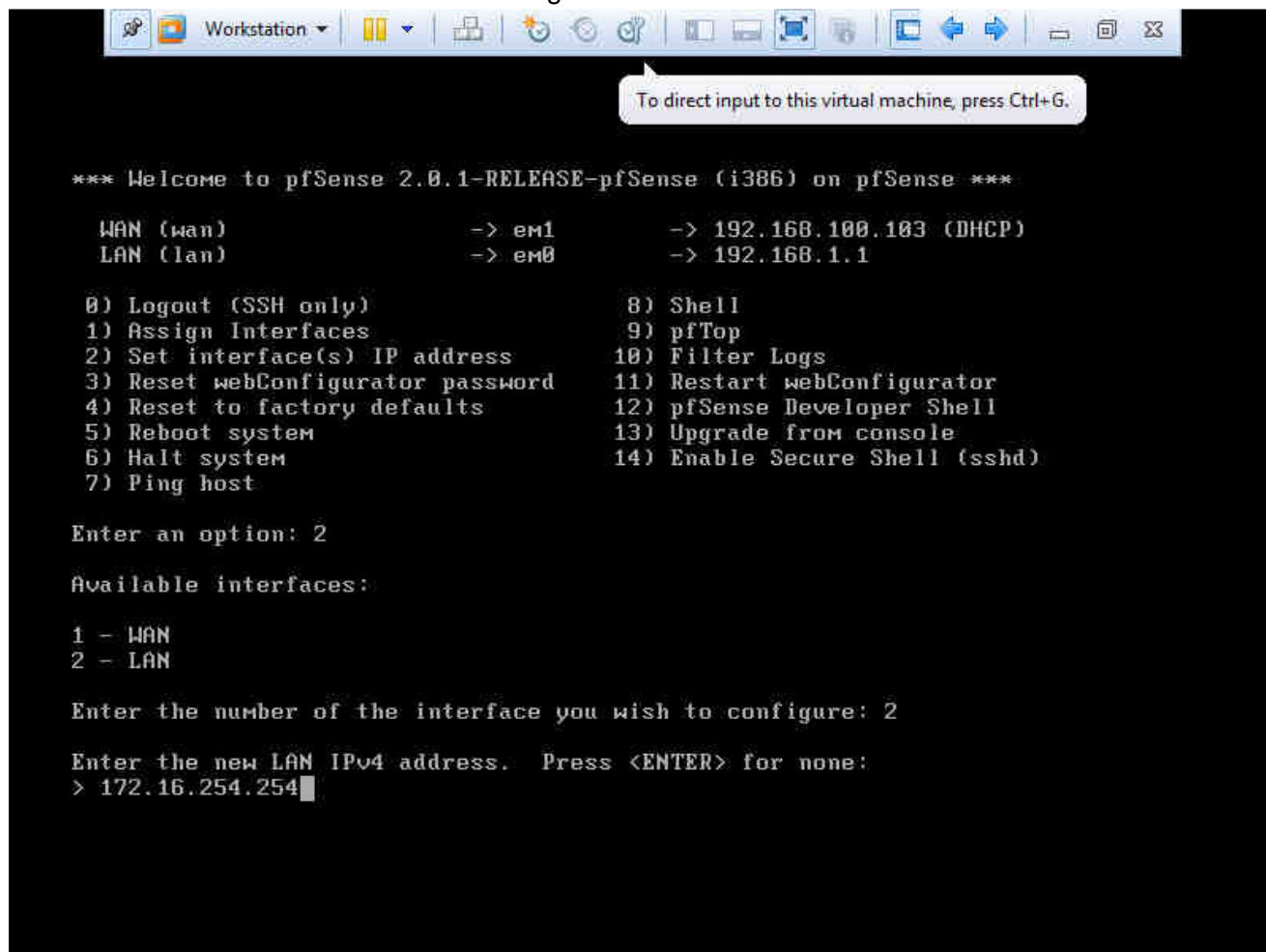
Enter an option: 2

Available interfaces:

1 - WAN
2 - LAN

Enter the number of the interface you wish to configure: 2
```

30- Agora iremos digitar o ip desejado para nossa LAN. Nesse caso usaremos o seguinte Ip: "172.16.254.254". Pressione "Enter" em seguida.



```
*** Welcome to pfSense 2.0.1-RELEASE-pfSense (i386) on pfSense ***

WAN (wan)          -> em1          -> 192.168.100.103 (DHCP)
LAN (lan)           -> em0          -> 192.168.1.1

0) Logout (SSH only)      8) Shell
1) Assign Interfaces      9) pfTop
2) Set interface(s) IP address 10) Filter Logs
3) Reset webConfigurator password 11) Restart webConfigurator
4) Reset to factory defaults 12) pfSense Developer Shell
5) Reboot system         13) Upgrade from console
6) Halt system           14) Enable Secure Shell (sshd)
7) Ping host

Enter an option: 2

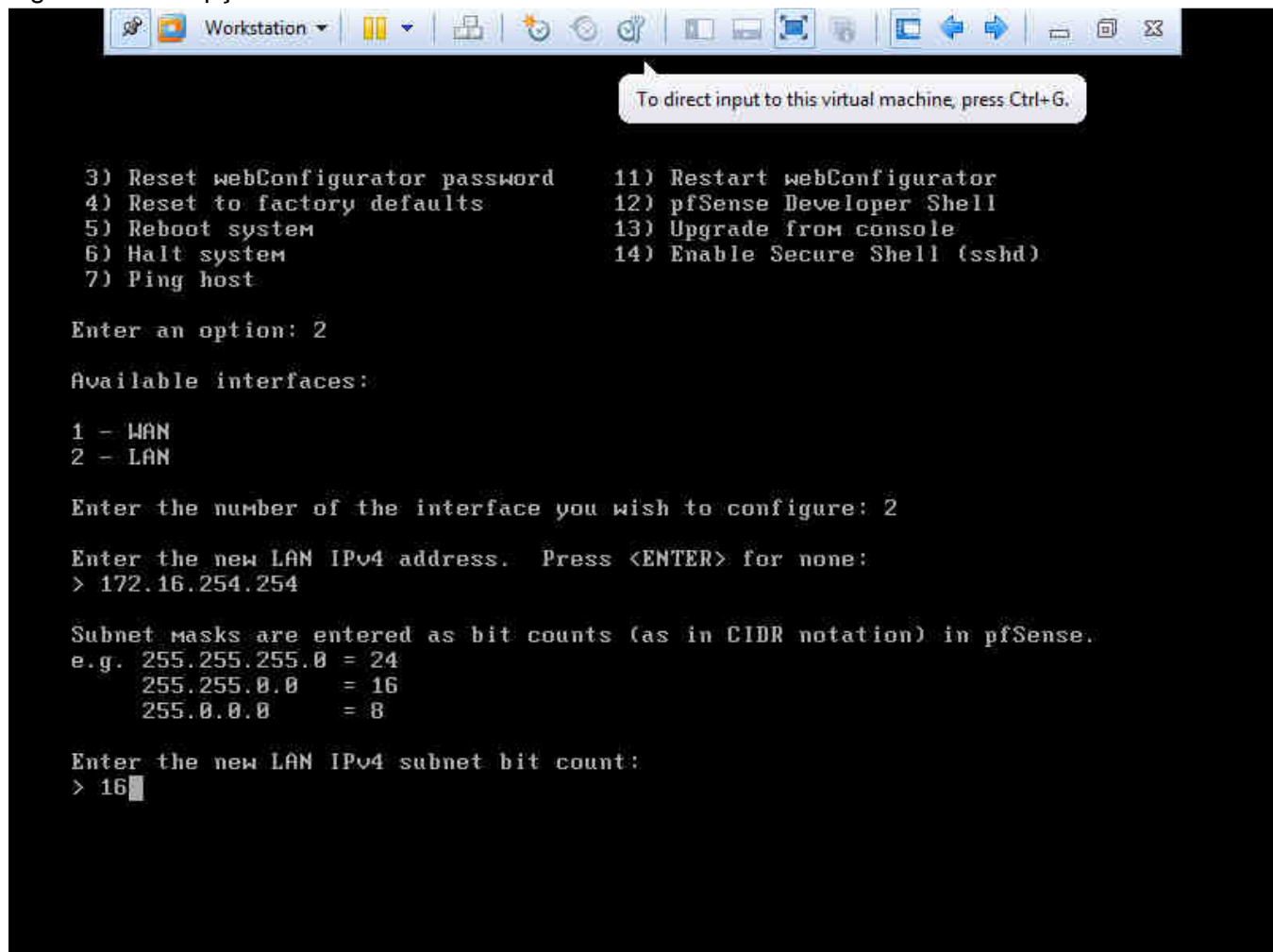
Available interfaces:

1 - WAN
2 - LAN

Enter the number of the interface you wish to configure: 2

Enter the new LAN IPv4 address. Press <ENTER> for none:
> 172.16.254.254
```

31- Agora iremos escolher qual a máscara. Nesse caso será "16" (Por padrão). Mas dependendo do ip digitado há as opções "24" e "8".



The screenshot shows a virtual machine window titled "Workstation" with a toolbar at the top. A tooltip above the console area reads: "To direct input to this virtual machine, press Ctrl+G." The console itself has a black background with white text. It displays a menu with 14 options, numbered 3 to 14. The user has entered '2' for the interface selection. The next prompt asks for the new LAN IPv4 address, and the user has entered '172.16.254.254'. Below this, the console explains that subnet masks are entered as bit counts in CIDR notation, with examples: 255.255.255.0 = 24, 255.255.0.0 = 16, and 255.0.0.0 = 8. The final prompt asks for the new LAN IPv4 subnet bit count, and the user has entered '16'.

```
3) Reset webConfigurator password      11) Restart webConfigurator
4) Reset to factory defaults           12) pfSense Developer Shell
5) Reboot system                       13) Upgrade from console
6) Halt system                         14) Enable Secure Shell (sshd)
7) Ping host

Enter an option: 2

Available interfaces:

1 - WAN
2 - LAN

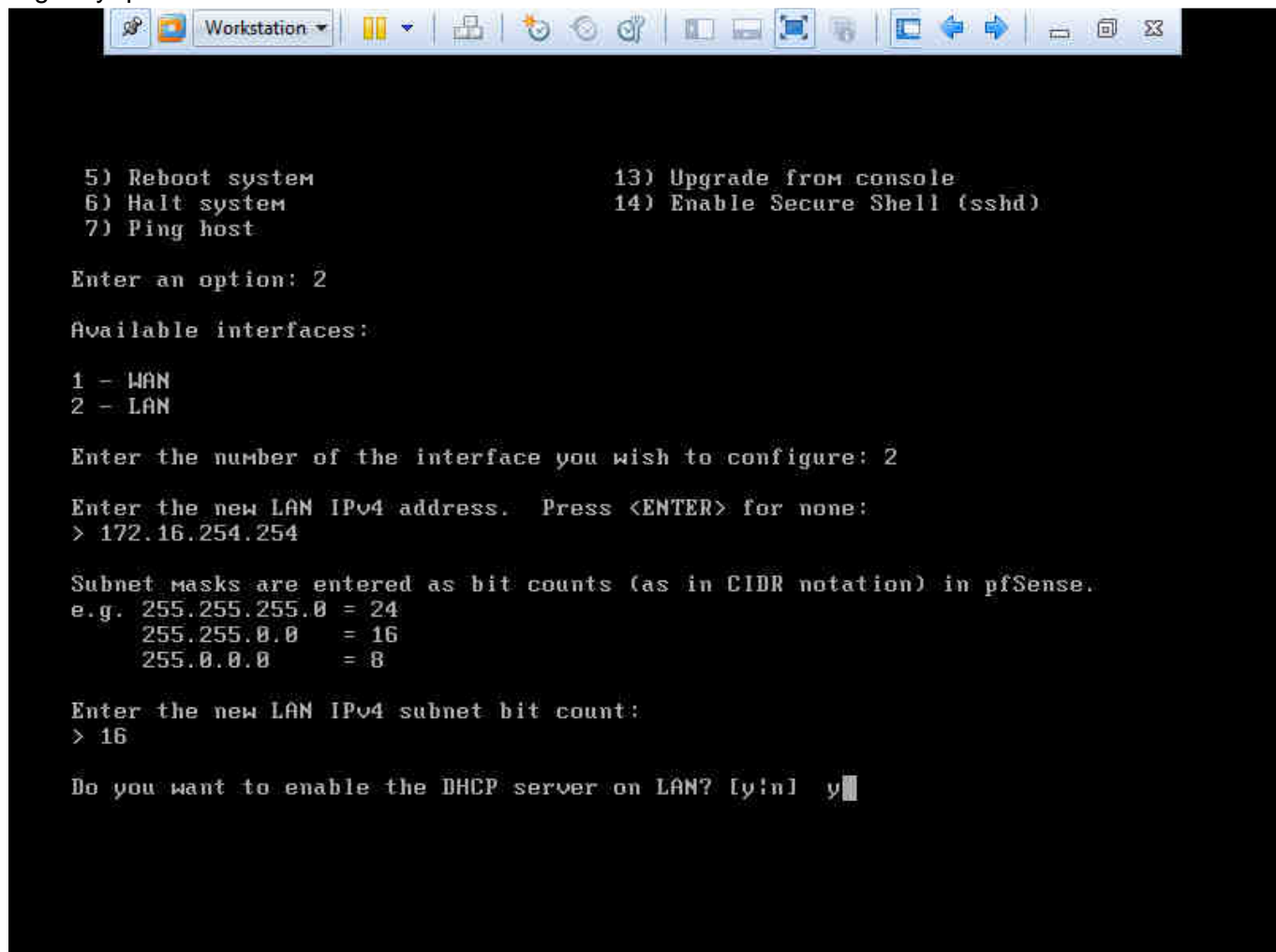
Enter the number of the interface you wish to configure: 2

Enter the new LAN IPv4 address. Press <ENTER> for none:
> 172.16.254.254

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count:
> 16
```

32- Logo em seguida aparecerá uma mensagem: "Você deseja permitir o servidor DHCP na LAN?". Digite "y" para confirmar.



```
Workstation: [Icons]

5) Reboot system
6) Halt system
7) Ping host

13) Upgrade from console
14) Enable Secure Shell (sshd)

Enter an option: 2

Available interfaces:

1 - WAN
2 - LAN

Enter the number of the interface you wish to configure: 2

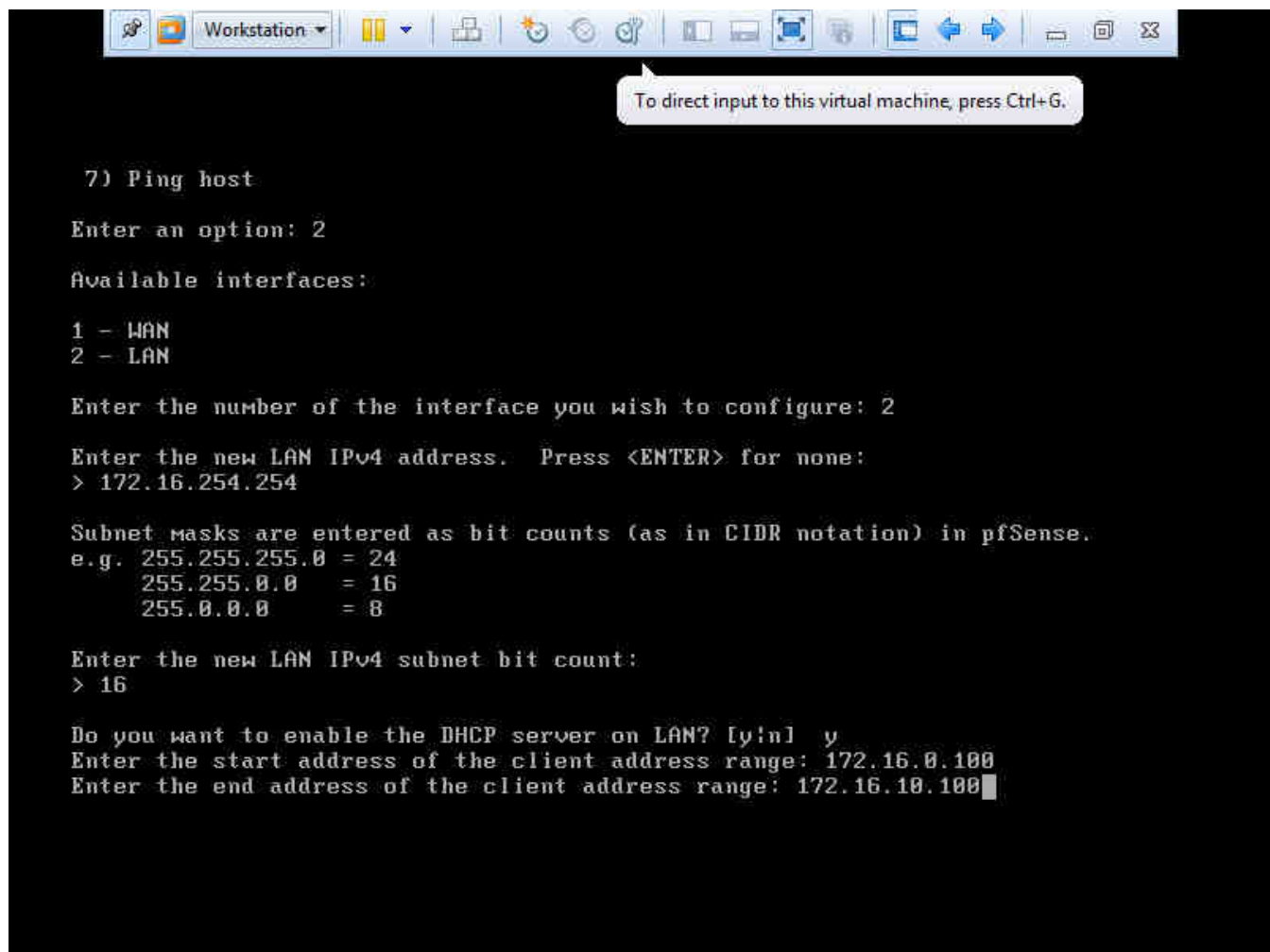
Enter the new LAN IPv4 address. Press <ENTER> for none:
> 172.16.254.254

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

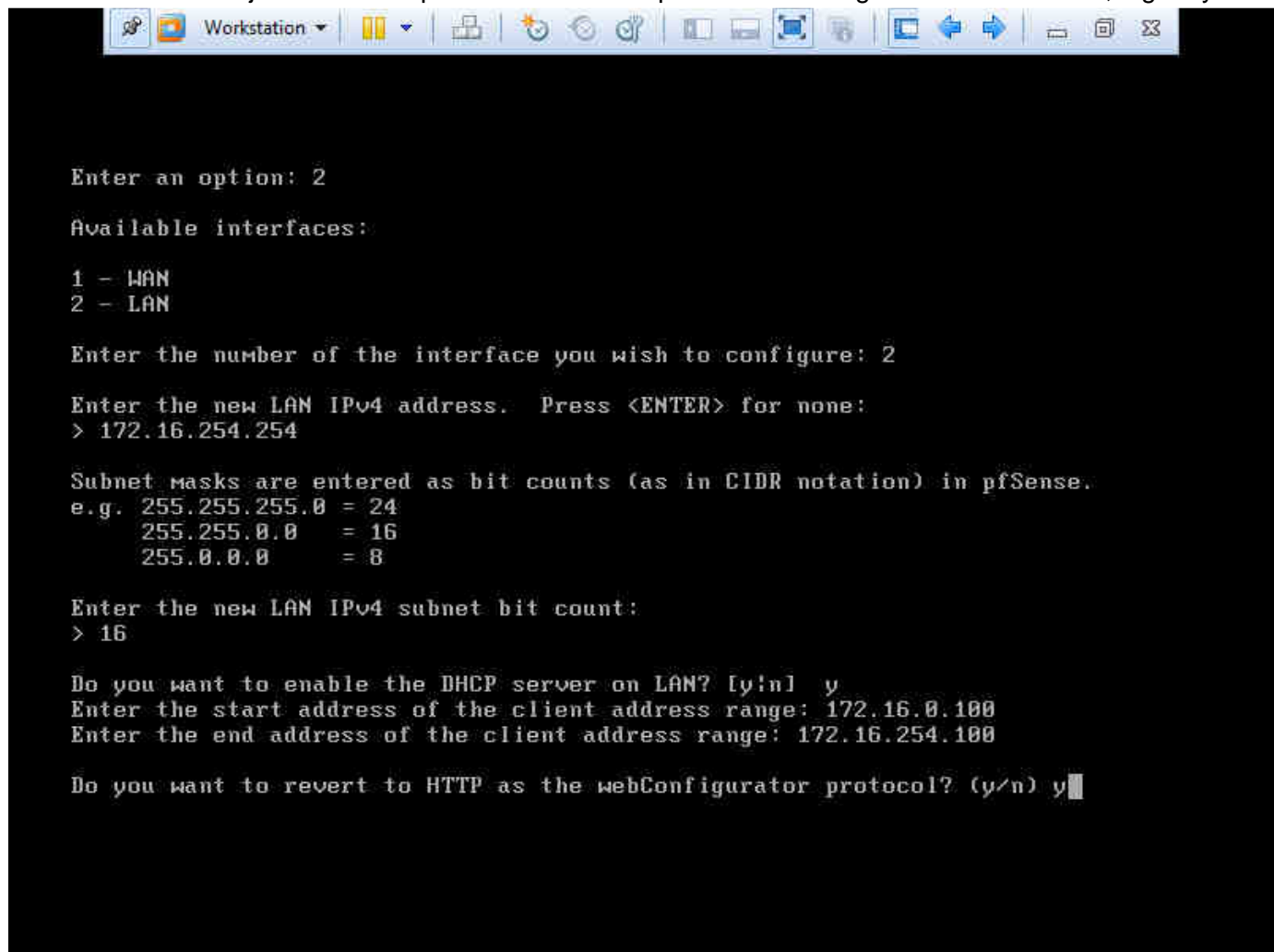
Enter the new LAN IPv4 subnet bit count:
> 16

Do you want to enable the DHCP server on LAN? [y!n] y
```

33- Agora vamos configurar nossa faixa de endereçamento IP. Começando em: "172.16.0.100" e terminando em "172.16.10.100".



34- Caso você deseje converter a para HTTP da LAN para o webConfigurador do PFSense, digite "y".



```
Enter an option: 2

Available interfaces:

1 - WAN
2 - LAN

Enter the number of the interface you wish to configure: 2

Enter the new LAN IPv4 address. Press <ENTER> for none:
> 172.16.254.254

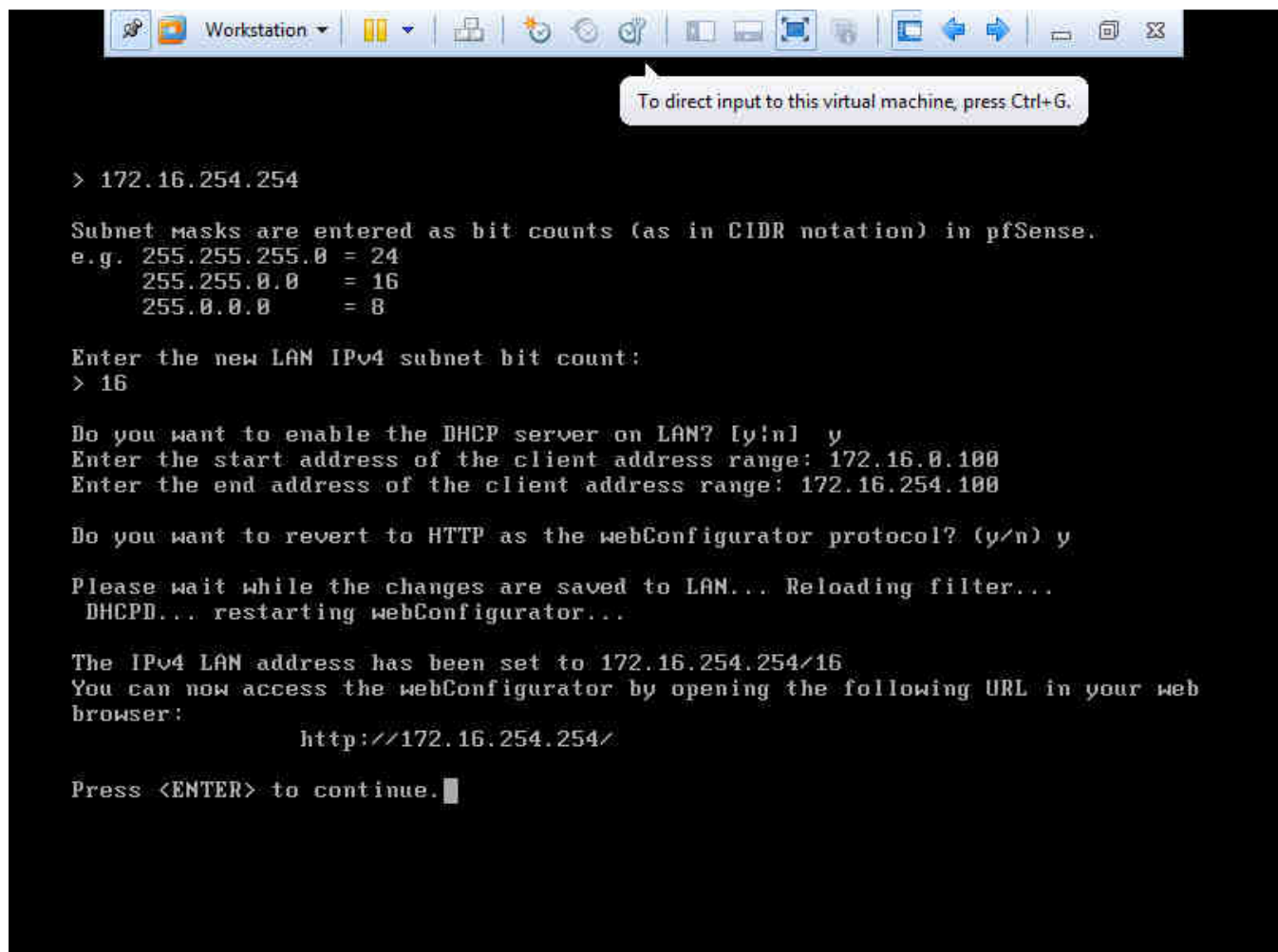
Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0  = 16
     255.0.0.0   = 8

Enter the new LAN IPv4 subnet bit count:
> 16

Do you want to enable the DHCP server on LAN? [y/n] y
Enter the start address of the client address range: 172.16.0.100
Enter the end address of the client address range: 172.16.254.100

Do you want to revert to HTTP as the webConfigurator protocol? (y/n) y
```

35- Pronto. Na tela irá aparecer uma mensagem de confirmação. Pressione “Enter” para continuar. Iremos agora configurar nosso PC para aceitar o endereço IP que criamos isso irá criar uma conexão do servidor para a máquina.



```
> 172.16.254.254

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count:
> 16

Do you want to enable the DHCP server on LAN? [y/n] y
Enter the start address of the client address range: 172.16.0.100
Enter the end address of the client address range: 172.16.254.100

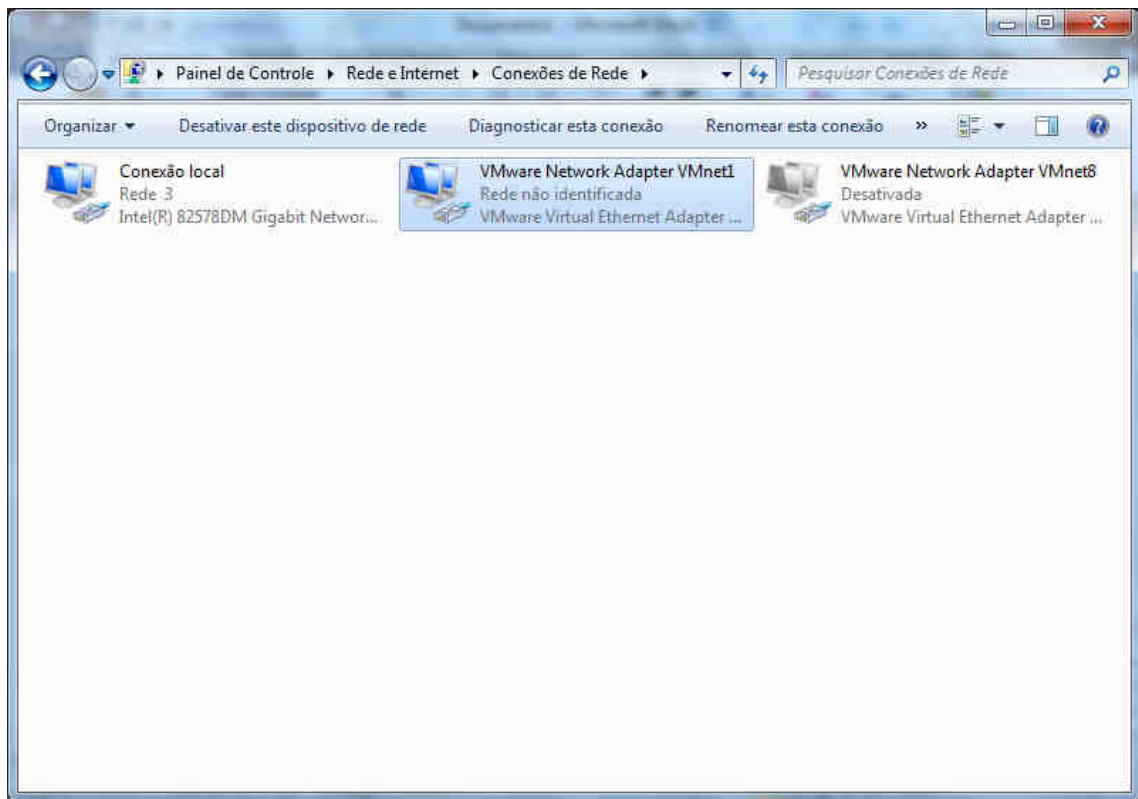
Do you want to revert to HTTP as the webConfigurator protocol? (y/n) y

Please wait while the changes are saved to LAN... Reloading filter...
DHCPD... restarting webConfigurator...

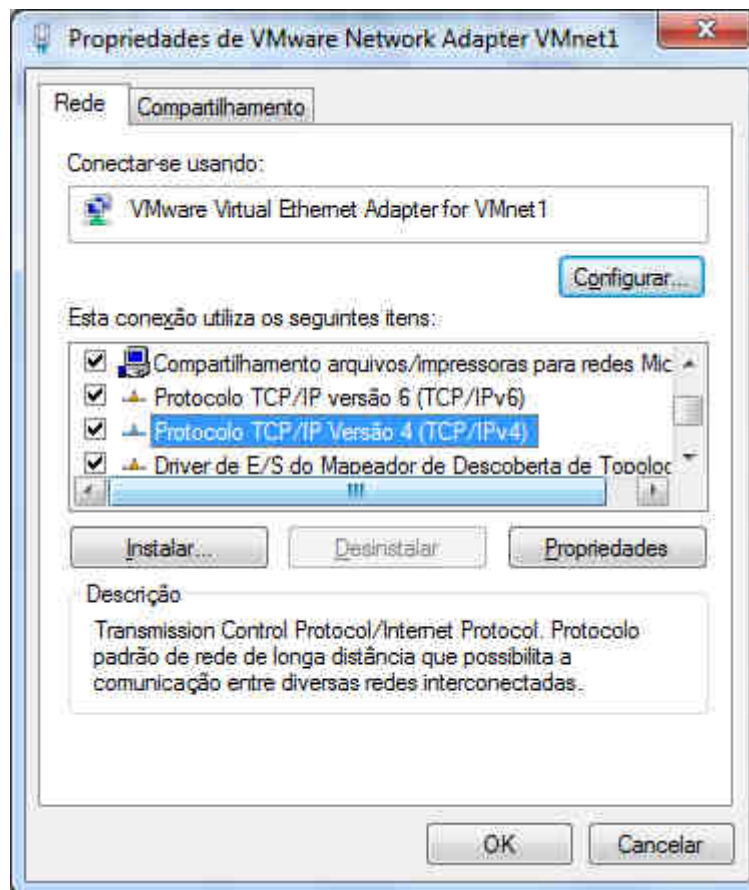
The IPv4 LAN address has been set to 172.16.254.254/16
You can now access the webConfigurator by opening the following URL in your web
browser:
      http://172.16.254.254/

Press <ENTER> to continue.
```

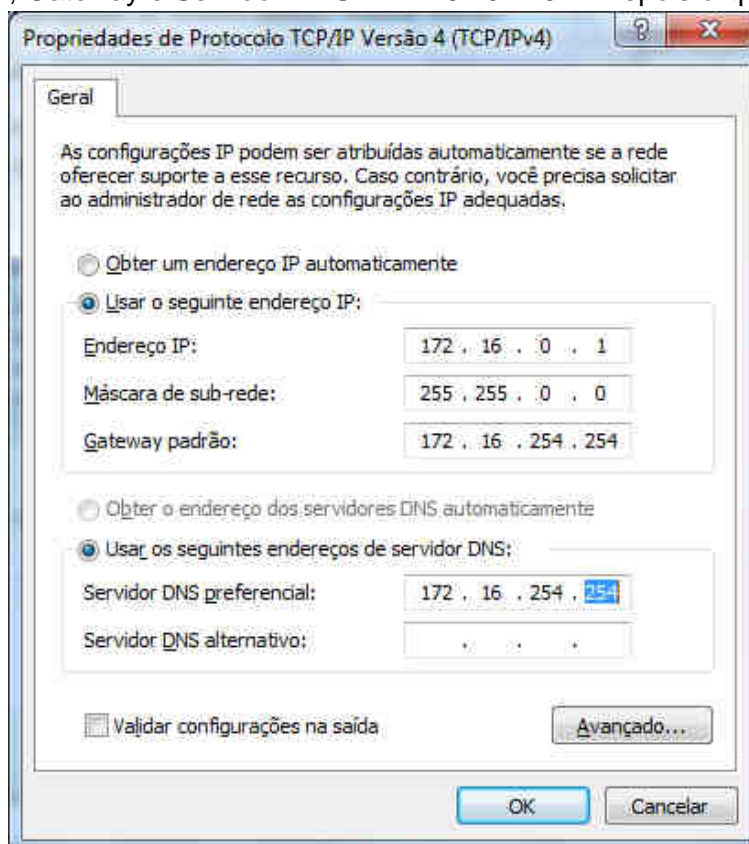
36- Abra as conexões locais do seu computador e procure a rede do Vmware.



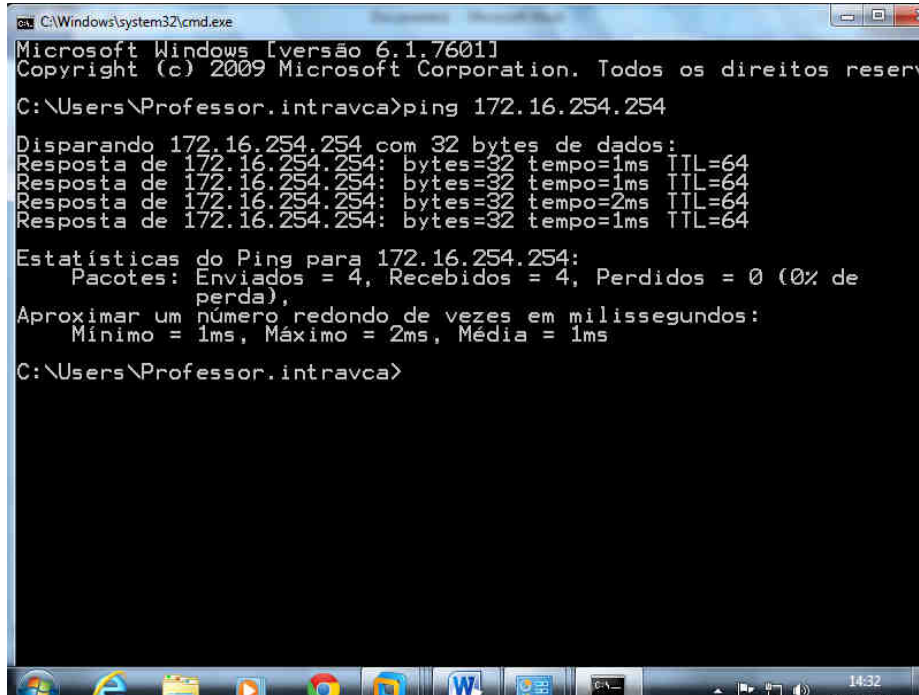
37- Clique em “Propriedades” e na opção “ Protocolo TCP/IP Versão4(TCP/IPv4), clique em “propriedades” novamente.



38- Altere seu endereço Ip de acordo com o configurado no Pfsense. Nesse caso foi "172.16.0.1". Máscara: "255.255.0.0", Gateway e Servidor DNS "172.16.254.254". Depois clique em "OK".



39- Para saber se sua configuração está correta, você pode fazer um teste simples usando o Prompt de comando do Windows. Clique em “iniciar”, digite “cmd”, dê enter e digite Ping 172.16.254.254”. Caso apareça a seguinte tela, mostrando resposta do Ip, está tudo certo.



```
C:\Windows\system32\cmd.exe
Microsoft Windows [versão 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Todos os direitos reservados

C:\Users\Professor.intravca>ping 172.16.254.254

Disparando 172.16.254.254 com 32 bytes de dados:
Resposta de 172.16.254.254: bytes=32 tempo=1ms TTL=64
Resposta de 172.16.254.254: bytes=32 tempo=1ms TTL=64
Resposta de 172.16.254.254: bytes=32 tempo=2ms TTL=64
Resposta de 172.16.254.254: bytes=32 tempo=1ms TTL=64

Estatísticas do Ping para 172.16.254.254:
    Pacotes: Enviados = 4, Recebidos = 4, Perdidos = 0 (0% de perda),
Aproximar um número redondo de vezes em milissegundos:
    Mínimo = 1ms, Máximo = 2ms, Média = 1ms

C:\Users\Professor.intravca>
```

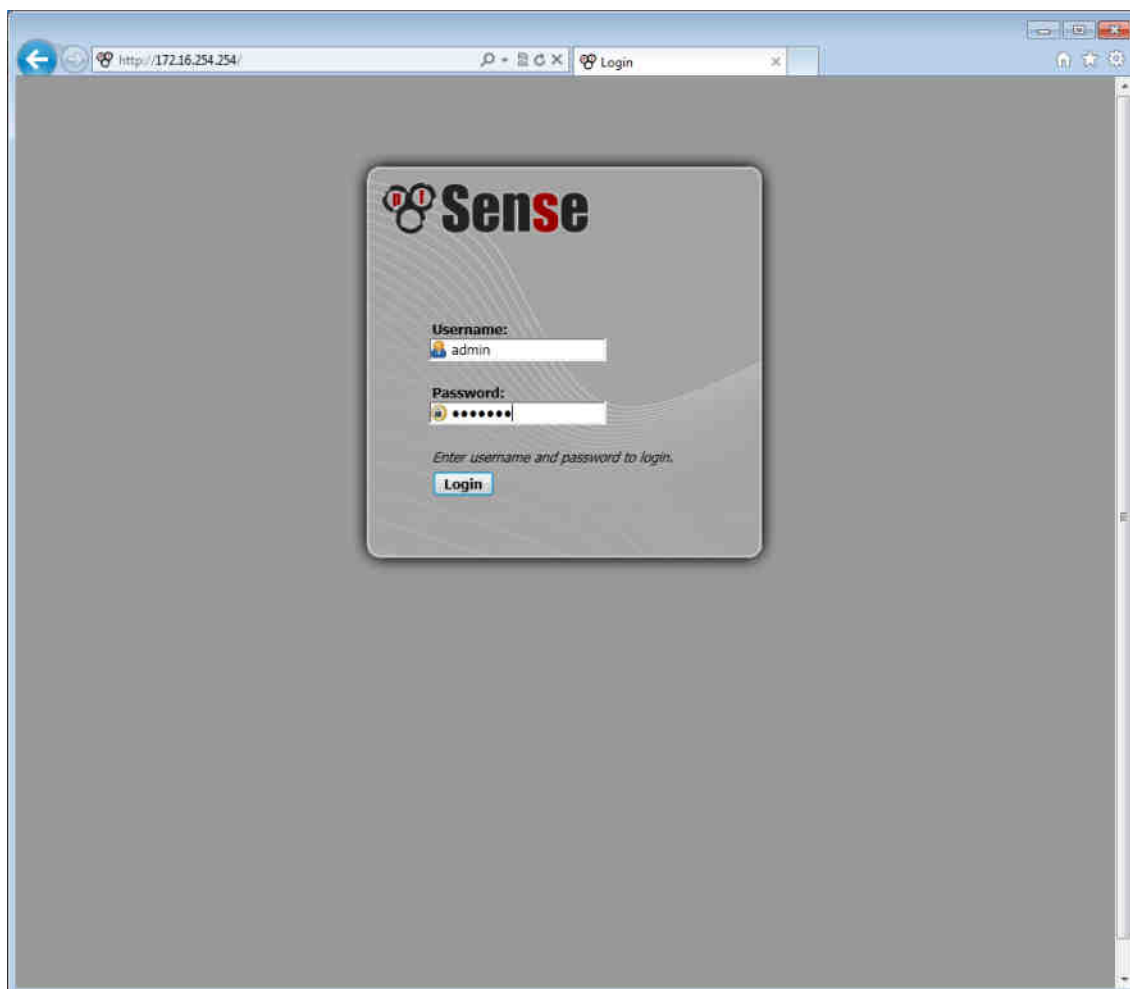
Configuração através do navegador

40- No seu navegador digite o endereço IP configurado anteriormente (172.16.254.254)

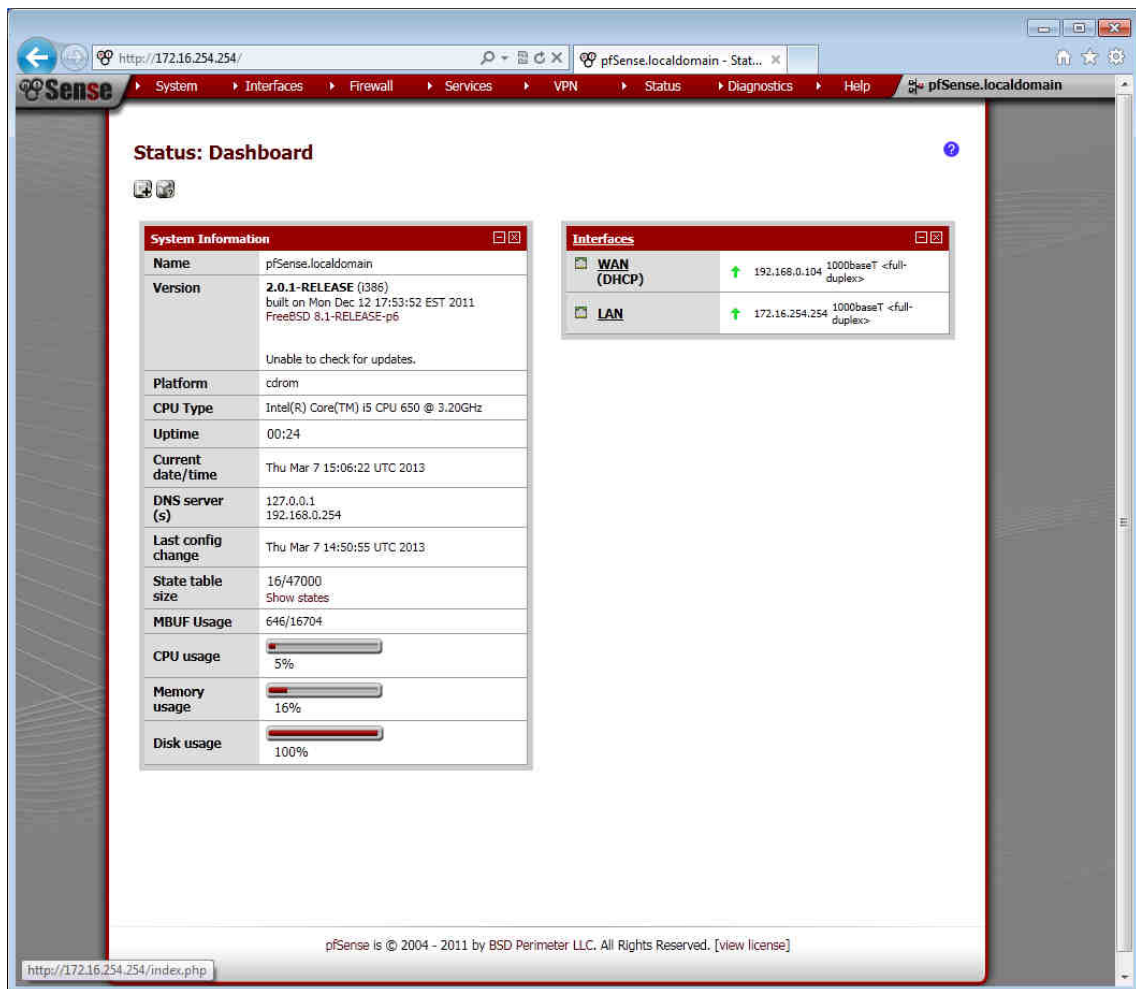
Se tudo estiver configurado corretamente essa tela aparecerá:



41- Digite no Username: “**admin**” e no Password: “**pfsense**” e clique em “**Login**”, para entrar.



Essa é a tela inicial do PfSense



The screenshot shows the pfSense web interface. The browser address bar displays `http://172.16.254.254/`. The navigation menu at the top includes System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. The main content area is titled "Status: Dashboard" and contains two panels: "System Information" and "Interfaces".

System Information

Name	pfSense.localdomain
Version	2.0.1-RELEASE (i386) built on Mon Dec 12 17:53:52 EST 2011 FreeBSD 8.1-RELEASE-p6 Unable to check for updates.
Platform	cdrom
CPU Type	Intel(R) Core(TM) i5 CPU 650 @ 3.20GHz
Uptime	00:24
Current date/time	Thu Mar 7 15:06:22 UTC 2013
DNS server(s)	127.0.0.1 192.168.0.254
Last config change	Thu Mar 7 14:50:55 UTC 2013
State table size	16/47000 Show states
MBUF Usage	646/16704
CPU usage	5%
Memory usage	16%
Disk usage	100%

Interfaces

WAN (DHCP)	↑ 192.168.0.104 1000baseT <full-duplex>
LAN	↑ 172.16.254.254 1000baseT <full-duplex>

At the bottom of the dashboard, the copyright notice reads: "pfSense is © 2004 - 2011 by BSD Perimeter LLC. All Rights Reserved. [view license]". The browser status bar at the bottom shows the URL `http://172.16.254.254/index.php`.

42- Clique em “System” depois em “Setup Wizard” para abrir o assistente de configuração.

The screenshot shows the pfSense web interface. The top navigation bar includes links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. The System menu is open, displaying a list of options: Advanced, Cert Manager, Firmware, General Setup, Logout, Routing, Setup Wizard, and User Manager. The Setup Wizard option is highlighted. The main content area displays the pfSense dashboard, which includes a table of system information and a section for network interfaces.

Item	Value
System	pfSense.localdomain
Version	2.0.1-RELEASE (1086) built on Mon Dec 12 17:53:52 EST 2011 FreeBSD 8.1-RELEASE-p6
Platform	Unable to check for updates.
CPU Type	Intel(R) Core(TM) i5 CPU 650 @ 3.20GHz
Uptime	00:27
Current date/time	Thu Mar 7 15:08:56 UTC 2013
DNS server(s)	127.0.0.1 192.168.0.254
Last config change	Thu Mar 7 14:50:55 UTC 2012
State table size	8/47000 Show states
MBUF Usage	646/16704
CPU usage	5%
Memory usage	16%
Disk usage	100%

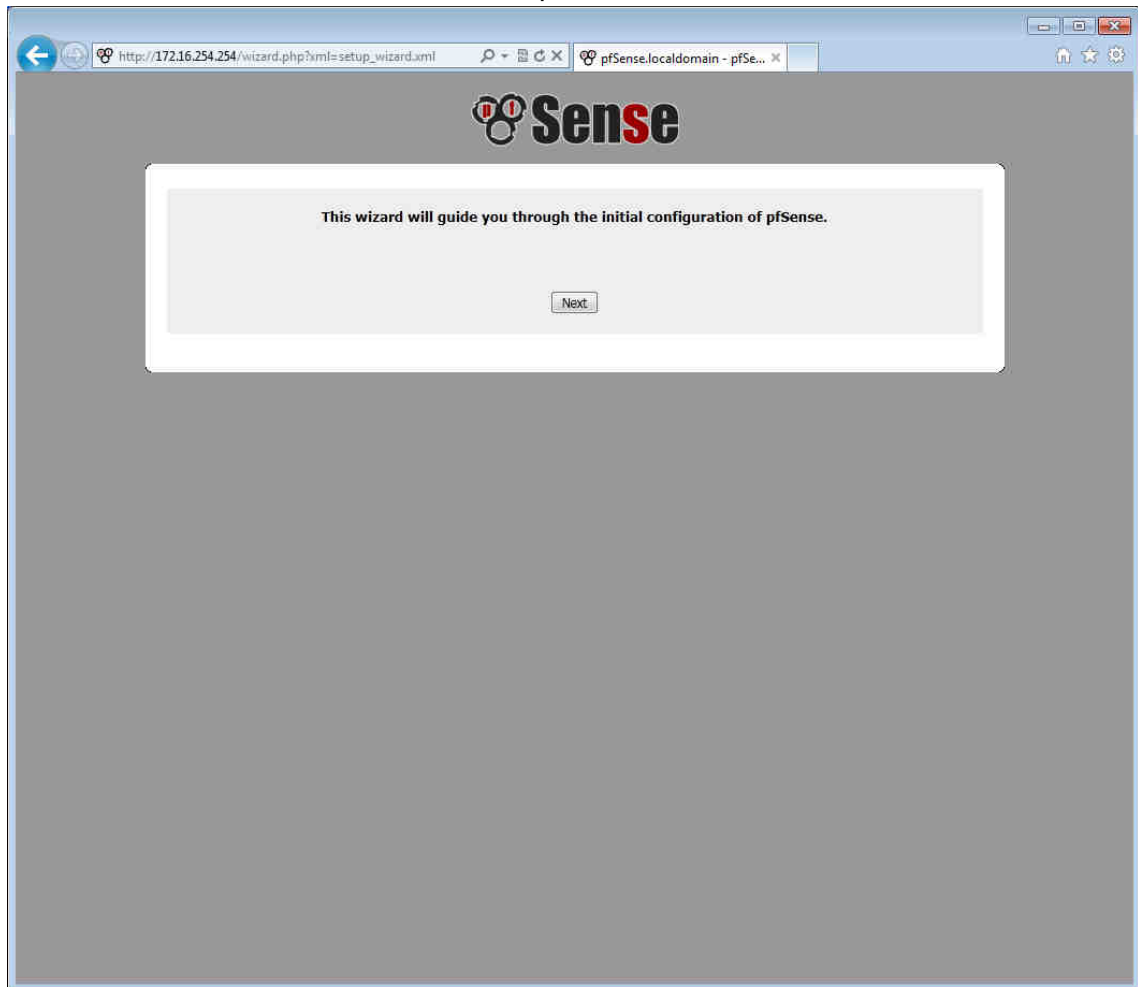
Interfaces

Interface	IP Address	Netmask	MTU	Speed	Duplex
WAN (DHCP)	192.168.0.104	255.255.255.0	1500	1000baseT	<full-duplex>
LAN	172.16.254.254	255.255.255.0	1500	1000baseT	<full-duplex>

pfSense is © 2004 - 2011 by BSD Perimeter LLC. All Rights Reserved. [\[view license\]](#)

http://172.16.254.254/wizard.php?xml=setup_wizard.xml

43- Clique em Next.



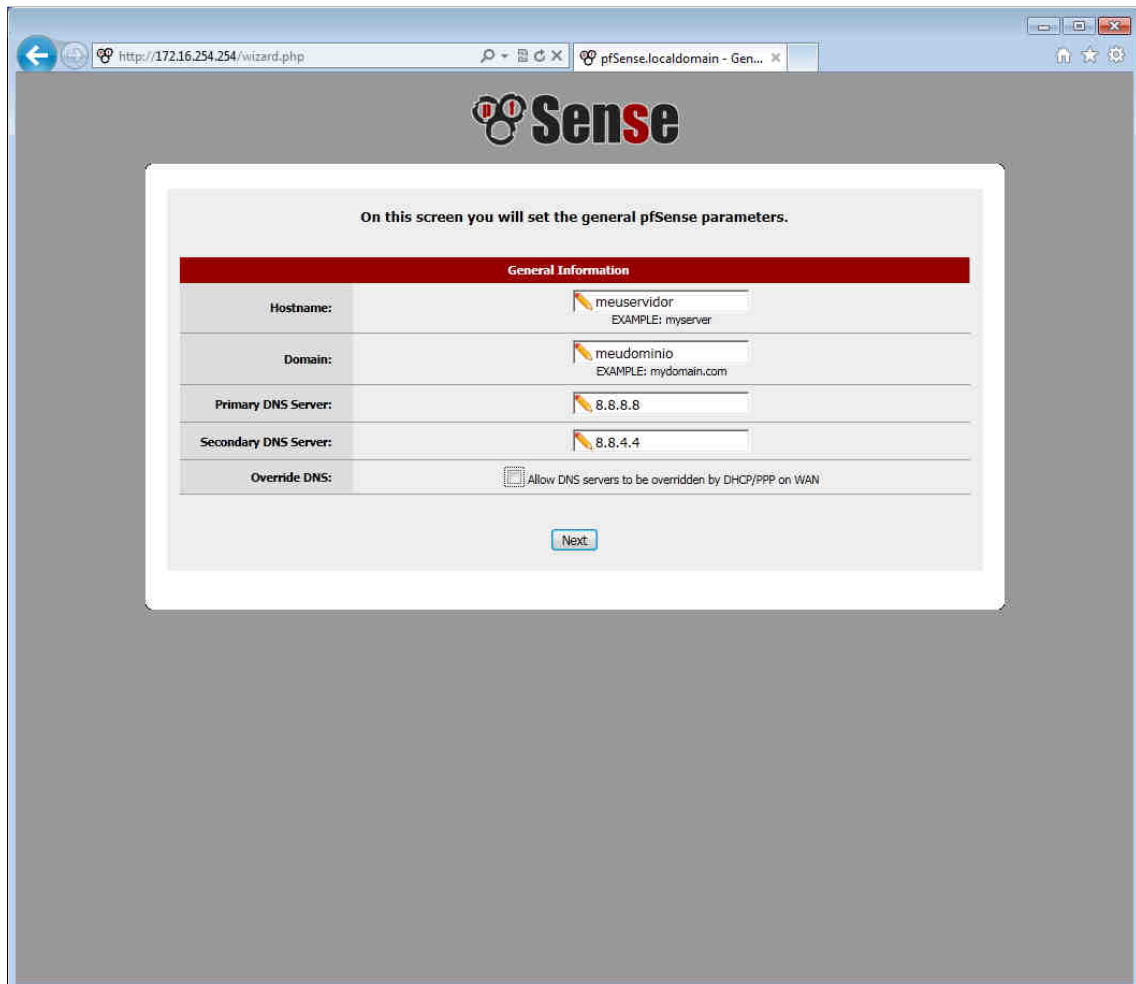
44- Nesta tela você irá definir os parâmetros Pfsense gerais. Como está sendo especificado na seguinte tela.

Hostname: Defina o nome do servidor **apenas com letras minúsculas(Mais indicado).**

Domain: Nome do domínio do servidor

Primary/Secondary DNS Server: Endereços do servidor DNS preferencial

Deixe a opção *“Allow DNS servers to be overridden by DHCP/PPP on WAN”* **desabilitada**, para que seja utilizado apenas o servidor DNS selecionado acima.



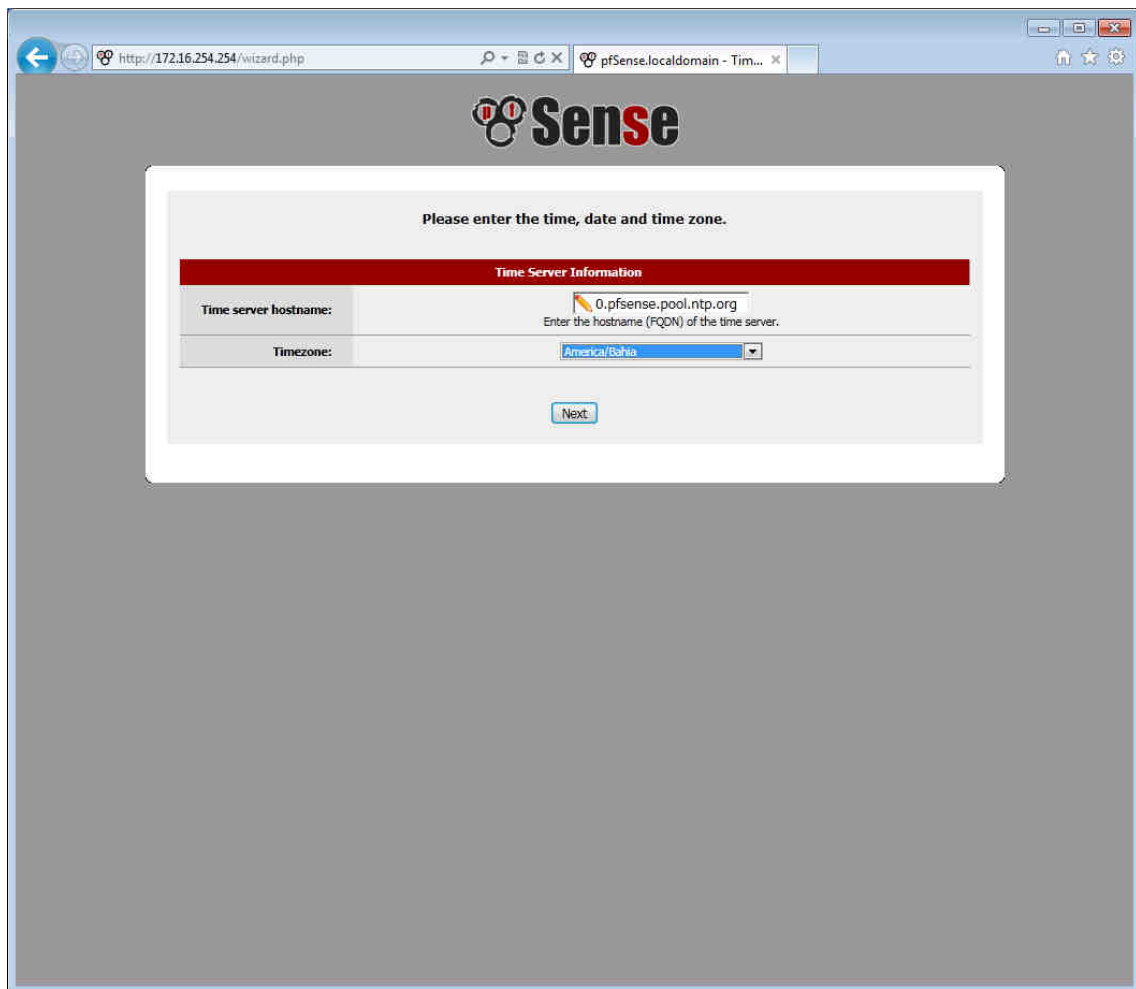
The screenshot shows the pfSense web interface in a browser window. The address bar shows 'http://172.16.254.254/wizard.php'. The page title is 'pfSense.localdomain - Gen...'. The main content area has a header with the pfSense logo and the text 'On this screen you will set the general pfSense parameters.' Below this is a form titled 'General Information' with a red header bar. The form contains five rows of input fields: 'Hostname' with the value 'meuservidor' and an example 'EXAMPLE: myserver'; 'Domain' with the value 'meudominio' and an example 'EXAMPLE: mydomain.com'; 'Primary DNS Server' with the value '8.8.8.8'; 'Secondary DNS Server' with the value '8.8.4.4'; and 'Override DNS' with a checkbox labeled 'Allow DNS servers to be overridden by DHCP/PPP on WAN'. A 'Next' button is located at the bottom of the form.

General Information	
Hostname:	meuservidor EXAMPLE: myserver
Domain:	meudominio EXAMPLE: mydomain.com
Primary DNS Server:	8.8.8.8
Secondary DNS Server:	8.8.4.4
Override DNS:	<input type="checkbox"/> Allow DNS servers to be overridden by DHCP/PPP on WAN

Next

Clique em **Next** para continuar.

45- Agora escolha o fuso horário local. Neste exemplo utilizamos o horário da Bahia.



The screenshot shows a web browser window with the URL `http://172.16.254.254/wizard.php`. The page features the 'Sense' logo at the top. A central white box contains the instruction 'Please enter the time, date and time zone.' Below this is a section titled 'Time Server Information' with a red header. It includes two input fields: 'Time server hostname:' with the value '0.pfsense.pool.ntp.org' and a sub-instruction 'Enter the hostname (FQDN) of the time server.', and 'Timezone:' with a dropdown menu set to 'America/Bahia'. A 'Next' button is located at the bottom of the form.

Clique em **Next** para continuar

45- Agora escolha o tipo de conexão com a internet. Nesse caso utilizamos uma conexão que adquire o endereço IP* automaticamente via DHCP. Então apenas selecionaremos a interface WAN como “DHCP”

(*IP: Endereço individual que identifica os computadores numa rede TCP/IP)

The image displays two screenshots of the pfSense configuration wizard, specifically the WAN configuration steps.

Top Screenshot: Configure WAN Interface

- SelectedType:** DHCP
- General configuration:**
 - MAC Address:** This field can be used to modify ("spoof") the MAC address of the WAN interface (may be required with some cable connections). Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.
 - MTU:** If you enter a value in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect. If you leave this field blank, an MTU of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed.
- Static IP Configuration:**
 - IP Address:**
 - Gateway:**
- DHCP client configuration:**
 - DHCP Hostname:** The value in this field is sent as the DHCP client identifier and hostname when requesting a DHCP lease. Some ISPs may require this (for client identification).
- PPPoE configuration:**
 - PPPoE Username:**
 - PPPoE Password:**
 - PPPoE Service name:** Hint: this field can usually be left empty
 - PPPoE Dial on demand:** ☐ This option causes the interface to operate in dial-on-demand mode, allowing you to have a virtual full time connection. The interface is configured, but the actual connection of the link is delayed until qualifying outgoing traffic is detected. Enable Dial-On-Demand mode

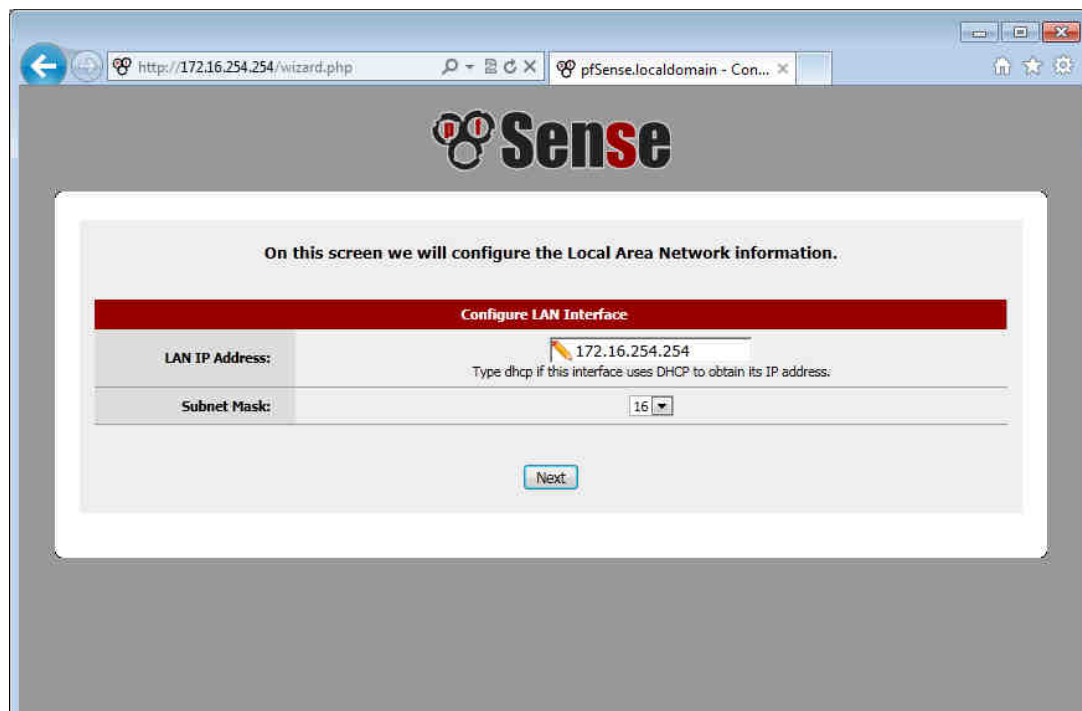
Bottom Screenshot: PPPoE configuration

- PPPoE Username:**
- PPPoE Password:**
- PPPoE Service name:** Hint: this field can usually be left empty
- PPPoE Dial on demand:** ☐ This option causes the interface to operate in dial-on-demand mode, allowing you to have a virtual full time connection. The interface is configured, but the actual connection of the link is delayed until qualifying outgoing traffic is detected. Enable Dial-On-Demand mode
- PPPoE Idle timeout:** If no qualifying outgoing packets are transmitted for the specified number of seconds, the connection is brought down. An idle timeout of zero disables this feature.
- PPTP configuration:**
 - PPTP Username:**
 - PPTP Password:**
 - PPTP Local IP Address:**
 - PPTP Remote IP Address:**
 - PPTP Dial on demand:** ☐ This option causes the interface to operate in dial-on-demand mode, allowing you to have a virtual full time connection. The interface is configured, but the actual connection of the link is delayed until qualifying outgoing traffic is detected. Enable Dial-On-Demand mode
 - PPTP Idle timeout:** If no qualifying outgoing packets are transmitted for the specified number of seconds, the connection is brought down. An idle timeout of zero disables this feature.
- RFC1918 Networks:**
 - Block RFC1918 Private Networks:** ☒ When set, this option blocks traffic from IP addresses that are reserved for private networks as per RFC 1918 (10/8, 172.16/12, 192.168/16) as well as loopback addresses (127/8). You should generally leave this option turned on, unless your WAN network lies in such a private address space, too. Block private networks from entering via WAN
- Block bogon networks:** ☒ When set, this option blocks traffic from IP addresses that are reserved (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and obviously should not appear as the source address in any packets you receive. Block non-Internet routed networks from entering via WAN

Next

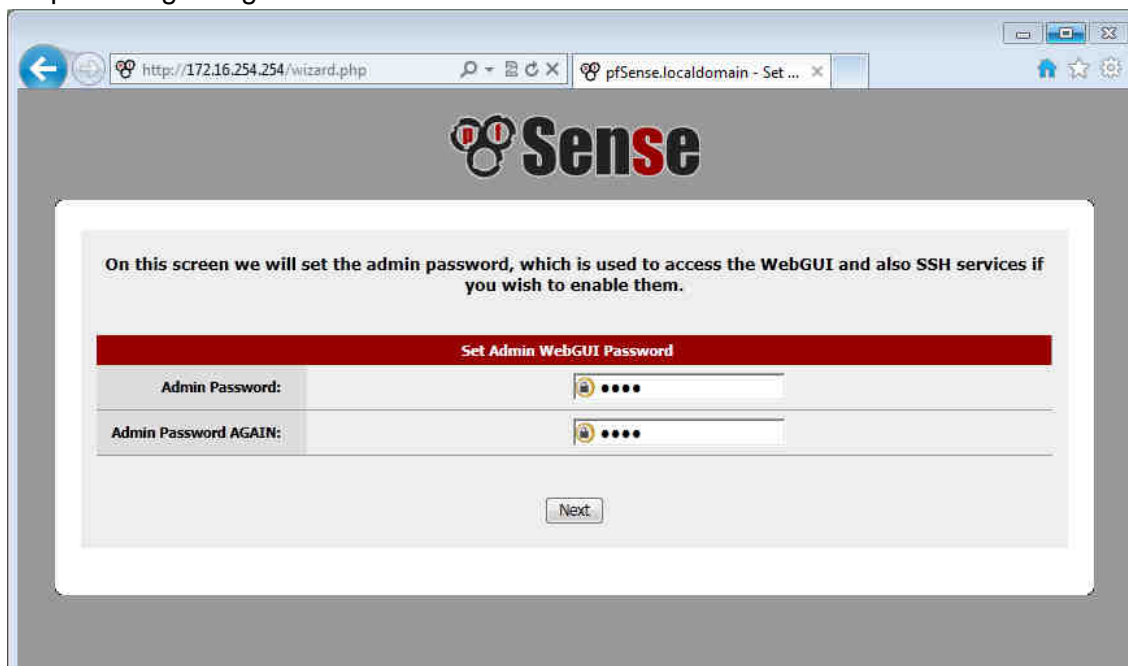
Role até o fim da página e clique em **Next**

46- Nessa janela pode-se escolher o endereço IP do servidor, mas como já foi configurado anteriormente não é necessária nenhuma alteração. Clique em **Next**



The screenshot shows a web browser window with the URL `http://172.16.254.254/wizard.php`. The page features the 'Sense' logo at the top. Below the logo, a message states: 'On this screen we will configure the Local Area Network information.' A red header bar reads 'Configure LAN Interface'. The form contains two fields: 'LAN IP Address:' with the value '172.16.254.254' and a note 'Type dhcp if this interface uses DHCP to obtain its IP address.', and 'Subnet Mask:' with a dropdown menu set to '16'. A 'Next' button is located at the bottom of the form.

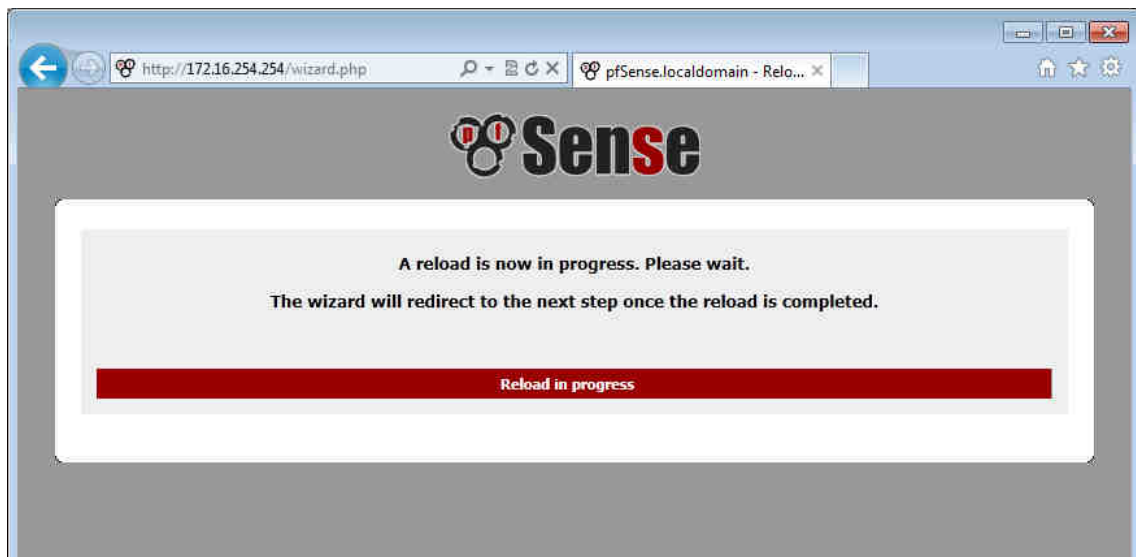
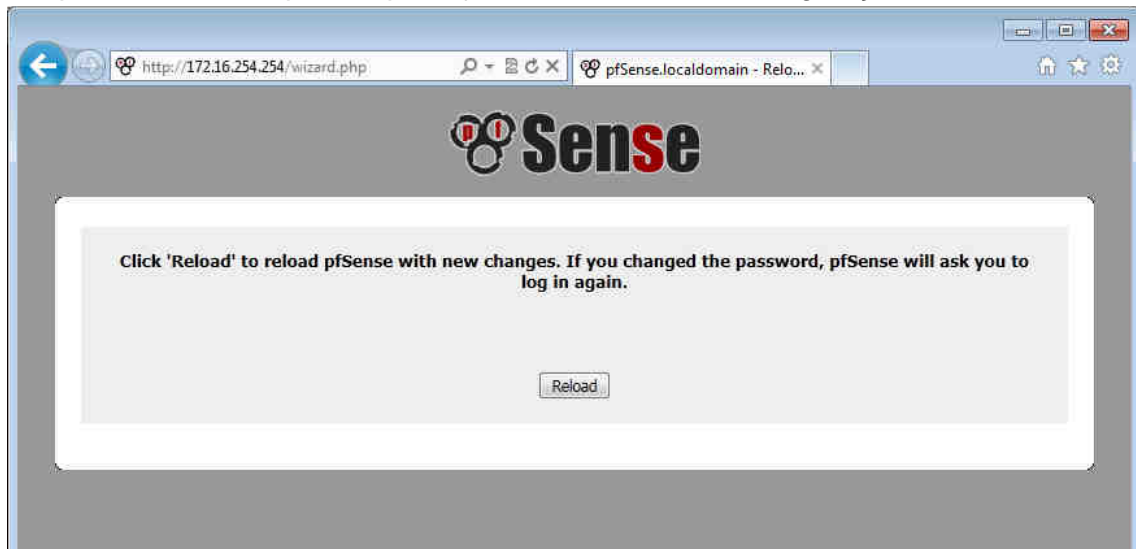
47- Nos campos a seguir digite a nova senha de acesso do administrador do servidor.



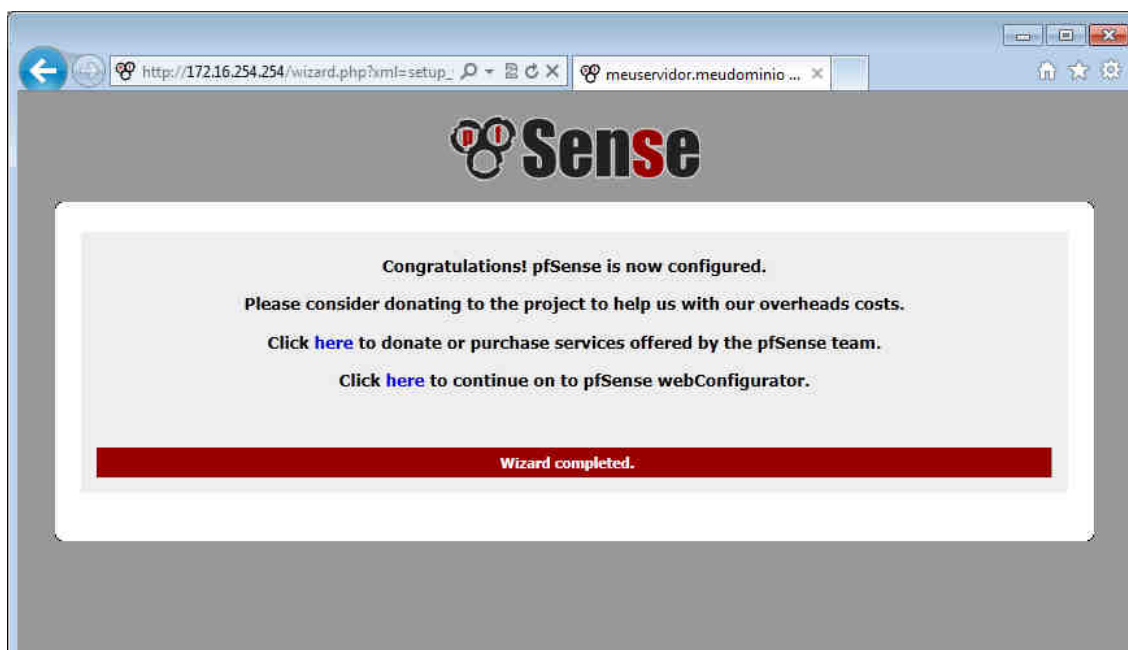
The screenshot shows the same web browser window, but the URL is `http://172.16.254.254/wizard.php` and the page title is 'pfSense.localdomain - Set ...'. The 'Sense' logo is at the top. A message states: 'On this screen we will set the admin password, which is used to access the WebGUI and also SSH services if you wish to enable them.' A red header bar reads 'Set Admin WebGUI Password'. The form contains two password fields: 'Admin Password:' and 'Admin Password AGAIN:', both with masked input (dots). A 'Next' button is located at the bottom of the form.

Clique em Next.

48- Agora clique em **“Reload”** para o que sejam salvas as novas configurações



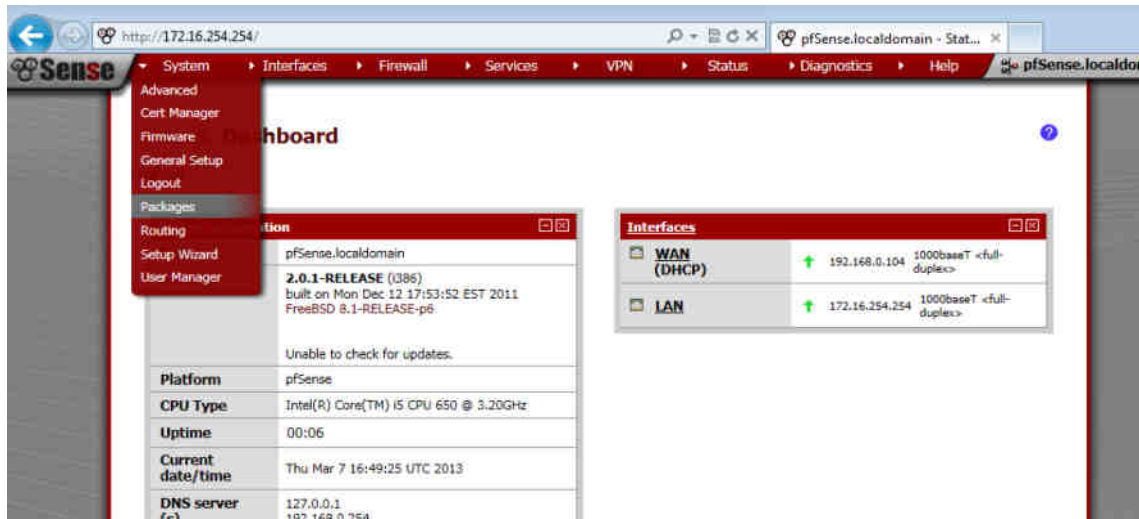
49- Clique na segunda palavra “**here**” para continuar a configuração. (ou na primeira, para fazer uma doação para a equipe Pfsense)



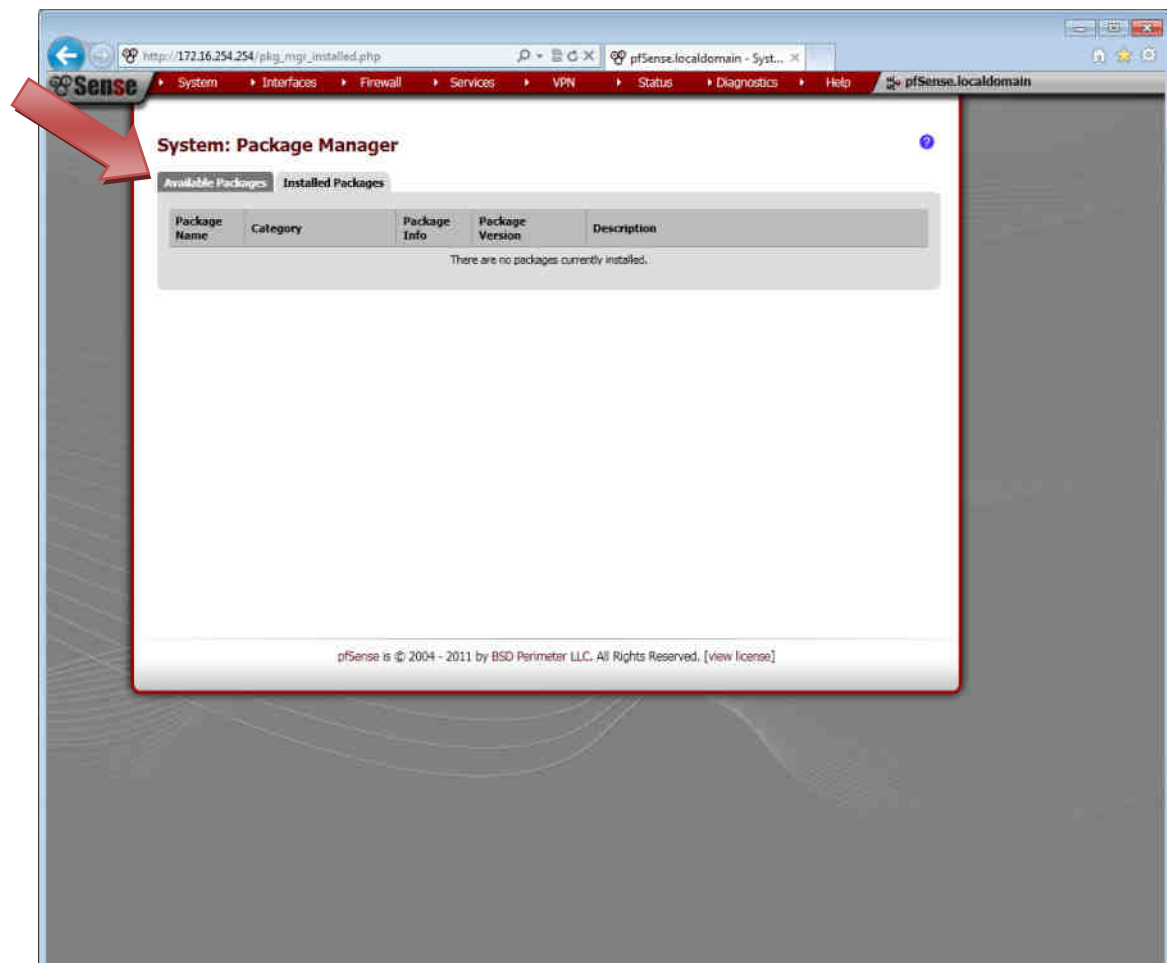
Instalação de pacotes

No pfSense é possível instalar novos pacotes, que adicionam novas funcionalidades ao servidor, vamos aprender a instalar e configurar duas delas: Squid – Como visto anteriormente ele tem a função de proxy, filtra conteúdos da WAN que poderão ser acessados na LAN e possui função Proxy Cache, que armazena dados baixados da WEB no HD do servidor, para um acesso mais rápido através da rede local. E o LightSquid que gera relatórios do squid.

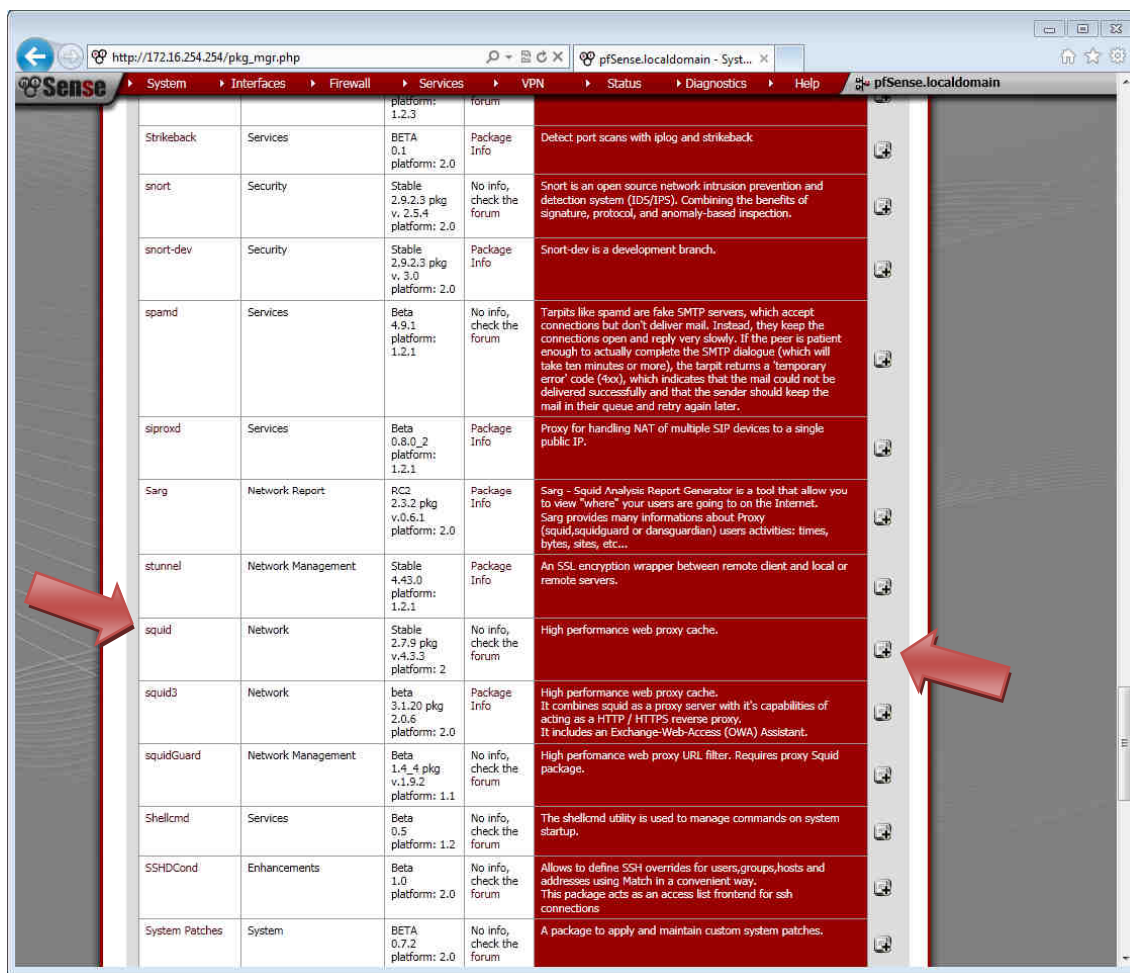
50- Acesse o menu de pacotes em **System>Packages**



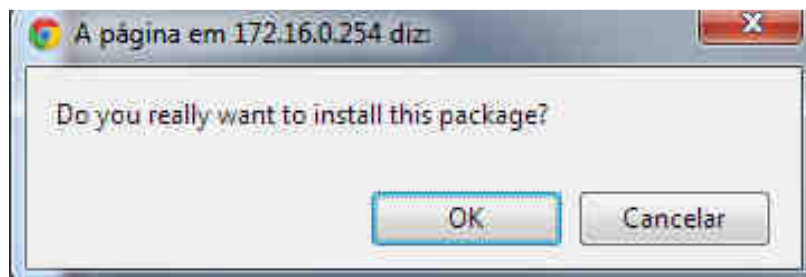
51- “Available Packages” para ver os pacotes disponíveis para download.



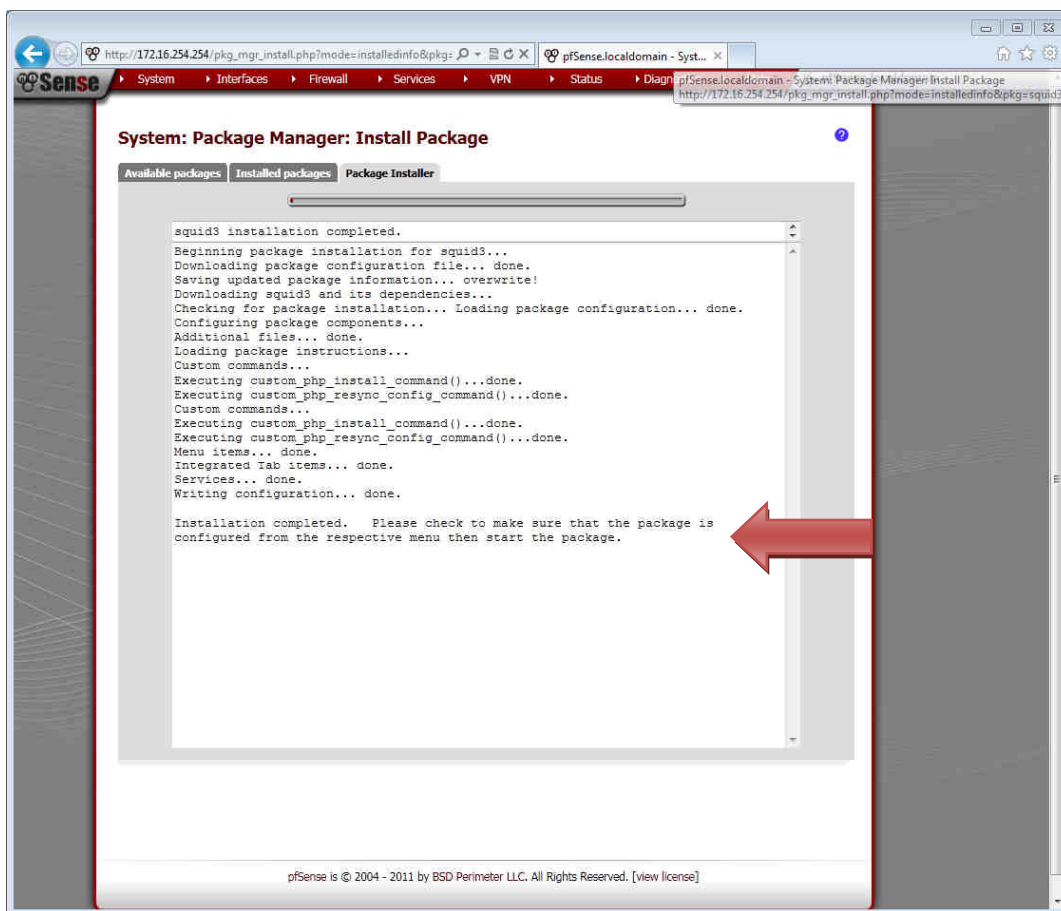
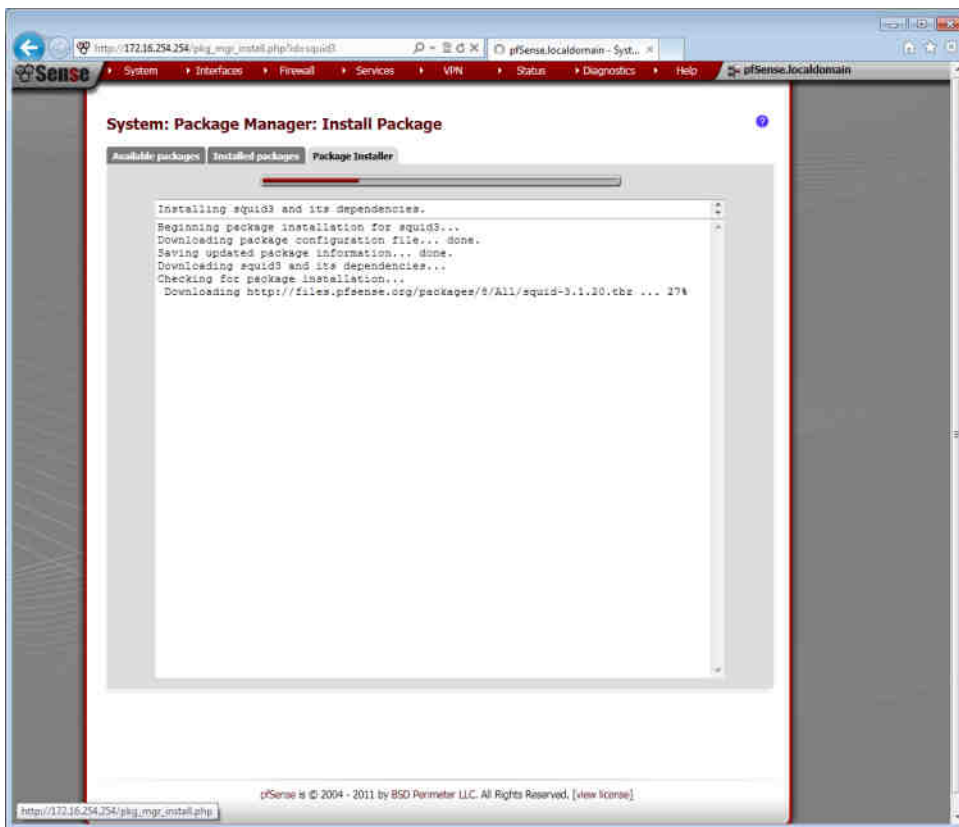
52- Encontre o pacote “squid” e clique no botão “Install package” como mostra a imagem abaixo.



Clique **OK** para iniciar a instalação

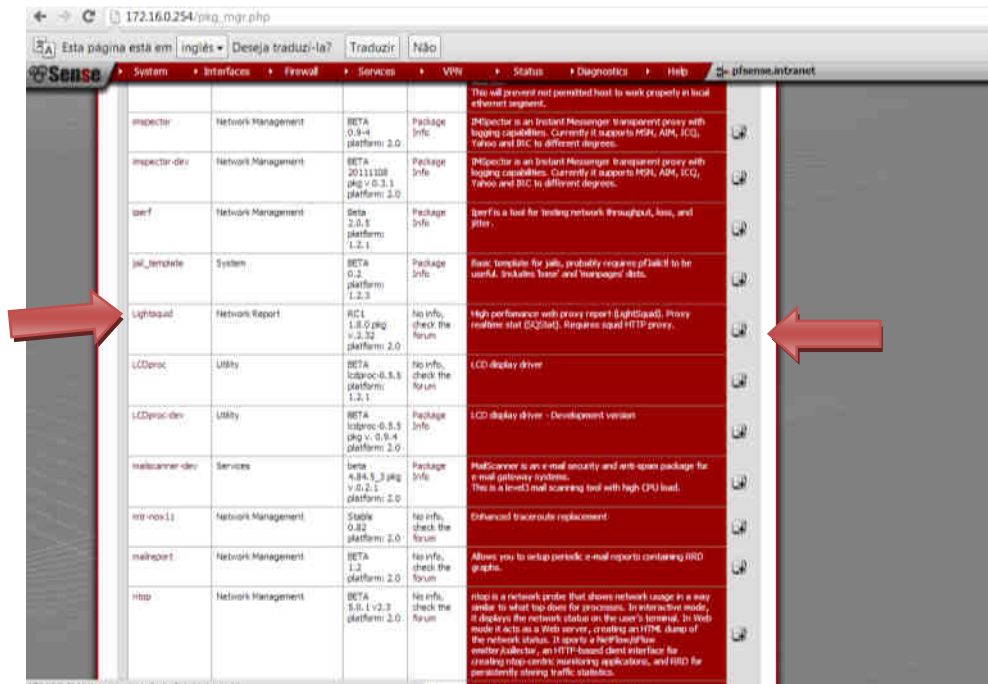


53- Aguarde o processo de download e instalação.



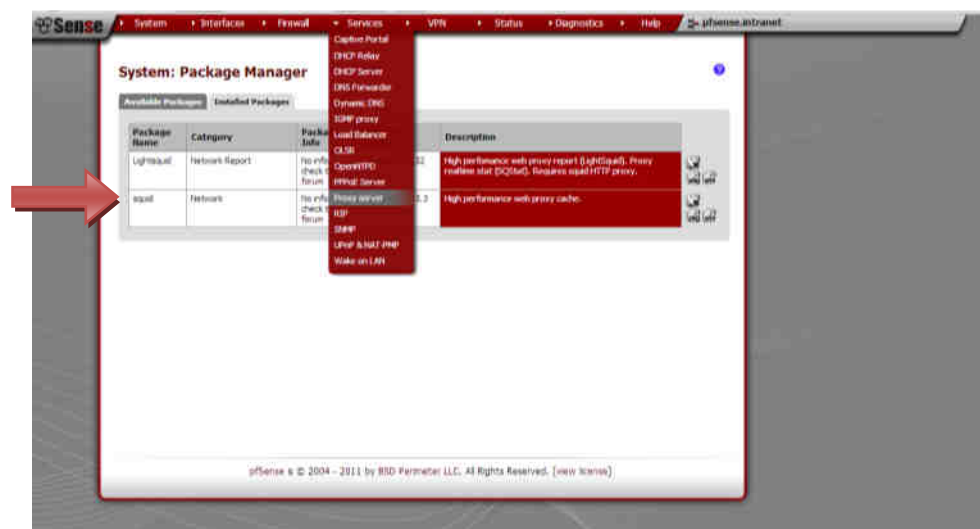
Instalação concluída

54- Agora instale o Lightsquid, da mesma forma do anterior.



Configuração do Squid

55- Agora configuraremos o Squid para entrar nas suas configurações vá em **Services> Proxy Server**.



56- Na pagina do Squid escolha a interface **LAN**.

- Marque a opção **Transparent Proxy** para que não ter que informar o Squid na porta do navegador.
- Escolha o idioma dos avisos (Language- Português).
- Marcamos **Allow users on interfaces** para os usuários conectados à interface selecionada no campo "interface de Proxy 'será permitido para usar o Proxy, ou seja, não haverá necessidade de adicionar sub-rede da interface para a lista de sub-redes permitidos.
- Escolhemos a porta (3128) Esta é a porta do servidor Proxy irá escutar,

The screenshot shows the 'Proxy server: General settings' page in the pfSense web interface. The 'General' tab is selected. The 'Proxy interface' is set to 'lan'. The 'Allow users on interface' checkbox is checked. The 'Transparent proxy' checkbox is checked and highlighted with a red arrow. The 'Proxy port' is set to 3128. The language is set to Portuguese. Other settings like 'Suppress proxy for Private Address Space', 'Suppress proxy for these source IPs', 'Suppress proxy for these destination IPs', 'Enable logging', 'Log store directory', 'Log rotate', 'ICP port', 'Verbose feedback', 'Administrator email', 'Language', 'Disable HTTP Forward', 'Disable V14', 'Use alternate DNS servers for the proxy server', 'Suppress Squid Version', and 'Custom Options' are also visible.

57- Gerenciamento do cache: O gerenciamento do cache é uma ferramenta útil para conexões de internet lentas, pois armazena os últimos dados baixados no HD do servidor, disponibilizando-os com maior velocidade quando solicitados novamente.

- Na página do squid clique na aba **Cache Mgmt**
- Escolha o tamanho do disco reservado ao cache, (colocamos 1024mb).
- A memória RAM reservada ao cache (128mb).
- Tamanho máximo dos objetos armazenados (8192kb).
- E o tamanho máximo da memória RAM a ser utilizada por cada objeto (32kb [padrão])
- Em (Memory replacement policy) escolha (GDSF) que é política de substituição de memória determina quais objetos são removidos da memória quando o espaço é necessário.
- E em (Cache replacement policy) escolha (LFUDA) que é política de substituição do cache que determina quais objetos são removidos da memória quando o espaço é necessário.

Proxy server: Cache management

General | Squid Proxy | **Cache Mgmt** | Access Control | Traffic Mgmt | Auth Settings | Local Users

Hard disk cache size: 1024
This is the amount of disk space (in megabytes) to use for cached objects.

Hard disk cache system: aio
This specifies the kind of storage system to use.
aio is the old well-known Squid storage format that has always been there.
aio uses POSIX threads to avoid blocking the main Squid process on disk I/O. (Formerly known as sync-io.)
diskd uses a separate process to avoid blocking the main Squid process on disk I/O.
null Does not use any storage. Ideal for Embedded/Headless.

Hard disk cache location: /var/squid/cache
This is the directory where the cache will be stored. (Note: do not end with a /). If you change the location, squid needs to make a new cache. This could take a while.

Memory cache size: 128
This is the amount of physical RAM (in megabytes) to be used for negative cache and in-transit objects. The value should not exceed more than 80% of the installed RAM. The minimum value is 1MB.

Maximum object size: 0
Objects smaller than the size specified (in kilobytes) will not be saved on disk. The default value is 0, meaning there is no maximum.

Maximum object size: 8192
Objects larger than the size specified (in kilobytes) will not be saved on disk. If you wish to increase speed more than you want to save bandwidth, this should be set to a low value.

Maximum object size in RAM: 32
Objects smaller than the size specified (in kilobytes) will be saved in RAM. Default is 32.

Level 2 subdirectories: 15
Each level 2 directory contains 256 subdirectories, so a value of 256 level 2 directories will use a total of 65536 directories for the hard disk cache. This will significantly slow down the startup process of the proxy service, but can speed up the caching under certain conditions.

Memory replacement policy: Heap GDSF
The memory replacement policy determines which objects are purged from memory when space is needed. The default policy for memory replacement is GDSF.
LRU: Last Recently Used Policy - The LRU policy keeps recently referenced objects, i.e., it replaces the object that has not been referenced for the longest time.
Heap GDSF: Greedy Dual Size Frequency - The heap GDSF policy optimizes object hit rate by keeping smaller, popular objects in cache. It achieves a lower dual hit rate than LFUDA though, since it keeps larger (possibly popular) objects.
Heap LFUDA: Least Frequently Used with Dynamic Aging - The heap LFUDA policy keeps popular objects in cache regardless of their size and thus optimizes hit rate at the expense of hit rate since one large, popular object will prevent many smaller, slightly less popular objects from being cached.
Heap LRU: Last Recently Used - works like LRU, but uses a heap instead.
Note: If using the LFUDA replacement policy, the value of Maximum Object Size should be increased above its default of 32kb to maximize the potential hit rate improvement of LFUDA.

Cache replacement policy: Heap LFUDA
The cache replacement policy decides which objects will remain in cache and which objects are replaced to make space for the new objects. The default policy for cache replacement is LFUDA. Please see the type descriptions specified in the memory replacement policy for additional detail.

Low-water-mark in %: 95
Cache replacement begins when the heap usage is above the low-water mark, and attempts to maintain utilization near the low-water-mark.

High-water-mark in %: 98
As heap utilization gets close to the high-water-mark, object eviction becomes more aggressive.

Do not cache:
Enter each domain or IP address on a new line that should never be cached.

Enable offline mode:
Enabling this option and the proxy server will attempt to validate cached objects. The offline mode gives access to more cached information than the proposed feature would allow (stable cached systems, where the origin server should have been contacted).

Save

58- Ainda na pagina do Squid, clique na aba controle de acesso (Access Control).

Nesta pagina você pode determinar quais sites ou endereços IPs pode ou não ser acessados. Neste exemplo bloqueamos o site google.com, logo os usuários não poderão acessá-lo.

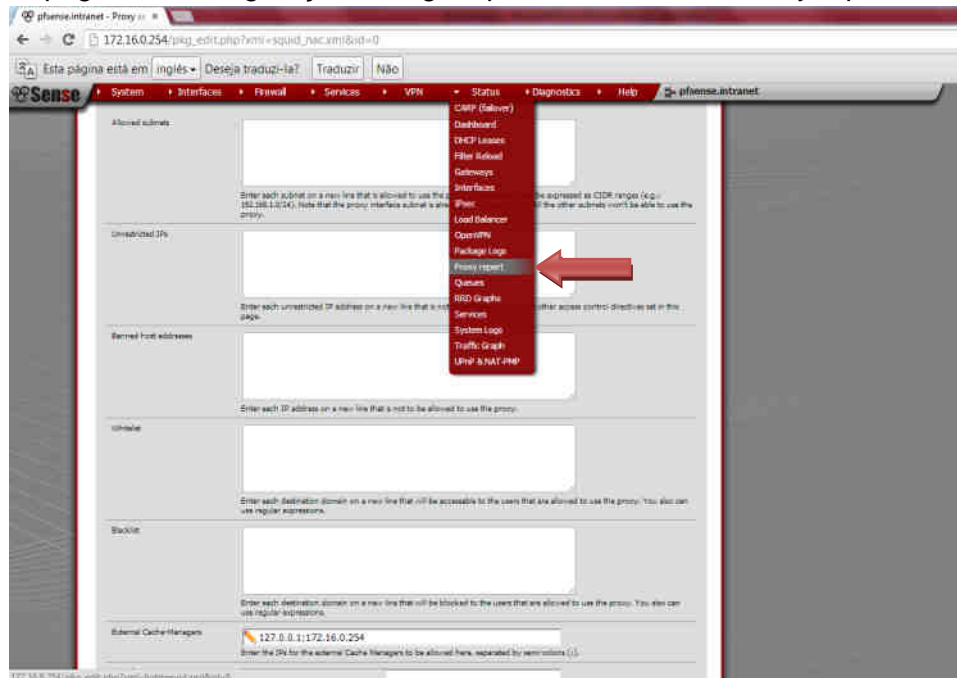
The screenshot shows the 'Proxy server: Access control' configuration page in the pSense.intranet interface. The page has a navigation bar with tabs: General, Advanced Proxy, Cache Manager, Access Control (selected), Traffic Manager, Auth Settings, and Local Users. The 'Access Control' tab is active, displaying several configuration sections:

- Allowed subnets:** A text area for entering allowed subnets. A note states: 'Enter each subnet on a new line that is allowed to use the proxy. The subnets must be expressed as CIDR ranges (e.g.: 192.168.1.0/24). Note that the proxy interface subnet is already an allowed subnet. All the other subnets won't be able to use the proxy.'
- Unrestricted IPs:** A text area for entering unrestricted IP addresses. A note states: 'Enter each unrestricted IP address on a new line that is not to be filtered out by the other access control directives in this page.'
- Banned IP addresses:** A text area for entering banned IP addresses. A note states: 'Enter each IP address on a new line that is not to be allowed to use the proxy.'
- Banned host:** A text area for entering banned host addresses. A red arrow points to this field, which contains the text 'www.google.com'. A note states: 'Enter each destination domain on a new line that will be blocked to the users that are allowed to use the proxy. You also can use regular expressions.'
- External Cache Managers:** A text area for entering the IP addresses of external cache managers. A note states: 'Enter the IP for the external Cache Managers to be allowed here, separated by semicolons (,)'.
- ac allports:** A text area for entering a space-separated list of 'all ports' in addition to the already defined ports 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96, 97, 98, 99. A note states: 'This is a space-separated list of "all ports" in addition to the already defined ports 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96, 97, 98, 99.'
- ac allports:** A text area for entering a space-separated list of ports to allow SSL "CONNECT" in addition to the already defined port 443. A note states: 'This is a space-separated list of ports to allow SSL "CONNECT" in addition to the already defined port 443.'

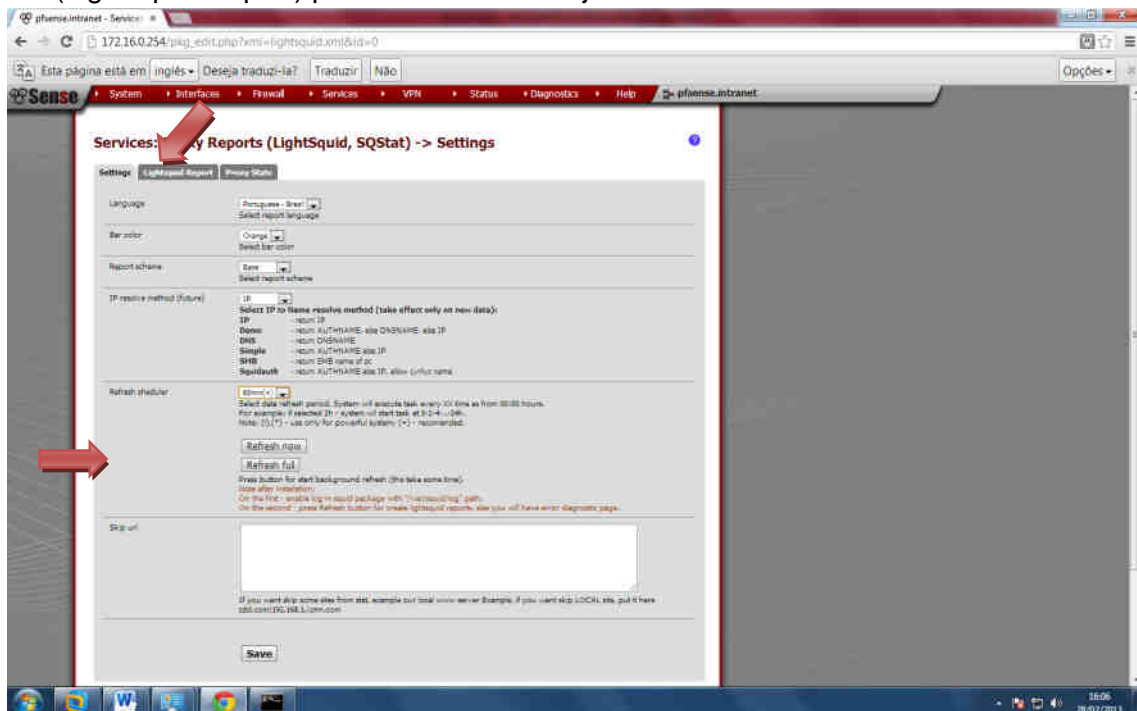
A 'Save' button is located at the bottom of the configuration area. The footer of the page reads: 'pSense is © 2004 - 2011 by BSD Perimeter LLC. All Rights Reserved. [view license]'.

Lightsquid

59- Para entrar na pagina de configuração do Lightsquid vá em Status> Proxy report.



60- Na primeira pagina coloque o idioma para (Português-Brasil).
Para ver os relatórios dos usuários é só clicar em (Refresh now e depois Refresh full).
E depois em (Lightsquid Report) para abrir uma nova janela com os relatórios.



61- Esta é a tela dos relatórios. Para ver mais detalhadamente clique em um dia.

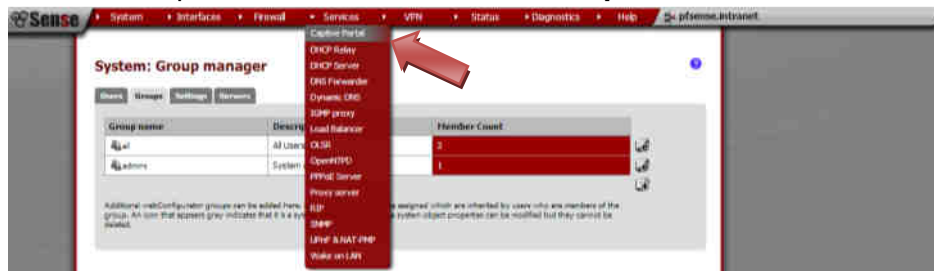


Relatório detalhado.



Configuração Captive Portal (Portal de Autenticação)

62- Para acessar a tela de Captive Portal vá em **Services> Captive Portal**.



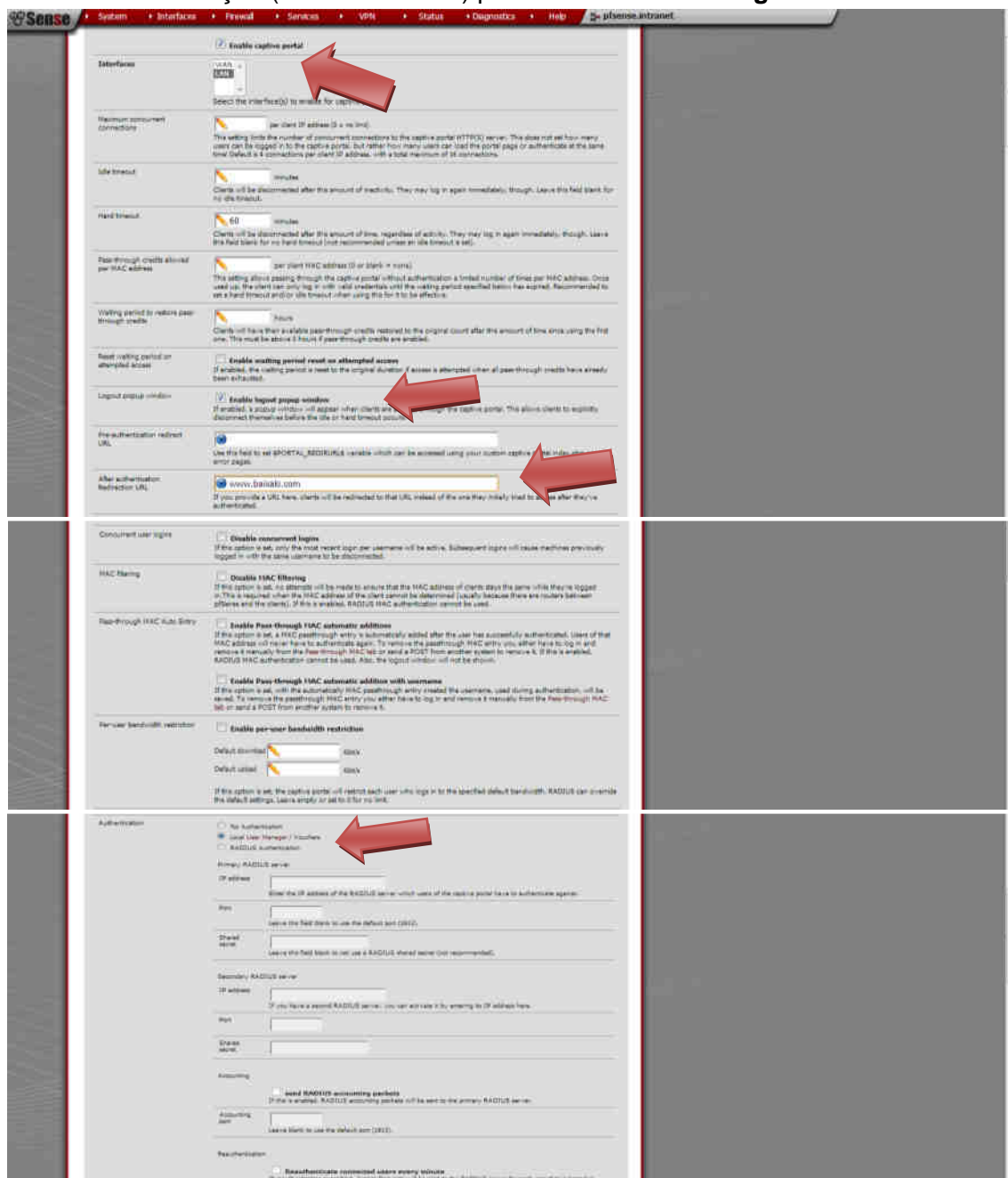
63- Antes de tudo habilite este recurso, marcando “**Enable captive portal**”.

-Depois selecione a interface LAN para que a autenticação seja feita pelos usuários da rede local.

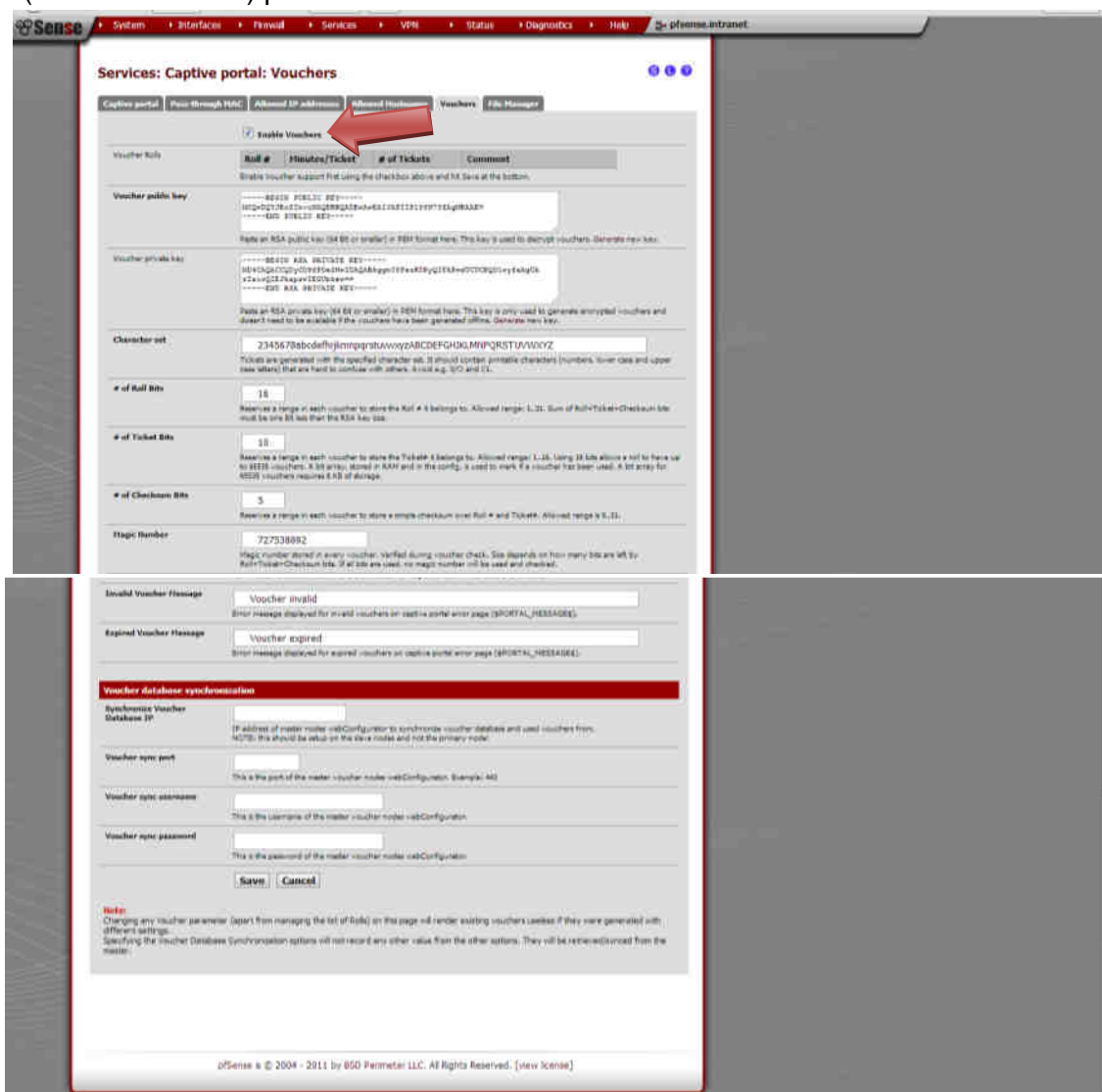
-Ative janela de logout, para que o usuário possa se desconectar, assim os minutos do seu Voucher não serão gastos quando ele não estiver conectado.

-Escolha a pagina que o usuário será redirecionado após a autenticação.

-Altere a forma de autenticação (“Authentication”) para “**Local User Manager/Voucher**”



64- Para criar vouchers ou (Códigos gerados para acesso a internet) vá a aba **Vouchers**. Clique em (Enable vouchers) para habilitar.



Services: Captive portal: Vouchers

☒ Enable Vouchers

Voucher public key:
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA...

Voucher private key:
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEA...

Character set:
23456789abcdefhijklmnopqrstuvwxyzABCDEFGHIJKLMNPQRSTUWXYZ

of Rul Bits:
18

of Ticket Bits:
18

of Checksum Bits:
5

Magic Number:
727538892

Invalid Voucher Message:
Voucher invalid

Expired Voucher Message:
Voucher expired

Voucher database synchronization

Synchronize Voucher Database IP:
[Field]

Voucher sync port:
[Field]

Voucher sync username:
[Field]

Voucher sync password:
[Field]

Save **Cancel**

Note:
Changing any voucher parameter (apart from managing the list of rules) on this page will render existing vouchers useless if they were generated with different settings.
Specifying the Voucher Database Synchronization options will not record any other value from the other options. They will be retrieved/synced from the master.

pSense © 2008 - 2011 by BSD Parameter LLC. All Rights Reserved. [view license]

65- Para criar regras no vouchers Escolha quantos minutos cada ticket poderá acessar e depois quantos tickets deseja, coloque o nome da regra e clique em **Save**.

Sense System Interfaces Firewall Services VPN Status Diagnostics Help

Services: Captive portal: Edit Voucher Rolls

Roll#
Enter the Roll# (0..65535) found on top of the generated/printed vouchers.

Minutes per Ticket
Defines the time in minutes that a user is allowed access. The clock starts ticking the first time a voucher is used for authentication.

Count
Enter the number of vouchers (1..1023) found on top of the generated/printed vouchers. WARNING: Changing this number for an existing Roll will mark all vouchers as unused again.

Comment
Can be used to further identify this roll. Ignored by the system.

Save


66- Para baixar os códigos, volte para aba vouchers e clica no (i) ao lado da regra criada.

Sense System Interfaces Firewall Services VPN Status Diagnostics Help

Services: Captive portal: Vouchers

Captive portal Pass-through MAC Allowed IP addresses Allowed Hostnames **Vouchers** File Manager

☒ Enable Vouchers

Voucher Rolls	Roll #	Minutes/Ticket	# of Tickets	Comment	
	1	3	100	Tempo encerrado	

Create, generate and activate Rolls with Vouchers that allow access through the captive portal for the configured time. Once a voucher is activated, its clock is started and runs uninterrupted until it expires. During that time, the voucher can be re-used from the same or a different computer. If the voucher is used again from another computer, the previous session is stopped.

Voucher public key

```
-----BEGIN PUBLIC KEY-----
MCQwDQYJKoZIhvcNAQEBBQADAwEAIAJALRQ71fe7nWzAgMBAAE=
-----END PUBLIC KEY-----
```

Paste an RSA public key (64 Bit or smaller) in PEM format here. This key is used to decrypt vouchers. Generate new key.

Voucher private key


```
-----BEGIN RSA PRIVATE KEY-----
MD8CAQACCQCyk0Sx3u51gwIDAQABAgghjWNSAKEMukQIFAFWYtkcBQDK30oDAgR0
UbsRaqUAWa3MlQIFAIO66KI=
-----END RSA PRIVATE KEY-----
```

Paste an RSA private key (64 Bit or smaller) in PEM format here. This key is only used to generate encrypted vouchers and doesn't need to be available if the vouchers have been generated offline. Generate new key.

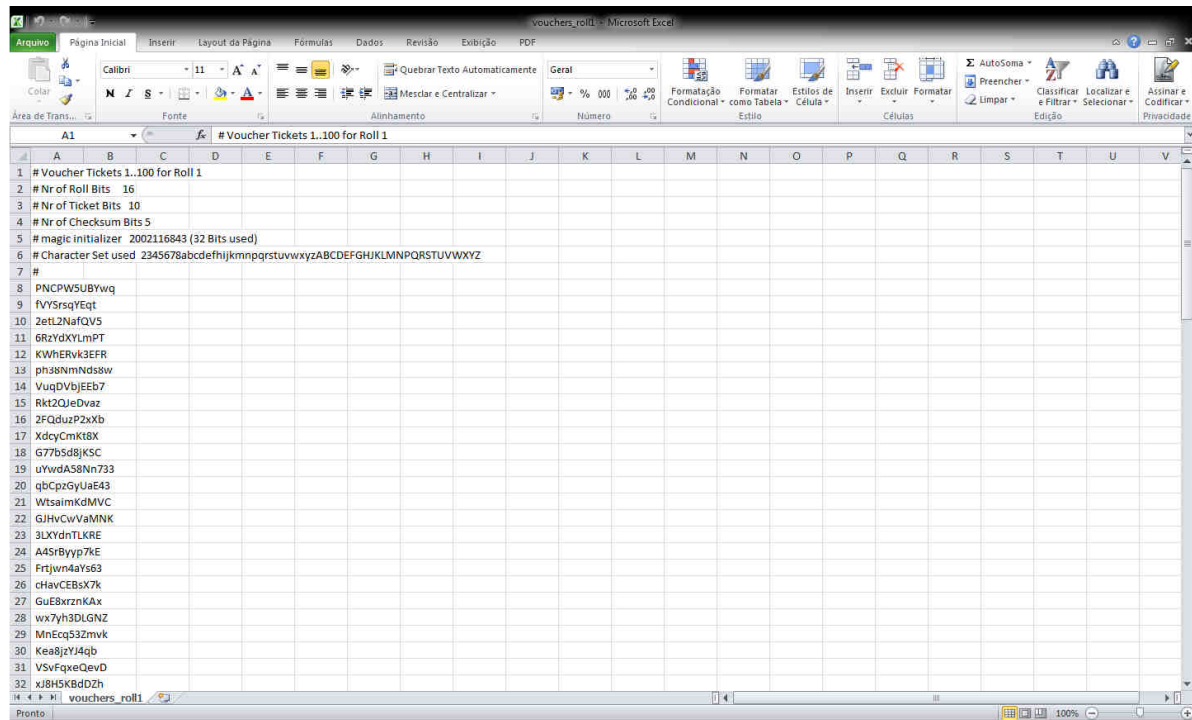
Character set

Tickets are generated with the specified character set. It should contain printable characters (numbers, lower case and upper case letters) that are hard to confuse with others. Avoid e.g. 0/O and l/1.

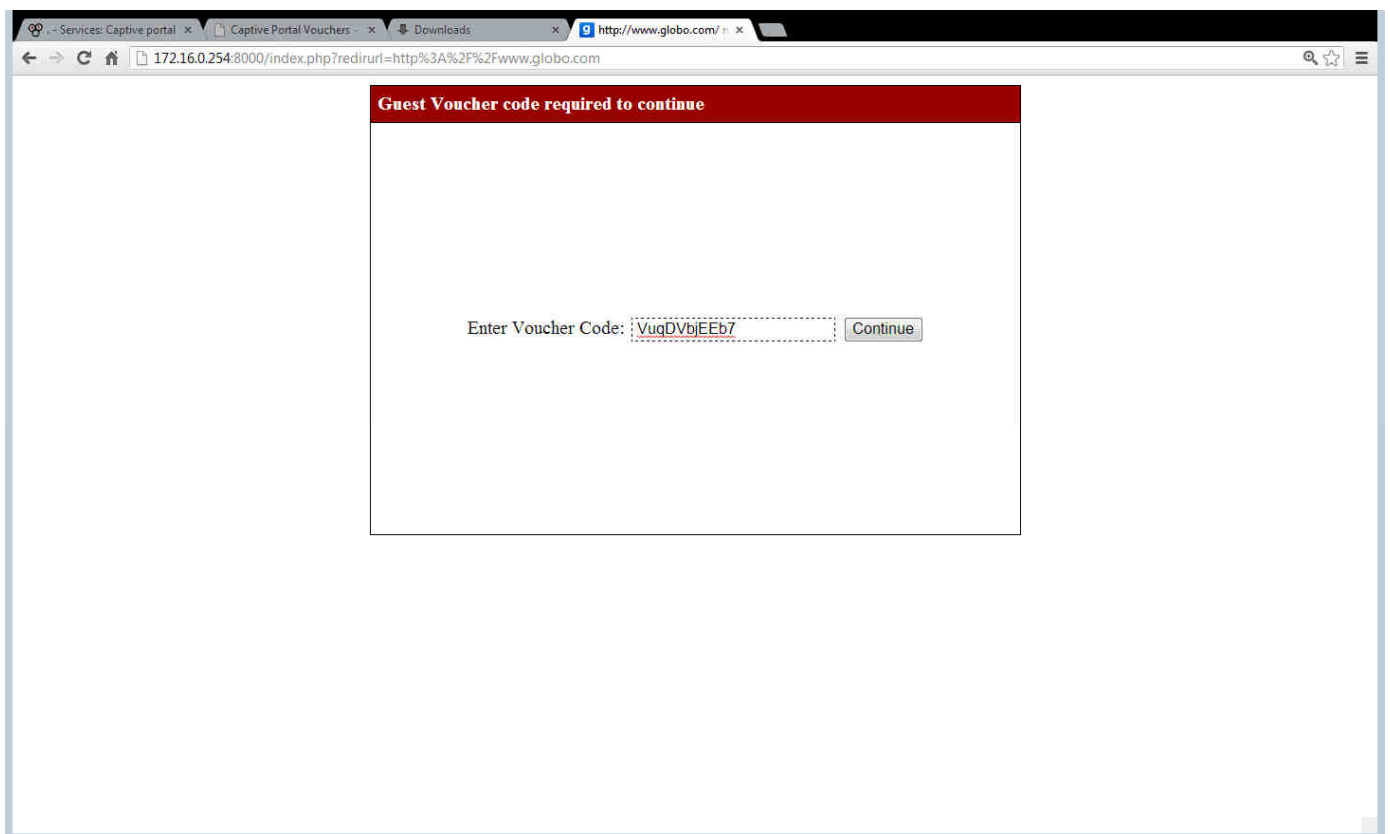
of Roll Rols

 vouchers_roll1.csv

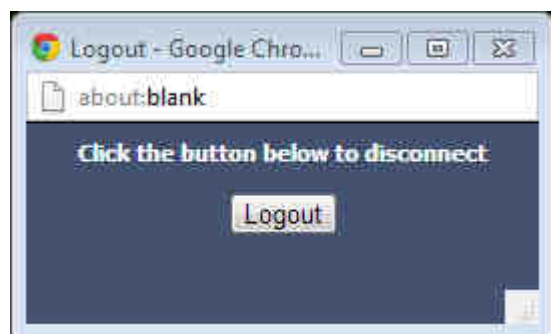
Códigos baixados



67- Tente acessar qualquer site, e uma janela como essa aparecerá, pedindo o Voucher. Insira um dos Vouchers criados no campo indicado e clique em continue.



68- Você será redirecionado para a página configurada pelo Captive portal.



E uma janela Pop-up será aberta para que seja possível fazer Logout, fazendo com que não se gaste os minutos do voucher cedido.