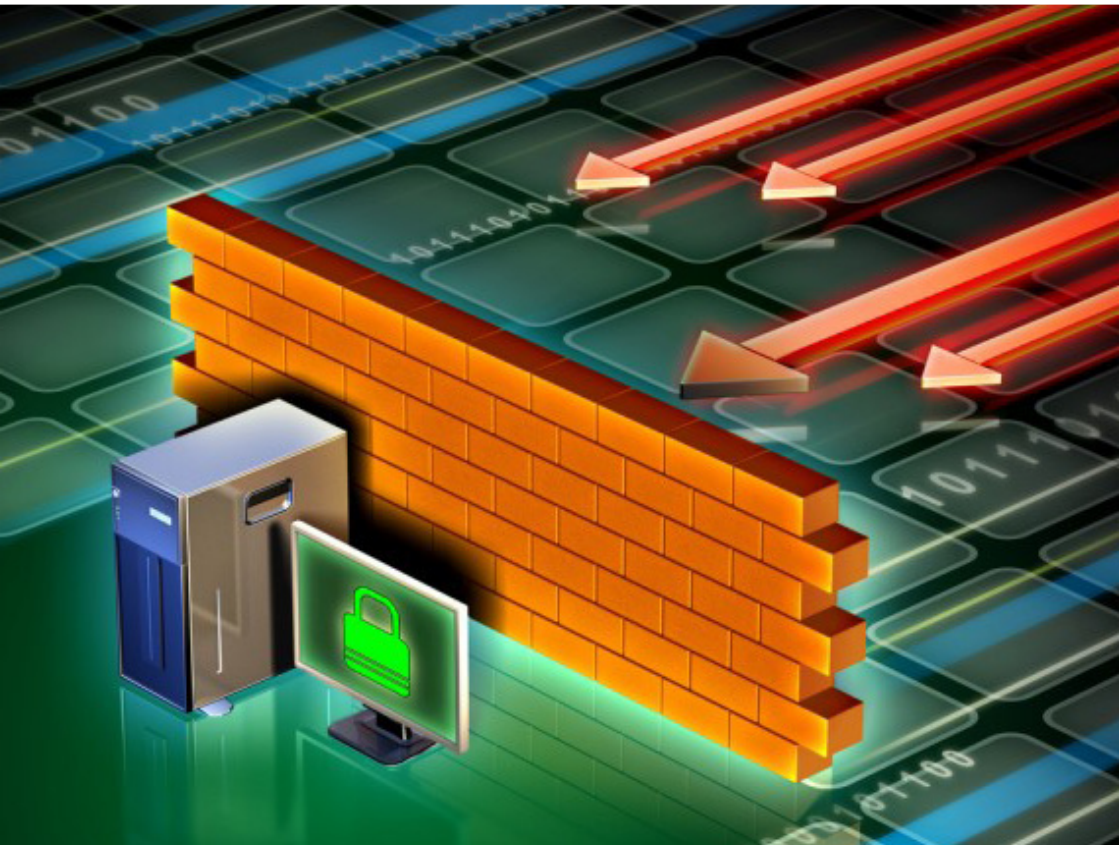


Introdução ao pfSense: implementando um firewall



*Empresa Brasileira de Pesquisa Agropecuária
Embrapa Informática Agropecuária
Ministério da Agricultura, Pecuária e Abastecimento*

Documentos 139

Introdução ao pfSense: implementando um firewall

Jorge Luiz Corrêa

Embrapa Informática Agropecuária

Av. André Tosello, 209 - Barão Geraldo
Caixa Postal 6041 - 13083-886 - Campinas, SP
Fone: (19) 3211-5700
www.embrapa.br/informatica-agropecuaria
SAC: www.embrapa.br/fale-conosco/sac/

Comitê de Publicações

Presidente: *Giampaolo Queiroz Pellegrino*

Secretária: *Carla Cristiane Osawa*

Membros: *Adhemar Zerlotini Neto, Stanley Robson de Medeiros Oliveira, Thiago Teixeira Santos, Maria Goretti Gurgel Praxedes, Adriana Farah Gonzalez, Neide Makiko Furukawa, Carla Cristiane Osawa*

Membros suplentes: *Felipe Rodrigues da Silva, José Ruy Porto de Carvalho, Eduardo Delgado Assad, Fábio César da Silva*

Supervisor editorial: *Stanley Robson de Medeiros Oliveira, Neide Makiko Furukawa*

Revisor de texto: *Adriana Farah Gonzalez*

Normalização bibliográfica: *Maria Goretti Gurgel Praxedes*

Editoração eletrônica: *Neide Makiko Furukawa*

Imagem capa: <<http://betanews.com/2016/03/30/firewalls-and-network-security/>>

1ª edição

publicação digitalizada 2016

Todos os direitos reservados.

A reprodução não autorizada desta publicação, no todo ou em parte, constitui violação dos direitos autorais (Lei nº 9.610).

Dados Internacionais de Catalogação na Publicação (CIP) Embrapa Informática Agropecuária

Corrêa, Jorge Luiz.

Introdução ao pfSense: implementando um firewall / Jorge Luiz Corrêa. - Campinas : Embrapa Informática Agropecuária, 2016.

76 p. : il. - (Documentos / Embrapa Informática Agropecuária, ISSN 1677-9274 ; 139).

1. Firewall. 2. Segurança. 3. Rede. 4. pfSense. I. Título. II. Embrapa Informática Agropecuária. III. Série.

CDD (21. ed.) 004.678

© Embrapa 2016

Autor

Jorge Luiz Corrêa

Cientista da Computação, mestre em Ciência da Computação
Analista da Embrapa Informática Agropecuária, Campinas, SP

Apresentação

Em tempos de alta conectividade, ascensão da internet das coisas, substituição de diversas atividades manuais por sistemas automatizados e online e uma busca cada vez maior pela execução de serviços digitalmente, a manutenção de uma boa conectividade tornou-se, mais do que nunca, de grande relevância. E, neste contexto, a conectividade vem acompanhada de um outro conceito tão importante quanto ela própria: a segurança. Conectar uma rede à internet representa, atualmente, um risco que muitas pessoas não têm dimensionamento, principalmente caso esta rede dê acesso a informações sensíveis e de valor.

A conectividade de uma rede é mantida por equipamentos dedicados a esta atividade, sendo também responsáveis por tarefas como a ligação física, segmentação lógica, encaminhamento e roteamento de pacotes. Ademais destas atribuições, consideradas básicas, para o estabelecimento de uma boa conectividade, estes equipamentos também lidam com conceitos como a utilização de redundância a fim de evitar a criação de um Single Point of Failure (SPOF) - ponto único de falha, alta disponibilidade para que o sistema opere sem interrupções e diminuição do Mean Time to Repair (MTTR) - tempo médio de reparação.

Os sistemas de firewall são um dos componentes de uma infraestrutura de rede para fornecimento de conectividade. São parte essencial para o estabelecimento de um ambiente seguro, junto de outras técnicas e ferramentas, sendo responsáveis essencialmente pela implementação de políticas de segurança relativas à filtragem de pacotes. No entanto, além de sua atividade primária, um firewall pode desempenhar outros papéis como o de um sistema de Proxy para navegação WEB, servidor de DNS, DHCP e controlador de redes sem fio, por exemplo.

Este documento apresenta uma introdução ao pfSense, um sistema de firewall que contempla todas estas características, sendo de grande importância para a melhoria da segurança no fornecimento de conectividade com a internet. O pfSense permite o estabelecimento de um filtro de pacotes com diversos outros serviços, utilizando redundância, aumentando assim a disponibilidade da infraestrutura e o MTTR, graças as suas características de backup, sincronização e alta disponibilidade.

Silvia Maria Fonseca Silveira Massruhá

Chefe-geral

Embrapa Informática Agropecuária

Sumário

1 Firewall pfSense	11
1.1 Pré-requisitos.....	11
2 Principais usos	12
3 Versões	13
4 Plataformas de execução	13
5 Compatibilidade de hardware	14
6 Instalação	15
6.1 Instalação básica	16
6.2 <i>Wizard</i> para configuração na interface web	28
7 Características e configurações básicas	32
7.1 Arquivo de configuração XML.....	32
7.2 Perda de acesso.....	33
7.3 Interfaces	35
7.3.1 Interface física.....	35
7.3.2 Interface virtual (VLANs)	35
7.4 Backup e restauração.....	35
7.4.1 Backup utilizando a interface web	36
7.4.2 Backup utilizando wget e cron.....	37
7.4.3 Backup utilizando SCP	37
7.4.4 Restauração utilizando a interface web.....	38
7.4.5 Restauração a partir do histórico de configuração	38
7.4.6 Restauração utilizando o Pre-Flight Installer	39

7.5	Firewall - filtragem e encaminhamento	40
7.5.1	Regras de filtragem	40
7.5.2	Regras de NAT	40
7.5.2.1	Criação de regra de Port Forward usando Filter Rule Association.....	41
7.5.2.2	Criação de regra de Outbound com Manual outbound NAT Rule generation	42
7.5.2.3	NAT 1:1	43
7.5.3	<i>Aliases</i>	44
7.5.4	Ordem de processamento dos NATs e regras de filtragem	44
7.5.5	Roteamento	46
7.6	Virtual LANs (VLANs)	48
7.7	Captive Portal	50
7.8	Instalação de pacotes	53
7.9	Serviços básicos	54
7.9.1	DHCP.....	54
7.9.2	DNS.....	55
7.10	Alta disponibilidade com CARP	56
7.10.1	CARP.....	56
7.10.2	pfsync	59
7.10.3	XML-RPC	60
7.11	Atualização	62
7.11.1	Atualização via interface web.....	62
7.11.2	Atualização via console.....	64
7.11.3	Atualização de sistemas com alta disponibilidade (master e slave).....	65
8	Dicas e <i>troubleshooting</i>	66
8.1	Problema ao realizar download de pacotes.....	67
8.2	Interfaces de rede Broadcom em servidores Dell.....	67
8.3	Captive Portal quando utilizando arquivo WPAD.....	67

8.4	Monitoramento com ping em redes com Captive Portal e alta disponibilidade	68
8.5	Problema com os relatórios do SARG (pacote para geração de relatórios dos logs do Squid)	68
8.6	Logs do Squid Proxy	69
8.7	Utilização de tabelas para thresholds em regras de filtragem ..	70
8.8	Configuração da time zone sem efeito	70
8.9	Tabela de proteção contra tentativas de login	71
8.10	Utilização do CARP VIP em ambientes com Squid Proxy	72
9	Exercícios	73
9.1	Instalação e inicialização básica	73
9.2	Navegação básica	73
9.3	Remoção de todas as regras	74
9.4	DHCP e DNS	74
9.5	Pacotes	74
9.6	CARP na LAN + pfSync + XML-RPC Sync	74
3	Referências	76
4	Literatura recomendada	76

Introdução ao pfSense: implementando um firewall

Jorge Luiz Corrêa

1 Firewall pfSense

O pfSense é uma distribuição baseada no FreeBSD dedicada exclusivamente a ser um firewall. Seu código é aberto e pode ser obtido no GitHub¹.

O pfSense oferece uma interface web para configuração de quase todos os parâmetros de um firewall. Algumas poucas opções devem ser configuradas via linha de comando.

Este conteúdo foi baseado no Guia Definitivo do pfSense e não abrange extensivamente todas as funcionalidades do sistema. Este tutorial objetiva, além da introdução do sistema e seus principais conceitos, avançar em pontos específicos de um sistema de filtragem de pacotes. Espera-se que o conteúdo aqui exposto possibilite o estabelecimento de grande parte dos sistemas de firewall utilizados, sem muitas peculiaridades.

1.1 Pré-requisitos

Para um melhor aproveitamento deste material, é desejável ter conhecimentos nos seguintes tópicos:

- Pilha de protocolos TCP/IP.

¹ Disponível em: <<https://github.com/pfsense/>>. Acesso em: 16 nov. 2015.

- Firewall e tipos de regra (filtragem e NAT).
- Endereçamento (CIDR) e roteamento IP.
- 802.1Q (Vlan).
- FreeBSD.

Este material objetiva apresentar as principais funcionalidades da ferramenta pfSense, de modo que fica subentendido que alguns tópicos relativos a sistemas de firewall já são de conhecimento do leitor. Embora o material se desenvolva de uma maneira didática quanto aos conceitos sobre firewall, o foco está na utilização da ferramenta e não no funcionamento deste tipo de sistema.

2 Principais usos

Dentre as principais aplicações do pfSense estão:

- **Firewall de perímetro:** é a aplicação mais comum onde o firewall possui interface(s) ligada(s) à WAN e interface(s) ligada(s) à LAN, separando estes dois segmentos. Este tipo de firewall também pode executar protocolos de roteamento do lado da WAN, como BGP.
- **Roteador:** casos em que o pfSense é utilizado para roteamento entre redes, porém, ainda delegando a filtragem geral ou parcial a um firewall de perímetro. Um dos casos é a interligação de redes internas segmentadas em VLANs, onde o pfSense faria o papel de roteador entre cada uma dessas redes.
- **Wireless Access Point:** é comum a utilização do pfSense como ponto de acesso sem fio, para fornecer conectividade a dispositivos móveis, além de todas as funcionalidades de filtragem de pacotes.
- **Propósitos específicos:** são outros usos, menos comuns que os anteriores, que incluem serviço de Virtual Private Network (VPN), servidor de DNS, inspeção de pacotes (*sniffer* em pontos de rede para diversas funcionalidades), servidor DHCP, servidor Proxy, dentre outros.

3 Versões

O pfSense recebe diversas atualizações que vão desde correções na interface, pacotes, sistema, até no kernel do sistema FreeBSD. O projeto tenta acompanhar o desenvolvimento da versão do FreeBSD. Por exemplo, o *release 2.2.5* utiliza o FreeBSD 10.1-RELEASE-p24.

As atualizações podem ser obtidas a partir do próprio firewall, na interface web, e prontamente aplicadas. Também podem ser baixadas como novas versões de *firmware* e aplicadas ao sistema, enviando-a pela interface, assim como em roteadores e outros equipamentos que suportam atualização de *firmware*.

Seja qual for o modo de atualização é importante planejá-la, conforme será discutido mais adiante, principalmente se o sistema operar em alta disponibilidade, com um *master* e um *slave*.

4 Plataformas de execução

O pfSense pode ser utilizado de três maneiras diferentes em relação ao tipo de implantação.

- **Live CD (incluindo USB):** permite a execução sem utilizar um disco com uma instalação, diretamente da mídia.
- **Instalação completa:** o sistema é instalado no disco tornando-se persistente no hardware em questão. Não é permitido *dual boot* e todo o disco é sobrescrito.
- **Embarcado:** a versão embarcada é utilizada em hardware que utilizam cartões Compact Flash como disco. Uma vez que estes cartões possuem um número limitado de escritas e leituras, a versão embarcada executa em somente leitura no Compact Flash e com permissões de escrita e leitura em áreas de memória que atuam como disco (RAM disk).

5 Compatibilidade de hardware

O pfSense é compatível com qualquer hardware que é suportado pela versão do FreeBSD do *release* sendo utilizado. Assim sendo, o melhor lugar para se obter informações de compatibilidade com a *release* é verificar a *FreeBSD Hardware Notes* desta².

Conforme mencionado, diversas placas são compatíveis com o pfSense desde que sejam compatíveis com a *release* do FreeBSD sendo utilizado. No entanto, por se tratar de um sistema de firewall, a estabilidade da placa e a performance são dois itens muito importantes. Neste sentido, é altamente recomendado a utilização de placas Intel Pro/100 e Intel Pro/1000 pelo motivo que a própria Intel é quem escreve e suporta os drivers destes modelos para o FreeBSD. Em um contra exemplo, placas Realtek são propensas a apresentarem problemas pois normalmente não suportam corretamente a utilização de VLANs, modo promíscuo para utilização de *bridges*, entre outras funcionalidades, além da performance ser bastante baixa. Também não é recomendada a utilização de placas de rede USB, principalmente devido à performance.

Em relação às configurações mínimas de hardware, os atuais computadores oferecem recursos suficientes para o estabelecimento de um firewall capaz de gerar grande *throughput*. O pfSense é capaz de executar a partir de um processador de 200 MHz e com 256 MB de memória. No caso da instalação completa, no disco rígido, é necessário no mínimo 1 GB de espaço.

A medida considerada mais importante na relação hardware/performance quando se estabelece um firewall é a *Packets per Second* (PPS). Um hardware conseguirá encaminhar uma quantidade máxima de pacotes por segundo e, dependendo do tamanho de pacote, isso representará uma determinada *vazão* (*throughput*) em bits. Isto ocorre pois o encaminhamento dos pacotes depende de interrupções geradas pela interface. Assim, é dependente da velocidade do barramento da placa de rede, da placa-mãe e da CPU.

Dependendo do tipo de pacote gerado na rede, obtém-se determinado *throughput*. Por exemplo, se um hardware consegue encaminhar 500.000

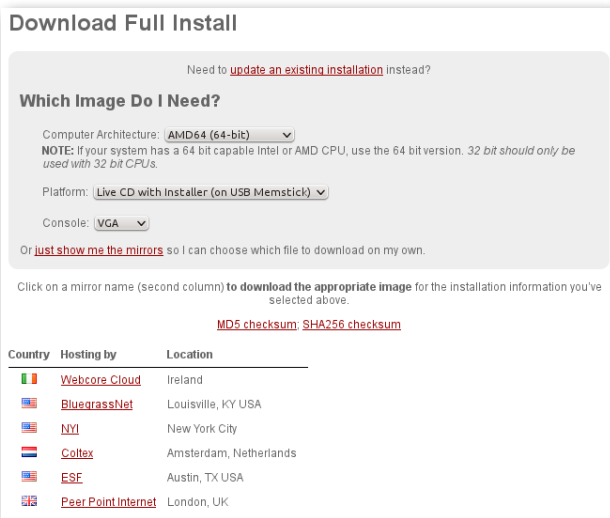
² Disponível em: <<https://www.freebsd.org/releases/>>. Acesso em 16 nov. 2016.

pps, com tamanho médio de 500 bytes, este hardware terá um *throughput* de 1,87 Gbps. Logo, o dimensionamento de um firewall em termos de hardware vai depender da vazão que deve ser alcançada. A título de exemplo, um hardware com um processador Pentium 4 de 3 GHz ou mais rápido, com interfaces de rede em barramento PCI-e, consegue gerar um *throughput* de 1 Gbps.

6 Instalação

O pfSense deve ser obtido na área de downloads do site oficial³.

No site, escolher a versão desejada. Neste documento, será utilizada uma versão amd64, sendo baixada no formato Live CD com o instalador para USB Memstick, o que permitirá a geração de um *pendrive* para instalação no servidor. O console escolhido é o VGA (console VGA é usado em hardware que possui um monitor e um teclado enquanto o console serial é usado em um hardware que não possui monitor e teclado, apenas uma porta serial, por onde o sistema será acessado inicialmente), conforme a Figura 1.



Download Full Install

Need to [update an existing installation](#) instead?

Which Image Do I Need?

Computer Architecture: **AMD64 (64-bit)**

NOTE: If your system has a 64 bit capable Intel or AMD CPU, use the 64 bit version. 32 bit should only be used with 32 bit CPUs.

Platform: **Live CD with Installer (on USB Memstick)**

Console: **VGA**

Or [just show me the mirrors](#) so I can choose which file to download on my own.

Click on a mirror name (second column) to **download the appropriate image** for the installation information you've selected above.

[MD5 checksum](#) [SHA256 checksum](#)







Country	Hosting by	Location
	Webcore Cloud	Ireland
	BluegrassNet	Louisville, KY USA
	NYI	New York City
	Coltex	Amsterdam, Netherlands
	ESF	Austin, TX USA
	Peer Point Internet	London, UK

Figura 1. Site de download do pfSense.

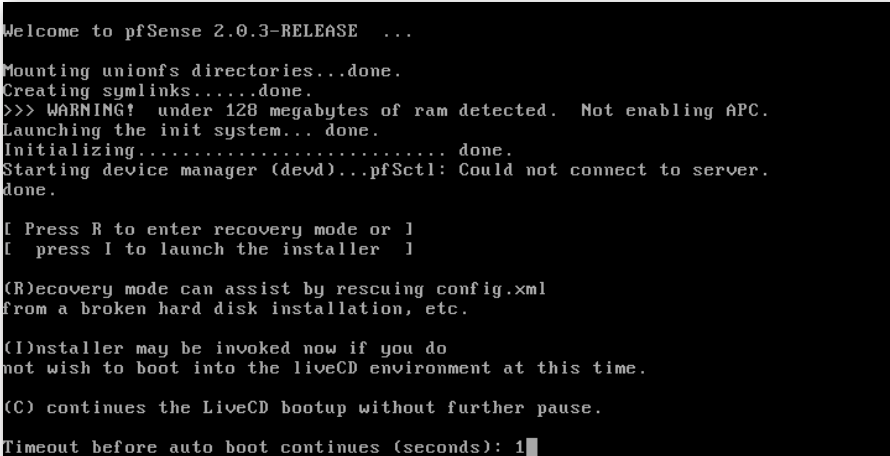
³ Disponível em: <<https://www.pfsense.org/download/>>.

Concluído o download, deve-se gerar o pendrive a partir do utilitário 'dd', comum nos sistemas *NIX. Supondo que o dispositivo onde o pendrive está conectado seja o /dev/sdz, executar:

```
$ gzip -dc pfSense-memstick-2.2.3-RELEASE-amd64.img.gz | sudo dd of=/dev/sdz bs=1M
[sudo] password for user:
0+7416 records in
0+7416 records out
243048448 bytes (243 MB) copied, 26.3313 s, 9.2 MB/s
$
```

6.1 Instalação básica

Ao inicializar o hardware com a mídia contendo o pfSense, o *boot* oferecerá algumas opções, dentre elas a possibilidade de recuperar um sistema instalado, instalar um novo ou continuar em modo LiveCD (Figura 2).



```
Welcome to pfSense 2.0.3-RELEASE ...

Mounting unionfs directories...done.
Creating symlinks.....done.
>>> WARNING! under 128 megabytes of ram detected. Not enabling APC.
Launching the init system... done.
Initializing..... done.
Starting device manager (devd)...pfSctl: Could not connect to server.
done.

[ Press R to enter recovery mode or ]
[ press I to launch the installer ]

(R)ecovery mode can assist by rescuing config.xml
from a broken hard disk installation, etc.

(I)nstaller may be invoked now if you do
not wish to boot into the liveCD environment at this time.

(C)ontinues the LiveCD bootup without further pause.

Timeout before auto boot continues (seconds): 1
```

Figura 2. Inicialização do pfSense com opções para recuperação de um sistema, instalação ou operação em LiveCD.

Selecionando a opção (I) será iniciada a instalação do sistema no disco. Os passos a serem seguidos são mostrados nas Figuras de 3 a 16, em sequência.



Figura 3. Aceitar as configurações padrão de vídeo, tela e teclado (pode-se customizá-las, caso necessário).

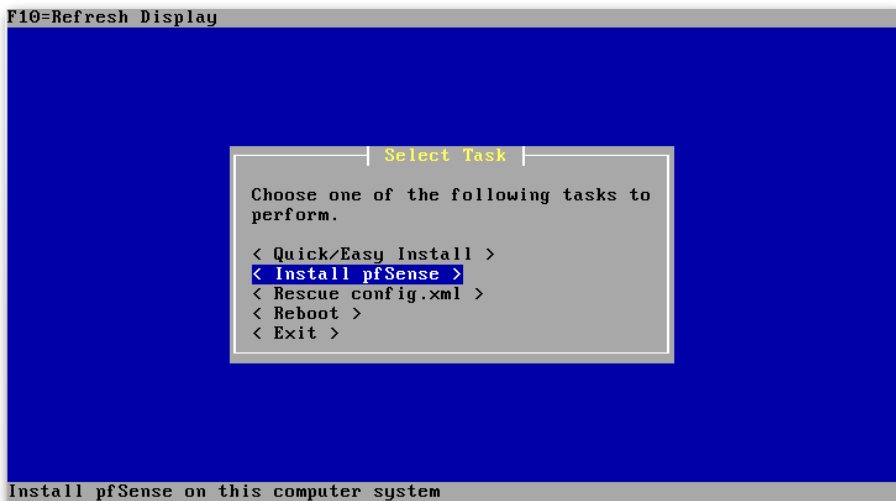


Figura 4. Escolher a opção de instalação.

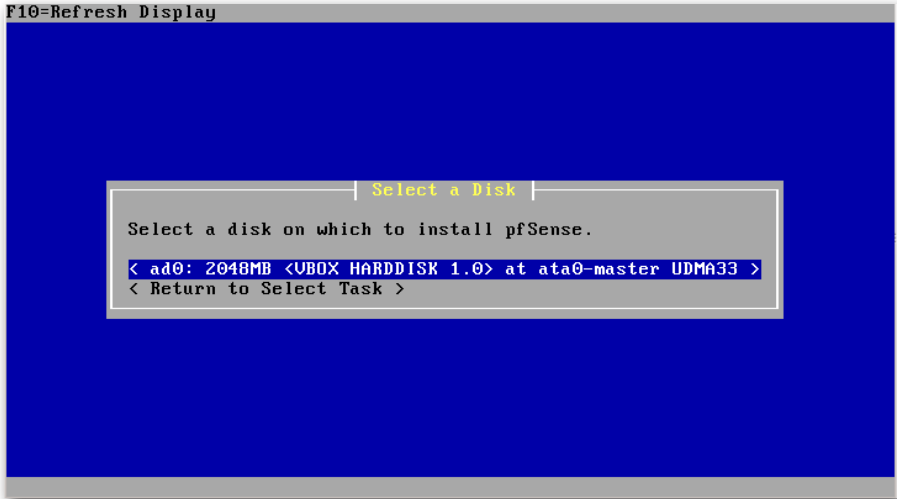


Figura 5. Escolher o disco onde o pfSense será instalado. Caso se utilize RAID o device deverá aparecer nesta lista.

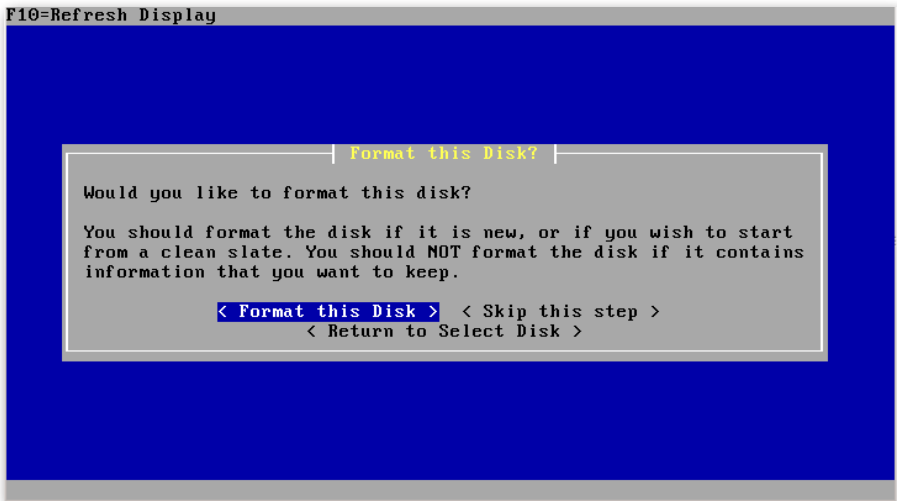


Figura 6. Escolher a opção para que o disco seja formatado.

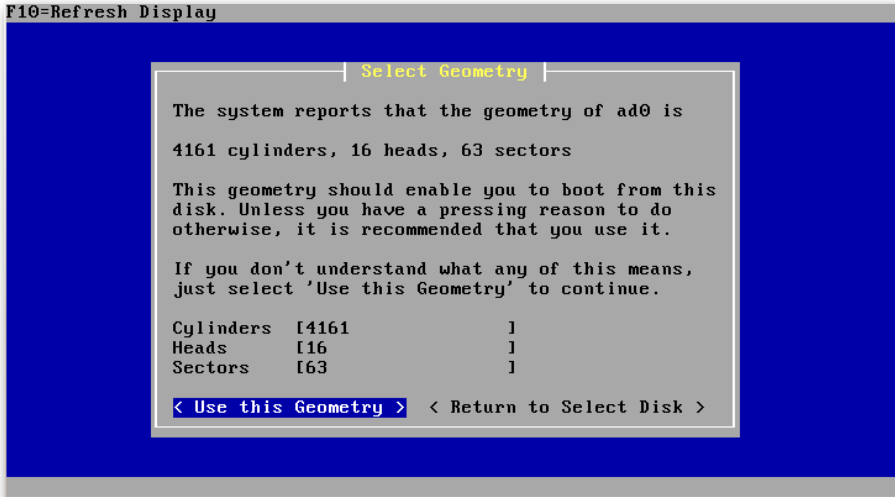


Figura 7. Escolher a opção padrão para geometria do disco.

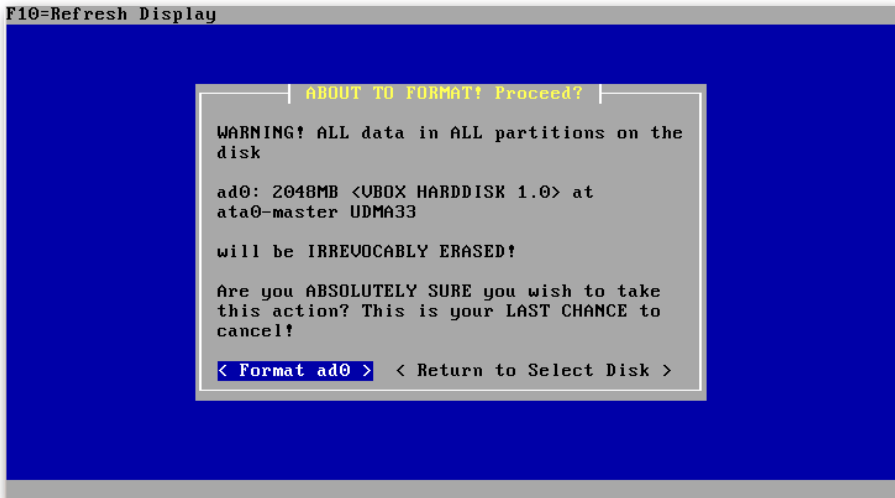


Figura 8. Confirmar a formatação.

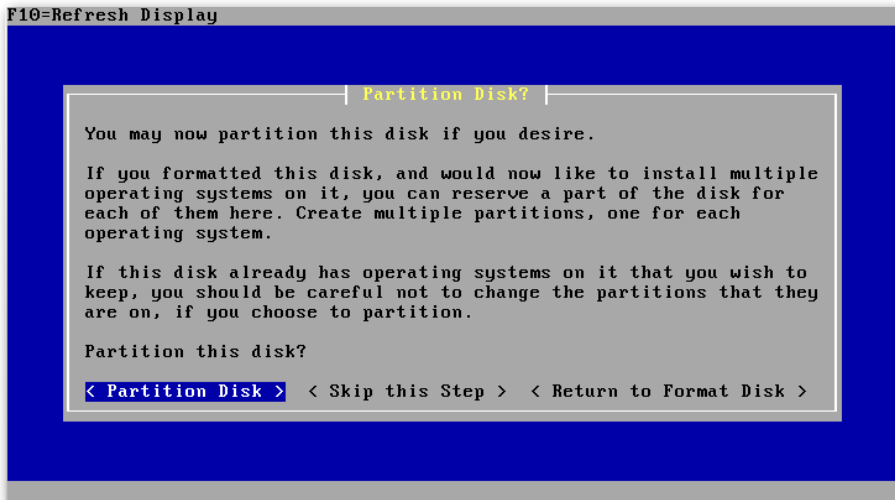


Figura 9. Escolher a opção de particionamento do disco.

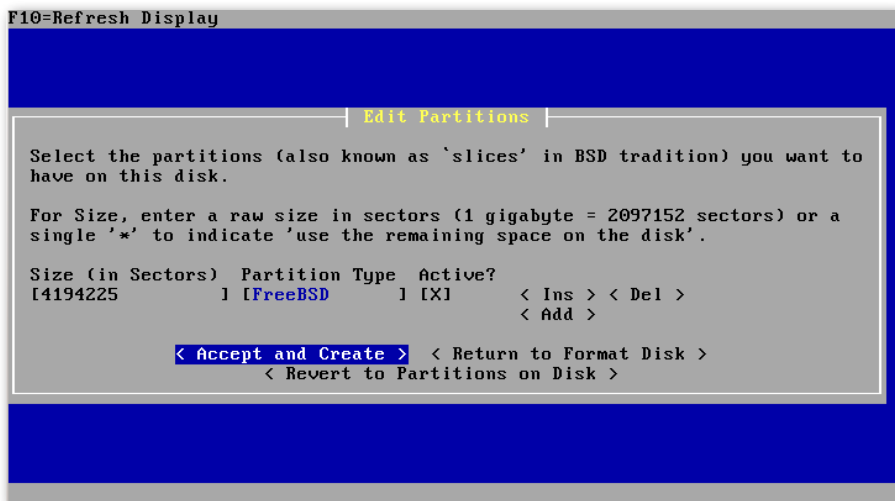


Figura 10. Aceitar a opção padrão. O pfSense não permite dual boot, ou seja, ele utilizará o disco todo.

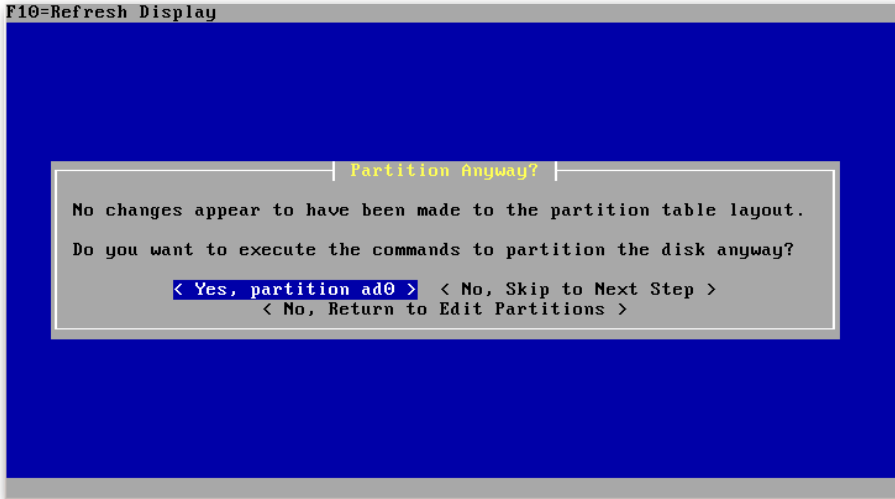


Figura 11. Confirmar o particionamento.

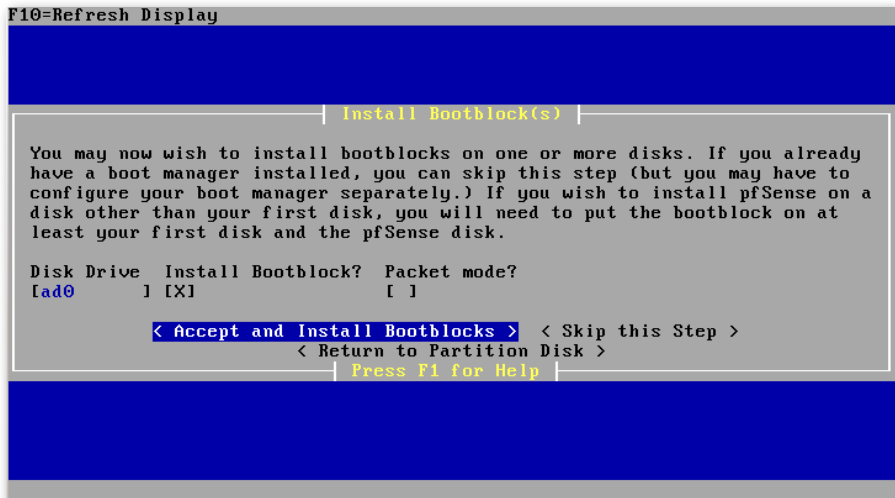


Figura 12. Aceitar a opção de instalação de bootblocks, ou seja, um gerenciador de boot.

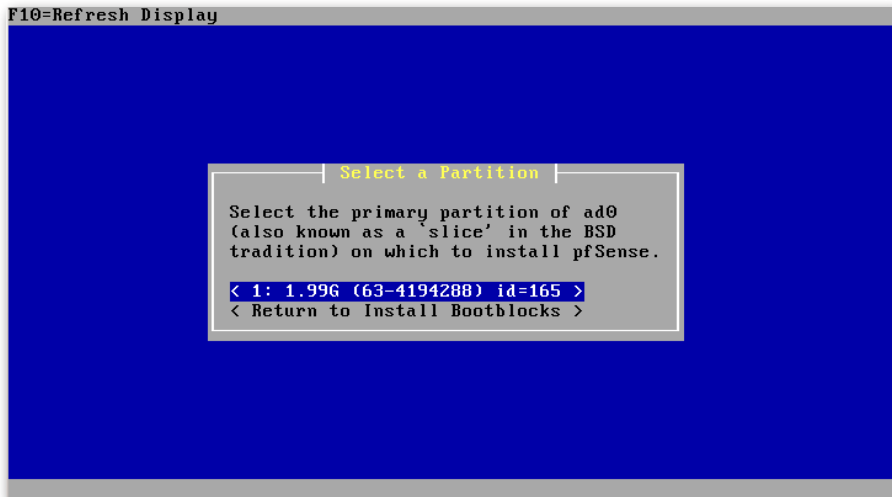


Figura 13. Escolher a partição onde o gerenciador de boot será instalado.

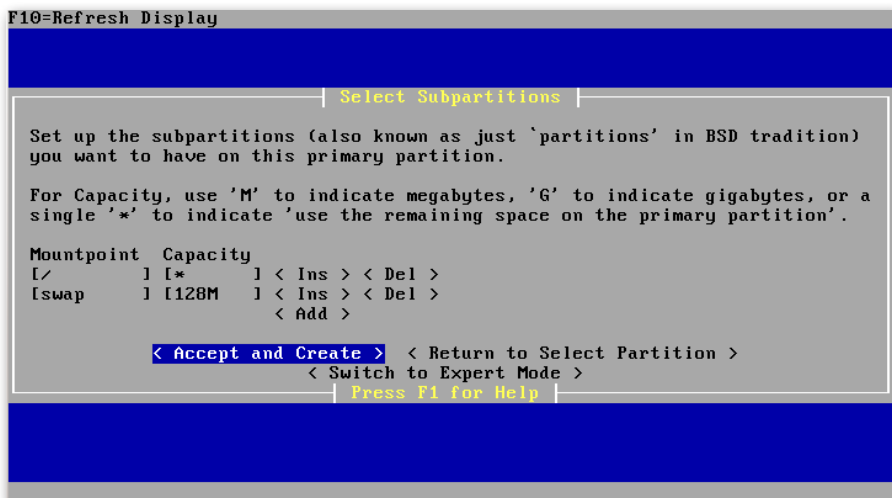


Figura 14. Aceitar as configurações padrão para a definição de subpartições, tais como a de swap.

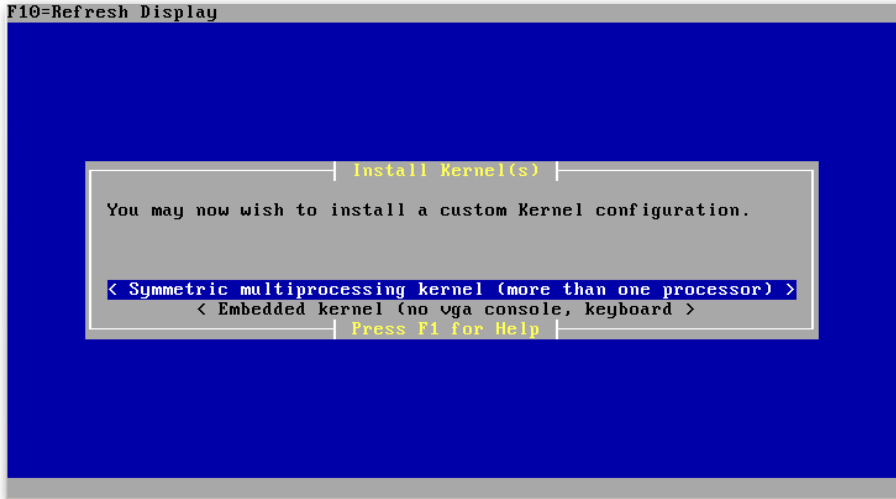


Figura 15. Escolher a opção de kernel SMP (multiprocessing).

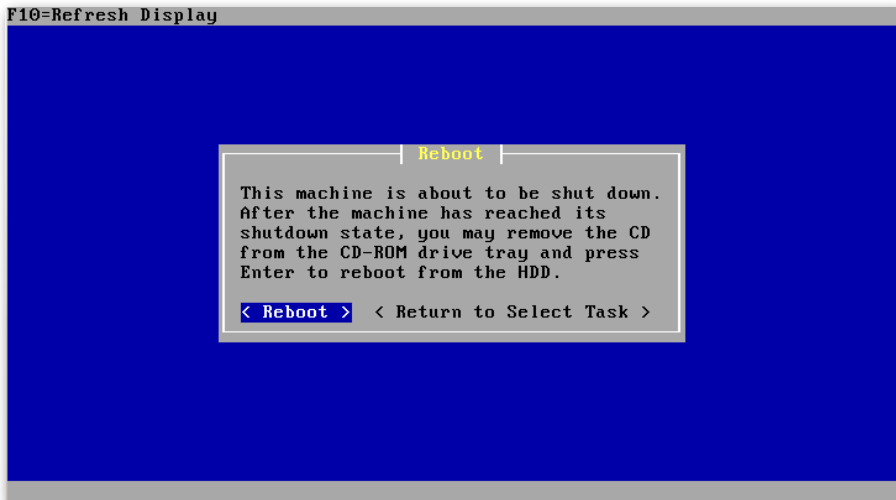


Figura 16. Reinicializar o sistema.

Após a reinicialização já com o sistema instalado, a primeira tarefa solicitada pelo pfSense é a configuração de alguns parâmetros das interfaces. O primeiro deles é sobre a utilização de VLANs, pois em um ambiente onde se usa pacotes com TAG, seria necessário criar a configuração de camada 2 para que estes pudessem ser recebidos. Neste caso, não serão informadas VLANs (Figura 17).

```
External config loader 1.0 is now starting... ad@s1b
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  08:00:27:ce:d6:be  (up) Intel(R) PRO/1000 Legacy Network Connection 1.0.4
em1  08:00:27:82:b3:61  (up) Intel(R) PRO/1000 Legacy Network Connection 1.0.4
em2  08:00:27:0c:9f:87  (up) Intel(R) PRO/1000 Legacy Network Connection 1.0.4
em3  08:00:27:5d:f1:e5  (up) Intel(R) PRO/1000 Legacy Network Connection 1.0.4

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 [yn]? █
```

Figura 17. Configuração de parâmetros das interfaces (VLANs).

Em seguida, será necessário informar ao menos uma interface de rede para que o processo de configuração continue. É solicitada a interface que funcionará como WAN, ou seja, a interface de saída do firewall para internet ou *gateway* seguinte, no lado externo da rede. Conforme a lista de interfaces mostrada na Figura 17, a interface em0 será atribuída para a WAN (Figura 18).

```
*NOTE*  pfSense requires *AT LEAST* 1 assigned interface(s) to function.
        If you do not have *AT LEAST* 1 interfaces you CANNOT continue.

        If you do not have at least 1 *REAL* network interface card(s)
        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: em0 █
```

Figura 18. Atribuição da interface WAN.

Em seguida será solicitada a interface LAN. Neste caso, por padrão, o pfSense considera que o firewall será de perímetro e que a rede interna será estabelecida com endereçamento inválido, sendo necessário a realização de tradução de endereços (NAT - *Network Address Translation*) para que os pacotes sejam enviados à internet. Posteriormente, quando a interface web estiver operacional, será possível visualizar as regras de NAT sendo criadas neste momento. Neste caso, a interface em1 será utilizada como LAN. É importante configurar no mínimo uma interface LAN pois será por ela que a interface web será acessada para a realização das configurações (Figura 19).

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

Figura 19. Atribuição da interface LAN: informar em1.

Observação 1: embora as regras criadas neste momento busquem facilitar a configuração do firewall, é uma boa prática remover todas elas para posteriormente criá-las, de acordo com as necessidades. Estas criações automáticas auxiliam no caso de usuários que precisam estabelecer um firewall simples, como os de uso doméstico, apenas para acesso à internet, sem regras de filtragem.

Observação 2: conforme será de entendimento posterior, a política padrão do pfSense é de bloqueio. Assim, quando se remove todas as regras de todas as interfaces, o efeito obtido é que estas interfaces estão bloqueando todos os pacotes. Se não há regras, nada está liberado.

Após a configuração de LAN o pfSense pergunta se alguma interface opcional necessita ser indicada. Estas interfaces representariam outros segmentos de rede, pois o firewall pode ter várias redes LANs ligadas a ele. Neste caso, não será informada uma rede opcional (basta continuar sem informar nada). Esta configuração pode ser realizada posteriormente pela interface web, indicando novas interfaces. Ao finalizar as atribuições de interfaces será mostrada uma lista conforme a Figura 20.

```
The interfaces will be assigned as follows:  
WAN -> em0  
LAN -> em1  
Do you want to proceed [y/n]?
```

Figura 20. Confirmação das interfaces atribuídas no firewall.

Prosseguindo com a instalação, o sistema gravará estas informações no disco e mostrará a tela padrão após a inicialização normal conforme a Figura 21.

```
FreeBSD/amd64 (pfSense.localdomain) (ttyv0)  
*** Welcome to pfSense 2.0.3-RELEASE-pfSense (amd64) on pfSense ***  
  
WAN (wan) -> em0 -> 10.0.2.15 (DHCP)  
LAN (lan) -> em1 -> 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) Disable Secure Shell (sshd)  
7) Ping host  
Enter an option:
```

Figura 21. Tela padrão quando o pfSense é inicializado, depois da configuração inicial de interfaces.

A tela mostrada após o boot do sistema mostra a configuração de todas as interfaces e diversas opções. As opções são:

- 0) **Logout (SSH Only)**: esta opção é usada quando se está conectado no firewall por meio de uma sessão SSH. Ela desloga o usuário.
- 1) **Assign Interface**: reinicia o processo de atribuição de interfaces, desde a atribuição de VLANs às próprias interfaces.
- 2) **Set interface(s) IP address**: permite configurar o endereçamento de uma ou mais interfaces. A opção 1) é diferente pois ela é utilizada para se ligar uma interface. Perceba que é possível ligar uma interface e não configurar nenhum IP, como é o caso de uma interface em Trunk, por exemplo.

- 3) **Reset webConfigurator password:** utilizada para reinicializar o usuário e a senha da interface web para admin e pfsense, respectivamente.
- 4) **Reset to factory defaults:** apaga as configurações do sistema, retornando-o para o padrão de instalação. Esta opção não altera o sistema de arquivos nem os pacotes instalados. Assim, se o sistema de arquivos em si estiver corrompido, será necessário refazer a instalação e não apenas usar esta opção.
- 5) **Reboot system:** reinicializa o sistema.
- 6) **Halt system:** desliga o sistema.
- 7) **Ping host:** executa um teste de ICMP echo request (ping).
- 8) **Shell:** abre uma shell para o usuário, possibilitando que ele acesse todo o sistema de arquivos do pfSense.
- 9) **pfTop:** executa o pfTop, uma ferramenta semelhante ao top dos sistemas *NIX, mas voltada para o PF (Packet Filter), mostrando informações de rede relativas ao firewall, como sessões estabelecidas, quantidades de pacotes, bytes, entre outras.
- 10) **Filter Logs:** permite visualizar os pacotes que estão sendo bloqueados em tempo real. É o equivalente a executar um tcpdump no dispositivo pflog0 utilizado pelo PF do FreeBSD.
- 11) **Restart webConfigurator:** reinicializa o processo do sistema que executa a interface web. Em casos raros é necessário reiniciar a interface web para que algumas modificações passem a ter efeito. Caso a interface web trave e esta opção não a restaure, também é possível executar o comando `'killall -9 php; killall -9 lighttpd; /etc/rc.restart_webgui'` da linha de comando.
- 12) **pfSense Developer Shell:** utilitário que permite a execução de código PHP no âmbito do sistema em execução (utilizado por desenvolvedores).
- 13) **Upgrade from console:** permite executar um upgrade a partir do console, informando a URL de uma imagem do pfSense.
- 14) **Disable Secure Shell (sshd):** habilita ou desabilita o SSH.

6.2 Wizard para configuração na interface web

Realizada a instalação e configuração mínima, é possível conectar-se à interface web do pfSense para realizar diversas outras configurações. Esta conexão deve ser realizada pela interface LAN. Por padrão, o pfSense não permite que seja utilizada a interface web através da WAN. Assim, é importante que ao menos uma interface LAN seja configurada.

Conectando-se à interface web pelo navegador (utilizar o IP da LAN configurado nos passos da instalação), no primeiro acesso será exibido um *wizard* que guiará o usuário em mais algumas configurações. As Figuras de 22 a 30 mostram os passos do *wizard*.



Figura 22. Tela de login.

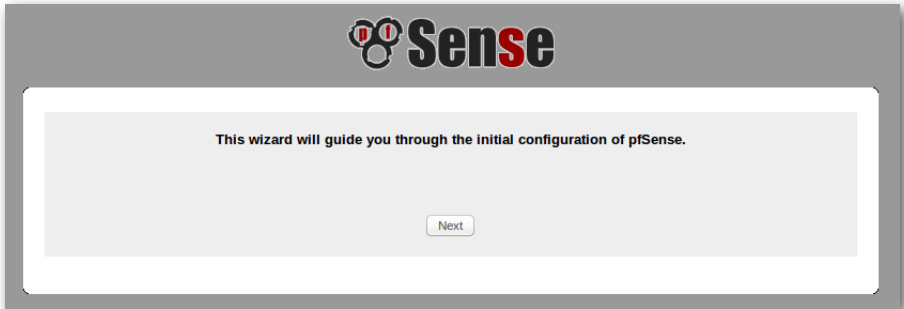


Figura 23. Início do *wizard*.

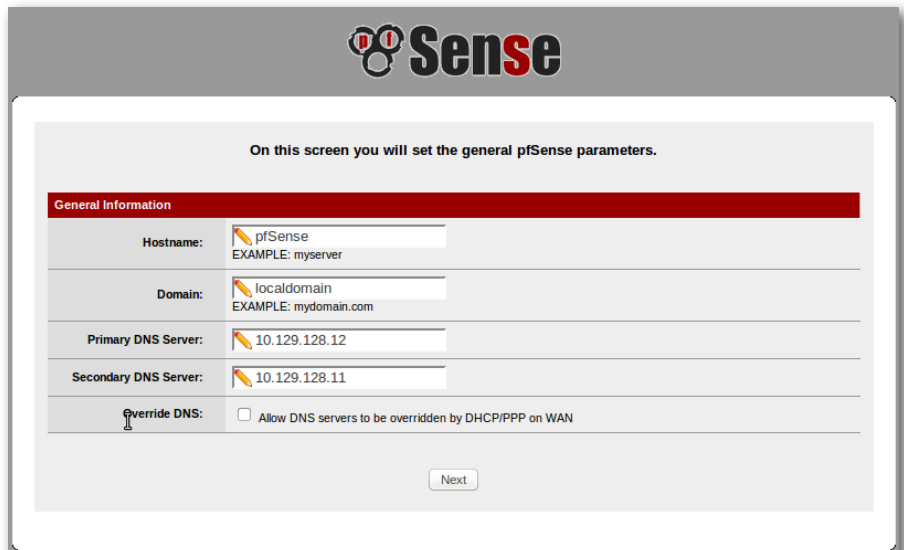
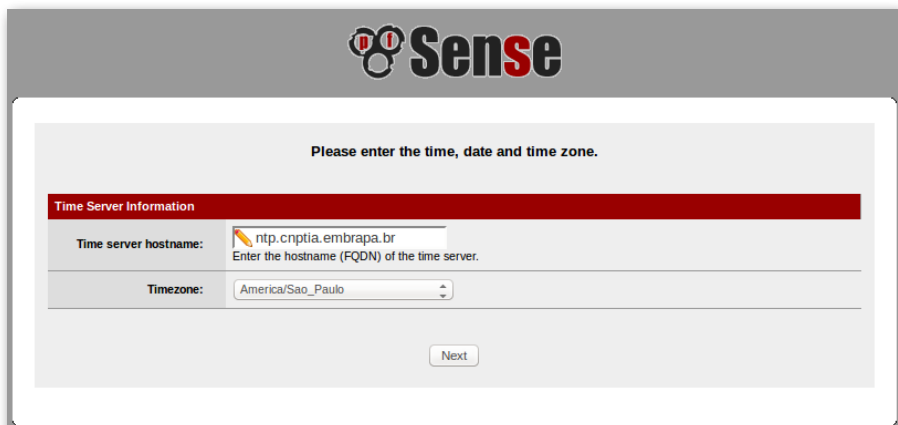
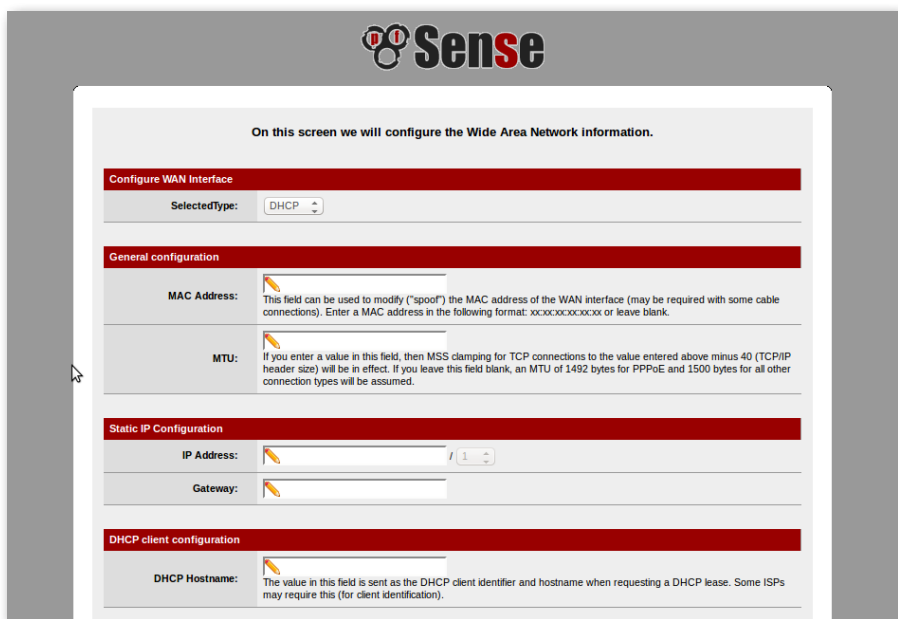


Figura 24. Parâmetros gerais do pfSense: configurar os servidores de DNS.



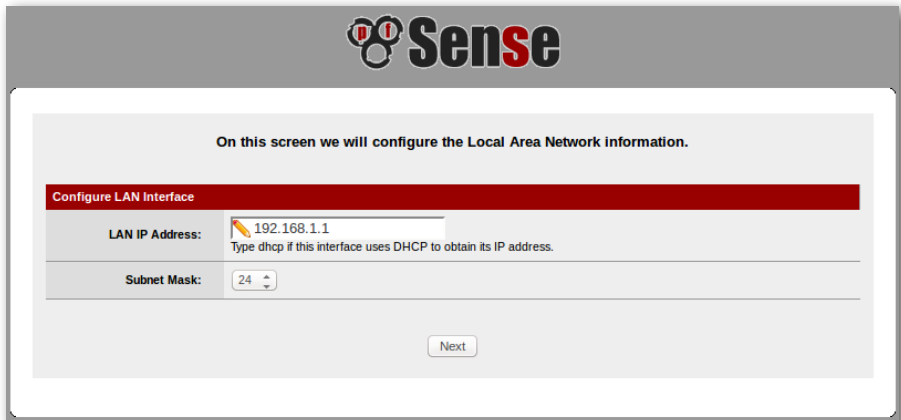
The screenshot shows the 'Time Server Information' configuration page in pfSense. At the top, the pfSense logo is displayed. Below it, a message reads 'Please enter the time, date and time zone.' The main configuration area has a red header 'Time Server Information'. It contains two fields: 'Time server hostname' with the value 'ntp.cnptia.embrapa.br' and a subtext 'Enter the hostname (FQDN) of the time server.', and 'Timezone' with a dropdown menu set to 'America/Sao_Paulo'. A 'Next' button is located at the bottom right of the form.

Figura 25. Configurar o servidor NTP para sincronização de relógio e o timezone.



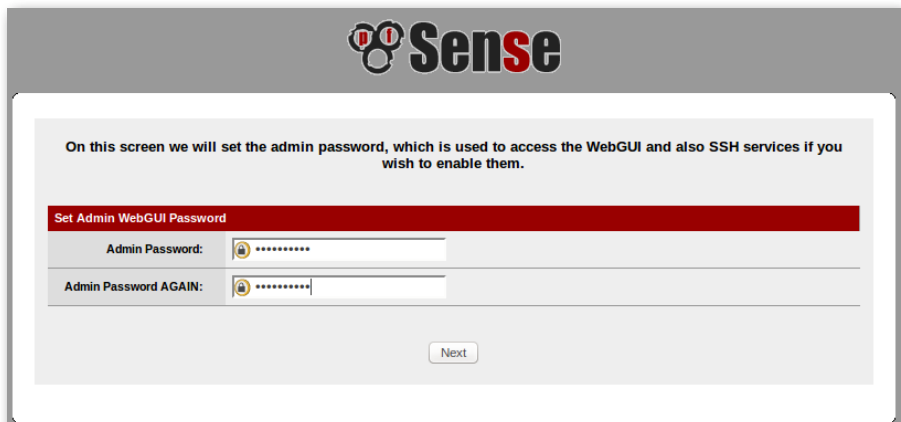
The screenshot shows the 'Configure WAN Interface' page in pfSense. At the top, the pfSense logo is displayed. Below it, a message reads 'On this screen we will configure the Wide Area Network information.' The main configuration area has a red header 'Configure WAN Interface'. It contains a 'SelectedType' dropdown menu set to 'DHCP'. Below this is a red header 'General configuration'. It contains two fields: 'MAC Address' with a subtext '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: xxxxxxxxxx or leave blank.', and 'MTU' with a subtext '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.' Below this is a red header 'Static IP Configuration'. It contains two fields: 'IP Address' and 'Gateway'. Below this is a red header 'DHCP client configuration'. It contains one field: 'DHCP Hostname' with a subtext '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).' A mouse cursor is visible on the left side of the page.

Figura 26. Na configuração de WAN deve-se informar como será o endereçamento desta interface (para os exercícios deste material deve-se utilizar o DHCP).



The screenshot shows the 'Configure LAN Interface' screen in the pfSense installation wizard. At the top, the pfSense logo is displayed. Below it, a message states: 'On this screen we will configure the Local Area Network information.' A red header bar contains the title 'Configure LAN Interface'. The main form area has two input fields: 'LAN IP Address' with a pencil icon and the value '192.168.1.1', and a subtext 'Type dhcp if this interface uses DHCP to obtain its IP address.' Below this is the 'Subnet Mask' field with the value '24'. A 'Next' button is located at the bottom right of the form area.

Figura 27. Na configuração da LAN pode-se alterar o endereçamento que fora inicialmente informado durante a instalação.



The screenshot shows the 'Set Admin WebGUI Password' screen in the pfSense installation wizard. At the top, the pfSense logo is displayed. Below it, 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 contains the title 'Set Admin WebGUI Password'. The main form area has two password input fields: 'Admin Password:' and 'Admin Password AGAIN:', both with eye icons and masked characters. A 'Next' button is located at the bottom right of the form area.

Figura 28. Alterar a senha de administrador do sistema.

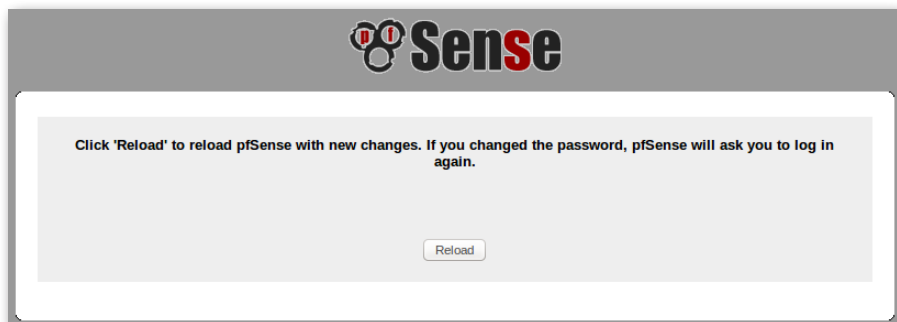


Figura 29. Ao término desta configuração o pfSense fará o *reload*, aplicando-as, sendo necessário autenticar-se novamente.



Figura 30. Tela indicando que o pfSense aplicou as configurações. Clicar na opção para continuar no pfSense webConfigurator.

7 Características e configurações básicas

Esta seção abordará diversas características do pfSense bem como mostrará orientações para determinadas configurações.

7.1 Arquivo de configuração XML

As configurações do pfSense são armazenadas em um arquivo no formato XML, inclusive as dos pacotes instalados. Todos os outros arquivos de

configuração para os serviços do sistema e sua operação são gerados dinamicamente em tempo de execução, baseados no arquivo de configuração XML. Assim sendo, quaisquer modificações executadas diretamente em arquivos de configuração do sistema serão sobrescritas.

O arquivo de configuração fica armazenado em `/cf/conf/config.xml`. Existe um link simbólico, `/conf`, que aponta para `/cf/conf`. Em `/cf/conf` existe ainda o diretório `backup` que armazenará cópias do arquivo de configuração. A cada alteração o sistema realiza uma cópia do arquivo antigo neste diretório.

Na interface web, em `Diagnostics` → `Config History`, é possível configurar a quantidade de arquivos que se deseja manter (estes arquivos funcionam como backups de versões anteriores, pois a quantidade informada representará as últimas modificações do arquivo de configuração). Neste mesmo local também é possível realizar comparações entre arquivos de configuração para identificar modificações realizadas no sistema.

Edição manual da configuração

Algumas poucas configurações somente são possíveis pela edição manual do arquivo de configuração. Para tanto, pode-se utilizar a opção `Diagnostics` → `Backup/Restore` para baixar o arquivo de configuração, realizar as alterações e então restaurá-lo no sistema. Outra maneira é utilizando o utilitário de linha de comandos `'viconfig'`, que editará a configuração que está em execução no sistema. Ao sair deste utilitário salvando as modificações, o arquivo de cache de configuração será removido do diretório `/tmp/config.cache` e as alterações já estarão visíveis a partir da interface web. Elas serão ativadas na próxima vez que os serviços para os quais as modificações foram feitas forem reiniciados.

7.2 Perda de acesso

É comum a perda de acesso ao firewall por diversos fatores, como por exemplo, regras que bloqueiem o acesso. O pfSense possui a opção *anti-lockout rules* que cria regras justamente para evitar esta situação. No entanto, como alguns administradores preferem desabilitar qualquer criação de regras dinâmicas, aumenta-se as chances de ocorrer uma situação de bloqueio.

O acesso físico ao firewall sempre permitirá que esta situação seja contornada. Uma vez que a maior parte dos problemas desta natureza ocorrem com as regras, existe um comando chamado *easyrule* facilitador da recuperação. Pode-se, por exemplo, liberar temporária e rapidamente o acesso à interface web com uma regra semelhante a:

```
$ easyrule pass wan tcp x.x.x.x y.y.y.y 443
```

onde WAN é a interface, x.x.x.x o endereço de origem e y.y.y.y o endereço de destino (pode ser o próprio firewall).

Outras alternativas, extremamente perigosas, porém existentes, são:

- Adicionar um allow all na interface WAN a partir da shell:

```
$ pfSsh.php playback enableallowallwan
```

- Desabilitar o firewall, inclusive as regras de NAT (caso algo seja salvo na interface o firewall sofrerá um reload e as regras serão aplicadas novamente):

```
$ pfctl -d
```

- Para retornar o firewall:

```
$ pfctl -e
```

Outra maneira interessante de se alterar regras no firewall, principalmente para quem tem familiaridade com o PF do FreeBSD, é alterar diretamente o arquivo que contém as regras aplicadas no firewall. Este arquivo é o `/tmp/rules.debug`. Basta editá-lo e executar o seguinte comando para que as regras sejam recarregadas.

```
$ pfctl -f /tmp/rules.debug
```

Ao entrar na interface e salvar alguma alteração, estas modificações passam a ser permanentes e sobrescrevem o arquivo de configuração antigo.

7.3 Interfaces

O pfSense permite a utilização de diversos tipos de interface através da opção Interfaces → (assign). Os usos mais comuns são a interface física e a interface virtual.

7.3.1 Interface física

No menu Interfaces → (assign) haverá a opção *Available network ports*: que listará todas as interfaces físicas do hardware sendo utilizado. Ao selecionar uma interface e clicar no botão de adicionar, diz-se que esta interface foi atribuída ao firewall. Ele passará a constar na lista de interfaces atribuídas e só então poderá ser configurada.

7.3.2 Interface virtual (VLANs)

Para utilizar uma interface pertencente a uma VLAN, é necessário primeiro criar esta VLAN dentro do firewall para depois atribuir a interface e configurá-la. No caso de uma interface em uma VLAN, a atribuição ficará vinculada a uma interface física. É o equivalente a colocar a interface física em Trunk e criar uma interface virtual, pertencente a uma VLAN, nesta interface.

Para criar uma VLAN deve-se acessar o menu Interfaces → (assign) → VLANs e clicar em adicionar. Será necessário informar qual é a interface física pai para esta VLAN (por qual interface os pacotes trafegarão), a VLAN tag e uma descrição. Ao criar esta VLAN no sistema, deve-se então voltar ao menu Interfaces → (assign). Dentre as opções em *Available network ports*: tornar-se-á disponível uma interface virtual dentro desta VLAN. Basta então selecioná-la e atribuí-la ao firewall. Após a atribuição, os parâmetros de configuração poderão ser customizados.

7.4 Backup e restauração

Ao utilizar um arquivo de configuração único, em XML, o pfSense facilita as tarefas de backup e *recovery* de um sistema. Conforme já mencionado, os arquivos originais do sistema operacional não são (nem devem ser) alterados. Arquivos de configuração do sistema e serviços são sempre gerados em tempo de execução com base no arquivo de configuração config.xml.

Desta forma, todas as configurações do sistema podem ser geradas a partir deste arquivo.

Realizando o backup deste arquivo de configuração é possível reestabelecer um sistema rapidamente. Existem pouquíssimas exceções de configuração que residem fora do arquivo de configuração XML do sistema. São casos de alguns poucos pacotes.

A cada modificação o pfSense faz um backup interno no diretório `/cf/conf/backup`. Estas cópias são importantes para o caso de reverter configurações para momentos anteriores. No entanto, não é eficaz para a recuperação de problemas como panes em hardware, quando não será possível ligar o equipamento para copiar o arquivo de configuração.

Portanto, é importante que os arquivos de configuração sejam copiados do firewall para um sistema de backup externo, mantidos seguros. Neste processo de backup é importante lembrar que, caso alguma alteração tenha sido executada diretamente no sistema, estas alterações devem ter um meio de backup próprio. Por exemplo, usuários familiarizados com FreeBSD podem fazer alterações via shell em alguns arquivos que não são sobrescritos pelo pfSense. Estas modificações não estarão presentes em um novo sistema instalado e restaurado a partir de um backup de arquivo de configuração. Fica a cargo do administrador realizar o backup destas áreas. Arquivos comuns que se incluem neste contexto são o `/boot/device.hints` e `/boot/loader.conf.local`, por exemplo.

7.4.1 Backup utilizando a interface web

Para salvar o arquivo de configuração pela interface web deve-se acessar o menu Diagnostics → Backup/Restore. Na aba Backup/Restore haverá a opção *Download configuration*. Por padrão fica selecionada a opção para não salvar as informações dos gráficos RRD. Caso seja necessário manter as informações de histórico das estatísticas e gráficos do sistema, basta desmarcar esta opção que as informações serão colocadas dentro do arquivo XML. O arquivo é nomeado da forma `config-<hostname>-<timestamp>.xml`.

7.4.2 Backup utilizando wget e cron

É possível utilizar o wget agendado no cron para obter o arquivo de configuração do pfSense, a partir de outro host. Para tanto, pode-se utilizar um script conforme a seguir.

```
#!/bin/bash
wget -qO/dev/null --keep-session-cookies --save-cookies cookies.txt \
--post-data "login=Login&usernamefld=admin&passwordfld=SENHA" \
--no-check-certificate https://fwintl.cnptia.embrapa.br/diag_backup.php
wget --keep-session-cookies --load-cookies cookies.txt \
--post-data "Submit=download&donotbackuprrd=no" \
https://fwintl.cnptia.embrapa.br/diag_backup.php \
--no-check-certificate -O config-hostname-`date +%Y%m%d%H%M%S`.xml
rm cookies.txt
```

Este script se autentica no firewall, guarda uma cookie de sessão e depois realiza o download do arquivo de configuração.

7.4.3 Backup utilizando SCP

Também é possível utilizar o sentido inverso para backup, de forma que o firewall envia o arquivo de configuração para um host remoto, utilizando para tanto uma chave SSH sem senha. O comando a ser utilizado é:

```
scp /cf/conf/config.xml \
usuario@hostremoto:caminho/config-`hostname`-`date +%Y%m%d%H%M%S`.xml
```

7.4.4 Restauração utilizando a interface web

Este é o modo mais simples de restauração. Basta acessar na interface web o caminho Diagnostics → Backup/Restore e utilizar a parte de restauração. O mais comum é escolher ALL para a área de restauração, conforme a Figura 31.



Figura 31. Seção de restauração da interface web.

A restauração por este método prevê que já se tenha um sistema completo instalado e uma configuração de rede funcionando para que seja possível se conectar no firewall e enviar o arquivo de configuração. Após aplicar a restauração, o sistema reinicializará com a nova configuração.

7.4.5 Restauração a partir do histórico de configuração

No mesmo menu Diagnostics → Backup/Restore existirá uma aba chamada Config History. Esta página mostra uma lista de arquivos de configuração mantidos pelo sistema. É possível verificar a diferença entre dois arquivos selecionados. Esta é mais uma forma de se restaurar um arquivo de configuração (Figura 32).

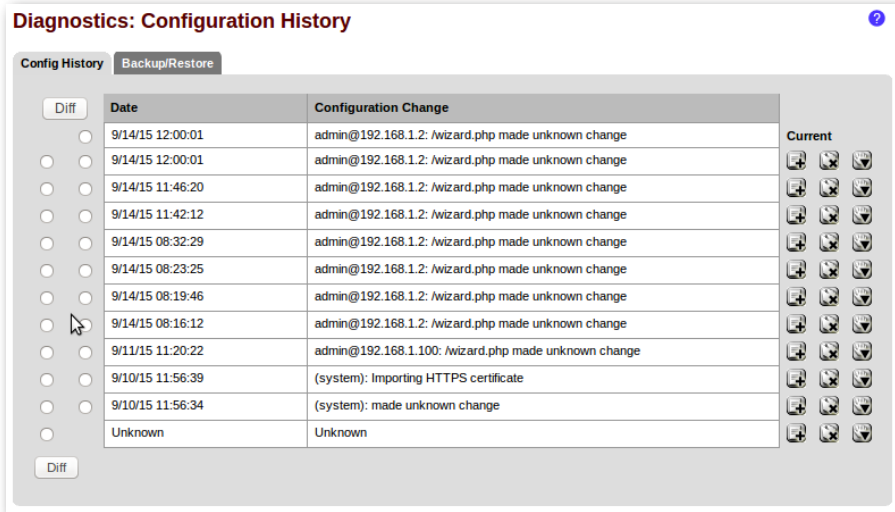


Figura 32. Histórico de arquivos de configuração para restauração.

7.4.6 Restauração utilizando o Pre-Flight Installer

O pfSense possui, como parte da rotina de instalação, um esquema de restauração de configuração chamado Pre-Flight Installer (PFI). Para utilizá-lo é necessário criar um pendrive com sistema de arquivos FAT e, na raiz, criar um diretório chamado 'conf'. Dentro deste diretório deve-se colocar o arquivo de configuração com o nome config.xml.

O PFI serve para instalar um sistema no disco, a partir do Live CD, mas utilizando um arquivo de configuração já existente. Esta instalação se dará conforme descrito a seguir. Será possível observar que a parte de configuração de interfaces, normalmente executada em uma instalação inicial, não será executada, pois estas configurações serão obtidas do arquivo config.xml do pendrive.

Deve-se então iniciar o *live* CD do pfSense no hardware que será utilizado para restaurar a configuração, com o pendrive inserido. Não se deve utilizar a opção 'i' de instalação no *prompt* que aparece durante o *boot*. Basta deixar o *boot* se completar totalmente. Desta forma o arquivo de configuração do pendrive será utilizado, sendo possível verificar que não aparecerá o *prompt* para configuração das interfaces. Neste momento o sistema estará inicializado com a configuração disponibilizada. Haverá então um opção

para que este sistema, junto da configuração, seja instalado no disco. Basta executá-la para que a restauração seja finalizada permanentemente no hardware.

O pendrive deve ser removido e o sistema reinicializado. Caso exista algum pacote na configuração restaurada, ao se autenticar na interface web, eles serão reinstalados.

7.5 Firewall - filtragem e encaminhamento

No pfSense as regras são avaliadas segundo a política da primeira encontrada. Desta forma, ao se ler um conjunto de regras de cima para baixo, a primeira regra que casar será a utilizada. A avaliação das regras cessa neste momento e as regras posteriores não são analisadas.

O pfSense é um firewall *stateful*. Isto significa que é necessário permitir o tráfego apenas na interface onde ele é iniciado. Informações deste tráfego serão mantidas na tabela de estados para que os pacotes da volta possam passar novamente. Esta tabela de estados é finita e, por padrão, o pfSense utiliza 10% da memória do sistema para ela. Cada entrada da tabela ocupa 1 KB e, para uma conexão, são mantidos dois estados, um para cada sentido do fluxo de dados. Caso se deseje alterar este tamanho, pode-se utilizar o menu System → Advanced e procurar o campo correspondente na aba Firewall/NAT.

7.5.1 Regras de filtragem

Para a criação de regras de filtragem é necessário acessar o menu Firewall → Rules e escolher uma interface (abas). Dentro de cada interface basta adicionar a regra desejada. Cada regra possui uma ação. Deve-se tomar cuidado para que as regras não causem sobreposição, lembrando-se sempre da política da primeira encontrada. As configurações das regras são, na maioria, referentes aos protocolos de camada de rede e transporte.

7.5.2 Regras de NAT

NAT é o acrônimo para *Network Address Translation*, ou seja, qualquer tipo de tradução de endereço. Além disso, é comum o termo ser empregado de

forma geral para se referir até mesmo a uma mudança de porta nos pacotes, não necessariamente havendo uma tradução 'de endereço'.

Para a criação de regras de NAT deve-se utilizar o menu Firewall → NAT. De modo resumido, as regras de tradução de endereços para entrada devem ser criadas na aba Port Forward, como, por exemplo, para receber pacotes em um endereço IP público e redirecionar para um *host* interno com IP privado. Já as traduções para saídas devem ser criadas na aba Outbound. Por exemplo, pode-se criar uma regra que faça um NAT, para tráfego cuja origem seja a rede LAN, atribuindo como endereço de origem o IP público da interface WAN, de modo que o pacote saia com o IP público do Firewall e possa retornar até ele. A aba 1:1 serve para criar uma tradução direta, de um IP público para um IP privado.

No caso das regras de NAT é importante ter em mente como os pacotes são processados. Embora regras de NAT existam em um sistema pfSense, os pacotes podem ainda ser filtrados em outros momentos. Por exemplo, pode existir a regra de NAT para saída, conforme exemplo anterior, mas a interface LAN, que recebe os pacotes de todos os *hosts* da rede interna, não ter regra de liberação. Neste caso, os pacotes serão filtrados nesta interface LAN, pois não existirão regras que permitam que eles entrem para o firewall. Somente após a criação de regras que permitam o tráfego nesta interface é que os pacotes entrarão no firewall e serão processados.

Um maneira amigável de se entender este contexto é considerar que, para um pacote atravessar o firewall, ele deverá ter regras para entrar no firewall, por alguma das interfaces, deverá então ser processado (roteado, por exemplo) e, por fim, deverá ter regras para sair do firewall por alguma interface (por exemplo, na saída ele pode sofrer um NAT).

Para facilitar a criação das regras de NAT o pfSense possui algumas opções relativas a este tipo de regra.

7.5.2.1 Criação de regra de Port Forward usando Filter Rule Association

Ao adicionar uma regra de Port Forward, além das opções de endereçamento e portas normalmente utilizadas, o pfSense oferece uma diretiva chama Filter Rule Association. Caso a opção nesta diretiva seja "Add associated filter rule" (padrão), ao adicionar esta regra de NAT, o pfSense

automaticamente criará a regra de permissão dos pacotes na interface associada (Figura 33). Na tela com a lista de regras da interface (Firewall → Rules, Interface), na coluna *Description*, a regra criada automaticamente terá seu nome iniciando com a indicação ‘NAT’. Estas regras ficarão relacionadas e, caso a regra de NAT seja alterada, a regra da interface será atualizada automaticamente.

Hint: you can leave this field empty if you only want to map a single port.

Redirect target IP

 Enter the internal IP address of the server on which you want to map the ports.
 e.g. 192.168.1.12

Redirect target port

 Specify the port on the machine with the IP address entered above. In case of a port range, specify the beginning port of the range (the end port will be calculated automatically).
 Hint: this is usually identical to the 'from' port above

Description

 You may enter a description here for your reference (not parsed).

No XMLRPC Sync

 HINT: This prevents the rule from automatically syncing to other CARP members.

NAT reflection

Filter rule association

 None
 Add associated filter rule
 Add unassociated filter rule
 Pass

is not work properly with Multi-WAN. It will only work on an interface containing the

Figura 33. Diretiva Filter Rule Association para regras de NAT Port Forward: será criada uma regra automaticamente em outra interface com a indicação em seu nome, que se iniciará pelo acrônimo NAT.

Conforme pode ser observado, existem ainda as opções “Add unassociated filter rule”, de forma que a regra criada não fica relacionada, sendo necessária sua atualização manual em caso de alteração da regra de NAT, e “Pass”, que é uma característica das regras de NAT do PF que indica que o tráfego deve passar mesmo sem a regra de firewall na interface.

7.5.2.2 Criação de regra de Outbound com Manual outbound NAT Rule generation

O Outbound NAT também é conhecido com Source NAT ou SNAT, por alterar o endereço de origem do pacote ao deixar uma interface do firewall. É importante mencionar que o Outbound NAT controla o que acontece com o pacote quando ele deixa uma interface. Em qual interface um pacote irá deixar o firewall depende da tabela de roteamento e não das regras de NAT. Esse tipo de regra pode ser criado no menu Firewall → NAT, na aba Outbound.

Existem duas opções básicas no pfSense para a criação deste tipo de regra: “Automatic outbound NAT rule generation” e “Manual outbound NAT rule generation (Advanced Outbound NAT (AON))”. Quando a opção automática é utilizada, o pfSense criará, automaticamente, regras para traduzir o endereço de origem de todo tráfego saindo de redes internas (LANs), para o endereço IP da interface WAN por onde o tráfego sair (estas regras serão internas, ele não mostrará na interface, apenas encaminhará os pacotes). Já no caso da opção manual, o usuário deverá entrar as regras explicitamente, sobre quais endereços devem ser traduzidos e para quais endereços.

Dica: na aba de configuração das regras de NAT Outbound, caso não se tenha nenhuma regra cadastrada, ao alterar a política de Outbound de automática para manual, será possível perceber que o pfSense criará, explicitamente, regras de Outbound para todas as LANs existentes no firewall.

Duas observações são pertinentes neste momento. Ao operar no modo manual o administrador tem claro e total controle sobre quais regras estão em operação no firewall. Este tipo de política é mais adequado quando se deseja ter clara e explicitamente todas as ações executadas pelo firewall. A utilização de regras automáticas pode facilitar a configuração do firewall para ambientes que não requerem muitos filtros. Uma segunda observação, diretamente relacionada às regras de Outbound, é relativa à utilização de endereços virtuais CARP quando o firewall opera em uma arquitetura de alta disponibilidade. Neste contexto, haverá no mínimo a figura de um firewall master e um firewall *slave*, cada um com seu endereço IP. Existirá então um IP virtual que ficará atribuído ao firewall em operação, seja o master ou o slave. As regras de Outbound, portanto, deverão utilizar o IP virtual pois, caso um dos firewall falhe, este IP passará a ser utilizado pelo hardware ainda funcional e os pacotes deverão continuar a utilizar o mesmo endereço IP de saída, principalmente devido às entradas mantidas na tabela de estados do firewall, sincronizada entre eles.

7.5.2.3 NAT 1:1

O NAT 1:1 mapeia um endereço público para um endereço privado. Todo tráfego destinado ao endereço público será então mapeado para o host com o endereço privado.

7.5.3 Aliases

Aliases são apelidos utilizados para facilitar a configuração e documentação de um firewall. No pfSense, um *alias* é um agrupamento de portas, *hosts* ou redes. Quando se cria um *alias* este pode ser referenciado durante a criação de regras de filtragem ou de NAT. Os *aliases* podem ser criados no menu Firewall → *Alias* (Figura 34).

Figura 34. Criação de um *alias*.

Após a declaração de um *alias*, quando se estiver criando regras, deve-se atentar para que diversos campos, tais como os de endereços e portas, possuem um tipo com a opção “Single host or *alias*”. Ao escolher esta opção na lista de tipos, o campo de valor se tornará vermelho. Qualquer caixa de entrada de valores que se apresente vermelha aceita um *alias*.

7.5.4 Ordem de processamento dos NATs e regras de filtragem

Entender a ordem de processamento das regras é talvez a mais importante informação para a construção de um firewall. Isso é importante principalmente ao lidar com regras de NAT, pois a ordem com que as regras são verificadas pode significar o aceite de um pacote ou não.

As Figuras 35 e 36 ilustram dois sentidos de fluxos de rede, da Internet para o ambiente de rede protegido pelo firewall pfSense e de um cliente interno para a Internet. Ainda, como é bastante comum a utilização da

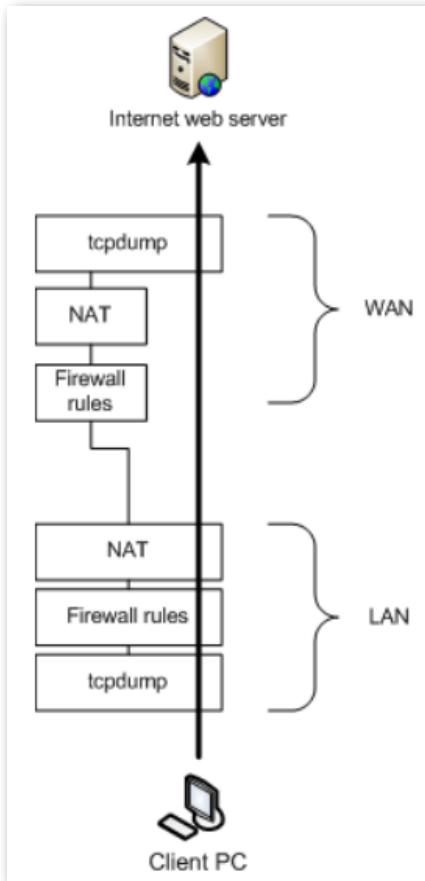


Figura 35. Caminho de validação de regras para um pacote partindo de um cliente interno com destino a um servidor web na Internet. Figura retirada de "pfSense: The definitive guide version 2.1".

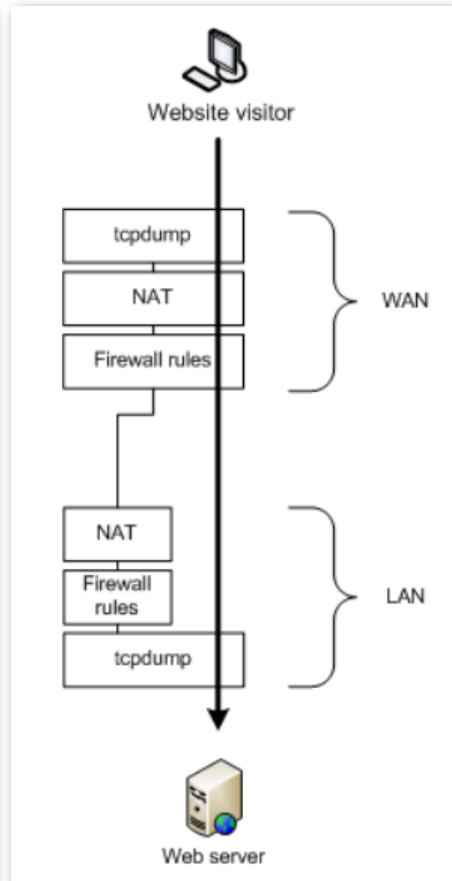


Figura 36. Caminho de validação de regras para um pacote chegando da Internet com destino a um servidor web interno. Figura retirada de "pfSense: The definitive guide version 2.1".

ferramenta TCPDUMP para a solução de problemas, as figuras indicam em que ponto do caminho de um pacote o TCPDUMP ou captura. Isso é importante pois, caso seja necessário criar filtros no TCPDUMP, deve-se entender se em determinado momento o pacote já sofreu tradução de endereço ou não.

Nas caixas "Firewall rules" das figuras deve-se incluir também o processamento da tabela de estados do firewall, conferindo sua característica de

stateful. Por exemplo, na Figura 35, quando a resposta do servidor web retornar ao cliente, ela passará pelo ponto de captura do TCPDUMP, pelas regras de NAT e pelas “Firewall rules”. É provável que não exista uma regra de firewall que permita este pacote, pois ele foi criado com uma porta de origem aleatória. No entanto, haverá uma entrada na tabela de estados que permitirá sua volta ao cliente interno. Caso não exista esta entrada, ou a tabela de estados não seja checada neste momento, o pacote será filtrado.

Embora não esteja discriminado nas figuras, é comum os tipos de traduções de endereços ocorrerem em pontos específicos. Ao se analisar os diagramas é possível perceber que um pacote passa duas vezes pela validação de regras de NAT. Quando ele está entrando no firewall, normalmente executa-se o NAT do tipo Port Forward (ou DNAT - Destination NAT, quando se troca o endereço de destino). Quando o pacote está deixando o firewall, normalmente executa-se o NAT do tipo Outbound (ou SNAT - Source NAT, quando se troca o endereço de origem).

7.5.5 Roteamento

O roteamento de pacotes é uma das tarefas fundamentais de um firewall, possibilitando que pacotes de redes diferentes possam ser encaminhados. No pfSense, os *gateways* podem ser configurados no menu System → Routing, na aba Gateways (Figura 37).

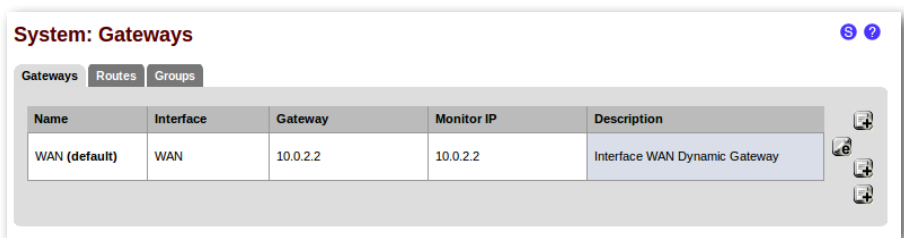


Figura 37. Configuração de gateways.

Na Figura 37 existe um *gateway* nomeado “WAN (default)” na interface WAN do firewall. Ele envia pacotes para o host 10.0.2.2 (next hop) e monitora este IP (a monitoria de IP é um serviço padrão do pfSense para gateways, de modo que ele envia ICMP Echo Request constantemente ao endereço). Por ser o *gateway* padrão, os pacotes roteados por este firewall

serão enviados para o host 10.0.2.2 caso não sejam para redes conectadas ao próprio firewall.

Uma outra maneira de se utilizar um *gateway* dentro do pfSense é na configuração de uma interface. Caso esta seja uma interface que se conecta à Internet, por exemplo, será possível escolher um *gateway* para ela (Figura 38).



Figura 38. Opção de escolha de gateway, dentro das configurações de uma interface.

Para que seja possível escolher um *gateway*, é necessário que ele exista em System → Routing, aba Gateways, e que a interface em questão esteja na mesma rede (endereçoamento). Interfaces que operam em DHCP recebem o *gateway* por meio deste protocolo.

Um *gateway* também pode ser entendido como um “próximo *hop*” na configuração de um firewall, não necessariamente para uma conexão externa. Por exemplo, pode existir um cenário em que o firewall pfSense esteja posicionado entre um roteador interno e a conectividade com a Internet. Neste caso, ele servirá de firewall de perímetro para todas as redes internas e estará ligado ao roteador interno. Para que ele envie pacotes a este roteador, ele deverá conhecer o mesmo, que será um próximo *hop*, do lado interno. Provavelmente existirá uma rede de trânsito (normalmente /30) entre o roteador interno e o firewall. Nas configurações do firewall, o IP do roteador será cadastrado como um *gateway*, ou seja, é um ponto para onde o firewall poderá enviar pacotes.

Neste cenário anterior, apenas a existência da configuração do roteador interno como *gateway* não compreende a configuração total necessária para o funcionamento desta rede. Como este não representa um *gateway default*, será necessário declarar para quais redes o firewall deve utilizar este *gateway*. Trata-se da criação de rotas, que pode ser realizada no menu System → Routing, aba Routes. Para cada rede interna será necessário indicar a utilização do gateway em questão. Desta forma, o firewall tomará conhecimento que, para atingir destinos nas redes informadas, deverá en-

viar pacotes para o roteador interno. A Figura 39 ilustra um cenário desses, com a configuração de uma rota estática.

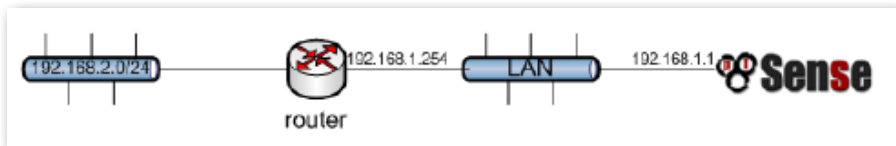


Figura 39. Firewall pfSense posicionado antes de um roteador interno: rotas estáticas são necessária para os pacotes chegarem às redes internas. Figura retirada de “pfSense:The definitive guide version 2.1”.

A configuração das rotas são realizadas no menu System → Routing, aba Routes (Figura 40).

Edit route entry	
Destination network	192.168.2.0 / 24 Destination network for this static route
Gateway	OtherRouter - 192.168.1.254 Choose which gateway this route applies to or add a new one.
Disabled	<input type="checkbox"/> Disable this static route Set this option to disable this static route without removing it from the list.
Description	<input type="text"/> You may enter a description here for your reference (not parsed).

Figura 40. Configuração de um rota estática para chegar até a rede 192.168.2.0/24, utilizando como gateway o roteador 192.168.1.254. Figura retirada de “pfSense:The definitive guide version 2.1”.

A tabela de roteamento do firewall pode ser visualizada no menu Diagnostics → Routes.

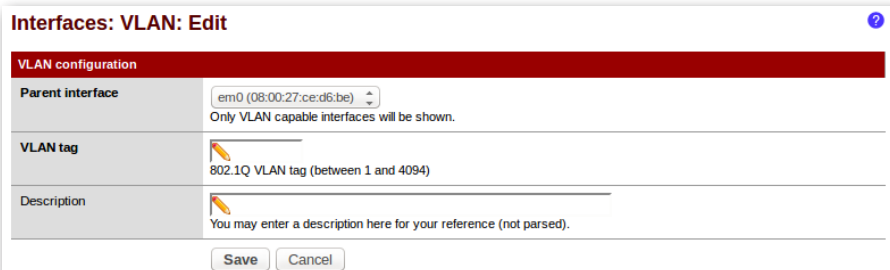
7.6 Virtual LANs (VLANs)

O 802.1Q é um padrão de rede que define as redes locais virtuais (VLANs). Uma VLAN é um segmento de rede que compreende um domínio de *broadcast*, criada dentro de um *switch*, permitindo que este equipamento único opere como se fosse diversos equipamentos independentes.

O tráfego de uma VLAN só pode ser levado a outra VLAN por meio de roteamento. Mais informações sobre este padrão podem ser encontradas em (802.1Q, 2012).

A maneira mais comum de se trabalhar com VLANs, principalmente em um sistema de firewall, é utilizando uma ligação conhecida por Trunk. Uma ligação Trunk permite que várias VLANs sejam passadas em uma mesma interface de rede. Ao serem enviados por um Trunk, os pacotes são marcados (*tagging*) com um identificador de VLAN (VLAN ID). O padrão 802.1Q é quem define o cabeçalho e como ocorrem as marcações de um pacote. Desta forma, um roteador pode estar conectado a diversas redes diferentes, cada uma sendo representada por uma VLAN. Todo este tráfego pode ser levado ao firewall por apenas uma ligação Trunk. Os pacotes serão marcados na saída do roteador e, ao chegarem no firewall, este saberá a qual rede física (domínio de *broadcast*) o pacote pertence.

Em equipamentos de rede, como switches, é comum a configuração indicar explicitamente que uma porta opera em modo Trunk. No caso do pfSense, as configurações são realizadas de modo apenas a criar uma VLAN dentro do firewall e, neste momento, indicar uma interface pai (*parent interface*). A *parent interface* indicará a interface que está operando em modo Trunk, ou seja, capaz de suportar pacotes marcados pelo 802.1Q. A criação de uma VLAN pode ser executada no menu Interfaces → (assign), na aba VLANs (Figura 41).



VLAN configuration	
Parent interface	em0 (08:00:27:ce:d6:be) Only VLAN capable interfaces will be shown.
VLAN tag	802.1Q VLAN tag (between 1 and 4094)
Description	You may enter a description here for your reference (not parsed).

Figura 41. Criação de uma VLAN: indicação da interface pai, do ID e uma descrição.

Após a criação da VLAN é necessário atribuir uma interface no firewall que pertença a esta VLAN. Somente assim os pacotes poderão chegar ao firewall. Para tal, deve-se acessar o menu Interfaces → (assign), aba Interface assignments e clicar sobre o ícone “+”, para atribuir uma nova

interface ao firewall. Ao atribuir uma nova interface, o pfSense utiliza a nomenclatura OPT1, de interface opcional. Clicando no menu Interfaces → OPT1, é possível habilitar esta interface e renomeá-la. Deve-se entender por “atribuir uma interface ao firewall” a ação de informar o sistema que uma nova interface existe e poderá ser configurada. Esta interface tanto pode ser física quanto virtual.

Após a atribuição e renomeação da interface, é possível então vincular a VLAN a esta interface. No exemplo a seguir, a interface atribuída chama-se Interface_vlan_200 e a porta utilizada é a “VLAN 200 on em3 (Rede da Vlan 200)”. Estas configurações representam o seguinte cenário: a interface Interface_vlan_200 é uma interface do firewall, ligada na VLAN 200, utilizando para isso a porta física em3 que opera como um Trunk (Figura 42).

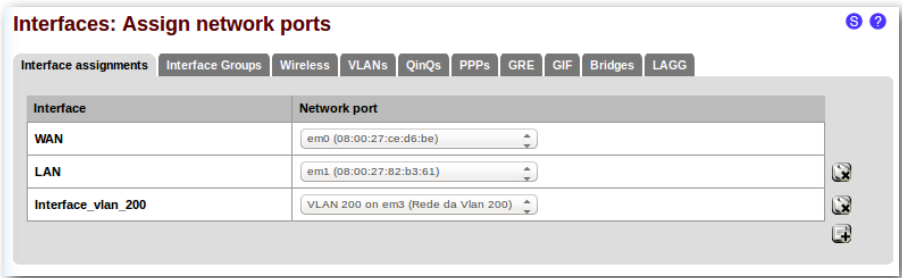


Figura 42. Atribuição de uma interface na VLAN 200 no firewall: interface atrelada à interface física em3 que é a interface pai desta VLAN.

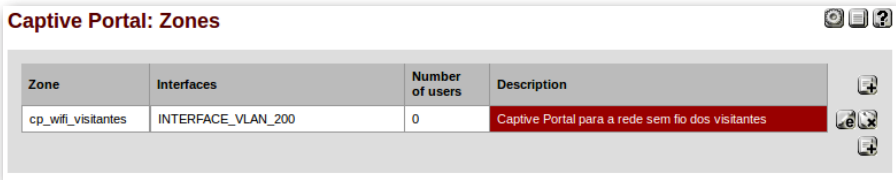
Desta mesma forma é possível adicionar diversas outras interfaces virtuais em cada uma das VLANs utilizadas no ambiente de rede. Cada uma dessas interfaces, independente de serem físicas ou virtuais, aparecerão na lista de interfaces no menu Firewall → Rules, de modo que passa a ser possível a criação de regras para o tráfego relacionado a cada uma dessas redes.

7.7 Captive Portal

Captive Portal é uma funcionalidade que permite ao administrador de rede um controle prévio do usuário antes que este possa, de fato, se conectar a outras redes. Ele normalmente é utilizado para redirecionar o usuário a uma página de aviso ou mesmo para autenticá-lo, só permitindo o uso da

rede para usuários autorizados. O uso mais comum é para controle de redes sem fio. Porém, o Captive Portal do pfSense pode ser utilizado normalmente em redes cabeadas.

O pfSense utiliza o conceito de ‘zonas’ para a criação de portais. Desta forma, é possível criar vários portais no mesmo firewall, relacionando-os com as interfaces existentes. Uma zona pode conter várias interfaces mas uma interface pode estar associada a apenas uma zona. Para a criação de uma zona deve-se utilizar o menu Services → Captive Portal (Figura 43).



Zone	Interfaces	Number of users	Description
cp_wifi_visitantes	INTERFACE_VLAN_200	0	Captive Portal para a rede sem fio dos visitantes

Figura 43. Services → Captive Portal: lista de portais criados.

Ao entrar na edição da zona criada existem diversas opções de customização que podem ser utilizadas pelo administrador para adequar o portal às suas configurações de rede. As mais comumente utilizadas são:

Interfaces: em quais interfaces o portal irá operar.

Pre-authentication redirect URL: uma URL que pode ser acessada pelo usuário antes de sua autenticação. Esta URL ficará disponível na página customizada do portal.

After authentication Redirection URL: caso informada, os usuários serão redirecionados a esta URL após a autenticação.

Authentication: método de autenticação a ser utilizado pelo Captive Portal. O Radius é um dos mais comuns.

Portal page contents: esta opção é utilizada para fazer *upload* de uma página HTML ou PHP customizada que será a página inicial mostrada ao usuário. Conforme indicações de configuração, esta página deverá conter um formulário com método POST para a ação `action="$PORTAL_ACTION$"`, com um botão de submissão chamado ‘accept’ e um campo oculto com `name="redirect url"` e valor `value="$PORTAL_REDIRURL$"`, os valores de input `auth_user` e `auth_pass` (e/ou `auth_voucher`), para o caso

de se utilizar autenticação. Estes são os campos mínimos para utilizar um portal que execute autenticação.

Authentication error page contents: trata-se da página que será mostrada ao usuário caso a autenticação falhe. Nesta página pode-se incluir a variável “\$PORTAL_MESSAGE\$”, que será substituída pelo erro ou mensagem de retorno quando utilizando um servidor Radius para a autenticação.

Outras configurações importantes para os portais estão nas abas ‘Allowed IP addresses’ e ‘Allowed Hostnames’. Estas abas permitem a declaração de hosts que podem ser acessados sem que o usuário esteja autenticado. Um exemplo seria a utilização de um sistema de cadastro de usuários que esteja hospedado em um host diferente do firewall. Assim, será necessário que o usuário tenha acesso a este servidor antes de ser autenticado para que possa, justamente, solicitar um cadastro. A página inicial do portal pode conter um link para este sistema de cadastro e o servidor que o hospeda deverá ser liberado por meio dessas opções, utilizando seu endereço IP ou um nome.

Considerações sobre o uso do Radius

O pfSense oferece algumas opções de autenticação para o uso do Radius. Ao se implementar um Captive Portal, o administrador deve escolher o método que melhor o atende. Ao utilizar os padrões MS-CHAP, as senhas devem estar neste padrão e o Radius corretamente configurado para aceitar autenticações desta maneira.

Uma observação importante para caso se opte pela utilização de PAP, o método mais simples de autenticação, é que, embora seja possível manter as senhas em *hash* na base de dados, elas vão trafegar em texto plano até o Radius. O Radius, por sua vez, possui diretivas de *log* e, por padrão, registra todas as tentativas. Para desabilitar o registro de senhas no arquivo de *log* do Radius, deve-se alterar o arquivo de configuração *radiusd.conf* e na seção *log*, utilizar as diretivas *auth_badpass = no* e *auth_goodpass = no*.

7.8 Instalação de pacotes

O pfSense permite a instalação de pacotes utilizados para estender as funcionalidades da distribuição. Os pacotes são desenvolvidos, na maioria, pela comunidade e não pelo time de desenvolvimento do próprio pfSense. Também é importante mencionar que os pacotes para o pfSense não são os pacotes do Ports utilizado pelo FreeBSD.

Observação: é possível utilizar pacotes do ports no pfSense, mas esta não é uma recomendação. Os ports devem ser construídos fora do sistema, pois o pfSense não possui compilador. Também é possível utilizar os gerenciadores de pacote, como o 'pkg'. No entanto, fica a ressalva que, ao instalar um pacote, bibliotecas do sistema podem ser sobrescritas por bibliotecas deste pacote, o que pode gerar mal funcionamento do firewall.

Os pacotes do pfSense podem ser instalados através do menu System → Packages que é dividido nas abas Available Packages e Installed Packages (Figura 44).

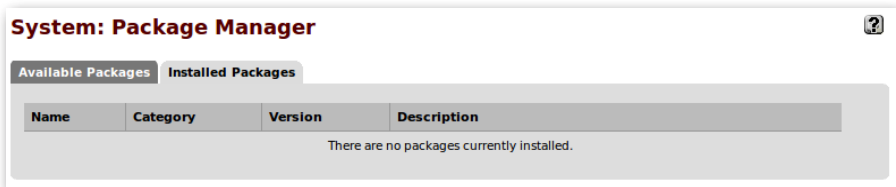


Figura 44. Instalação de pacotes do pfSense.

Até a versão 2.0.x o pfSense utilizava o mesmo formato binário de pacotes do FreeBSD. Esta solução apresentava problemas em determinados casos, quando a instalação de um pacote sobrepunha arquivos do sistema base. Ao desinstalá-lo, existia então a possibilidade de se remover algum arquivo do sistema base, o que poderia tornar o pfSense inoperante. A partir da versão 2.1 o pfSense passou a utilizar o formato PBI - *Push Button Install*. Um PBI é um arquivo 'self-contained', ou seja, ele possui todas as dependências que o pacote necessita para funcionar e é instalado em um diretório isolado. Desta forma, o sistema base permanece sem nenhuma alteração.

Uma vez que um pacote é instalado, normalmente suas entradas são criadas nos menus correspondentes. Por exemplo, é possível que um pacote crie uma entrada no menu Services, onde será possível configurar o serviço em questão, e outra no menu Status, onde será possível verificar a operação do mesmo.

Os pacotes mais utilizados no pfSense são o SquidProxy e pacotes relacionados, como o SquidGuard e LightSquid. Além destes pacotes relacionados às atividades de operação de redes, um pacote bastante importante é o Cron. Conforme mencionado anteriormente, o pfSense sobrescreve diversos arquivos do sistema de acordo com as configurações do config.xml. O crontab é um desses arquivos. Desta forma, caso algum agendamento seja criado diretamente nele, em algum momento o arquivo será sobrescrito. O pacote Cron permite que os agendamentos sejam configurados pela interface web e permaneçam no sistema.

7.9 Serviços básicos

Considerando a operacionalização de uma rede, dois serviços básicos facilmente configuráveis no pfSense são o DHCP e o DNS.

7.9.1 DHCP

O DHCP é o serviço responsável pela atribuição de IPs e algumas outras configurações de rede para os dispositivos clientes. O pfSense pode operar ou como DHCP Relay, de forma que as requisições serão encaminhadas para outro servidor DHCP, ou como o próprio servidor DHCP. O mais comum é a utilização do firewall como servidor de DHCP. As configurações podem ser realizadas pela interface web (Figura 45), compreendendo diversas informações que podem ser enviadas aos clientes. Para obter maiores informações deve-se consultar a definição do padrão (DHCP, 2015).

Dentre as diversas opções, em “Additional BOOTP/DHCP Options” existem várias opções de informações possíveis de serem enviadas pelo protocolo DHCP. Exemplo disso são informações de Proxy via WPAD (WPAD, 2015).

Services: DHCP server

LAN

Enable DHCP server on LAN interface

Deny unknown clients
If this is checked, only the clients defined below will get DHCP leases from this server.

Subnet 192.168.1.0

Subnet mask 255.255.255.0

Available range 192.168.1.1 - 192.168.1.254

Range 192.168.1.10 to 192.168.1.245

Additional Pools
If you need additional pools of addresses inside of this subnet outside the above Range, they may be specified here.

Pool Start	Pool End	Description

WINS servers

DNS servers

NOTE: leave blank to use the system default DNS servers - this interface's IP if DNS Forwarder or Resolver is enabled, otherwise the servers configured on the General page.

Gateway

The default is to use the IP on this interface of the firewall as the gateway. Specify an alternate gateway here if this is not the correct gateway for your network. Type "none" for no gateway assignment.

Domain name

The default is to use the domain name of this system as the default domain name provided by DHCP. You may specify an alternate domain name here.

Domain search list

The DHCP server can optionally provide a domain search list. Use the semicolon character as separator

Default lease time seconds

Figura 45. Configuração do servidor de DHCP na interface LAN.

7.9.2 DNS

Outro serviço essencial em uma rede é a resolução de nomes (DNS). De maneira semelhante ao DHCP, o pfSense pode ser tanto um Forwarder de requisições DNS quando o responsável pela resolução.

Quando configurado como Forwarder, o pfSense encaminhará as requisições, por padrão, para o servidor DNS configurado para o próprio firewall em 'System: General Setup', ou àqueles obtidos por DHCP na interface WAN. Já quando estiver operando como Resolver, o pfSense fará o papel de recursivo, consultando outros servidores DNS para realizar as traduções de nomes.

Ambas as configurações podem ser encontradas no menu Services. Uma observação importante é relativa à operação como Forwarder. Caso o ambiente de rede utilize Views ou qualquer esquema de DNS com alguma separação, como por exemplo, resolução de nomes internos que não são resolvidos externamente, é importante utilizar a configuração Domain Overrides, dentro da configuração do Forwarder. Desta forma, será possível indicar servidores autoritativos para diferentes domínios de maneira manual, fazendo com que as consultas para estes domínios sejam encaminhadas para os servidores informados.

7.10 Alta disponibilidade com CARP

O pfSense oferece meios para o estabelecimento de um sistema de firewall com alta disponibilidade, utilizando hardware redundante, possibilitando alternar entre master e slave mantendo até mesmo o estado das conexões. São três as tecnologias que permitem este grau de redundância, descritas a seguir.

7.10.1 CARP

O Common Address Redundancy Protocol é um protocolo livre criado pelos desenvolvedores do OpenBSD como resposta a soluções semelhantes, como o VRRP (Virtual Router Redundancy Protocol), que esbarravam em requisitos de patentes. O CARP possibilita que duas (ou mais) interfaces em um mesmo segmento de rede compartilhem um IP virtual (VIP), de forma que a interface *master* responderá por este IP e, no caso de seu desligamento, a interface *slave* passe a responder. O CARP utiliza um grupo para comunicação entre as interfaces participantes. Pacotes de controle são enviados via Multicast para que todas as interfaces se monitorem.

Cada grupo CARP utiliza um identificador chamado VHID (Virtual Host ID). O *'advertisement base'* representa um intervalo de tempo em que os pacotes de controle são enviados, sendo o padrão de 1 segundo. Skew é uma prioridade utilizada para se definir o *master*, que responderá pelo IP virtual. Caso um pacote de controle não seja visto no intervalo *'advertisement base'*, a interface configurada com o menor valor em skew assumirá que um erro ocorreu e passará a ser a *master* para o IP compartilhado. No

pfSense, a configuração do CARP é tal que, se alguma interface apresente falha, o outro firewall é promovido a *master*, mesmo que as outras interfaces continuem com problema. Este chaveamento é necessário para evitar problemas de aceitação de pacotes com estados, roteamento e NATs.

Duas observações são importantes sobre o CARP: 1) é comum existir a confusão de que os pacotes de controle do CARP são enviados por uma interface isolada que liga os dois firewalls, conforme será visto no pfsync, o que de fato não ocorre, pois esses pacotes são enviados justamente na rede em que se liga as interfaces participantes do grupo; 2) o CARP necessita de um endereço IP para cada interface mais o IP virtual, ou seja, no mínimo três endereços IPs, de forma que o menor bloco para uma rede com CARP é um /29, com 6 endereços utilizáveis.

Para a configuração do CARP deve-se utilizar o menu Firewall → Virtual IPs, clicando no ícone de adicionar. Vale lembrar que, para realizar a configuração de um IP virtual é necessário ter no mínimo duas interfaces ligadas no mesmo segmento de rede, já configuradas. As informações a serem configuradas estão dispostas na Figura 46, sendo elas: a indicação do tipo de IP virtual como CARP; em qual interface ele operará; o endereço

Firewall: Virtual IP Address: Edit ?

Edit Virtual IP

Type	<input type="radio"/> IP Alias <input checked="" type="radio"/> CARP <input type="radio"/> Proxy ARP <input type="radio"/> Other
Interface	INT_UPL ▼
IP Address(es)	Type: Single address ▼ Address: 10.129.192.1 / 24 ▼ <small>This must be the network's subnet mask. It does not specify a CIDR range.</small>
Virtual IP Password Enter the VHID group password.
VHID Group	8 ▼ Enter the VHID group that the machines will share
Advertising Frequency	Base: 1 ▼ Skew: 0 ▼ The frequency that this machine will advertise. 0 means usually master. Otherwise the lowest combination of both values in the cluster determines the master.
Description	IP virtual da rede 192 UPLink Core Fwints You may enter a description here for your reference (not parsed).

Figura 46. Configuração de um IP virtual CARP.

IP virtual; a máscara da sub-rede (deve ser a mesma máscara utilizada na interface); uma senha a ser utilizada por todos os integrantes deste grupo CARP, para fins de sincronização; o identificador do grupo (VHID); a frequência de anúncios (Base); um valor de precedência para se tornar o *master* (Skew, quanto menor mais prioritário); e, por fim, uma descrição.

Uma vez que o IP virtual tenha sido criado, através do menu Status → CARP (failover) é possível visualizar seu estado (Figura 47). A indicação será de MASTER quando o IP estiver em operação no firewall em questão, ou BACKUP, quando o IP estiver em operação em outro firewall.

Status: CARP 🔍 🔄 ?

Temporarily Disable CARP Enter Persistent CARP Maintenance Mode

CARP Interface	Virtual IP	Status
WANUPLKGW2@1	245	▶ MASTER
WANUPLKGW2@2	246	▶ MASTER
INT_EBPX@6	254	▶ MASTER
INT_EBPV@7	254	▶ MASTER
INT_UPL@8	10.129.192.1	▶ MASTER
WANUPLKGW2@9	254	▶ MASTER
INT_SPM@10	.1	▶ MASTER
INT_200_0A127@11	26	▶ MASTER

Figura 47. Status dos IPs virtuais CARP: firewall respondendo por todos eles (MASTER).

A seção “Atualização de sistemas com alta disponibilidade (master e slave)” traz explicações sobre as opções “Temporary Disable CARP” e “Enter Persistent CARP Maintenance Mode”.

Uma observação muito importante sobre a utilização do CARP é que, após o estabelecimento do IP virtual, dependendo dos serviços utilizados, é necessário que estes sejam reconfigurados para que a rede se torne, de fato, altamente disponível. Por exemplo, se o firewall atua como servidor de DHCP para alguma rede, será necessário configurar o servidor DHCP para distribuir como *gateway* o **IP virtual**. O mesmo acontece com qualquer outro serviço que utilize um IP do firewall.

7.10.2 pfsync

O pfsync permite a sincronização da tabela de estados entre o firewall *master* e o *slave*. Esta sincronização utiliza pacotes Multicast por padrão e pode ocorrer em qualquer interface ativa do firewall. Desta forma, pode-se sincronizar do *master* para vários *slaves*. Quando o cenário utiliza apenas dois firewall é possível indicar nas configurações do pfSense um endereço para que a sincronização ocorra em modo Unicast.

É recomendado utilizar uma interface dedicada para o pfsync pois, além de não haver dispositivos de segurança neste protocolo, o que torna possível, por exemplo, a inserção de entradas na tabela de estados do firewall secundário, a banda utilizada pode representar até 10% da banda passante do firewall, ou seja, o tráfego de sincronização pode impactar na performance geral da filtragem e encaminhamento de pacotes.

A sincronização da tabela de estados permite o que é conhecido como ‘*seamless failover*’, ou seja, a troca do hardware que executa os serviços de firewall sem que as conexões sejam interrompidas. O pfsync deve ser habilitado em todos os nós participantes de uma configuração em alta disponibilidade.

Para configurar a sincronização com pfsync deve-se utilizar o menu System → High Avail. Sync (Figura 48).

Para o pfsync, deve habilitar “Synchronize States”, escolher a interface dedicada para este tráfego (caso de dois firewall – unicast) e o IP do slave. Neste mesmo menu constam as configurações do XML-RPC, descritas a seguir.

System: High Availability Sync

State Synchronization Settings (pfsync)

Synchronize States

pfsync transfers state insertion, update, and deletion messages between firewalls. Each firewall sends these messages out via multicast on a specified interface, using the PFSYNC protocol (IP Protocol 240). It also listens on that interface for similar messages from other firewalls, and imports them into the local state table.

This setting should be enabled on all members of a failover group.

NOTE: Clicking save will force a configuration sync if it is enabled! (see Configuration Synchronization Settings below)

Synchronize Interface SYNC

If Synchronize States is enabled, it will utilize this interface for communication.

NOTE: We recommend setting this to a interface other than LAN! A dedicated interface works the best.

NOTE: You must define a IP on each machine participating in this failover group.

NOTE: You must have an IP assigned to the interface on any participating sync nodes.

pfsync Synchronize Peer IP 172.16.0.2

Setting this option will force pfsync to synchronize its state table to this IP address. The default is directed multicast.

Configuration Synchronization Settings (XMLRPC Sync)

Synchronize Config to IP 172.16.0.2

Enter the IP address of the firewall to which the selected configuration sections should be synchronized.

NOTE: XMLRPC sync is currently only supported over connections using the same protocol and port as this system - make sure the remote system's port and protocol are set accordingly!

NOTE: Do not use the Synchronize Config to IP and password option on backup cluster members!

Remote System Username admin

Enter the webConfigurator username of the system entered above for synchronizing your configuration.

NOTE: Do not use the Synchronize Config to IP and username option on backup cluster members!

Remote System Password ••••••••

Enter the webConfigurator password of the system entered above for synchronizing your configuration.

NOTE: Do not use the Synchronize Config to IP and password option on backup cluster members!

Figura 48. Configuração do pfsync e XML-RPC: indicar o par para a sincronização (Unicast).

7.10.3 XML-RPC

O XML-RPC é característico do pfSense e permite a sincronização da maior parte das configurações (existem seções e pacotes cujas configurações não são sincronizadas). As configurações devem ser realizadas **sempre no nó *master***, sendo então replicadas para o *slave*. Desta forma,

o administrador sempre altera um único local, o sistema *master* (raramente tem que alterar o *slave*). As áreas cuja sincronização é suportada são:

- Usuários e grupos.
- Servidores de autenticação.
- Certificados.
- Regras de firewall.
- Agendamentos de regras de firewall.
- *Aliases*.
- NAT.
- IPSec.
- OpenVPN.
- DHCP.
- Wake on Lan.
- Rotas.
- Gateways.
- Load Balancer.
- IPs virtuais.
- Traffic shaper.
- DNS forwarder.
- Captive Portal.

Outras configurações devem ser executadas diretamente no firewall secundário (exemplos importantes são as configurações de interfaces e do Squid Proxy, quando utilizado). A sincronização de configurações deve usar a mesma interface do tráfego pfsync. Por fim, e muito importante, as configurações de XML-RPC devem ser habilitadas **apenas no *master***. Todos os

outros nós devem ficar com a configuração **desabilitada**. A Figura 48 mostra a configuração do XML-RPC, no mesmo menu System → High Avail. Sync utilizado para o pfsync. Deve-se indicar o endereço do *slave*, a senha de acesso ao firewall slave e marcar todas as opções existentes.

7.11 Atualização

Na maioria dos casos o pfSense pode ser atualizado normalmente. No entanto, como parte do procedimento, é sempre recomendada a verificação da nova versão, principalmente relativa às compatibilidades de versões com hardware. Novas versões contêm novas funcionalidades, correções de erros e várias outras mudanças.

Atualizações nos chamados *point releases* (por exemplo, 2.0.4 para 2.0.5) são simples e geralmente não causam problemas. Trocas de versões distantes merecem mais cuidados, como por exemplo da versão 1.2.3 para a 2.0. Nestes casos, recomenda-se testar em hardware idêntico para se determinar se a migração é possível.

Os dois passos iniciais para se iniciar um processo de atualização é realizar um backup utilizando o menu Dignostics → Backup/Restore, escolhendo as opções para copiar todos os dados e, ter de antemão uma cópia da mídia de instalação da versão atualmente em execução. Desta forma, qualquer problema pode ser rapidamente revertido, instalando-se novamente o sistema e restaurando suas configurações.

7.11.1 Atualização via interface web

A atualização via interface web pode tanto ser pelo *upload* manual de uma nova versão quanto utilizando a própria interface. Para a atualização manual, o *firmware* deve ser obtido previamente do site do pfSense. É importante observar que existem duas versões de disponibilização no site, sendo uma para a instalação e outra para a atualização (*upgrade*). Para a atualização manual deve-se baixar a versão '*upgrade*'. Para instalar, deve-se utilizar o menu System → Firmware e clicar em 'Enable firmware upload', escolher o arquivo baixado e enviá-lo ao firewall. A atualização iniciará e, quando finalizada, o firewall reiniciará (Figura 49).

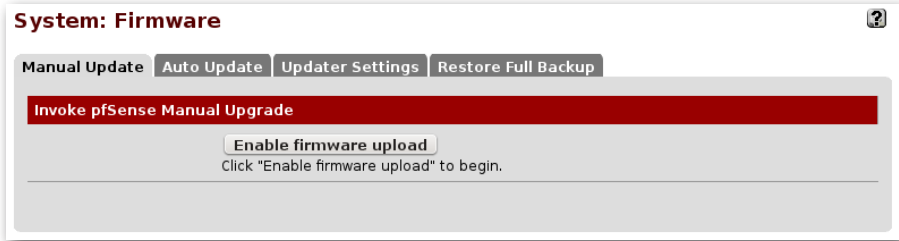


Figura 49. Atualização manual pela interface web: deve-se baixar o firmware (arquivo do tipo upgrade) e enviá-lo ao firewall.

A segunda maneira é utilizar a própria interface web. Esta funcionalidade contacta o servidor do pfSense para a identificação da versão atual e de novas versões. Caso exista uma nova versão, o administrador será notificado na página inicial, Dashboard (Figura 50).

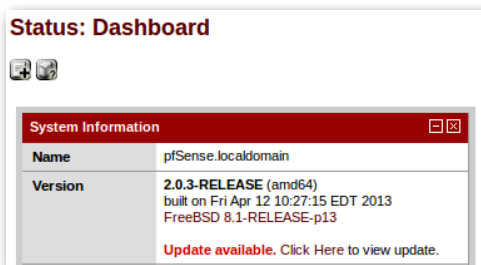


Figura 50. Página inicial do pfSense indicando ao administrador que existe uma nova versão para atualização.

Deve-se clicar na indicação para visualizar o update. Será aberta a página de 'autoupdate' (Figura 51).

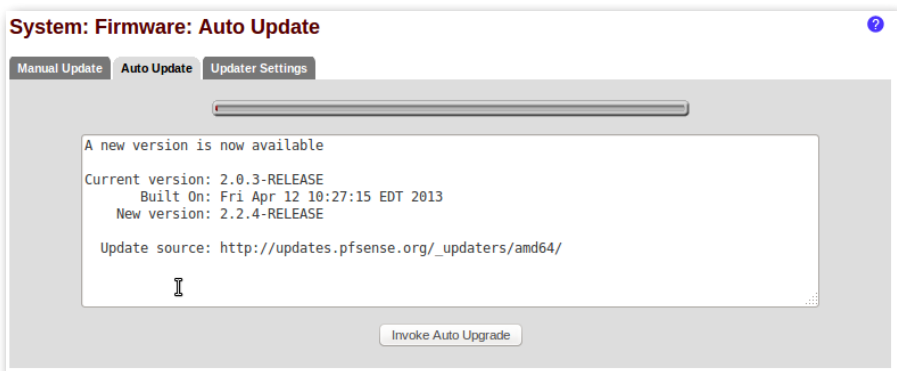


Figura 51. Página de autoupdate: indicações sobre a versão corrente e a versão a ser utilizada.

Ao clicar em 'Invoke Auto Upgrade', a interface realizará o download da nova versão e aplicará a atualização (Figura 52).

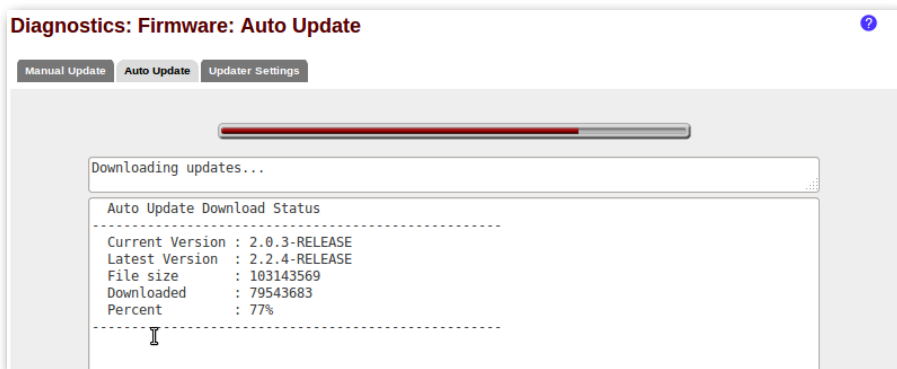


Figura 52. Interface web realiza o download da nova versão automaticamente.

Ao terminar o download, a atualização é aplicada e o firewall reiniciado (Figura 53).

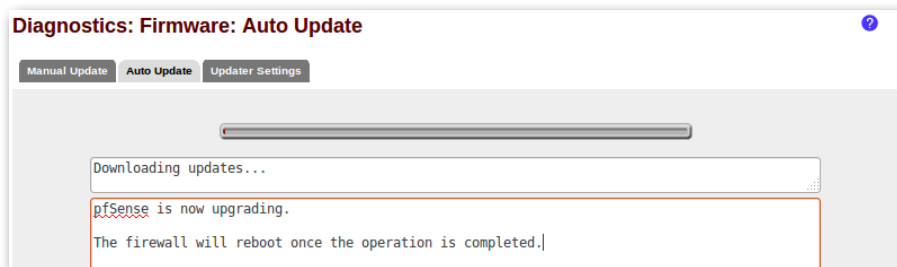


Figura 53. Aplicação da atualização: reboot após finalização.

7.11.2 Atualização via console

Além da atualização via interface, é possível utilizar o console. Para tal, na tela inicial do console, escolher a opção '13) Upgrade from console' (Figura 54).

Ao escolher a opção 13, deve-se então optar por uma das duas maneiras de se obter a atualização: pode-se informar uma URL onde o pfSense fará o download ou indicar um arquivo local, que deve ser enviado previamente para o firewall. No caso da URL, se o administrador apenas teclar ENTER,

```

WAN (wan)      -> em0      -> v4/DHCP4: 10.0.2.15/24
LAN (lan)     -> em1      -> v4: 192.168.1.1/24
INTERFACE_OLAN_200 (opt1) -> em3_vlan200 ->
0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) pfSense Developer Shell
4) Reset to factory defaults    13) Upgrade from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                15) Restore recent configuration
7) Ping host                  16) Restart PHP-FPM
8) Shell

Enter an option: 13

Starting the pfSense console firmware update system..

1) Update from a URL
2) Update from a local file
Q) Quit

Please select an option to continue: █

```

Figura 54. Atualização via console (opção 13): download do firmware via URL ou de um arquivo local.

o pfSense utilizará as informações que possui para o *autoupdate*. Caso deseje-se informá-la, deve-se buscar nos repositórios online do pfSense pela versão pretendida e copiar o endereço.

7.11.3 Atualização de sistemas com alta disponibilidade (*master* e *slave*)

Para sistemas que operam em alta disponibilidade, utilizando um *master* e um *slave* com IPs virtuais CARP e sincronização de configurações e tabelas de estado, o procedimento de atualização deve tomar determinados cuidados.

Neste cenário recomenda-se a atualização primeiramente do sistema *slave*. Desta forma, é possível testar primeiro se a atualização finalizará com sucesso e, depois, se o sistema atualizado realmente opera conforme deveria.

Constatando-se operação normal do *master* e do *slave*, ao se desligar o *slave* não haverá prejuízos para o sistema de firewall. Desta forma, pode-se atualizá-lo e reiniciá-lo sem interrupções.

Assim que o *slave* esteja atualizado e ligado é possível, por opções do CARP, passar o papel do firewall ativo para o slave. Deve-se acessar o menu Status → CARP (failover).

Conforme observado na Figura 55, a opção ‘Enter Persistent CARP Maintenance Mode’ permite que o firewall em questão entre em modo de manutenção, significando que a operação como firewall ativo será passada ao slave. **Este modo persiste após reinicializações.** Assim, pode-se reinicializar o firewall quantas vezes forem necessárias sem que, ao ligar, ele volte ao papel de master. Quando ele estiver pronto para voltar ao papel de **master**, deve-se clicar no mesmo botão que estará visível como ‘Leave Persistent CARP Maintenance Mode’.

Status: CARP

Temporarily Disable CARP Enter Persistent CARP Maintenance Mode

CARP Interface	Virtual IP	Status
WANUPLKGW2@1	245	▶ MASTER
WANUPLKGW2@2	246	▶ MASTER
INT_EBPX@6	254	▶ MASTER
INT_EBPV@7	254	▶ MASTER
INT_UPL@8	2.1	▶ MASTER
WANUPLKGW2@9	254	▶ MASTER
INT_SPM@10	1.1	▶ MASTER
INT_200_0A127@11	26	▶ MASTER

Figura 55. Status → CARP (failover): lista de IPs virtuais e indicação de que o sistema opera como master para todos os endereços. Opção ‘Enter Persistent CARP Maintenance Mode’ permite que o papel seja passado ao *slave*.

8 Dicas e troubleshooting

Esta seção tem por finalidade elencar algumas dicas relacionadas a problemas solucionados em um ambiente de produção, considerados de certa forma comuns.

8.1 Problema ao realizar download de pacotes

Caso esteja ocorrendo problemas ao tentar efetuar o download de pacotes, pode ser necessário alterar o *mirror* de onde estes são baixados. Para isso, deve entrar em modo console e alterar o arquivo `/etc/inc/globals.inc` na diretiva `'xmlrpcbaseurl'`. Este problema pode ocorrer caso se esteja executando o pfSense através de um proxy. Pode-se tentar, por exemplo, utilizar HTTP em vez de HTTPS, pois o problema pode ser na checagem do certificado, ou alterar a fonte dos pacotes [Forum pfSense, 2015].

8.2 Interfaces de rede Broadcom em servidores Dell

O pfSense recomenda que alguns modelos de placas tenham configurações específicas, como é o caso de algumas Broadcom. As alterações devem ser realizadas no arquivo `/boot/loader.conf.local` adicionando as seguintes linhas:

```
kern.ipc.nmbclusters="131072"  
hw.bce.tso.enable=0  
hw.pci.enable_msix=0
```

Caso seja observada uma perda de pacotes pequenos UDP, deve-se utilizar também:

```
net.isr.direct_force=1  
net.isr.direct=1
```

8.3 Captive Portal quando utilizando arquivo WPAD

O WPAD (WPAD, 2015) é utilizado para a autoconfiguração de proxy nos *hosts* que obtêm IPs automaticamente por DHCP. É utilizado um arquivo descritor do proxy e, ao obter informações do servidor DHCP, os clientes que suportam WPAD automaticamente configuram o proxy do sistema.

No entanto, em um cenário de Captive Portal, o firewall realiza uma filtragem por Mac Address de forma que, somente quando o usuário for autori-

zado, o Mac Address será liberado e o firewall encaminhará seus pacotes. Para que esta autorização ocorra é necessário que o cliente realize algum acesso HTTP, a fim de que seja redirecionado para a página de autenticação.

O problema ocorre quando o cliente obtém informações do proxy e o configura no sistema automaticamente, na fase de obtenção do IP. O efeito é que, as requisições HTTP que este cliente realizar irão diretamente para o proxy (não haverá um acesso HTTP na porta 80). Para evitar este problema, na configuração do proxy (Squid Proxy, usar o menu Services → Proxy Server), existe uma opção que deve ser marcada, chamada 'Patch captive portal'. Esta opção configurará o proxy para não liberar os clientes da rede do Captive Portal.

8.4 Monitoramento com ping em redes com Captive Portal e alta disponibilidade

Caso se possua um cenário com alta disponibilidade utilizando CARP, deve-se ficar atento ao monitoramento e testes com ICMP Echo Request (ping). Uma vez que o Captive Portal apenas passa a aceitar tráfego de um cliente autorizado, é comum que o firewall *slave*, por exemplo, não consiga pingar o *master*. Ao enviar os pacotes de ICMP Echo Request, o IP do *slave* não estará autorizado no Captive Portal que está em execução no *master* e, conseqüentemente, esses pacotes serão todos descartados, **sem a geração de nenhum registro de log**. Para facilitar a manutenção, é recomendado que o VIP que responde como gateway da rede do Captive Portal seja inserido nas configurações do próprio Captive Portal, em Services → Captive Portal → zona em questão → aba Allowed IP Addresses, como liberado. Desta forma os sistemas poderão realizar pings sem problemas.

8.5 Problema com os relatórios do SARG (pacote para geração de relatórios dos logs do Squid)

Em algumas instalações do SARG ele pode não gerar os relatórios após sua configuração normal, conforme instrui a documentação do pacote. Em

alguns casos trata-se de uma indicação errada do diretório dos relatórios que pode ser resolvida com os seguintes comandos:

```
rm -r /usr/local/sarg-reports
ln -s /usr/pbi/sarg-amd64/local/sarg-reports /usr/
local/sarg-reports
```

8.6 Logs do Squid Proxy

O Squid não gera logs através do Syslog do sistema de forma que, mesmo que a exportação de logs esteja configurada para ser executada de forma remota, os logs do proxy ficam em arquivos separados, em `/var/squid/logs`. Para exportá-los pode-se utilizar uma chave SSH sem senha, de modo que os logs possam ser copiados para um servidor remoto periodicamente. Exemplos de comandos que podem ser utilizados para esta cópia são:

```
/usr/bin/scp /var/squid/logs/access.log.0 cnptia@log.
cnptia.embrapa.br:/home/cnptia/fwint_squid_log_master/
access.log.`/bin/date -v -ld +%Y%m%d`
/usr/bin/scp /var/squid/logs/cache.log.0 cnptia@log.
cnptia.embrapa.br:/home/cnptia/fwint_squid_log_master/
cache.log.`/bin/date -v -ld +%Y%m%d`
```

Estes comandos devem constar configurados dentro do pacote Cron (atenção para os caminhos completos dos binários e escapes de caracteres especiais). Apenas lembrando, o pacote Cron é necessário para que alterações feitas no arquivo `/etc/crontab` não sejam sobrescritas pelo sistema (o pfSense gera os arquivos de configuração do sistema com base no arquivo `config.xml`). Os comandos acima presumem que os logs são rotacionados todos os dias à 0h e estão agendados para executar **após** este horário. Desta forma, os logs `‘.0’` correspondem ao dia anterior e são copiados para o servidor remoto com o nome que reflita o dia de seus registros.

8.7 Utilização de tabelas para *thresholds* em regras de filtragem

Um tipo de controle comum para administradores que trabalham com o PF é a utilização de tabelas de endereços e opções avançadas de filtragem nas regras, de forma que, se determinado valor é atingido, o *host* entra para a tabela. Em uma verificação posterior, *hosts* que estão nesta tabela serão bloqueados. No pfSense, estas opções ficam no botão “Advanced Options”, no momento em que uma regra está sendo criada.

No PF é possível utilizar diversas tabelas, nomeadas pelo criador do firewall. No caso do pfSense é utilizada uma tabela *default* chamada ***virusprot***. Esta tabela pode ser verificada no menu Diagnostics → Tables, escolhendo a tabela *virusprot* na caixa de seleção. Sempre que uma opção avançada for adicionada a uma regra de filtragem, conforme botão mencionado acima, a regra de fato criada trará, além de seus parâmetros de filtragem, uma indicação “*overload virusprot*”. E, por padrão, o pfSense já possui um regra de bloqueio para hosts que estejam nesta tabela (pode ser verificado com o comando `pfctl -sr`):

```
block drop in log quick from <virusprot> to any label
"virusprot overload table"
```

Algumas correlações das opções do PF com as opções avançadas de regras de filtragem do pfSense são:

```
max-src-states = Maximum state entries per host
max-src-nodes = Maximum number of unique source hosts
max-src-conn-rate = Maximum new connections per host /
per second(s) (TCP only)
max-src-conn = Maximum number of established
connections per host (TCP only)
```

8.8 Configuração da *time zone* sem efeito

Quando se altera a time zone do sistema no menu System → General Setup, opção Time zone, é necessário reiniciar o firewall para que os logs

do PF passem a registrar a nova data. Os logs de sistema alteram-se imediatamente mas os logs do PF não (filterlog).

8.9 Tabela de proteção contra tentativas de login

O pfSense possui um sistema interno de bloqueio contra tentativas de login, o `sshlockout_pf` (`ps aux | grep lockout`). Ele detecta tentativas de login no firewall e insere na tabela `sshlockout`. Esta tabela não aparece nos *aliases*, mas pode ser vista em Diagnostics -> Tables. Há uma tabela semelhante chamada `webConfiguratorlockout`, para o caso da interface web. Caso não se esteja conseguindo efetuar login a partir de determinado *host*, pode ser que ele esteja bloqueado em alguma dessas tabelas. Existem duas regras criadas automaticamente:

```
block drop in log quick proto tcp from <sshlockout> to
(self) port = ssh label "sshlockout"
block drop in log quick proto tcp from
<webConfiguratorlockout> to (self) port = https label
"webConfiguratorlockout"
```

Essas regras são criadas de acordo com o arquivo `/etc/inc/filter.inc`. É possível customizar algo, mas esta configuração será sobrescrita em **atualizações** do sistema.

O `sshlockout_pf` é um binário simples. Ele aceita como parâmetro o número máximo de tentativas. Segundo o processo em execução (e documentação), o padrão é 15. Isso é definido no código em C, *hardcoded* (`sshlockout_pf.c`).

As informações utilizadas para bloqueios são do arquivo de log, conforme entrada no arquivo `/etc/syslog.conf`:

```
auth.info;authpriv.info |exec /usr/local/sbin/
sshlockout_pf 15
```

Essas tabelas elas podem ser observadas com:

```
pfctl -s Tables
```

Para usar as tabelas deve-se criar regras como:

```
pfctl -s Tables
```

Mais informações podem ser obtidas em [Docs pfSense, 2015].

8.10 Utilização do CARP VIP em ambientes com Squid Proxy

Em ambientes com alta disponibilidade que implementem o Squid Proxy, existe uma configuração extra do pacote Squid para que o ambiente realmente tenha alta disponibilidade para o serviço de proxy. Isto ocorre pois, na configuração normal do Squid, ele executa no endereço IP da interface do firewall. Ou seja, no *master* haverá um Squid executando na interface com o IP do *master* e no *slave* um Squid executando na interface com o IP do *slave*. No entanto, em todo o ambiente de rede, provavelmente os sistemas estarão configurados para utilizar o proxy a partir de um nome, por exemplo, proxy.dominio. Este nome resolverá para apenas um endereço IP. Para se obter a alta disponibilidade, quando um firewall cair e outro assumir, o firewall ativo deverá responder pelo IP do proxy.

É justamente esta configuração que deve ser realizada no Squid: inserção do VIP do CARP. Esta configuração não se dá automaticamente por se tratar de um pacote do sistema. Para realizá-la, deve-se acessar o menu Service → Proxy Server, aba General, na seção Custom Settings, em Custom ACLS (Before_Auth), adicionar a configuração:

```
acl rede_interna src 192.168.0.0/16
http_access allow rede_interna
http_port 192.168.0.1:3128
```

A primeira linha define a acl `rede_interna` como sendo os pacotes com origem na rede 192.168.0.0/16. É importante mencionar que, se a interface LAN do firewall, por exemplo, onde o proxy está sendo configurado, for uma rede /24 e este firewall recebe tráfego de outras redes, por exemplo, o segmento /16 inteiro, deve-se criar esta acl e permitir seu tráfego, caso contrário, o Squid só realizará proxy para a rede /24. A segunda linha é a

liberação da acl criada. A terceira linha é a responsável por instruir o Squid a também executar utilizando o IP 192.168.0.1. **Este IP representa, neste caso, o VIP do CARP.** Esta configuração deve ser realizada também no slave. Desta forma, caso o slave assuma o papel de firewall ao receber o VIP, o proxy funcionará corretamente.

9 Exercícios

Esta seção traz a sugestão de alguns exercícios para fixação dos conteúdos. Eles podem ser executados em ambientes de máquinas virtuais.

9.1 Instalação e inicialização básica

Neste exercício deve-se verificar a configuração padrão das interfaces LAN e WAN, com o NAT *default* criado pelo pfSense.

- Configurar parâmetros básicos para o próprio firewall tais como servidores de DNS, proxy, nomes aceitos na interface web etc.
- Configurar o cliente com IP fixo, na mesma rede da interface LAN, colocando o pfSense como gateway.

9.2 Navegação básica

Verificar as regras de NAT e deixar apenas a opção de Outbound NAT Automática.

- Verificar que o pfSense, embora não mostre as regras, já faz NAT para tráfego proveniente das LANs utilizando o IP da interface WAN.
- Sem nenhuma regra de Outbound, trocar para a opção “Manual”. Verificar que, ao passar para manual, essas regras automáticas são criadas explicitamente na aba Outbound.

9.3 Remoção de todas as regras

Esta prática objetiva a criação manual da regra de NAT masquerading para saída e liberação de tudo a partir da LAN. Testar acessos da máquina cliente para outros destinos.

9.4 DHCP e DNS

Utilizando o ambiente com NAT configurado em alguma das práticas anteriores, realizar a configuração do servidor DHCP e do DNS Forwarder na LAN. Na máquina cliente, remover o IP fixo e configurar a obtenção por DHCP. Verificar se a distribuição de IPs e DNS ocorreram corretamente.

9.5 Pacotes

Instalar os pacotes Squid3, Sarg e Cron. Navegar pelas configurações dos mesmos nos menus que são adicionados para cada um desses serviços, realizando customizações.

Na máquina cliente, configurar o proxy e realizar uma navegação na Internet. Verificar os logs gerados, tanto pelo terminal quanto pelos relatórios do Sarg.

Realizar o agendamento de alguma tarefa no pacote Cron.

9.6 CARP na LAN + pfSync + XML-RPC Sync

Criar uma nova máquina virtual com pfSense e configurar o endereçamento nas interfaces. Uma possível organização, considerando um ambiente no VirtualBox é:

Fw1

- Interface em0 com DHCP será a WAN – obtenção de IP do próprio VirtualBox, que fará NAT.
- Interface em1 com IP fixo 192.168.0.1/24 – será uma interface do tipo ‘Rede interna’ do VirtualBox.

- Interface em2 com IP fixo 172.16.0.1/30 – será uma interface do tipo ‘Rede interna’ do VirtualBox.

Fw2

- Interface em0 com DHCP será a WAN – obtenção de IP do próprio VirtualBox, que fará NAT.
- Interface em1 com IP fixo 192.168.0.2/24 – será uma interface do tipo ‘Rede interna’ do VirtualBox.
- Interface em2 com IP fixo 172.16.0.2/30 – será uma interface do tipo ‘Rede interna’ do VirtualBox.

Cliente

- Host configurado para obter IP via DHCP conectado a uma interface do tipo ‘Rede interna’ do VirtualBox. Ele apenas se comunicará com as máquinas Fw1 e Fw2. Todo seu tráfego deverá, obrigatoriamente, passar por um dos firewall.

Configurar o pfSync e o XML-RPC Sync para utilização das interfaces em2.

Habilitar alta disponibilidade com CARP, criando o VIP 192.168.0.254/24 nas interfaces em1.

Configurar o serviço de DHCP (utilizar o VIP como gateway) e DNS Forwarder.

Configurar o proxy e colocá-lo para executar no VIP.

Checar o status do CARP; disparar um ping e derrubar o firewall master.

3 Referências

802.1Q virtual bridged local area networks - bridge port extension. Disponível em: <<http://standards.ieee.org/getieee802/download/802.1BR-2012.pdf>> Acesso em: 4 nov. 2015.

DHCP Dynamic Host Configuration Protocol. Disponível em: <<https://www.ietf.org/rfc/rfc2131.txt>>. Acesso em: 4 nov. 2015.

DOCS PFSense Sshlockout. Disponível em: <<https://doc.pfsense.org/index.php/Sshlockout>>. Acesso em: 13 nov. 2015.

FORUM pfSenseTopic: [bug since 2.1.2] Unable to communicate with <https://packages.pfsense.org>. Disponível em: <<https://forum.pfsense.org/index.php?topic=75265.0>>. Acesso em: 12 nov. /2015.

WPAD. Web Proxy Auto-Discovery Protocol. Disponível em: <<https://tools.ietf.org/html/draft-ietf-wrec-wpad-01>>. Acesso em: 4 nov. 2015.

4 Literatura recomendada

BUECHLER, C. M.; PINGLE, J. **pfSense**: the definitive guide. Version 2.1. The definitive guide to the pfSense Open Source Firewall and router distribution. pfSense Forum. Disponível em: <<https://forum.pfsense.org/>>. Acesso em: 4 nov. 2016.



Informática Agropecuária

MINISTÉRIO DA
**AGRICULTURA, PECUÁRIA
E ABASTECIMENTO**



CGPE 12941