

Livro do PfSense 2.0



**Um guia prático com exemplos ilustrados de configurações,
para usuários iniciantes e avançados sobre o PfSense 2.0**

Feito originalmente em inglês por **Matt Williamson**
Traduzido por **Christopher Persaud**

Considerações iniciais

Eu, como um usuário que admira, uso e curto o PfSense 2.0, vi que existem poucas apostilas e livros em português referente a esse excelente sistema operacional, como vi que esse livro é muito bom e muito bem explicativo, decidi refazê-lo passando para o Português, não sei se já foi feito isso, mas estou fazendo a minha parte, espero que me desculpem por alguns erros de tradução, apesar de eu ter um pouco de noção em inglês eu traduzi a maior parte pelo Tradutor do Google, mas não passei para o livro ao pé da letra, eu li e passei para o livro de uma forma mais explicativa possível, algumas palavras que se referem ao Sistema PfSense 2.0 mantive em inglês (até o momento em que foi traduzido esse documento em 12/01/2012, ainda não tinha saído o PfSense em português).

Não quero tirar o mérito de toda a equipe que fez o livro originalmente já que é muito explicativo e ilustrativo, e aborda muitos recursos que com certeza muitos não sabiam que existia ou como usar.

Espero ter ajudado, essa foi minha contribuição para a melhora do projeto PfSense no Brasil.

**Acessem o fórum em português do PfSense para aperfeiçoar a aprendizado
<http://forum.pfsense.org/index.php?board=12.0>**

Um Salve a toda equipe PfSense do Brasil!!

“Compartilhar conhecimento traz mais crescimento do que se imagina”

Tabela de Conteúdo

<u>Capítulo 1 – Configuração Inicial</u>	1
Introdução	1
Aplicando configurações básicas em General Setup	2
Identificando e atribuindo interfaces	3
Configurando a Interface WAN	6
Configurando a Interface LAN	8
Configurando Interfaces Opcionais	10
Habilitando o Secure Shell (SSH)	12
Gerando chaves RSA autorizada	14
Configurando o SSH com autenticação de Chave RSA	16
Acessando por Secure Shell (SSH)	18
<u>Capítulo 2 – Servicos Essenciais</u>	20
Introdução	20
Configurando o Servidor DHCP	20
Criando DHCP com mapeamentos estático	23
Criando o DHCP relay	25
Especificando DNS alternativo	26
Configurando o DNS Forwarder	28
Configurando servidor de DNS/DCHP dedicado	30
Configurando DNS dinâmico	32
<u>Capítulo 3 – Configuração Geral</u>	35
Introdução	35
Criação de Alias	35
Criação de regras em NAT port forward	41
Criação de regras no Firewall	44
Criando agendamento	51
Acesso remoto ao desktop, usando exemplo completo	55
<u>Capítulo 4 – Rede privada Virtual (VPN)</u>	60
Introdução	60
Criando VPN em um túnel IPSec	60
Configurando o serviço L2TP VPN	63
Configurando o serviço OpenVPN	69
Configurando o serviço PPTP VPN	75
<u>Capítulo 5 – Configurações Avançadas</u>	87
Introdução	87
Criando um IP Virtual	87
Criando regra de NAT 1:1	93
Criando uma regra de NAT outbound	95
Criando Gateway	98

Criando uma rota estática	100
Configurando o Traffic Shaping	102
Interfaces do tipo ponte	107
Criando uma LAN Virtual	108
Criando um Captive Portal	110
<u>Capítulo 6 – Redundância, Balanceamento de carga e Failover</u>	<u>114</u>
Introdução	114
Configurando Multiplas Interfaces	114
Configurando o balanceamento de carga em uma multi-WAN	119
Configurando o Failover em uma multi-WAN	122
Configurando um servidor de web com balanceamento de carga	125
Configurando um servidor web com Failover	129
Configurando um firewall CARP com Failover	132
<u>Capítulo 7 – Servicos e Manutenção</u>	<u>139</u>
Introdução	139
Habilitando OLSR	139
Habilitando PPPoE	141
Habilitando RIP	143
Habilitando SNMP	144
Habilitando UPnP e NAT-PMP	145
Habilitando OpenNTPD	147
Habilitando Wake On Lan (WOL)	148
Habilitando o log externo (servidor syslog)	151
Usando o PING	153
Usando o Traceroute	154
Fazer backup do arquivo de configuração	156
Restaurando o arquivo de configuração	159
Configurando o backup automático do arquivo de configuração	161
Atualização do Firmware do PfSense	162
<u>Apêndice A – Monitoramento e Registros</u>	<u>168</u>
Introdução	168
Personalizar a tela de Status Dashboard	168
Monitoramento de tráfego em tempo real	170
Configurando SMTP de e-mail de notificação	171
Vendo os logs do sistema	173
Configurando um servidor de syslog externo	176
Visualizações de gráficos RRD	177
Visualizações de mapeamentos DHCP	183
Monitoramento de filtro de pacotes com PfInfo	186
Monitoramento de tráfego com PfTop	187
Monitoramento de atividades do sistema	188

Apêndice B – Determinar os requisitos de hardware	190
Introdução	190
Determinando o cenário de implantação	190
Determinando os requisitos de rendimento	193
Determinando os requisitos das interfaces	194
Escolher o tipo de instalação	196
Melhor forma de uso	197
Informações do tradutor	200

1

Configuração Inicial

Nesse capítulo, iremos abordar:

- Aplicando configurações básicas em General Setup
- Identificando e atribuindo interfaces
- Configurando a Interface WAN
- Configurando a Interface LAN
- Configurando Interfaces Opcionais
- Habilitando o Secure Shell (SSH)
- Gerando Chaves RSA Autorizada
- Configurando o SSH com autenticação de Chave RSA
- Acessando por Secure Shell (SSH)

Introdução

PfSense é um sistema operacional de código aberto usado para transformar o computador em um firewall, roteador. PfSense é uma distribuição FreeBSD feita com base no projeto m0n0wall, uma distribuição de firewall poderoso e leve. PfSense se baseia basicamente em m0n0wall e toma decisões de todas as suas funções, e foi adicionado mais uma variedade de serviços de rede mais usadas.

Nesse capítulo iremos abordar as definições básicas para implantação do PfSense; sendo um firewall, roteador, ou até mesmo um AP sem fio! Uma vez o PfSense instalado e configurado de acordo com o descrito nesse capítulo, você vai ter um firewall operacional q vai além de um roteador. Em seu nível mais básico, uma máquina PfSense pode ser usado para substituir um roteador doméstico com a funcionalidade que deseja. Em configurações mais avançadas, PfSense pode ser usado para estabelecer um túnel seguro para um escritório remoto, equilíbrio de carga de tráfego. Existem realmente centenas de formas de se configurar um PfSense.

Uma vez o PfSense instalado, há duas maneiras de acessar o servidor remotamente, SSH e os WebGUI, uma conexão SSH você iria ver o menu igual ao visto se você plugasse o monitor no servidor, no menu de opções do SSH são básicas e muito pouca configuração é feita aqui. Toda configuração descrita em cada capítulo do livro é feita através da interface WebGUI, que pode ser acessada através do endereço de ip de qualquer interface que você configurou durante a instalação (como 192.168.1.1)

Aplicando Configurações básicas em General Setup

Nessa receita iremos abordar configurações básicas feita no PfSense.

Se preparando...

Tudo que é preciso pra fazer as configurações é uma base de instalado bem feita e acesso ao WebGUI. Algumas dessas configurações podem ter sido configuradas durante a instalação mas nada impede que possa ser modificada a qualquer momento.

Em uma nova instalação as credencias de acesso padrão:

Usuário: admin

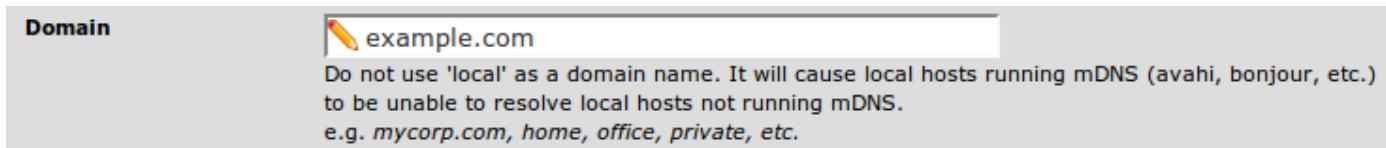
Senha: pfsense

Como fazer...

1. Vá em **System | General Setup**.
2. Digite um **Hostname**. Esse nome será usado pra acessar a maquina pelo nome e não pelo endereço de IP. Por exemplo podemos acessar digitando apenas **http://pfsense** em vez de **http://192.168.1.1**:



3. Digite o domínio em **Domain**.



4. Servidores de DNS podem ser especificados aqui. Por padrão o PfSense vai atuar como DNS primário e esses campos ficarão em branco. Mas você pode usar outros servidores de DNS. Consulte o DNS alternativo no Capítulo 2 – Serviços Essenciais, para maiores informações.

DNS servers

DNS Server	Use gateway
	None ▾

IP addresses: these are also used for the DHCP service, DNS forwarder and for PPTP VPN clients.

In addition, select the gateway for each DNS server. You should have a unique DNS server per gateway.

5. Marcar **Allow DNS server list to be overridden by DHCP/PPP on WAN**. Isso garante que todas as solicitações de DNS que não são resolvidas internamente, vão passar a ser resolvidas pelo servidor de DNS do seu provedor ISP.

Allow DNS server list to be overridden by DHCP/PPP on WAN

If this option is set, pfSense will use DNS servers assigned by a DHCP/PPP server on WAN for its own purposes (including the DNS forwarder). However, they will not be assigned to DHCP and PPTP VPN clients.

6. Digite o Fuso Horário em **Time Zone** e deixe o padrão **NTP time server** como **0.pfsense.pool.ntp.org**.

Time zone

America/New_York ▾
Select the location closest to you

NTP time server

0.pfsense.pool.ntp.org
Use a space to separate multiple hosts (only one required). Remember to set up at least one DNS server if you enter a host name here!

7. Eu recomendo o Tema padrão, PfSense 2.0 ou novo pfsense_ng. Os menus do topo agora são estáticos e não vai desaparecer se você percorrer o conteúdo da página.

Theme

pfsense_ng ▾ This will change the look and feel of pfSense.

Veja também...

- Configurando DNS Forwarder no capítulo 2 – Serviços Essenciais.
- Especificando DNS alternativo no capítulo 2 – Serviços Essenciais.

Identificando e atribuindo as Interfaces

Aqui vamos descrever como identificar e atribuir as configurações apropriadas para cada interface no PfSense.

Se Preparando...

Você precisa identificar o endereço MAC de cada placa Ethernet no seu PfSense antes de atribuir as interfaces.

Como fazê-lo...

1. Acessar o console da maquina física através do monitor ou ativar o SSH acessando remotamente (Veja ativando o Secure Shell(SSH) para mais detalhes).
2. A tela inicial exibirá uma lista de interfaces, portas de rede e endereço de IP.

```
matt@thinkpad:~$ ssh admin@192.168.1.1
Password:
*** Welcome to pfSense 2.0-BETA5-nanobsd (i386) on pfsense ***

WAN (wan)          -> fxp0      -> [REDACTED] (DHCP)
LAN (lan)          -> em0      -> 192.168.1.1
OPT1 (opt1)        -> em1      -> NONE

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: [REDACTED]
```

3. Escolha a opção 1 **Assign Interfaces**.
4. Pule a configuração de VLANs agora. Veja a criação de VLANs no Capítulo 5 – Serviços Essenciais para mais informação.

```
Enter an option: 1

Valid interfaces are:

em0  00:90:0b:12:01:52  (up)  Intel(R) PRO/1000 Network Connection 7.1.8
em1  00:90:0b:12:01:51  (down)  Intel(R) PRO/1000 Network Connection 7.1
.8
em2  00:90:0b:12:01:50  (down)  Intel(R) PRO/1000 Network Connection 7.1
.8
em3  00:90:0b:12:01:4f  (down)  Intel(R) PRO/1000 Network Connection 7.1
.8
fxp0 00:90:0b:12:01:53  (up)  Intel 82562ET/EZ/GT/GZ PRO/100 VE Ethernet

Do you want to set up VLANs first?

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

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

5. Atribuir para cada interface, a interface de sua escolha correspondente ao endereço MAC para cada endereço da interface na tela.

```
*NOTE* pfSense requires *AT LEAST* 1 assigned interfaces 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 cards  
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: fxp0  
  
Enter the LAN interface name or 'a' for auto-detection  
NOTE: this enables full Firewalling/NAT mode.  
(or nothing if finished): em0  
  
Optional interface 1 description found: OPT1  
Enter the Optional 1 interface name or 'a' for auto-detection  
(or nothing if finished): em1  
  
Enter the Optional 2 interface name or 'a' for auto-detection  
(or nothing if finished):  
  
The interfaces will be assigned as follows:  
  
LAN -> em0  
WAN -> fxp0  
OPT1 -> em1  
  
Do you want to proceed [y|n]?y  
  
Writing configuration...done.
```

A capacidade de configurar apenas uma interface é novo para o PfSense 2.0, sendo que nas versões anteriores era preciso WAN e LAN.

Como ele funciona...

PfSense como qualquer outro sistema operacional para computador, usa referencia pra cada Placa de Rede atribuindo valor único pra cada interface (fxp0, em0, em1, e assim por diante). Esses identificadores estão associados ao driver identificado pelo sistema para tornar fácil a nossa identificação na hora de associar o MAC (00:80:0c:12:01:52). Sendo assim uma interface um nome dado a cada porta Ethernet: fxp0=WAN, LAN=em0, em1=DMZ, e assim por diante.

Há mais...

Agora você sabe qual porta esta direcionada pra qual interface, você pode gerenciar as futuras mudanças através do WebGUI. Indo até **Interfaces | (assign)**.

Interfaces: Assign network ports

S ?

Interface	Network port
WAN	fxp0 (00:90:0b:12:01:53) ▾
LAN	em0 (00:90:0b:12:01:52) ▾
OPT1	em1 (00:90:0b:12:01:51) ▾

Veja também...

- O acessando o Secure Shell em SSH
- O configurando interface WAN
- O configurando interface LAN
- O configurando Interface Opcional

Configurando WAN interface

Aqui vamos aprender a configurar o **Wide Area Network (WAN)** na interface externa do nosso firewall.

Se Preparando...

A interface WAN é que conecta seu firewall a internet. Você vai precisar configurar corretamente a WAN interface (como foi feito no capítulo anterior) pra uma conexão com a internet. No exemplo q vamos usar um modem a cabo fornece acesso à internet, mas o PfSense pode fazer outros tipos de conexão.

Como fazê-lo...

1. Vá até **Interfaces | WAN**.
2. Marque **Enable Interface**.
3. Escolha o tipo de configuração de endereço em **Type**.
4. Deixe em branco o **MAC address**. Você só vai precisar inserir endereço MAC se for usar o “spoofing”. O seu provedor não pode verificar seus endereços MAC, então atribuindo manualmente você vai forçar o Provedor fornecer um IP ou um conjunto diferente de DNS.
5. Deixe **MTU**, **MSS**, **Hostname**, e **Alias IP Address** em branco.

General configuration

Enable	<input checked="" type="checkbox"/> Enable Interface
Description	 WAN Enter a description (name) for the interface here.
Type	DHCP ▾
MAC address	 Insert my local MAC address This field can be used to modify ("spoof") the MAC address of the WAN interface (may be required with some cable connections) Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank
MTU	 If you leave this field blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary on some hardware.
MSS	 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.
DHCP client configuration	
Hostname	 The value in this field is sent as the DHCP client identifier and hostname when requesting a DHCP lease. Some ISPs may require this (for client identification).
Alias IP address	 32 ▾ DHCP client. The value in this field is used as a fixed alias IP address by the DHCP client.

6. Marque **Block private networks**. Essa configuração normalmente é marcada em uma só WAN interface.
7. Marque **Block bogon networks**. Essa configuração normalmente é marcada em uma só WAN interface.
8. Clique em **Save**.

Private networks

Block private networks

When set, this option blocks traffic from IP addresses that are reserved for private networks as per RFC 1918 (10/8, 172.16/12, 192.168/16) as well as loopback addresses (127/8). You should generally leave this option turned on, unless your WAN network lies in such a private address space, too.

Block bogon networks

When set, this option blocks traffic from IP addresses that are reserved (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and obviously should not appear as the source address in any packets you receive.

Save

Cancel

Como ele funciona...

Devemos primeiro criar uma conexão com a internet antes de começarmos a configurar o PfSense e permitir q a rede conecte a internet através dele. Se colocarmos o nosso firewall como única maquina com acesso direto a internet, estamos garantindo um ambiente seguro, estabelecendo um controle completo sobre o tráfego que flui dentro e fora da rede, toda o tráfego deve passar agora pelo nosso firewall e respeitar as nossas regras.

Há Mais...

Agora podemos conectar o cabo de rede do modem na interface WAN que definimos na configuração anterior do PfSense. Uma vez conectado o cabo de rede, podemos verificar o status de conexão na porta WAN em **Status | Interfaces**:

Status: Interfaces

WAN interface (fxp0)	
Status	up
DHCP	up Release
MAC address	00:90:0b:12:01:53
IP address	[REDACTED]
Subnet mask	255.255.254.0
Gateway	GW_WAN [REDACTED]
ISP DNS servers	[REDACTED]
Media	100baseTX <full-duplex>
In/out packets	158488436/157239137 (72.99 GB/164.77 GB)
In/out packets (pass)	157239137/181687613 (72.86 GB/164.77 GB)
In/out packets (block)	1249299/0 (135.75 MB/0 bytes)
In/out errors	0/0
Collisions	0

Veja também...

- O Identificando a Atribuindo as interfaces
- O configurando interface LAN
- O configurando interface opcional

Configurando a Interface LAN

Aqui vamos aprender a configurar o **Local Area Network (LAN)** interface interna do nosso firewall.

Se Preparando...

A interface LAN é usada pra conectar seus dispositivos internos em uma rede interna segura. É necessário configurar a interface LAN corretamente.

Como fazê-lo...

1. Vá até **Interface | Lan**.
2. Marque **Enable Interface**.
3. Escolha a configuração de endereço em **Type**.
4. Digite seu ip em **IP address** e mascara de subrede. Deixe **Gateway** em **None**.

The screenshot shows two configuration sections for a network interface:

- General configuration:**
 - Enable:** A checked checkbox labeled "Enable Interface".
 - Description:** A text input field containing "LAN". Below it is a placeholder: "Enter a description (name) for the interface here."
 - Type:** A dropdown menu set to "Static".
 - MAC address:** An input field with a pencil icon and placeholder text: "Insert my local MAC address". Below it is a note: "This field can be used to modify ("spoof") the MAC address of the WAN interface (may be required with some cable connections)". Another note says: "Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank".
 - MTU:** An input field with a pencil icon and note: "If you leave this field blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary on some hardware."
 - MSS:** An input field with a pencil icon and note: "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."
- Static IP configuration:**
 - IP address:** An input field containing "192.168.1.1" with a subnet mask of "/24".
 - Gateway:** A dropdown menu set to "None". Below it is a note: "If this Interface Is an Internet connection, select an existing Gateway from the list or add a new one."

5. Deixe **Block private networks** e **Block bogon networks** desmarcadas.
6. Clique em **Save**.

The screenshot shows the "Private networks" configuration section:

- Block private networks:** A checkbox that is unchecked. A note explains: "When set, this option blocks traffic from IP addresses that are reserved for private networks as per RFC 1918 (10/8, 172.16/12, 192.168/16) as well as loopback addresses (127/8). You should generally leave this option turned on, unless your WAN network lies in such a private address space, too."
- Block bogon networks:** A checkbox that is unchecked. A note explains: "When set, this option blocks traffic from IP addresses that are reserved (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and obviously should not appear as the source address in any packets you receive."

At the bottom are two buttons: **Save** and **Cancel**.

Como ele funciona...

Você acabou de configurar sua primeira rede interna. Se você fez a configuração de acordo com o livro, agora você já conhece os requisitos mínimos para um bom funcionamento de um firewall! Você já definiu uma rede externa (WAN) e uma rede interna (LAN). Agora você pode definir as regras de tráfego entre os dois.

Há Mais...

Agora você pode conectar o cabo de rede da rede interna na interface LAN do seu PfSense. Isso permitirá que você se conecte aos computadores da rede interna.

Veja também...

- O Identificando a Atribuindo as interfaces
- O configurando interface WAN
- O configurando interface opcional

Configurando Interface Opcional

Aqui iremos descrever como criar e atribuir interface de rede opcional no nosso firewall.

Se Preparando...

A rede opcional que você vai criar nesse exemplo, se refere a uma DMZ. A ideia de usar **Zona Militar Desmilitarizada** é de permitir a passagem de tráfego direta ou não. A ideia do DMZ é controlada separada de outras áreas, se aplica DMZ nesse exemplo:

Trafego de internet | ← DMZ ← Trafego rede interna

O tráfego de internet inseguro é permitido entrar na DMZ, para acessar um servidor web por exemplo. O tráfego da Lan também pode entrar na DMZ se quiser acessar o servidor web também. No entanto o ponto chave fica na ultima regra não permitindo a entrada de DMZ na rede interna.

A rede DMZ é a rede menos segura, vamos permitir acesso externo só a determinado IP, para configurar uma DMZ ou qualquer outra rede opcional, vamos precisar de outra interface disponível.

Como fazê-lo...

1. Vá até uma interface disponível, **Interfaces** | **OPT1**
2. Marque **Enable Interface**.
3. Em **Description** digite **DMZ**.
4. Escolha a configuração de endereço em **Type**, no exemplo foi escolhido **Static**.
5. Digite em **IP Address** o ip e selecione o tipo de máscara. Usaremos o 192.168.2.1 e selecione o tipo de máscara a partir de 24 na lista.
6. Deixe **Gatway** em **None**.

General configuration	
Enable	<input checked="" type="checkbox"/> Enable Interface
Description	<input type="text"/> DMZ Enter a description (name) for the interface here.
Type	Static ▾
MAC address	<input type="text"/> Insert my local MAC address This field can be used to modify ("spoof") the MAC address of the WAN interface (may be required with some cable connections) Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank
MTU	<input type="text"/> If you leave this field blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary on some hardware.
MSS	<input type="text"/> 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.
Static IP configuration	
IP address	<input type="text"/> 192.168.2.1 / 24 ▾
Gateway	<input type="text"/> None ▾ If this Interface is an Internet connection, select an existing Gateway from the list or add a new one.

7. Deixe **Block private networks** e **Block bogon networks** desmarcados.
8. Clique em **Save**.

Private networks	
<input type="checkbox"/>	Block private networks When set, this option blocks traffic from IP addresses that are reserved for private networks as per RFC 1918 (10/8, 172.16/12, 192.168/16) as well as loopback addresses (127/8). You should generally leave this option turned on, unless your WAN network lies in such a private address space, too.
<input type="checkbox"/>	Block bogon networks When set, this option blocks traffic from IP addresses that are reserved (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and obviously should not appear as the source address in any packets you receive.
Save Cancel	

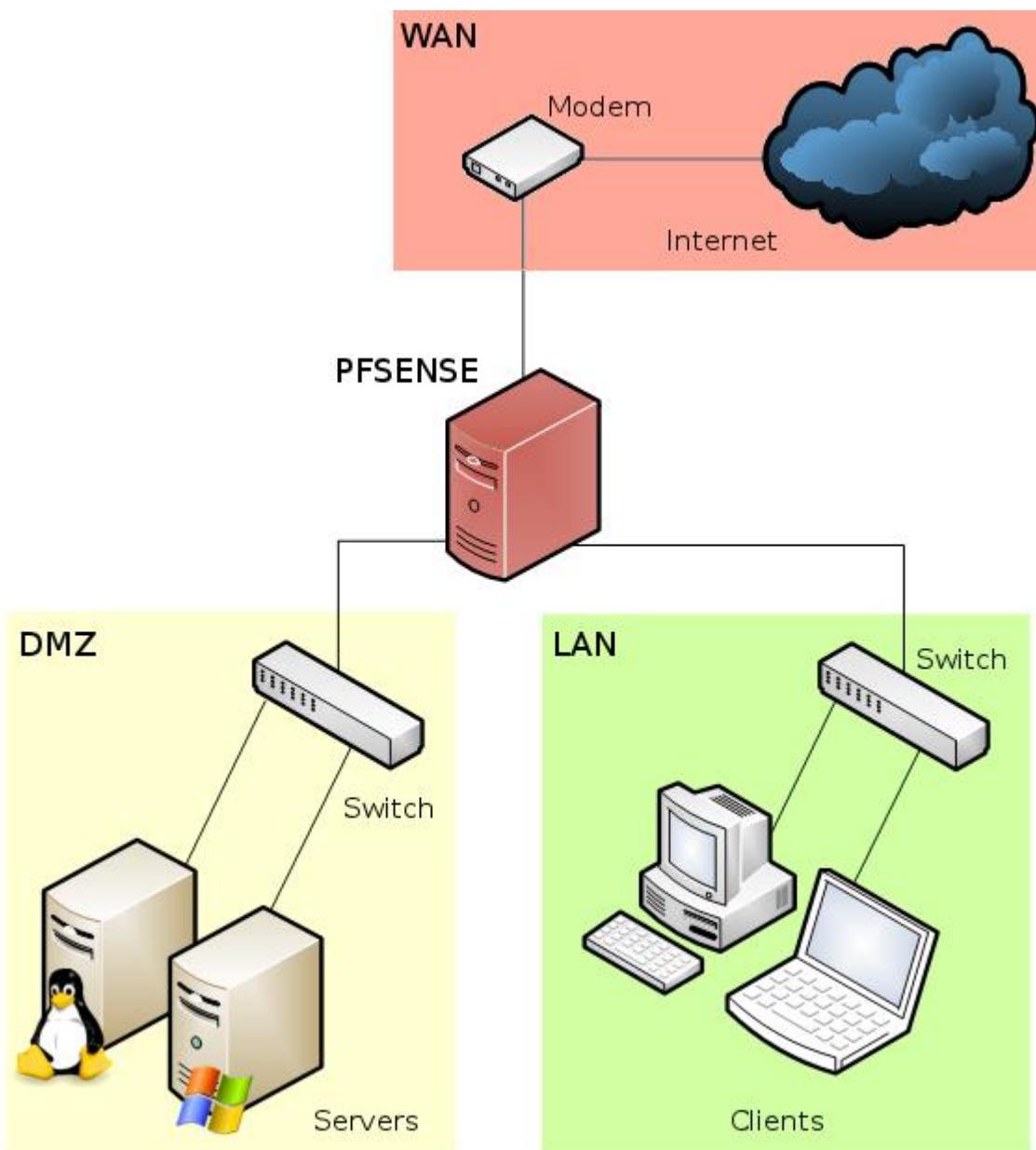
9. Clique em **Apply Changes**.

Como ele funciona...

Sua rede DMZ vai permitir acesso externo (WAN). Sua DMZ também permitira acesso a partir da LAN, mas não terão permissão de enviar tráfego para LAN. Isso irá permitir que as requisições vindas da internet para acessar recursos do seu DMZ (websites, e-mail, assim por diante) não enxerguem sua rede interna (LAN).

Há mais...

Agora você pode conectar um switch ligado à interface DMZ para se conectar em varias maquinas. Iria ficar como o diagrama a seguir:



Veja também...

- O Identificando a Atribuindo as interfaces
- O configurando interface WAN
- O configurando interface LAN

Habilitando o Secure Shell (SSH)

Aqui iremos descrever como habilitar o Secure Shell (SSH) no PfSense.

Se preparando...

SSH é um protocolo de rede que permite q comunicação criptografada entre dois dispositivos. Ativando o SSH permiti acesso seguro para o console do PfSense remotamente, como se você estivesse sentado na frente do servidor com o PfSense.

Como fazê-lo...

1. Vá até **System | Advanced | Secure Shell**.
2. Marque **Enable Secure Shell**.
3. Voce sera solicitado a fornecer credenciais quando você se conectar remotamente por SSH (use o mesmo nome de usuário e senha que você conecta por WebGUI), você pode marcar **Disable password login for Secure Shell**. Isso ira permitir q você use chave RSA, veja mais a frente para maiores informações.
4. Deixe **SSH Port** em branco, que vai ser usado à porta padrão 22.

The screenshot shows the 'Secure Shell' configuration page. It has a red header bar with the title 'Secure Shell'. Below it, there are three sections: 'Secure Shell Server' with a checked checkbox for 'Enable Secure Shell'; 'Authentication Method' with an unchecked checkbox for 'Disable password login for Secure Shell (RSA key only)' and a note below it; and 'SSH port' with a text input field containing the number '22' and a note below it.

5. Clique em **Save** que o serviço de SSH eh habilitado automaticamente.

Como ele funciona...

Ativando o Secure Shell SSH permiti ao PfSense ouvir as requisições da porta 22 ou a porta que você especificar em **SSH Port**.

Assim como todos os serviços. O serviço SSH irá ouvir em cada interface disponível. Assim como outros serviços, regras de firewall são usadas para permitir ou bloquear acesso a esses serviços. Consulte o Capítulo 3 – Configurações Geral, para obter mais informações de como configurar regras de firewall.

Há mais...

Mudando o método de autenticação do SSH para usar chaves RSA é uma ótima maneira de proteger acesso ao seu sistema. Veja abaixo para mais detalhes.

Além disso você pode alterar a porta em que o servidor escuta o SSH. Fazendo isso você pode aumentar a segurança ainda mais do seu sistema, reduzindo o numero de tentativas de login não autorizado, mas é preciso se lembrar da porta que você alterou se não, não irá poder se conectar novamente.

Veja também...

- O Gerando Chaves autorizadas RSA
- O Criando regras de firewall no Capítulo 3 – Configurações Geral

Gerando Chaves autorizadas RSA

Aqui vamos descrever como gerar uma chave RSA autorizada para que um usuário possa se conectar ao PfSense sem ser solicitado uma senha.

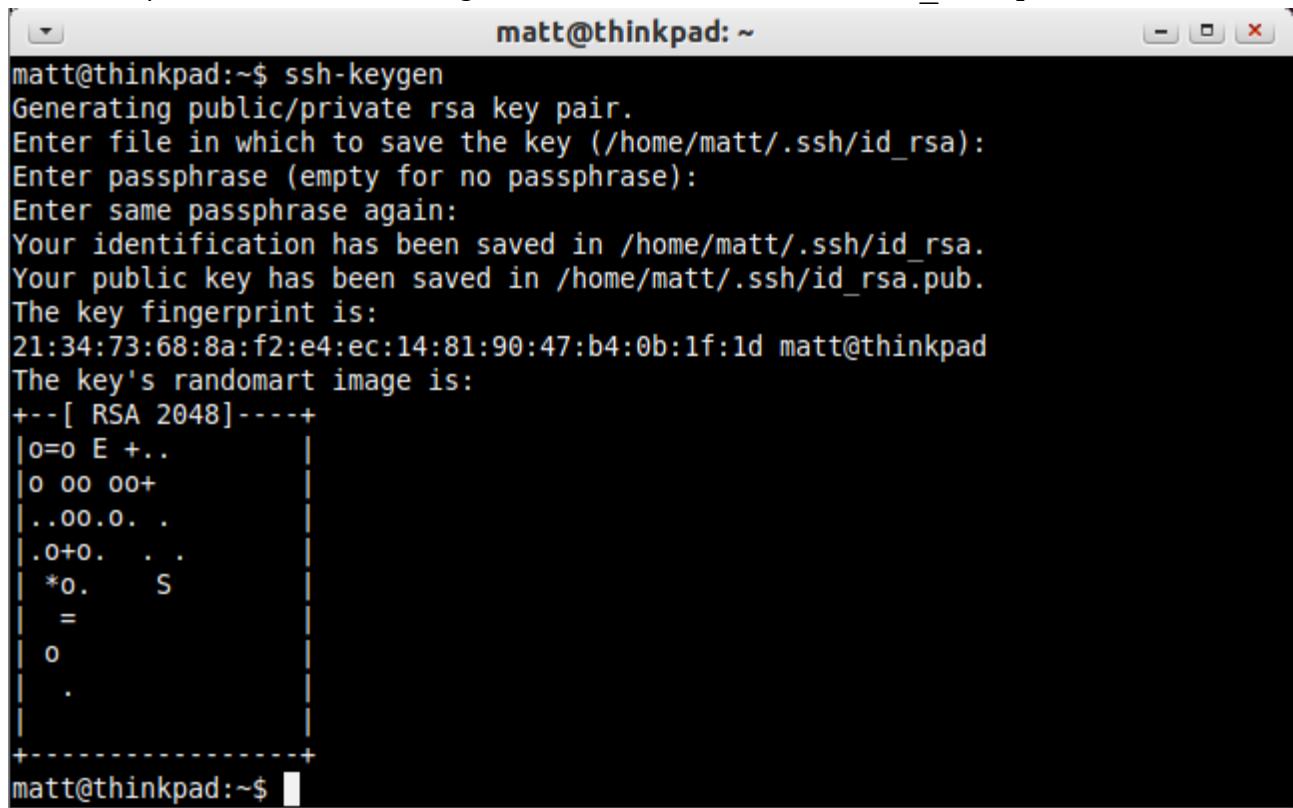
Se preparando...

Usuários de Linux e Mac terão que ter o ssh-keygen instalado em seu sistema (quase todas as distribuições já vêm instalado por padrão em seu sistema). Usuários do Windows terão que baixar e instalar a ferramenta PuTTYgen.

Como fazê-lo...

Gerando chaves SSH em computadores Linux/Mac da seguinte maneira:

1. Abrir terminal e digite:
ssh-keygen
2. Guardar a chave no local padrão /home/user/.ssh e especificar uma senha (opcional, mas recomendado).
3. Sua chave pública está localizada agora em /home/user/.ssh/id_rsa.pub

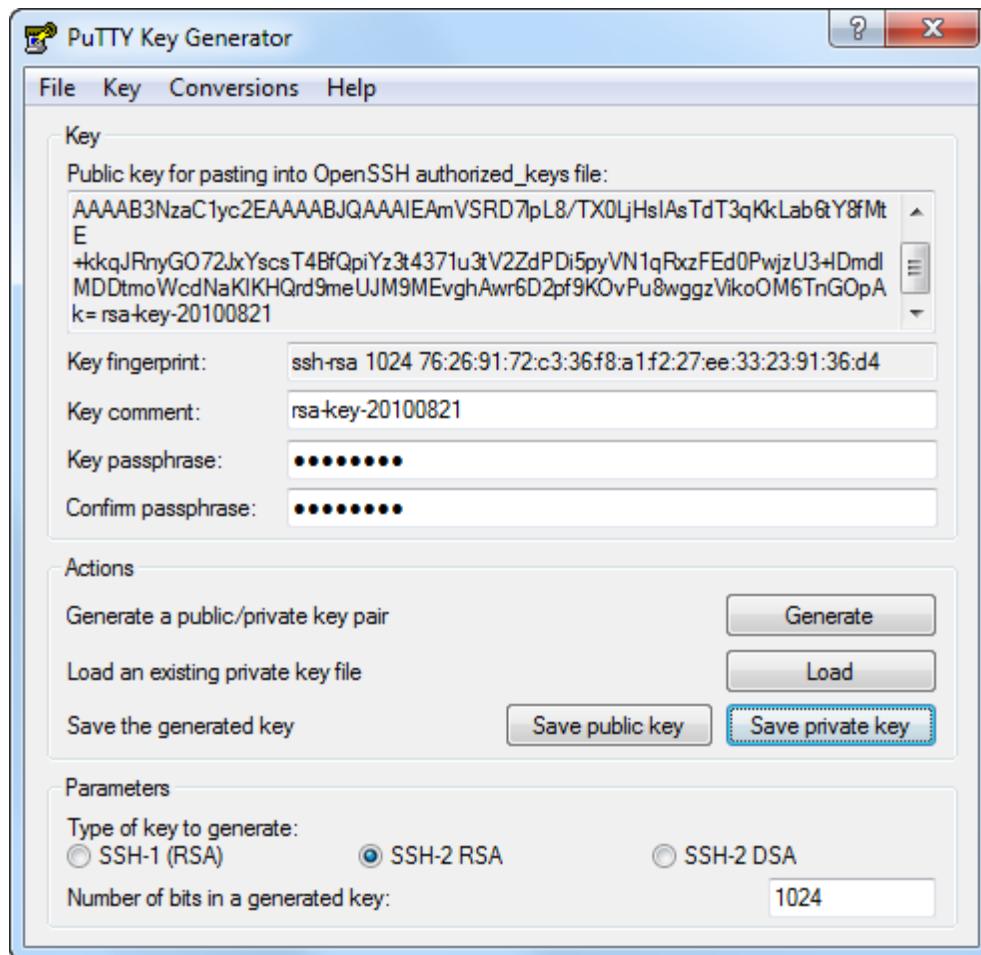


```
matt@thinkpad:~$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/matt/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/matt/.ssh/id_rsa.
Your public key has been saved in /home/matt/.ssh/id_rsa.pub.
The key fingerprint is:
21:34:73:68:8a:f2:e4:ec:14:81:90:47:b4:0b:1f:1d matt@thinkpad
The key's randomart image is:
+-- [ RSA 2048] ----+
|o=o E +..
|o oo oo+
|..oo.o. .
|.o+o. ..
*o. S
|=.
|o
|.
+-----+
matt@thinkpad:~$
```

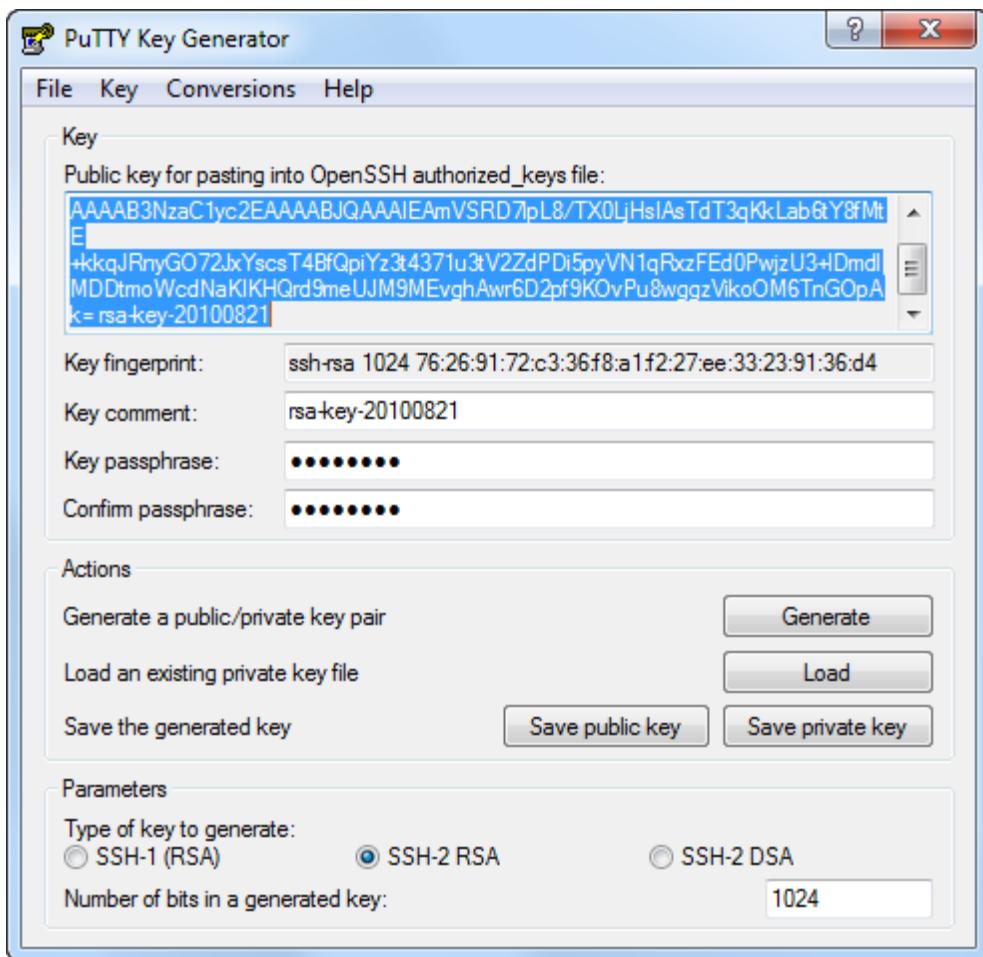
Gerando chaves SSH em computadores Windows usando PuTTY da seguinte forma:

4. Abra PuTTYgen e gere um par de chaves pública/privada clicando no botão **Generate**.
5. Digite uma senha (Opcional, mas recomendado)

6. Clique em **Save Private Key** e escolha um local como C:\MyPrivateKey.ppk



7. Selecione a chave publica q foi gerada na caixa de texto, copie e cole em um novo arquivo, digamos C:\MyPrivateKey.txt (Não use o botão **Save public key** que adiciona comentários e outros campos q são as vezes incompatíveis).



Como ele funciona...

Chaves RSA se tornaram um padrão para proteger as conexões de Cliente/Servidor para qualquer serviço. Um cliente gera um par de arquivos uma chave privada e uma chave publica(uma senha opcional pode ser usada para maior segurança), agora qualquer administrador do servidor pode adicionar uma chave publica de clientes em seu sistema, e o cliente pode se autenticar no servidor sem precisar digitar uma senha.

Há mais...

Autenticação de chave RSA é mais usada com acesso SSH, e muitas vezes se referem a ela como Chaves SSH, mas isso não é verdade. Chave RSA é uma forma de segurança que também pode ser usada em SSH. Embora é muito usado em SSH ela também pode ser usada como VPN, VoIP, FTP, e assim por diante.

Veja também...

- O Habilitando o Secure Shell (SSH)
- O Gerando Chaves autorizadas RSA

Configurando SSH com autenticação de chave RSA

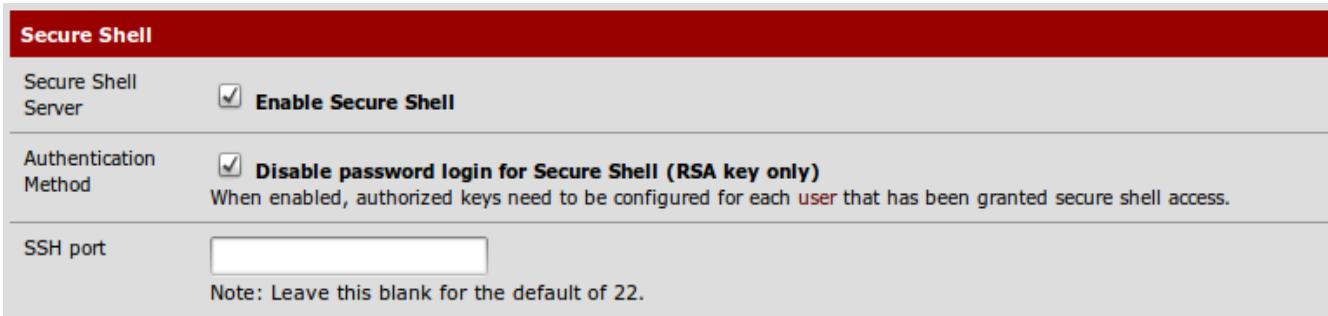
Aqui vamos descrever como configurar o PfSense para usar uma chave RSA em vez de senha para autenticação SSH.

Se preparando...

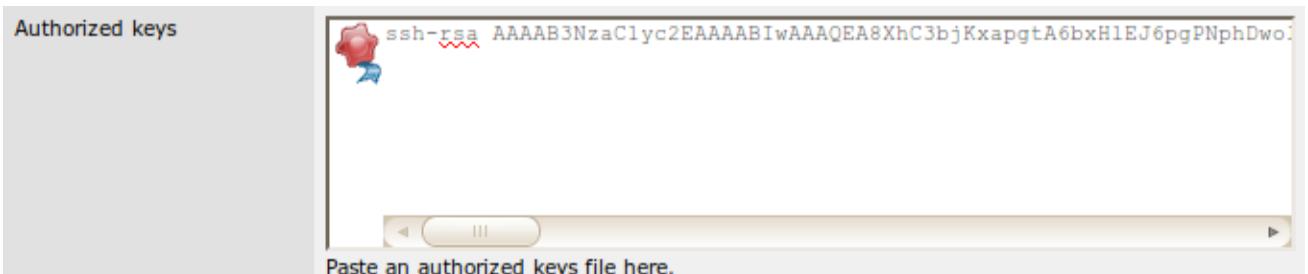
Certifique-se que você já ativou o SSH e já gerou uma chave publica.

Como fazê-lo...

1. Vá até **System | Advanced | Secure Shell**
2. Marque **Disable password login for Secure Shell (RSA key only)**.



3. Editar o usuário que irá associar com a chave publica, vá em **System | User | Manager | Edit admin**.
4. Cole em **Authorized Keys** a chave publica do cliente RSA. Quando ele for colado, a chave deve aparecer em uma única linha. Certifique-se de que seu editor de texto não insira quaisquer caracteres que alimente a linha do espaço ou então a autenticação pode falhar.



5. Clique em **Save**.

Como ele funciona...

Quando um cliente se conectar por SSH, não será solicitado uma senha. Ao invés disso, o SSH usa a sua copia da chave publica RSA para enviar uma comparação com a chave privada do cliente correspondente.

Há mais...

Chaves RSA privadas também podem ser salvas criptografadas na máquina do cliente. O cliente SSH vai pedir uma senha pra descriptografar a chave privada antes de ser usada para autenticação com o servidor.

Veja também...

- O Habilitando o Secure Shell (SSH)
- O Gerando Chaves autorizadas RSA

- O acessando o Secure Shell em SSH

Acessando o Secure Shell SSH

Aqui vamos descrever como acessar o console do PfSense usando cliente Linux, Mac ou Windows.

Se preparando...

O SSH já deve estar habilitado e configurado no PfSense. Usuários do Linux, Mac terão o cliente SSH instalado por padrão. Os usuários Windows terão q baixar o PuTTY.

Como fazê-lo...

Conectando via SSH usando cliente Linux/Mac:

1. Abra a janela do terminal e execute:

```
ssh admin@192.168.1.1
```

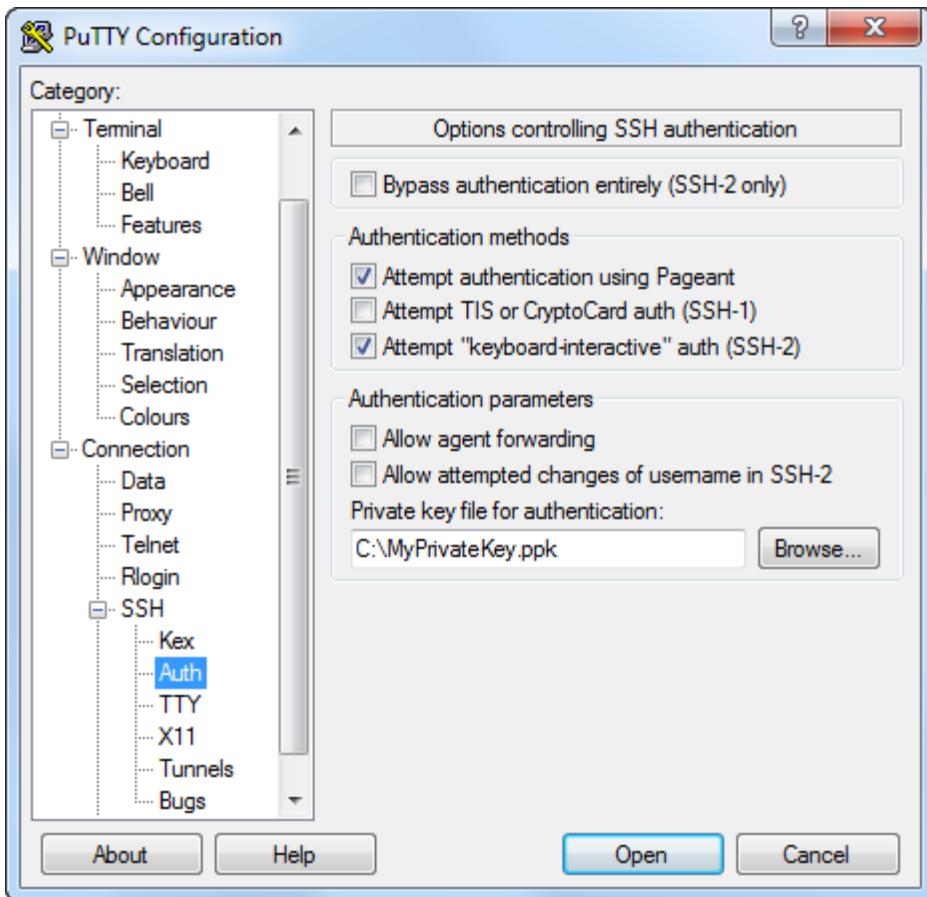
2. Se você estiver usando a configuração padrão, então será solicitado uma senha.
3. Se você estiver usando chave de autenticação RSA, você vai ser conectado diretamente ou ser solicitado a digitar uma senha associada com sua chave. Se precisar especificar a localização do seu arquivo de chave privada, você pode usar a opção `-i` dessa forma:

```
ssh -i /home/matt/key/id_rsa admin@192.168.1.1
```
4. Se você configurou o PfSense pra usar uma porta diferente, você pode especificar usando a opção `-p`, igual o exemplo a seguir:

```
ssh -p 12345 admin@192.168.1.1
```

Conectando via SSH usando cliente Windows com o PuTTY:

5. Abra o PuTTY e digite o Hostame ou o IP do servidor
6. Especifique uma porta alternativa se houver a necessidade, a padrão é 22.
7. Se você usar a chave de autenticação RSA. Procure o arquivo da chave privada em **Connection | SSH | Auth | Private key file for authentication.**



8. Você vai se conectar e será solicitado um nome de usuário.
9. Você vai ter q digitar uma senha, ou se você usar autenticação por RSA você vai ser conectado diretamente ou vai ser solicitado uma senha pra descriptografar sua chave privada.

Como ele funciona...

O SSH permite ter acesso ao console de configuração do PfSense a partir de qualquer computador que tenha um cliente SSH. Você pode até acessar o console a partir do seu telefone, se você instalar o cliente SSH no seu dispositivo móvel.

Veja também...

- O Habilitando o Secure Shell (SSH)
- O Gerando Chaves autorizadas RSA
- Configurando SSH com chave de autenticação RSA

2

Serviços Essenciais

Nesse capítulo, iremos abordar:

- Configurando o Servidor DHCP
- Criando DHCP com mapeamento estático
- Configurando o DHCP relay
- Especificando DNS alternativo
- Configurando o DNS Forwarder
- Configurando servidor de DNS/DHCP dedicado
- Configurando DNS dinâmico

Introdução

Depois de instalar o PfSense e executar os passos se configuração inicial, temos agora a estrutura básica do nosso sistema funcionando, até agora temos:

- Determinamos a necessidade do nosso sistema
- Configuramos o acesso por SSH
- Configuramos a WAN, LAN e o Opcional DMZ

Agora estamos prontos para começar a configurar os serviços de rede essenciais que o nosso PfSense vai proporcionar.

- O serviço de DHCP permite que as estações peguem endereços de ip automaticamente.
- O serviço de DNS converte os IPs em nomes legíveis de endereço de internet, e vive-versa.
- O serviço de DNS dinâmico permite o PfSense atualizar automaticamente o registro e DNS ao publico assim q ele mudar.

Configurando o servidor DHCP

Aqui iremos descrever como configurar o serviço de DHCP do PfSense. O serviço de DHCP atribui um endereço de ip a qualquer cliente q solicitar um.

Se preparando...

O PfSense só pode ser configurado como um servidor de DHCP se a interface estiver com endereço de ip estático. Nesse livro iremos abordar a interface LAN e DMZ, e não a WAN. O Exemplo abaixo aborda configurar o servidor DHCP para a interface DMZ.

Como fazê-lo...

1. Vá em **Services | DHCP Server**.
2. Selecione a aba **DMZ**.
3. Marque **Enable DHCP Server on DMZ interface**.

Services: DHCP server

S L ?

Enable DHCP server on DMZ interface

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

4. Selecione em **Range** os ips que os clientes poderão usar. Os ips deverão estar dentro da faixa de ip contida em **Available range**.

Subnet	192.168.2.0
Subnet mask	255.255.255.0
Available range	192.168.2.1 - 192.168.2.254
Range	<input type="text" value="192.168.2.50"/> to <input type="text" value="192.168.2.99"/>

5. Clique em **Save** para salvar e habilitar o serviço de DHCP.
6. Clique em **Apply Changes**, é necessário para que as alterações entre em vigor.

Como ele funciona...

O servidor DHCP aceita as solicitações de requerimento de IP, e atribui um ip disponível sem que haja algum problema de duplicidade de IP.

Há mais...

Um servidor DHCP manda um ip disponível pra um cliente que esteja solicitando, eh provável que quando o cliente faça novamente a solicitação o ip que o servidor manda vai mudar a cada pedido. Para garantir que o cliente sempre receba o mesmo endereço de IP podemos criar um mapeamento estático do DHCP. Veja no próximo exemplo.

Negar clientes desconhecidos

Habilitando essa opção garante que apenas os clientes com mapeamento cadastrado irão receber endereços de ip. Solicitações de DHCP vindo de clientes não cadastrados serão ignorados.

É diferente do que marcar a opção **Enable static ARP entries** onde os clientes desconhecidos irão receber endereços de ip, mas não vão ser capazes de se comunicar com o firewall de nenhuma forma.

Servidor de DNS

Você pode especificar manualmente qual DNS os clientes irão ser atribuídos. Se deixar em branco o PfSense irá atribuir o DNS em uma das duas formas:

- Se o **DNS forwarder** estiver habilitado, o DNS vai ser o IP da interface local do PfSense, isso porque o DNS Forwarder torna a própria máquina PfSense em um servidor DNS.
- Se o **DNS forwarder** estiver desabilitado, então deverão ser configurados em General Setup os endereços de DNS. E claro, se **Allow DNS server list to be overridden by DHCP/PPP on WAN** estiver habilitado em **General Setup** os servidores DNS serão obtidos através da porta WAN.

Gateway

O gateway das máquinas clientes por padrão será o ip da interface local usada como servidor de DHCP, mas pode ser mudada colocando um valor, se necessário.

Domain Name

O nome de domínio configurado em **General Setup** vai ser usado como padrão mas pode ser usado um nome de domínio diferente especificado se houver a necessidade.

Default Lease Time

É um valor que pode ser usado para especificar um tempo mínimo que expire o acesso por DHCP. O tempo padrão é 7200 segundos

Maximum Lease Time

É um valor que pode ser usado para especificar um tempo máximo que expire o acesso por DHCP. O tempo padrão é 86400 segundos.

Failover Peer IP

Sistema que pode configurar um endereço de ip que sirva como Fail-Over de balanceamento de carga. Veja a configuração de balanceamento de carga e Fail-Over no capítulo 6.

Static ARP

Habilitando o **Static Arp** vai permitir que somente os ips cadastrados no mapeamento estático de DHCP irão se comunicar com o firewall. Clientes não cadastrados até poderão pegar ip mas não se comunicarão com o firewall.

Isso eh diferente de **Deny unknown clientes** onde os ips que não estão cadastrados nem se quer chegam a pegar ip.

Dynamic DNS

Permite que os clientes sejam registrados automaticamente com o domínio de DNS dinâmico especificado.

Additional BOOTP/DHCP Options

Digite um valor a sua escolha obedecendo as regras listadas nesse site:
<http://www.iana.org/assignments/bootp-dhcp-parameters/bootp-dhcp-parameters.xml>

Veja também...

- Criando mapeamento estático por DHCP
- Configuração de balanceamento de carga e Fail-Over no capítulo 6.

Criando DHCP com mapeamento estático

Aqui vamos descrever como ativar e configurar o mapeamento estático do DHCP no PfSense. O mapeamento estático garante que o cliente sempre pegue o mesmo IP.

Se preparando...

O DHCP com mapeamento estático só se aplica para as interfaces que utilizam o serviço de DHCP.

Como fazê-lo...

1. Vá até **Status | DHCP leases** então você verá a lista de clientes que fizeram a requisição de ip pro DHCP.

Status: DHCP leases



IP address	MAC address	Hostname	Start	End	Online	Lease Type	
192.168.1.50	00:1e:37:8a:cc:43	thinkpad	2011/01/16 11:55:24	2011/01/16 13:55:24	online	active	
192.168.2.50	00:22:43:64:22:f3	asus1000he	2011/01/16 11:28:20	2011/01/16 13:28:20	offline	active	

Show all configured leases

2. Então clique no botão com o símbolo “+” pra adicionar o ip no mapeamento estático.
3. O endereço MAC será cadastrado.
4. Digite em **IP address** o ip que você deseja atribuir para aquele cliente, esse ip tem que estar fora dos ips cadastrados em **Range**, que esse vai ser atribuído pra outros clientes que fizerem a requisição de ip.
5. Deixe o **Hostname** já pre configurado, ou então digite um a sua escolha.
6. Em **Description** digite uma descrição que você possa identificar o computador do cliente.

Services: DHCP: Edit static mapping

S L ?

Static DHCP Mapping	
MAC address	<input type="text" value="00:1e:37:8a:cc:43"/> Copy my MAC address Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx
IP address	<input type="text" value="192.168.1.100"/> If no IP address is given, one will be dynamically allocated from the pool.
Hostname	<input type="text" value="thinkpad"/> Name of the host, without domain part.
Description	<input type="text" value="Lenovo Thinkpad T61p"/> You may enter a description here for your reference (not parsed).
Save Cancel	

7. Clique em **Save**.
8. Clique em **Apply Changes**, vá até a página **DHCP Server** no final da pagina você vai ver o mapeamento que foi criado.

MAC address	IP address	Hostname	Description
00:1e:37:8a:cc:43	192.168.1.100	thinkpad	Lenovo Thinkpad T61p

Como ele funciona...

Quando um cliente faz uma requisição de ip automático no servidor DHCP do PfSense, se o endereço MAC estiver cadastrado no mapeamento então o cliente pega o ip cadastrado referente ao MAC. Se o MAC não estiver cadastrado então é atribuído um ip ao cliente dentro da gama de ip cadastrado em **Range**.

Há mais...

Os ips cadastrados no mapeamento estático podem ser vistos na pagina **DHCP Server** na parte inferior da página, você vai até **Services | DHCP Server | Interface** selecionando a aba correspondente da interface.

Todos os ips estáticos cadastrados você verá nessa tela, você pode modificar, remover, até criar um novo ip estático para o cliente, mas se você criar por aqui o endereço MAC vai precisar ser atribuído manualmente.

MAC address	IP address	Hostname	Description	
00:1e:37:8a:cc:43	192.168.1.100	thinkpad	Lenovo Thinkpad T61p	 

Veja também...

- O Configurando servidor DHCP
- O Configurando servidor DHCP relay

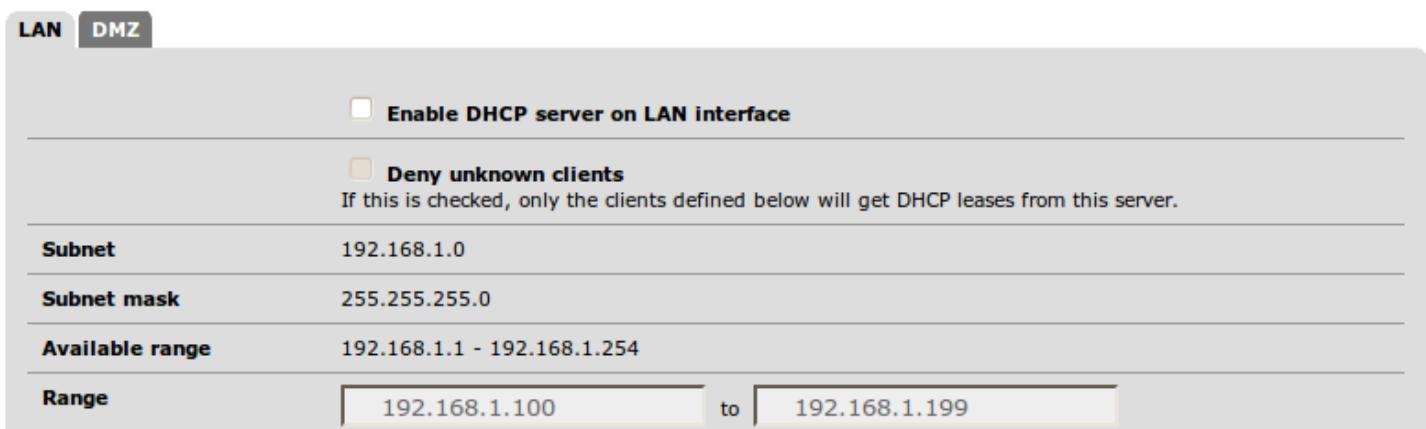
Configurando o DHCP relay

Aqui vamos configurar o DHCP para retransmitir pedidos DHCP de outro domínio. Especificando o DHCP relay é mais uma alternativa pra configurar o DHCP no PfSense.

Se preparando...

O DHCP relay só pode ser ativado se o serviço de DHCP de todas as interfaces estiver desativado, você pode desativar o serviço da seguinte forma:

1. Vá até **Services | DHCP Server | Interface** seleciona a aba (a LAN por exemplo).
2. Desmarque a opção **Enable DHCP Server on LAN Interface**.
3. Clique em **Save**.
4. E clique em **Apply Changes**.



LAN DMZ

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 192.168.1.100 to 192.168.1.199

Como fazê-lo...

1. Vá até **Services | DHCP relay**.
2. Marque a opção **Enable DHCP relay on Interface**.
3. Selecione qual interface vai usar o DHCP relay, se quiser selecionar mais de uma interface clique nas duas como botão “ctrl” pressionado.
4. Em **Destination Server** digite o endereço de ip do servidor DHCP que você deseja usar como destino. Vários ip podem ser usados desde que sejam separados por vírgula.
5. Clique em **Save**.
6. Clique em **Apply Changes**.

Services: DHCP Relay

?

DHCP Relay configuration

Enable	<input checked="" type="checkbox"/> Enable DHCP relay on interface
Interface(s)	<input type="checkbox"/> LAN <input type="checkbox"/> DMZ
Interfaces without an ip address will not be shown.	
<input type="checkbox"/> Append circuit ID and agent ID to requests If this is checked, the DHCP relay will append the circuit ID (pfSense interface number) and the agent ID to the DHCP request.	
Destination server	<input type="text"/> 192.168.1.22
This is the IP address of the server to which the DHCP packet is relayed. You can enter multiple ip address server entries separated by commas. Select "Proxy requests to DHCP server on WAN subnet" to relay DHCP packets to the server that was used on the WAN interface.	
Save	

Como ele funciona...

O PfSense pode ser configurado para retransmitir um pedido de DHCP feito a outro servidor DHCP existente, qualquer pedido de DHCP será enviado ao servidor com o ip configurado em DHCP relay e devolvida a resposta ao cliente que requisitou.

Append Circuit ID and Agent ID to Requests

Marcando essa opção o PfSense pode também acrescentar nas requisições de ip sua identificação junto ao pedido de ip se houver a necessidade.

Usando o DHCP relay pela interface WAN

Usando o DHCP relay pela interface WAN não foi implementado até a versão 2.0 do PfSense quando foi feito o livro.

Veja também...

- O Configurando servidor DHCP
- O Configurando servidor DHCP relay

Especificando DNS alternativo

Aqui vamos descrever como usar o DNS alternativo, que seja diferente do configurado por padrão pelo PfSense.

Se preparando...

Quando se trata de resolução de nomes DNS, na maioria dos ambientes é fornecida pelo seu provedor de internet ISP através da WAN. Por padrão não é preciso definir nenhum DNS, porque é atribuído pelo próprio PfSense se a opção **Allow DNS server list to be overridden by DHCP/PPP on WAN** estiver marcada. Mas se por algum motivo você quiser atribuir outro DNS alternativo terá que seguir os seguinte passos.

Como fazê-lo...

1. Vá em **System | General Setup**
2. O **DNS Servers** terá que conter as seguinte configurações:
 - Especificar o IP e gateway pra cada linha do **DNS Servers**.
 - Desmarque **Allow DNS server list to be overridden by DHCP/PPP on WAN**.
3. Clique em **Save**.
4. Clique em **Apply Changes**.

DNS servers

DNS Server	Use gateway
4.2.2.1	WAN ▾
4.2.2.2	WAN ▾
4.2.2.3	WAN ▾
4.2.2.4	WAN ▾

IP addresses: these are also used for the DHCP service, DNS forwarder and for PPTP VPN clients.

In addition, select the gateway for each DNS server. You should have a unique DNS server per gateway.

Allow DNS server list to be overridden by DHCP/PPP on WAN

If this option is set, pfSense will use DNS servers assigned by a DHCP/PPP server on WAN for its own purposes (including the DNS forwarder). However, they will not be assigned to DHCP and PPTP VPN clients.

Como ele funciona...

Os servidores DNS especificados manualmente sempre terão prioridade a menos se for substituído pelas seguintes opções.

Os servidores DNS que foram colocados no exemplo são servidores públicos que podem ser usados para diagnosticar problemas de DNS.

Usando o DNS Forwarder

Se o DNS Forwarder estiver habilitado podemos substituir os servidores DNS por domínios individuais ou até mesmo dispositivos individuais. Para saber mais informações consulte o Configurando o DNS Forwarder. O DNS Forwarder tem preferencia sobre todos os pedidos de DNS.

Usando o DNS da sua WAN

Quando **Allow DNS server list to be overridden by DHCP/PPP on WAN** estiver marcado. O PfSense usará o DNS da WAN se falhar então passará a usar os DNS's listados cadastrados. Depois do DNS Forwarder é ele que tem preferência sobre os pedidos de DNS.

Veja também...

- O Configurando DNS Forwarder.

Configurando o DNS Forwarder

Aqui vamos descrever como configurar o DNS Forwarder no PfSense. O DNS Forwarder do PfSense permite agir como um servidor de DNS com uma série de vantagens.

Se preparando...

O DNS Forwarder permite o PfSense resolver os pedidos do DNS usando o hostname obtido pelo serviço de DHCP, ou manualmente se você inseriu as informações manualmente. O DNS Forwarder também pode encaminhar todas as solicitações de DNS para um determinado domínio especificado manualmente.

Como fazê-lo...

1. Vá em **Services | DNS Forwarder | Enable DNS Forwarder**
2. Se **Register DHCP leases in DNS Forwarder** estiver marcado, todos os dispositivos em **Status | DHCP Leases** usará a função do DNS Forwarder.
3. Se **Register DHCP static mappings in DNS Forwarder** estiver marcado, todos os dispositivos conectados e mapeados em qualquer aba de interface em **Services | DHCP Server** usará o servidor configurado.

Services: DNS forwarder



Enable DNS forwarder

Register DHCP leases in DNS forwarder

If this option is set, then machines that specify their hostname when requesting a DHCP lease will be registered in the DNS forwarder, so that their name can be resolved. You should also set the domain in **System: General setup** to the proper value.

Register DHCP static mappings in DNS forwarder

If this option is set, then DHCP static mappings will be registered in the DNS forwarder, so that their name can be resolved. You should also set the domain in **System: General setup** to the proper value.

Save

4. Especificando individualmente em **Hosts** estará usando os registros do DNS. Clicando no botão "+" você adiciona um registro, dispositivos cadastrados nessa lista terá seu pedido imediatamente devolvido tendo preferencia.

5. Você pode especificar um DNS em particular em **Domain**, clicando no botão “+” para adicionar um registro. Esses registros são verificados imediatamente logo depois dos registros individuais a cima, por isso aqui pode ter preferencia em registros existentes em outros lugares.

Note:

If the DNS forwarder is enabled, the DHCP service (if enabled) will automatically serve the LAN IP address as a DNS server to DHCP clients so they will use the forwarder. The DNS forwarder will use the DNS servers entered in System: General setup or those obtained via DHCP or PPP on WAN if the "Allow DNS server list to be overridden by DHCP/PPP on WAN" is checked. If you don't use that option (or if you use a static IP address on WAN), you must manually specify at least one DNS server on the System:General setup page.

You may enter records that override the results from the forwarders below.

Host	Domain	IP	Description
wrt54gl	example.com	192.168.1.2	My wireless access point defines its own IP (i.e. it doesn't use DHCP) so when entered here it will be resolved by pfSense.

Below you can override an entire domain by specifying an authoritative DNS server to be queried for that domain.

Domain	IP	Description
google.com	192.168.1.222	This will direct any DNS requests for google.com to an internal IP. This is just an example, I wouldn't recommend doing this.

6. Clique em **Save**.
7. Clique em **Apply Changes**.

Como ele funciona...

Se o DNS Forwarder estiver marcado, ele vai ter prioridade sobre todos os pedidos de DNS, a resposta vai na seguinte ordem:

1. Registro de dispositivos individuais (**Services | DNS Forwarder**).
2. Registro de domínios específicos (**Services | DNS Forwarder**).
3. Mapeamento de DHCP estático (**Services | DHCP Server | Interface**) selecione a aba.
4. DHCP Leases (**Status | DHCP Leases**).

Veja também...

- O Configurando o servidor DHCP
- O Criando o DHCP com mapeamento estático
- O Configurando o servidor DHCP/DNS dedicado

Configurando o servidor DHCP/DNS dedicado

Aqui vamos descrever como configurar o PfSense com DNS e DHCP dedicado

Como fazê-lo...

1. Configure o PfSense como servidor DHCP. Veja *Configurando o servidor DHCP*.
2. Crie um mapeamento estático para cada dispositivo que vá se conectar com ip automático em seu sistema.
3. Vá em **System | General Setup**
4. Se certifique que nenhum outro DNS esta configurado na lista.
5. Marque a opção **Allow DNS server list to be overridden by DHCP/PPP on WAN**, nesse modo o PfSense vai resolver os nomes de DNS vindo direto da interface WAN.
6. Clique em **Save**.
7. Clique em **Apply Changes** se necessário.

System: General Setup

The screenshot shows the 'System' tab selected in the top navigation bar. The 'General Setup' section contains fields for 'Hostname' (pfsense) and 'Domain' (example.com). Below these, under 'DNS servers', there is a table with four entries. Each entry has a 'DNS Server' field (containing a pencil icon) and a 'Use gateway' dropdown menu set to 'None'. A note below the table states: 'IP addresses: these are also used for the DHCP service, DNS forwarder and for PPTP VPN clients.' Another note says: 'In addition, select the gateway for each DNS server. You should have a unique DNS server per gateway.' At the bottom of the section, there is a checked checkbox labeled 'Allow DNS server list to be overridden by DHCP/PPP on WAN' with the following description: 'If this option is set, pfSense will use DNS servers assigned by a DHCP/PPP server on WAN for its own purposes (including the DNS forwarder). However, they will not be assigned to DHCP and PPTP VPN clients.'

8. Vá até **System | DNS Forwarder**
9. Marque **Enable DNS Forwarder**.
10. Marque **Register DHCP static mappings in DNS Forwarder**.

Services: DNS forwarder

?

Enable DNS forwarder

Register DHCP leases in DNS forwarder

If this option is set, then machines that specify their hostname when requesting a DHCP lease will be registered in the DNS forwarder, so that their name can be resolved. You should also set the domain in **System: General setup** to the proper value.

Register DHCP static mappings in DNS forwarder

If this option is set, then DHCP static mappings will be registered in the DNS forwarder, so that their name can be resolved. You should also set the domain in **System: General setup** to the proper value.

Save

Note:

If the DNS forwarder is enabled, the DHCP service (if enabled) will automatically serve the LAN IP address as a DNS server to DHCP clients so they will use the forwarder. The DNS forwarder will use the DNS servers entered in **System: General setup** or those obtained via DHCP or PPP on WAN if the "Allow DNS server list to be overridden by DHCP/PPP on WAN" is checked. If you don't use that option (or if you use a static IP address on WAN), you must manually specify at least one DNS server on the **System:General setup** page.

11. Criar um registro em **Host** pra qualquer dispositivo que precise ser resolvido, mas não pode estar no mapeamento DHCP (ele deve ser configurado ip manualmente)
12. Criar um registro em **Domain** para todos os pedido de DNS que você gostaria que fosse direcionado pra um determinado domínio.

Host	Domain	IP	Description	
wrt54gl	example.com	192.168.1.2	Linksys WRT54GL Wireless Access Point	  

Below you can override an entire domain by specifying an authoritative DNS server to be queried for that domain.

Domain	IP	Description	
			 

13. Clique em **Save**
14. Clique em **Apply Changes**.

Como ele funciona...

Se o DNS Forwarder estiver habilitado, todas as solicitações de DNS de cada interface será solicitado pelo PFsense. Registros individuais cadastrados em **Host** vão ser verificados, se ele for correspondido então ele é imediatamente devolvido.

Se habilitar o **Register DHCP Static Mappings** você não terá que se preocupar com criação de registros DNS para os dispositivos. Esse é o meu método preferido de usar o PfSense como um servidor de DNS.

Contando que terá que mapear todos os endereços de ip pra cada dispositivo da rede que o hostname resolverá automaticamente.

Usando esse método nos vamos ter que adicionar os hostnames e ips de computadores que não usarem DHCP que devem ser poucos na rede.

Registrando em DHCP Leases o DNS Forwarder

Se **Register DHCP Leases in DNS Forwarder** estiver marcado, o PfSense vai registrar quaisquer dispositivos que tiver um hostname e fizer um pedido de DNS. A desvantagem é claro que nem todos os dispositivos vão se conectar se não estiver cadastrado no mapeamento estático do DHCP, eu prefiro registrar todos.

Veja também...

- O Configurando o servidor DHCP
- O Criando o DHCP com mapeamento estático
- O Configurando DNS Forwarder

Configurando DNS Dinâmico

Aqui vamos descrever como configurar o serviço de DNS dinâmico no PfSense.

Se preparando...

No PfSense já vem integrado o serviço de DNS dinâmico permitindo atualizar automaticamente toda vez que muda o endereço de ip da interface.

Como fazê-lo...

1. Vá em **Services | Dynamic DNS**
2. Clique na aba **DynDNS**
3. Clique no botão “+” para adicionar um novo registro
4. Escolha o **Service Type** (Ou seja, o prestador de serviço de DNS dinâmico)
5. Especifique em **Interface to Monitor** a interface ligada na internet pela qual deseja configurar (geralmente é usada a interface WAN)
6. Digite em **Hostname** o nome que você criou no provedor do DNS dinâmico, no exemplo é o DynDNS
7. Marque o **Wildcard**, se for o caso
8. Digite em **username** e **password** as credenciais que você configurou no provedor de DNS dinâmico, no exemplo é o DynDNS.
9. Digite em **Description** uma descrição qualquer que você possa reconhecer posteriormente.
10. Clique em **Save**.
11. Clique em **Apply Changes**.

Services: Dynamic DNS client

?

Dynamic DNS client	
Disable	<input type="checkbox"/>
Service type	DynDNS (dynamic) ▾
Interface to monitor	WAN ▾
Hostname	<input type="text"/> example.dyndns.org Note: Enter the complete host/domain name. example: myhost.dyndns.org
MX	<input type="text"/> Note: With DynDNS service you can only use a hostname, not an IP address. Set this option only if you need a special MX record. Not all services support this.
Wildcards	<input checked="" type="checkbox"/> Enable Wildcard
Username	<input type="text"/> johndoe Username is required for all types except Namecheap and FreeDNS.
Password	<input type="password"/> Note: This field is required for Namecheap and FreeDNS.
Description	<input type="text"/> Example DynDNS account information.

Save

Cancel

Note:

You must configure a DNS server in System: General setup or allow the DNS server list to be overridden by DHCP/PPP on WAN for dynamic DNS updates to work.

Como ele funciona...

Sempre que o endereço de ip muda da interface, o PfSense automaticamente se conecta com o provedor de DNS dinâmico usando as credenciais cadastradas e atualiza todos os dados.

Serviços de provedores de DNS dinâmico cadastrados

O PfSense já vem com os provedores de DNS dinâmico mais usados já cadastrados:

- DNS-0-Matic
- DynDNS
- DHS
- DyNS
- easyDNS
- No-ip
- ODS
- ZoneEdit
- Loopia
- freeDNS
- DNSexit

- OpenDNS
- NameCheap

Especificando um serviço alternativo usando o RFC 2136

Mas se você quiser usar um provedor DNS dinâmico que não esteja cadastrado, você pode usar ele desde que obedeça ao padrão RFC 2136. Vá em **Services | Dynamic DNS |** na aba **RFC 2136**, em seguida preencha nos campos apropriados os dados fornecido pelo seu provedor de DNS dinâmico.

Services: RFC 2136 client: Edit

RFC 2136 client	
Enable	<input checked="" type="checkbox"/>
Interface to monitor	WAN ▾
Hostname	<input type="text"/> example.dyndns.org
TTL	<input type="text"/> 3600 seconds
Key name	<input type="text"/> keyname This must match the setting on the DNS server.
Key type	<input type="radio"/> Zone <input type="radio"/> Host <input checked="" type="radio"/> User
Key	<input type="text"/> paste key here Paste an HMAC-MD5 key here.
Server	<input type="text"/> server
Protocol	<input type="checkbox"/> Use TCP Instead of UDP
Description	<input type="text"/> Standards compliant Dyn-DNS example connection.
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

Note:

You must configure a DNS server in **System: General setup** or allow the DNS server list to be overridden by DHCP/PPP on WAN for dynamic DNS updates to work.

3

Configuração Geral

Nesse capítulo, iremos abordar:

- Criação de Alias
- Criação de regras em Nat port forward
- Criação de regras no firewall
- Criando agendamento
- Acesso remoto ao desktop, usando exemplo completo

Introdução

A principal funcionalidade de qualquer firewall é a criação de portas, regras de segurança no firewall, e no PfSense não é diferente. Estas características, e outras, podem ser encontradas no menu **Firewall** na página principal da WebGUI.

Neste capítulo vamos explicar como configurar essas regras e explicar cada característica associada a cada uma, depois de ter feito de tudo um pouco você vai ver o quanto é fácil a configuração do firewall do PfSense.

Criando Alias

Aqui vamos explicar como usar, criar, editar e excluir Alias. O Alias fornece um grau de separação entre as regras e valores que podem mudar no futuro (por exemplo, endereços de IP, portas, e assim por diante). É sempre bom usar Alias.

Como fazê-lo...

1. Vá em **Firewall | Aliases**
2. Clique no botão “+” para adicionar um novo Alias.
3. Em **Name** digite o nome do Alias
4. Em **Description** digite uma descrição prévia do que você vai querer nesse Alias
5. Selecione um tipo de Alias em **Type**. Sua configuração a seguir vai se basear no que você selecionar.

Veja que a mais tipos de Alias, nas seções seguinte vamos ver detalhes sobre cada uma delas (Host, Rede, Usuários Open VPN, URL e tabelas URL)

Firewall: Aliases: Edit

The screenshot shows the 'Alias Edit' configuration screen. The 'Name' field is set to 'Computer1'. The 'Description' field contains 'IP address of Computer1.' Below these, the 'Type' is selected as 'Host(s)'. In the 'Host(s)' section, there is a text input field with placeholder text: 'Enter as many hosts as you would like. Hosts must be specified by their IP address.' Below this, a table lists one host entry: 'IP' (192.168.1.200) and 'Description' (The IP address of Computer1.). At the bottom are 'Save' and 'Cancel' buttons.

6. Clique em **Save**.
7. Clique em **Apply Changes**.

Como ele funciona...

Um Alias é um lugar de suporte para obter informações que podem mudar. Um Alias de host é um bom exemplo, podemos criar um Alias de host chamado **Computer 1**, e guardar um endereço de ip 192.168.1.200.

Podemos então criar varias regras de firewall e Nat e usar o nome **Computer 1** em vez de especificamente o endereço de IP do **Computer 1**. Se o endereço de ip do **Computer 1** mudar, é só mudar no Alias o ip referente ao **Computer 1** ao invés de mudar inúmeras regras criadas para aquele ip.

Os Alias permitem e flexibilidade e torna simples algumas mudanças futura. É sempre bom usar Aliases sempre que possível.

Há mais...

Adicionando Alias *dentro* de Alias, também é uma ótima maneira de gerenciar e simplificar regras. Para mostrar o poder do Alias, digamos que a nossa organização tem um telefone VoIP único, que deve se comunicar com o nosso servidor VoIP.

Um exemplo dessa regra sem Alias é a seguinte:

ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description		
<input checked="" type="checkbox"/>	TCP	192.168.1.111	*	192.168.1.200	5061	*	none		Allow Phone1 to our VoIP Server on our custom port		

Um exemplo melhor, usando Alias, é a seguinte:

ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	TCP	voip_phone1	*	voip_server	voip_server_port	*	none		Allow Phone1 to our VoIP Server on our custom port	

Um exemplo ainda melhor usando sub-Alias, é seguinte:

ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	TCP	voip_all_phones	*	voip_server	voip_server_port	*	none		Allow all phones to our VoIP Server on our port	

Com o sub-Alias nos permite modificar facilmente mais telefones, basta modificar um Alias.

Firewall: Aliases: Edit

Alias Edit

Name	<input type="text"/> voip_all_phones	The name of the alias may only consist of the characters "a-z, A-Z and 0-9".										
Description	<input type="text"/> All VoIP Phones	You may enter a description here for your reference (not parsed).										
Type	<input type="button" value="Host(s)"/>											
Host(s)	<p>Enter as many hosts as you would like. Hosts must be specified by their IP address.</p> <table border="1"><thead><tr><th>IP</th><th>Description</th></tr></thead><tbody><tr><td>voip_phone1</td><td><input type="text"/> </td></tr><tr><td>voip_phone2</td><td><input type="text"/> </td></tr><tr><td>voip_phone3</td><td><input type="text"/> </td></tr><tr><td></td><td></td></tr></tbody></table>		IP	Description	voip_phone1	<input type="text"/>	voip_phone2	<input type="text"/>	voip_phone3	<input type="text"/>		
IP	Description											
voip_phone1	<input type="text"/>											
voip_phone2	<input type="text"/>											
voip_phone3	<input type="text"/>											
<input type="button" value="Save"/> <input type="button" value="Cancel"/>												

Host Alias

Selecionando **Host(s)** como tipo de Alias permite que você crie um Alias contendo um ou mais endereços de IP:

Type	Host(s)	
Host(s)	Enter as many hosts as you would like. Hosts must be specified by their IP address.	
	IP	Description
	192.168.1.200	The IP address of Computer1.

Network Alias

Selecionando **Network(s)** como tipo de Alias, permite que você crie Alias um ou mais tipos de redes (ou seja, intervalos de endereço de rede).

Type	Network(s)		
Network(s)	Networks are specified in CIDR format. Select the CIDR mask that pertains to each entry. /32 specifies a single host, /24 specifies 255.255.255.0, etc. Hostnames (FQDNs) may also be specified, using a /32 mask. You may also enter an IP range such as 192.168.1.1-192.168.1.254 and a list of CIDR networks will be derived to fill the range.		
	Network	CIDR	Description
	192.168.0.0	16	CIDR format of a typical private network.
	192.168.0.0-192.168.255.255	32	Range format of a typical private network.
	www.bunkerhollow.com	32	An example of a FQDN hostname.

Port Alias

Selecione **Port(s)** como tipo de Alias, permite que você crie alias com um ou mais portas:

Type	Port(s)	
Port(s)	Enter as many ports as you wish. Port ranges can be expressed by separating with a colon.	
	Port	Description
	12345	An individual port.
	55100:55199	A range of ports.

OpenVPN Users Alias

Selecionar **OpenVPN Users** como tipo de Alias, permite que você crie um ou mais nomes de usuários OpenVPN.

Type	OpenVPN Users						
OpenVPN Users	<p>Enter as many usernames as you wish.</p> <table border="1"> <tr> <td>Username</td> <td>Description</td> </tr> <tr> <td>JohnDoe</td> <td>32 John Doe's OpenVPN username.</td> </tr> <tr> <td>JaneDoe</td> <td>32 Jane Doe's OpenVPN username.</td> </tr> </table>	Username	Description	JohnDoe	32 John Doe's OpenVPN username.	JaneDoe	32 Jane Doe's OpenVPN username.
Username	Description						
JohnDoe	32 John Doe's OpenVPN username.						
JaneDoe	32 Jane Doe's OpenVPN username.						

URL Alias

Selecionando **URL** como tipo de Alias, permite que você crie um ou mais alias contendo URL's:

Type	URL						
URL	<p>Enter as many URLs as you wish. After saving pfSense will download the URL and import the items into the alias. Use only with small sets of IP addresses (less than 3000).</p> <table border="1"> <tr> <td>URL</td> <td></td> </tr> <tr> <td>http://www.playboy.com</td> <td>32 Will use this alias to block access Playboy.com</td> </tr> <tr> <td>http://www.hustler.com</td> <td>32 Will use this alias to block access Hustler.com</td> </tr> </table>	URL		http://www.playboy.com	32 Will use this alias to block access Playboy.com	http://www.hustler.com	32 Will use this alias to block access Hustler.com
URL							
http://www.playboy.com	32 Will use this alias to block access Playboy.com						
http://www.hustler.com	32 Will use this alias to block access Hustler.com						

URL Table Alias

Selecionando **URL Table** como tipo de Alias, permite que você crie uma URL única apontando para uma grande lista de endereços. Isso é muito importante quando você precisa importar uma grande lista de endereços de ips e/ou subredes.

Usando o Alias

O Alias pode ser usado em qualquer lugar que você veja uma caixa de texto da cor vermelha. Basta começar a digitar que o PfSense vai exibir qualquer Alias disponível correspondente com o texto que você começou a digitar.

Redirect target IP	Computer1
	Computer1 final IP address of the server on which you want to map the ports.
	Computer2 .12
Redirect target port	Computer3 (other)

Editando o Alias

Para modificar um Alias existente, siga esses passos:

1. Vá até **Firewall | Aliases**

2. Clique no botão de “edição” para editar o Alias
3. Faça as mudanças necessárias
4. Clique em **Save**
5. Clique em **Apply Changes**.

Deletando um Alias:

Para remover um Alias existente, siga esses passos:

1. Vá até **Firewall | Aliases**.
2. Clique no botão de “delete” para deletar o Alias
3. Clique em **Save**
4. Clique em **Apply Changes**

Importando dados em lotes no Alias

Para importar uma lista de vários endereços IP, siga estes passos:

1. Vá até **Firewall | Aliases**
2. Clique no botão de importação de Alias para importar em lotes.
3. Digite um nome para a importação em **Alias Name**
4. Digite um nome para descrição do Alias em **Description**.
5. Cole a lista de endereços que você quer importar um por linha no Alias

Firewall: Aliases: Bulk import

Alias Import	
Alias Name	<input type="text" value="TimeWasters"/> TimeWasters The name of the alias may only consist of the characters "a-z, A-Z and 0-9".
Description	<input type="text" value="Websites I spend too much time on!"/> Websites I spend too much time on! You may enter a description here for your reference (not parsed).
Aliases to import	<input type="text" value="66.35.250.150
66.28.209.219
72.247.147.48"/> Paste in the aliases to import separated by a carriage return. Common examples are lists of IPs, networks, blacklists, etc. The list may contain only IP addresses.

6. Clique em **Salvar**.
7. Clique em **Apply Changes**

Veja também...

- O Criando Nat com regra de Port Forward
- O Criando regras de Firewall.

- Documento Oficial <http://doc.pfsense.org/index.php/Aliases>

Criando Nat com regras de Port Forward

Aqui vamos descrever como criar, editar e excluir regras de Port Forward.

Se preparando...

A complexidade das regras de Port Forward pode variar muito. Todos os aspectos de uma regra de Port Forward são aprofundados mais adiante. O seguinte cenário é um exemplo típico de Port Forward para encaminhar qualquer solicitação recebida pela web (HTTP) para um computador já configurado como servidor web

Como fazê-lo...

1. Vá até **Firewall | NAT**
2. Selecciona a aba **Port Forward**.
3. Clique em “+” para adicionar uma regra de Port Forward.
4. Em **Destination port range**, escolha **HTTP** em **from** e **to** na caixa de menu
5. Em **Redirect target IP** especifique o servidor web de tráfego para qual vai ser encaminhado, pode ser por Alias ou IP.
6. Em **Redirect target Port** escolha **HTTP**.
7. Digite uma descrição em **Description**, no exemplo usamos **Forward HTTP to webserver1**
8. Clique em **Save**.
9. Clique em **Apply Changes**.

Destination port range	from: <input type="text" value="HTTP"/> <input type="button" value="..."/>	to: <input type="text" value="HTTP"/> <input type="button" value="..."/>
Specify the port or port range for the destination of the packet for this mapping. Hint: you can leave the 'to' field empty if you only want to map a single port		
Redirect target IP	<input type="text" value="webserver1"/>	
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	<input type="text" value="HTTP"/> <input type="button" value="..."/>	
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	<input type="text" value="Forward HTTP to webserver1"/>	
You may enter a description here for your reference (not parsed).		
No XMLRPC Sync	<input type="checkbox"/>	
HINT: This prevents the rule from automatically syncing to other CARP members.		
NAT reflection	<input type="text" value="use system default"/>	
Filter rule association	<input type="text" value="Add associated filter rule"/>	

Save **Cancel**

Por padrão uma regra de firewall é criada para permitir que o tráfego passe, mas é muito importante lembrar que as regras de NAT e Firewall são distintos e separados. As regras de NAT servem para encaminhar o tráfego, enquanto as regras de firewall são para permitir ou bloquear o tráfego. É muito importante lembrar que só porque uma regra NAT está encaminhando um tráfego, não quer dizer que o Firewall não possa bloquear ela.

Como ele funciona...

Todo o tráfego passa através da lista de regras de NAT, com os seguintes critérios:

- Interface
- Protocolo
- Origem e intervalos de portas de origem
- Destino e intervalos de portas de destino

Se todo o tráfego corresponde a todos os critérios desta regra, que o tráfego será redirecionado para o **Redirect target IP** e **Redirect target port** específicos.

Assim como todas as regras do PfSense, regras de NAT são lidas de cima para baixo, a primeira regra é executada imediatamente e o restante é ignorado.

Nossos exemplos podem ser lidos assim:

O tráfego de:

- A Internet (**Interface**: WAN)
- A partir de qualquer cliente (**Source**) em qualquer porta (**Source Port Range**)

Indo para:

- Nossa endereço de IP Publico (**Destination** WAN address)
- Com um pedido de website (**Protocol**: TCP, **Destination Port Range**: HTTP)

Será redirecionado para:

- Um computador em particular (**Redirect Target IP**: Webserver1)
- Com o mesmo pedido (**Protocol**: TCP, **Redirect Target Port**: HTTP)

Há mais...

As regras de NAT podem ser configuradas usando uma variedade de opções:

- **Disabled**: Ativa ou desativa a regra de NAT marcando essa opção.
- **No RDR (NOT)**: Ativando essa opção irá desativar o redirecionamento de tráfego.
- **Interface**: Especifica a interface que a regra de NAT vai ser usada (a mais usada é a WAN)
- **Protocol**: Especifica o tipo de protocolo que vai ser usado na regra de NAT. A mais usada é TCP, UDP ou TCP/UDP, mas existem também GRE e ESP.
- **Source**: Normalmente a origem é deixada como padrão **any**, mas você pode especificar uma outra fonte, se necessário.
- **Source Port Range**: Geralmente é usada por padrão **any**, mas você pode especificar outra porta se houver a necessidade.
- **Destination**: Na maioria das vezes é deixado o valor padrão que é a WAN (o endereço publico), mas pode ser usada outra alternativa se houver a necessidade.
- **Destination Port Range**: Essa é a porta de tráfego solicitante. Se nós estamos encaminhando o tráfego da web, poderíamos selecionar **HTTP**, é tão comum que já vem no menu drop-down, mas a escolha (**other**), e especificando a porta 80 funcionaria da mesma forma. Poderíamos também personalizar uma porta (vamos usar como exemplo um encaminhamento de tráfego do torrente na porta 46635) lembre-se que você pode usar um Alias!
- **Redirect Target IP**: Aqui é o endereço do computador interno que vai ser transmitido o tráfego para ele. Lembre-se que você pode usar um Alias!
- **Redirect Target Port**: Aqui é a porta do ip do computador especificado em cima. Lembre-se que você pode usar um Alias!
- **Description**: A descrição feita aqui vai ser automaticamente copiada para as regras firewall (precedidas pela palavra “NAT”)
- **No XMLRPC Sync**: Marque essa opção para impedir que esta regra seja aplicada a qualquer firewall usando o CARP. Consulte o Firewall CARP Configurando Seção de failover no Capítulo 6, redundância, balanceamento de carga e Failover para mais da informação.
- **NAT Reflection**: É usado por padrão no sistema quase todas as vezes, mas **NAT Reflection** pode ser ativado ou desativado por padrão se for necessário.
- **Filter Rule Association**: Será criado a regra de firewall associada a regra do NAT.

Port Redirection

A verdadeira regra de encaminhamento de porta que vai passar o tráfego para maquina da rede interna é usada também pela porta configurada (ou seja, **Destination Port Range** e **Redirect target port** se correspondem). No entanto não a nada que impeça você redirecionar para uma porta diferente, se quiser. Há duas razões para você querer fazer isso:

- **Segurança por Obscuridade:** Todo mundo sabe que a porta padrão HTTP é 80, mas vamos supor que você tem um website “secreto” que você não quer que seja acessada facilmente. Você pode definir um intervalo de portas de destino para alguma porta obscura (por exemplo: 54321) então dai em diante usar a porta padrão HTTP 80. E os usuários que queiram acessar o site terão que digitar o endereço assim `http://www.exemplo.com:54321`
- **Um único endereço de IP público:** Em ambientes menores com apenas um endereço publico, você não vai poder acessar duas maquinas distintas remotamente porque você só tem um endereço de ip publico. Então você pode criar duas regras diferentes no NAT. O primeiro irá redirecionar a porta 50001 para o Computador 1 usando a porta 3389, e o segundo vai redirecionar a porta 50002 para o Computador 2 usando a mesma porta 3389. Fazendo isso você pode acessar o Computador1:50001 e o Computador2:50002, e assim por diante. Usando o mesmo ip publico.

Veja também...

- O Criando Alias
- O Criando regras de firewall
- O Configurando CARP firewall failover recipe in Chapter 6, Redundancy, Balanceamento de Carga,e Failover

Criando regras de Firewall

Aqui vamos descrever como criar uma regra de firewall

Se preparando...

Como exemplo, vamos criar uma regra de firewall para permitir o tráfego web encaminhado pela NAT (a regra que criamos anteriormente). Se você acompanhou, o NAT que criamos, automaticamente foi criado uma regra em Firewall, mas poderíamos marcar **None** em **Filter Rule Association** que essa regra não iria ser copiada para o Firewall.

Como fazê-lo...

1. Vá até **Firewall | Rules**.
2. Selecione a aba **WAN**
3. Clique no botão “+” para adicionar uma nova regra de firewall
4. Especifique a **WAN Interface**
5. Especifique o **Protocol TCP**
6. Especifique **any** em **Source**
7. Especifique **any** em **Source Port Range**

8. Especifique **Webserver1** em **Destination**
9. Especifique **HTTP** em **Destination Port Range**
10. Digite q descrição da regra em **Description**
11. Clique em **Save**
12. Clique em **Apply Changes**

Firewall: Rules: Edit

S L ?

Edit Firewall rule	
Action	<input style="background-color: #e0e0e0; border: 1px solid #ccc; padding: 2px 10px; margin-right: 5px;" type="button" value="Pass"/> <input style="background-color: #e0e0e0; border: 1px solid #ccc; padding: 2px 10px;" type="button" value="Block"/> <input style="background-color: #e0e0e0; border: 1px solid #ccc; padding: 2px 10px;" type="button" value="Reject"/> <input style="background-color: #e0e0e0; border: 1px solid #ccc; padding: 2px 10px;" type="button" value="Log"/>
<p>Choose what to do with packets that match the criteria specified below.</p> <p>Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.</p>	
Disabled	<input type="checkbox"/> Disable this rule Set this option to disable this rule without removing it from the list.
Interface	<input style="background-color: #e0e0e0; border: 1px solid #ccc; padding: 2px 10px; margin-right: 5px;" type="button" value="WAN"/> <input style="background-color: #e0e0e0; border: 1px solid #ccc; padding: 2px 10px;" type="button" value="LAN"/>
<p>Choose on which interface packets must come in to match this rule.</p>	
Protocol	<input style="background-color: #e0e0e0; border: 1px solid #ccc; padding: 2px 10px; margin-right: 5px;" type="button" value="TCP"/> <input style="background-color: #e0e0e0; border: 1px solid #ccc; padding: 2px 10px;" type="button" value="UDP"/> <input style="background-color: #e0e0e0; border: 1px solid #ccc; padding: 2px 10px;" type="button" value="ICMP"/>
<p>Choose which IP protocol this rule should match.</p> <p>Hint: in most cases, you should specify TCP here.</p>	
Source	<input type="checkbox"/> not Use this option to invert the sense of the match. Type: <input style="background-color: #e0e0e0; border: 1px solid #ccc; padding: 2px 10px; margin-right: 5px;" type="button" value="any"/> <input style="border: 1px solid #ccc; padding: 2px 10px;" type="button" value="Custom..."/> Address: <input type="text" value=""/> / <input type="text" value="31"/>
Source port range	from: <input style="background-color: #e0e0e0; border: 1px solid #ccc; padding: 2px 10px; margin-right: 5px;" type="button" value="any"/> <input style="border: 1px solid #ccc; padding: 2px 10px;" type="button" value="Custom..."/> to: <input style="background-color: #e0e0e0; border: 1px solid #ccc; padding: 2px 10px; margin-right: 5px;" type="button" value="any"/> <input style="border: 1px solid #ccc; padding: 2px 10px;" type="button" value="Custom..."/>
<p>Specify the source port or port range for this rule. This is usually random and almost never equal to the destination port range (and should usually be "any").</p> <p>Hint: you can leave the 'to' field empty if you only want to filter a single port.</p>	
Destination	<input type="checkbox"/> not Use this option to invert the sense of the match. Type: <input style="background-color: #e0e0e0; border: 1px solid #ccc; padding: 2px 10px; margin-right: 5px;" type="button" value="Single host or alias"/> <input style="border: 1px solid #ccc; padding: 2px 10px;" type="button" value="Custom..."/> Address: <input style="background-color: #e0e0e0; border: 1px solid #ccc; padding: 2px 10px; margin-right: 5px;" type="text" value="Webserver1"/> / <input type="text" value="31"/>
Destination port range	from: <input style="background-color: #e0e0e0; border: 1px solid #ccc; padding: 2px 10px; margin-right: 5px;" type="button" value="HTTP"/> <input style="border: 1px solid #ccc; padding: 2px 10px;" type="button" value="Custom..."/> to: <input style="background-color: #e0e0e0; border: 1px solid #ccc; padding: 2px 10px; margin-right: 5px;" type="button" value="HTTP"/> <input style="border: 1px solid #ccc; padding: 2px 10px;" type="button" value="Custom..."/>
<p>Specify the port or port range for the destination of the packet for this rule.</p> <p>Hint: you can leave the 'to' field empty if you only want to filter a single port</p>	
Log	<input type="checkbox"/> Log packets that are handled by this rule <p>Hint: the firewall has limited local log space. Don't turn on logging for everything. If you want to do a lot of logging, consider using a remote syslog server (see the Diagnostics: System logs: Settings page).</p>
Description	<input type="text" value="Allow any to Webserver1 HTTP"/> You may enter a description here for your reference.

Como ele funciona...

Todo o tráfego passa pela lista de regras de Firewall. Se qualquer pacote de tráfego corresponde a qualquer critério de qualquer regra, a regra seria executada (e o pacote seria permitido ou negado).

Essa regra pode ser lida como: "Qualquer porta de qualquer cliente na internet tem permissão para acessar a nossa web pela porta do servidor que é 80".

Há mais...

Regras de firewall são altamente configuráveis. Detalhes de cada opção de regra de firewall são as seguintes:

- **Action:** É o tipo de ação que a regra vai ter
 - **Pass:** Se os critérios forem correspondidos, a passagem do pacote é permitida.
 - **Block:** Se todos os critérios forem correspondidos, a passagem do pacote é bloqueada (alguns se referem a ela como Drop Silencioso).
 - **Reject:** Se todos os pacotes forem correspondidos, a passagem do pacote é devolvida ao remetente.
- **Disabled:** Desativa a regra sem ter que apaga-la.
- **Interface:** Se especifica de qual interface o tráfego vai ser originado, que estará sujeito a essa regra, geralmente é usada a WAN.
- **Protocol:** Corresponde o tipo de protocolo, variando de acordo com o tipo de regra que define o tráfego.
- **Source:** É geralmente marcado **any** quando se refere a tráfego de entrada.
- **Source Port Range:** É geralmente marcado **any** quando se refere a tráfego de entrada.
- **Destination:** Aqui é usado o Alias ou o endereço de IP do computador que o tráfego esta apontando.
- **Destination Port Range:** É geralmente a porta do computador que atende este tráfego.
- **Log:** Habilitar o log de registro do pacote que corresponde a regra.
- **Description:** Digite uma descrição que você possa identificar futuramente.

Raramente sabemos a porta de origem!

Ao especificar as regras, é muito importante lembrar que **Source Port Range** é quase sempre definida como **any**. Muitas vezes as pessoas cometem erro de especificar um **Source Port Range**. Lembre-se quando você solicita um site, você esta solicitando a porta 80 no computador do servidor web, e seu computador que vai decidir que porta sua vai ser aberta para receber a solicitação. Esta é sua porta de origem, uma porta sempre em mudança, que você provavelmente não vai saber qual será. Assim 99 por cento do tempo, não saberemos o **Source Port Range**.

A ordem das regras do Firewall

As regras do PfSense são sempre avaliadas de cima para baixo. Muitos administradores inclui uma regra muito específica na parte superior das outras regras e as mais genéricas na parte inferior. Para

reordenar uma regra, clique na regra e então clique no botão que parece uma mão na linha da regra que você quer colocar a cima dela.

ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	
X	*	RFC 1918 networks	*	*	*	*	*		Block private networks	
X	*	Reserved/not assigned by IANA	*	*	*	*	*	*	Block bogon networks	
	TCP	*	*	<u>Tigas</u>	22 (SSH)	*	none		NAT Forward TigasSshPort to Tigas SSH	
	TCP	*	*	<u>Webserver1</u>	80 (HTTP)	*	none		Allow any to Webserver1 HTTP.	

move selected rules before this rule

Duplicando regras de firewall

Muitas vezes, a gente pode querer criar uma nova regra muito parecida com a regra existente. Para poupar tempo nós podemos duplicar a regra e fazer as alterações específicas clicando no botão “+”.

	TCP	*	*	<u>Webserver1</u>	80 (HTTP)	*	none		Allow any to Webserver1 HTTP.	
	TCP	*	*	<u>Tigas</u>	22 (SSH)	*	none		NAT Forward TigasSshPort to Tigas SSH	

add a new rule based on this one

Recursos Avançados

Esse recurso é novo para o PfSense 2.0, nas regras de firewall tem uma seção chamada **Advanced Features**, cada um dos seguintes recursos podem ser especificados como critérios para uma regra. Se um recurso avançado é especificado, a regra só será executada se for encontrada uma correspondência. Clique no botão Avançado para exibir as seguintes definições de configuração para cada função:

- **Source OS:** Esta opção irá tentar comparar a fonte do tráfego com o sistema operacional do dispositivo:

Source OS	OS Type: <input type="button" value="Windows"/>
Note: this only works for TCP rules	

- **Diffserv Code Point:** É um mecanismo para fornecer Qualidade de Serviço (QoS) de tráfego de rede. Podendo priorizar tráfego com base nos valores especificados:

Diffserv Code Point	<input type="button" value="af11"/>
---------------------	-------------------------------------

- **Advanced Option:** Permite a opção de especificação avançada do IP:

Advanced Options

This allows packets with IP options to pass. Otherwise they are blocked by default. This is usually only seen with multicast traffic.

This will disable auto generated reply-to for this rule.

You can mark a packet matching this rule and use this mark to match on other NAT/filter rules. It is called **Policy filtering**

You can match packet on a mark placed before on another rule.

Maximum state entries this rule can create

Maximum number of unique source hosts

Maximum number of established connections per host

Maximum state entries per host

 /

Maximum new connections / per second(s)

State Timeout in seconds

NOTE: Leave fields blank to disable that feature.

- **TCP Flags:** Estes são bits de controle que indicam diversos estados de conexão ou informações sobre como um pacote deve ser tratado.

TCP flags

	FIN	SYN	RST	PSH	ACK	URG
set	<input type="checkbox"/>					
out of	<input type="checkbox"/>					

Any flags.

Use this to choose TCP flags that must be set or cleared for this rule to match.

- **State Type:** Especifica um mecanismo de rastreamento especial sobre o estado

State Type

keep state

HINT: Select which type of state tracking mechanism you would like to use. If in doubt, use keep state.

keep state	Works with all IP protocols.
sloppy state	Works with all IP protocols.
synproxy state	Proxies incoming TCP connections to help protect servers from spoofed TCP SYN floods. This option includes the functionality of keep state and modulate state combined.
none	Do not use state mechanisms to keep track. This is only useful if you're doing advanced queueing in certain situations. Please check the documentation.

- **No XMLRPC Sync:** Impede que a regra sincronize com outros membros do CARP:

No XMLRPC Sync

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

- **Schedule:** Especifica um agendamento do período que essa regra vai ser valida. Terá que cadastrar os horários em **Firewall | Schedule**. Então aparecerá aqui:

Schedule WorkHours

Leave as 'none' to leave the rule enabled all the time.

- **Gateway:** Se quiser definir outro gateway diferente do configurado como padrão, então defina aqui:

Gateway default

Leave as 'default' to use the system routing table. Or choose a gateway to utilize policy based routing.

- **In/Out:** Especificar filas alternativas de velocidade e interfaces virtuais:

In/Out none / none

Choose the Out queue/Virtual interface only if you have selected In too.
The Out selection is applied to traffic going out the interface the rule is created, In is the incoming one.
If you are creating a rule on the Floating tab if the direction is In then the same rules apply, if the direction is out the selections are reverted Out is for incoming and In is for outgoing and if you do not select any direction use only the In since the Out selection does not make sense in there to prevent oddities.

- **Ackqueue/Queue:** Especificar as alternativas de reconhecimento de filas de velocidades:

Ackqueue/Queue none / none

Choose the Acknowledge Queue only if you have selected Queue.

- **Layer7:** Especifica uma alternativa de Layer7:

Layer7 none

Choose a Layer7 container to apply application protocol inspection rules. These are valid for TCP and UDP protocols only.

Veja também...

- Criação de regras em Nat port forward
- Criando agendamento
- Criando Alias

Criando agendamentos

Agora vamos descrever como criar uma agenda

Se preparando...

A agenda nos permite configurar quando as regras entram em vigor e saem. Elas são usadas geralmente com regras de firewall, mas na concepção em geral vai ser permitido usar para muito mais funções no futuro em versões posteriores do PfSense. Se uma regra do firewall especifica um horário, a regra então só é ativada durante esse período de tempo. No exemplo a seguir, vamos definir um cronograma para o nosso horário de 9 horas da manhã ah 5 horas da tarde, horário comercial.

Ao criar horários, é essencial ter o fuso horário configurado corretamente, e o tempo de sincronização configurado devidamente em um servidor confiável.

Como fazê-lo...

1. Vá até **Firewall | Schedules**
2. Clique no botão “+” para criar uma nova agenda
3. Em **Schedule Name** digite um nome de referencia, o exemplo usamos **WorkHours**.
4. Digite em **Description** a descrição para que você possa reconhecer que tipo de horário você esta configurando, no exemplo usamos **Regular work week hours**.
5. Na seção **Month** selecione o mês, clique em **Mon, Tue, Wed, Thu e Fri** selecionando todos os dias da semana de trabalho.
6. Especificar 9 horas da manhã em **Start Time** e 17 horas em **Stop Time**.
7. Digite em **Time Range Description** a descrição do horário, no exemplo usou **Monday-Friday 9am-5pm**.
8. Clique em **Add Time**.

Firewall: Schedules: Edit

?

Schedule information																																											
Schedule Name	<input type="text" value="WorkHours"/> WorkHours The name of the alias may only consist of the characters a-z, A-Z and 0-9																																										
Description	<input type="text" value="Regular work week hours."/> You may enter a description here for your reference (not parsed).																																										
Month	<input type="text" value="March 00"/> March 2000 <table border="1" style="margin-top: 10px; width: 100%;"> <thead> <tr> <th>Mon</th><th>Tue</th><th>Wed</th><th>Thu</th><th>Fri</th><th>Sat</th><th>Sun</th></tr> </thead> <tbody> <tr><td></td><td></td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td></tr> <tr><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td><td>11</td><td>12</td></tr> <tr><td>13</td><td>14</td><td>15</td><td>16</td><td>17</td><td>18</td><td>19</td></tr> <tr><td>20</td><td>21</td><td>22</td><td>23</td><td>24</td><td>25</td><td>26</td></tr> <tr><td>27</td><td>28</td><td>29</td><td>30</td><td>31</td><td></td><td></td></tr> </tbody> </table> <p>Click individual date to select that date only. Click the appropriate weekday Header to select all occurrences of that weekday.</p>	Mon	Tue	Wed	Thu	Fri	Sat	Sun			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31		
Mon	Tue	Wed	Thu	Fri	Sat	Sun																																					
		1	2	3	4	5																																					
6	7	8	9	10	11	12																																					
13	14	15	16	17	18	19																																					
20	21	22	23	24	25	26																																					
27	28	29	30	31																																							
Time	Start Time Stop Time <input type="text" value="9"/> Hr <input type="text" value="00"/> Min <input type="text" value="17"/> Hr <input type="text" value="00"/> Min <p>Select the time range for the day(s) selected on the Month(s) above. A full day is 0:00-23:59.</p>																																										
Time Range Description	<input type="text" value="Monday-Friday 9am-5pm"/> You may enter a description here for your reference (not parsed).																																										
<input type="button" value="Add Time"/> <input type="button" value="Clear Selection"/>																																											

9. Note que o tempo de repetição é adicionado em **Configured Ranges**.

Schedule repeat				
Configured Ranges	Day(s)	Start Time	Stop Time	Description
	Mon - Fri	9:00	17:00	Monday-Friday 9am-5pm
<input type="button" value="Save"/> <input type="button" value="Cancel"/>				

10. Clique em **Save**.

11. Clique em **Apply Changes**.

Como ele funciona...

Um agendamento associado a uma regra só será válida durante o tempo especificado. Para saber associar uma regra de firewall com o agendamento que acabamos de criar:

1. Edite uma regra, ou adicione uma.

- Clique em **Schedule Advanced**, então vá na opção **Schedule** e selecione o agendamento que você deseja usar, no exemplo nós só criamos um.
- Escolha o agendamento que criamos **WorkHours** na opção **Schedule**.



- Clique em **Save**
- Clique em **Apply Changes**.

Há mais...

No PfSense vários ícones aparecem para auxiliar nas informações, no agendamento também, os ícones no agendamento aparecem para informar se o agendamento está ativou ou não.

➤ **Firewall | Schedules:** agendamentos ativados aparecem com um “relógio”:

Firewall: Schedules

Name	Time Range(s)	Description	
AwakeHours	Mon - Sun 6:00-20:00 Everday 6am-10pm	Hours I am awake.	
Weekend	Sat - Sun 0:00-23:59 Entire weekend.	Weekend hours.	
WorkHours	Mon - Fri 9:00-17:00 Weekdays 9am-5pm	Hours I am working.	

Note:
Schedules act as placeholders for time ranges to be used in Firewall Rules.

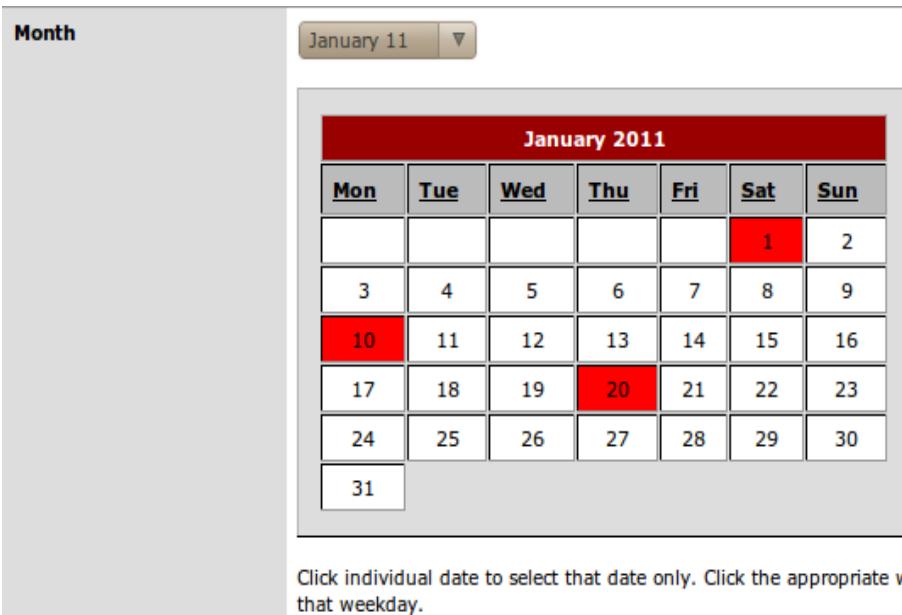
➤ **Firewall | Rules:** Regras com agendamento ativo aparecem uma “seta verde” na coluna **Schedule**, e diz qual o nome do agendamento.
Regras com agendamentos desativados, na coluna **Schedule** aparece um “x” vermelho com o nome do agendamento:

ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	
	*	RFC 1918 networks	*	*	*	*	*		Block private networks	
	*	Reserved/not assigned by IANA	*	*	*	*	*	*	Block bogon networks	
	TCP	*	*	<u>Webserver1</u>	80 (HTTP)	*	none	<u>WorkHours</u>	Allow any to Webserver1 HTTP during work hours.	
	TCP	*	*	<u>Webserver1</u>	80 (HTTP)	*	none	<u>Weekend</u>	Allow any to Webserver1 HTTP on the weekend.	

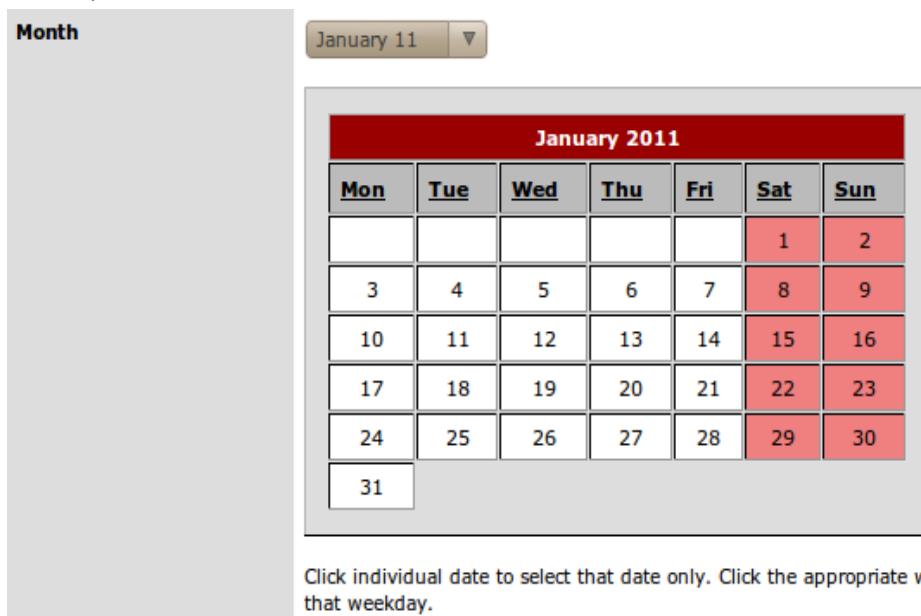
Seleção de dia ou dias da semana

A seleção Month funciona de duas formas:

- **Selecionando dias específicos:** Selecione o mês correto e clique nos dias específicos (o ano é irrelevante, qualquer dia especificado será repetido em cada ano).



- **Selecionando dias da semana:** Clique no dia da semana, selecionando todos os dias do mês referente aquele dia da semana (o mês é irrelevante, o dia da semana vai sempre repetir todos os meses).



Veja também...

- Criando Alias
- Criação de regras em Nat port forward
- Criando regras de firewall

Acesso remoto ao Desktop com exemplo completo

Vamos descrever aqui como liberar o acesso através de regras de firewall do PfSense, o acesso remoto ao computador da rede interna usando o acesso remoto da própria Microsoft que vem no Windows o (RDP).

Se preparando...

Vamos demonstrar como criar uma regra de firewall para liberar o acesso do inicio ao fim. O exemplo a seguir vai mostrar como acessar uma máquina da rede interna, com o pedido vindo da internet. Para fazer isso requer as configurações que vamos postar agora, vale ressaltar que as configurações feitas agora nos vamos ter que saber alguns pontos que foram tocadas no livro:

- DHCP Server
- DHCP com mapeamento estatico
- DNS Forwarder
- Aliases
- NAT port forwarding
- Regras de Firewall
- Agendamentos

Como fazê-lo...

1. Vamos cadastrar o computador na nossa rede:
2. Vá até **Status | DHCP Leases** e localize o computador que acabou de entrar na rede. Clique no botão “+” para atribuir um mapeamento estático para ele.

IP address	MAC address	Hostname	Start	End	Online	Lease Type
192.168.1.199	00:1e:37:8a:cc:43	t61p	2000/03/06 05:35:18	2000/03/06 07:35:18	online	active

3. Vamos atribuir um endereço de IP a ele, em **IP address** digite **192.168.1.200**, e em **Hostname**, digite o nome que vai querer identificar ele, pode ser **Laptop1**, e digite em **Description**, uma descrição do Laptop para você saber qual é o laptop que você adicionou.

Services: DHCP: Edit static mapping

S L ?

Static DHCP Mapping	
MAC address	<input type="text" value="00:1e:37:8a:cc:43"/> Copy my MAC address Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx
IP address	<input type="text" value="192.168.1.200"/> If no IP address is given, one will be dynamically allocated from the pool.
Hostname	<input type="text" value="laptop1"/> Name of the host, without domain part.
Description	<input type="text" value="Lenovo T61p Thinkpad Laptop"/> You may enter a description here for your reference (not parsed).

[Save](#) [Cancel](#)

4. Vamos agora fazer com que nosso **DNS Forwarder** seja configurado para transmitir automaticamente aos clientes com mapeamento estático, vá a **Services | DNS Forwarder**, para que possamos localizar com facilidade o computador pelo nome:

Services: DNS forwarder

?

Enable DNS forwarder

Register DHCP leases in DNS forwarder

If this option is set, then machines that specify their hostname when requesting a DHCP lease will be registered in the DNS forwarder, so that their name can be resolved. You should also set the domain in System: General setup to the proper value.

Register DHCP static mappings in DNS forwarder

If this option is set, then DHCP static mappings will be registered in the DNS forwarder, so that their name can be resolved. You should also set the domain in System: General setup to the proper value.

[Save](#)

5. Vamos agora criar um Alias para ser usado como referencia ao seu IP dentro do PfSense em **Firewall | Aliases**:

Firewall: Aliases: Edit

?

Alias Edit

Name	<input type="text" value="laptop1"/> <small>The name of the alias may only consist of the characters "a-z, A-Z and 0-9".</small>						
Description	<input type="text" value="My Thinkpad laptop."/> <small>You may enter a description here for your reference (not parsed).</small>						
Type	Host(s) <input type="button" value="▼"/>						
Host(s)	<p>Enter as many hosts as you would like. Hosts must be specified by their IP address.</p> <table border="1"> <thead> <tr> <th>IP</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>192.168.1.200</td> <td><input type="button" value="32"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/></td> </tr> <tr> <td><input type="button" value="Add"/></td> <td></td> </tr> </tbody> </table>	IP	Description	192.168.1.200	<input type="button" value="32"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>	<input type="button" value="Add"/>	
IP	Description						
192.168.1.200	<input type="button" value="32"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>						
<input type="button" value="Add"/>							
<input type="button" value="Save"/> <input type="button" value="Cancel"/>							

- Vamos criar um agendamento para a regra usando o mesmo que já criamos afinal se usarmos o agendamento que só funciona em horário comercial, vai ficar mais protegido contra ataque externo quando não estiver em horário comercial:

Name	Time Range(s)	Description
WorkHours	Mon - Fri 9:00-17:00	Regular work week hours.

- Vamos agora criar uma regra no NAT para encaminhar os pedido de RDP vindo de fora para o computador que acabamos de cadastrar, vá a **Firewall | NAT**. Se pesquisarmos na internet sobre “protocolo de acesso remoto ao desktop” vamos ver que a porta é a TCP 3389 (o PfSense já vem com um pré-definido no sistema com o nome MS RDP)

Port Forward

If	Proto	Src. addr	Src. ports	Dest. addr	Dest. ports	NAT IP	NAT Ports	Description
<input type="checkbox"/> WAN	TCP	*	*	WAN address	3389 (MS RDP)	<u>Laptop1</u>	3389 (MS RDP)	Forward RDP to Laptop RDP

- Agora vamos criar um agendamento para que essa regra funcione de acordo com o horário que criamos, vá a **Firewall | Rules**:

Floating	WAN	LAN	DMZ							
ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	
X	*	RFC 1918 networks	*	*	*	*	*		Block private networks	
X	*	Reserved/not assigned by IANA	*	*	*	*	*	*	Block bogon networks	
<input checked="" type="checkbox"/>	TCP	*	*	<u>Laptop1</u>	3389 (MS RDP)	*	none	<u>WorkHours</u>	NAT Forward RDP to Laptop RDP	

9. Clique em **Save**.

10. Clique em **Apply Changes**.

Como ele funciona...

A nossa regra de NAT encaminha todas as solicitações RDP para o nosso laptop. A regra NAT é sempre habilitada. Mas na regra de firewall faz com que esse encaminhamento só funcione durante o horário especificado

Há mais...

Para aumentar a segurança nós podemos fazer mais, podemos restringir o acesso liberando apenas nosso ip de acesso externo, e se esse IP mudar então teremos que mudar o Alias atualizando o IP então sempre íamos ter um controle de quando a pessoa acessou. Crie um Alias com o IP do escritório:

Firewall: Aliases: Edit



Alias Edit							
Name	<input type="text" value="MyWorkIpAddress"/> MyWorkIpAddress The name of the alias may only consist of the characters "a-z, A-Z and 0-9".						
Description	<input type="text" value="My company's public IP address."/> My company's public IP address. You may enter a description here for your reference (not parsed).						
Type	Host(s) <input type="button" value="▼"/>						
Host(s)	<p>Enter as many hosts as you would like. Hosts must be specified by their IP address.</p> <table border="1"> <thead> <tr> <th>IP</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>66.44.33.123</td> <td> Entry added Mon, 06 Mar 2000 08:49:05 -0500</td> </tr> <tr> <td><input type="button" value="New"/></td> <td></td> </tr> </tbody> </table>	IP	Description	66.44.33.123	Entry added Mon, 06 Mar 2000 08:49:05 -0500	<input type="button" value="New"/>	
IP	Description						
66.44.33.123	Entry added Mon, 06 Mar 2000 08:49:05 -0500						
<input type="button" value="New"/>							
<input type="button" value="Save"/> <input type="button" value="Cancel"/>							

Então podemos modificar nossa regra de firewall aplicando os pedidos provenientes ao IP da nossa empresa (lembre-se que o tráfego que não corresponde a regra **any** é bloqueado por padrão). Agora com a associação do NAT com as regras de firewall, pelas regras de firewall nós não poderíamos modificar a fonte diretamente.

Associated filter rule	NOTE: This is associated to a NAT rule. You cannot edit the interface, protocol, source, or destination of associated filter rules.
	View the NAT rule
Interface	<input type="button" value="WAN"/>
	Choose on which interface packets must come in to match this rule.
Protocol	<input type="button" value="TCP"/>
	Choose which IP protocol this rule should match. Hint: in most cases, you should specify TCP here.

Então vamos ter que modificar dentro do próprio NAT, clique na opção **Advanced**, e especifique o Alias com o endereço publico da nossa empresa.

Port Forward								
		1:1	Outbound					
If	Proto	Src. addr	Src. ports	Dest. addr	Dest. ports	NAT IP	NAT Ports	Description
<input type="checkbox"/>  WAN	TCP	<u>MyWorkIpAddress</u>	*	WAN address	3389 (MS RDP)	<u>Laptop1</u>	3389 (MS RDP)	Forward RDP to Laptop RDP

Então vamos checar se essas mudanças foram alteradas também em regras de firewall.

Floating									
ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
	*	RFC 1918 networks	*	*	*	*	*		Block private networks
	*	Reserved/not assigned by IANA	*	*	*	*	*	*	Block bogon networks
<input type="checkbox"/> 	TCP	<u>MyWorkIpAddress</u>	*	<u>Laptop1</u>	3389 (MS RDP)	*	none	 <u>WorkHours</u>	NAT Forward RDP to Laptop RDP

Veja também...

- Configurando servidor DHCP no Capítulo 2 – Serviços Essenciais
- Criando DHCP com mapeamento estático no Capítulo 2 – Serviços Essenciais
- Configurando DNS dinâmico no Capítulo 2 - Serviços Essenciais
- Criando Alias
- Criando Nat Port Forwarding
- Criando regras de firewall
- Criando agendamentos

4

Rede Privada Virtual (VPN)

Nesse capítulo iremos abordar:

- Criando VPN em um túnel IPSec
- Configurando o serviço L2TP VPN
- Configurando o serviço OpenVPN
- Configurando o serviço PPTP VPN

Introdução

Virtual Private Networking (VPN) (Vamos abordar no livro esse nome como Rede Privada Virtual (VPN)) é um sistema moderno muito eficaz. Uma conexão VPN permite que um usuário remoto conecte com segurança uma rede e use os recursos como se estivesse no próprio local.

Com todas as variedades de acesso VPN, O PfSense tem quatro implementações mais usadas, elas são construídas direto dentro do OpenVPN que esta migrado como o protocolo VPN. Mas nada impede que você baixe um software a sua escolha de VPN cliente para qualquer máquina usando Windows (suporte OpenVPN não vem no Windows). IPSec é mais complexo, mas também é uma aplicação muito popular do VPN. Serviço PPTP VPN e L2PTP VPN são menos usados entre os quatro, mas seu uso ainda é bem generalizado.

Neste capítulo vamos descrever como configurar o PfSense para usar qualquer um ou as quatro aplicações VPN-IPSec, L2TP, OpenVPN, e PPTP.

Criando VPN em um túnel IPSec

Aqui vamos descrever como criar uma VPN usando um túnel IPSec.

Se preparando...

IPSec é muitas vezes o método preferido para o tipo de conexão rede-a-rede (é oposto ao cliente-a-rede). Um cenário típico monta uma conexão permanente e segura entre sede e filial.

Redes conectadas através de VPN devem obrigatoriamente usar sub-redes diferentes. Por exemplo, se as duas redes usam sub-redes 192.168.1.0/24, o VPN não vai funcionar.

Como fazê-lo...

1. Vá até **VPN | Ipsec**
2. Clique no botão “+” para criar um túnel IPSec.
3. Especifique em **Remote Gateway** o IP publico ou o hostname do gateway remoto.
4. E em **Description** adicione uma descrição do seu IPSec

VPN: IPsec: Edit Phase 1

S L ?

Tunnels **Mobile clients** **Pre-shared keys**

General information

Disabled **Disable this phase1 entry**
Set this option to disable this phase1 without removing it from the list.

Interface **WAN** Select the interface for the local endpoint of this phase1 entry.

Remote gateway **texas.example.com** Enter the public IP address or host name of the remote gateway

Description **Tunnel to Houston office.** You may enter a description here for your reference (not parsed).

Phase 1 proposal (Authentication)

Authentication method **Mutual PSK** Must match the setting chosen on the remote side.

Negotiation mode **aggressive** Aggressive is more flexible, but less secure.

My identifier **My IP address**

Peer identifier **Peer IP address**

Pre-Shared Key **secret** Input your pre-shared key string.

5. Em **Pre-Shared Key** digite sua senha
6. Clique em **Save**
7. Marque **Enable IPsec**.
8. Clique em **Save**.

VPN: IPsec

S L ?

Tunnels Mobile clients Pre-shared keys

Enable IPsec

Save

Remote Gateway	Mode	P1 Protocol	P1 Transforms	P1 Description
WAN texas.example.com	aggressive	3DES	SHA1	Tunnel to Houston office.

+ - Show 0 Phase-2 entries

Note:
You can check your IPsec status at [Status:IPsec](#).

9. Clique em **Apply Changes**.
10. Vá até **Firewall | Rules**
11. Selecione a aba **IPSec**
12. Clique no botão “+” para adicionar uma nova regra no firewall
13. Em **Destination** selecione **Lan subnet**.
14. Em **Destination port** selecione **any**
15. Em **Description**, ponha uma descrição que você possa reconhecer a regra, nos usamos no exemplo **Allow IPsec traffic to LAN**.

Firewall: Rules

S L ?

Floating WAN LAN PUB DMZ PPTP VPN IPsec

ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
<input type="checkbox"/> <input checked="" type="checkbox"/>	TCP	*	*	LAN net	*	*	none		Allow IPsec traffic to LAN.

Actions:

- pass
- pass (disabled)
- block
- block (disabled)
- reject
- reject (disabled)
- log
- log (disabled)

Hint:

Rules are evaluated on a first-match basis (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you'll have to pay attention to the rule order. Everything that isn't explicitly passed is blocked by default.
You may drag and drop rules using your mouse to reorder the rule ordering.

16. Clique em **Save**

17. Clique em **Apply Changes**.

Como ele funciona...

Uma vez que o túnel IPSec foi estabelecido, os clientes conectados em qualquer uma das duas redes, terão acesso de um ao outro mesmo em sub-redes diferentes como se estivesse na mesma rede física.

Veja também...

- Configurando o serviço L2TP VPN
- Configurando o serviço OpenVPN
- Configurando o serviço PPTP VPN

Configurando o serviço L2TP VPN

Aqui vamos descrever como configurar o PfSense para ser servidor VPN L2TP

Se preparando...

É muito importante entender que ao contrário das outras implementações VPN, o L2TP não criptografa os dados. O L2TP é simplesmente um método de encapsulamento que só deve ser usado em redes já confiáveis, em conjunto com o IPsec. A grande vantagem do L2TP é que pode ser usado com redes sem precisar de IP.

Como fazê-lo...

1. Vá em **VPN | L2TP**
2. Na aba **Configuration**, marque **Enable L2TP Server**.
3. Especifique um IP sem uso em **Server address**.
4. Em **Remote address Range** digite o inicio da faixa de IP não usada de endereço remoto. O numero de IPs que vai ser usado vai estar indicado na etapa 6.
5. Em **Subnet mask** especifique o tipo de subrede.
6. Em **Number of L2TP users** especifique o numero de usuários que irão se conectar.

VPN: L2TP: L2TP

Configuration **Users**

Off
 Enable l2tp server

Interface **WAN**

Server address **192.168.3.254**
Enter the IP address the L2TP server should use on its side for all clients.

Remote address range **192.168.3.0**
Specify the starting address for the client IP address subnet.

Subnet netmask **24**
Hint: 24 is 255.255.255.0

Number of L2TP users **100**
Hint: 10 is ten L2TP clients

7. Clique em **Save**
8. Clique na aba **Users**.
9. Clique no botão “+” para adicionar um novo usuário
10. Digite o usuário em **username** e a senha em **password**.

VPN: L2TP: User: Edit

Username **johndoe**

Password *********
********* (confirmation)
If you want to change the user's password, enter it here twice.

IP address
If you want the user to be assigned a specific IP address, enter it here.

Save **Cancel**

11. Clique em **Save**.

VPN: L2TP: Users

Configuration **Users**

Username	IP address	
johndoe	Dynamic	  

12. Vá até **Firewall | Rules**

13. Selecione a aba **L2TP VPN**

14. Clique no botão “+” para adicionar uma nova regra de firewall

15. Selecione em **Destination o LanSubnet**

16. Selecione em **Destination port range o any**

17. Digite em **Description** uma descrição que você possa identificar a sua regra, no exemplo nos usamos **Allow L2TP Clients to LAN**.

18. Clique em **Save**.

Firewall: Rules



Floating	WAN	LAN	DMZ	L2TP VPN					
ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
<input type="checkbox"/>	TCP	*	*	LAN net	*	*	none		Allow L2TP Clients to LAN

pass block
 pass (disabled) block (disabled)

reject reject (disabled)

log log (disabled)

Hint:
Rules are evaluated on a first-match basis (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you'll have to pay attention to the rule order. Everything that isn't explicitly passed is blocked by default.

19. Clique em **Apply Changes**.

Como ele funciona...

O serviço permite que usuários conectem remotamente a interface de rede a nossa escolha usando o L2TP. Usando esse serviço é como se o cliente estivesse usando a rede como se estivesse fisicamente no local.

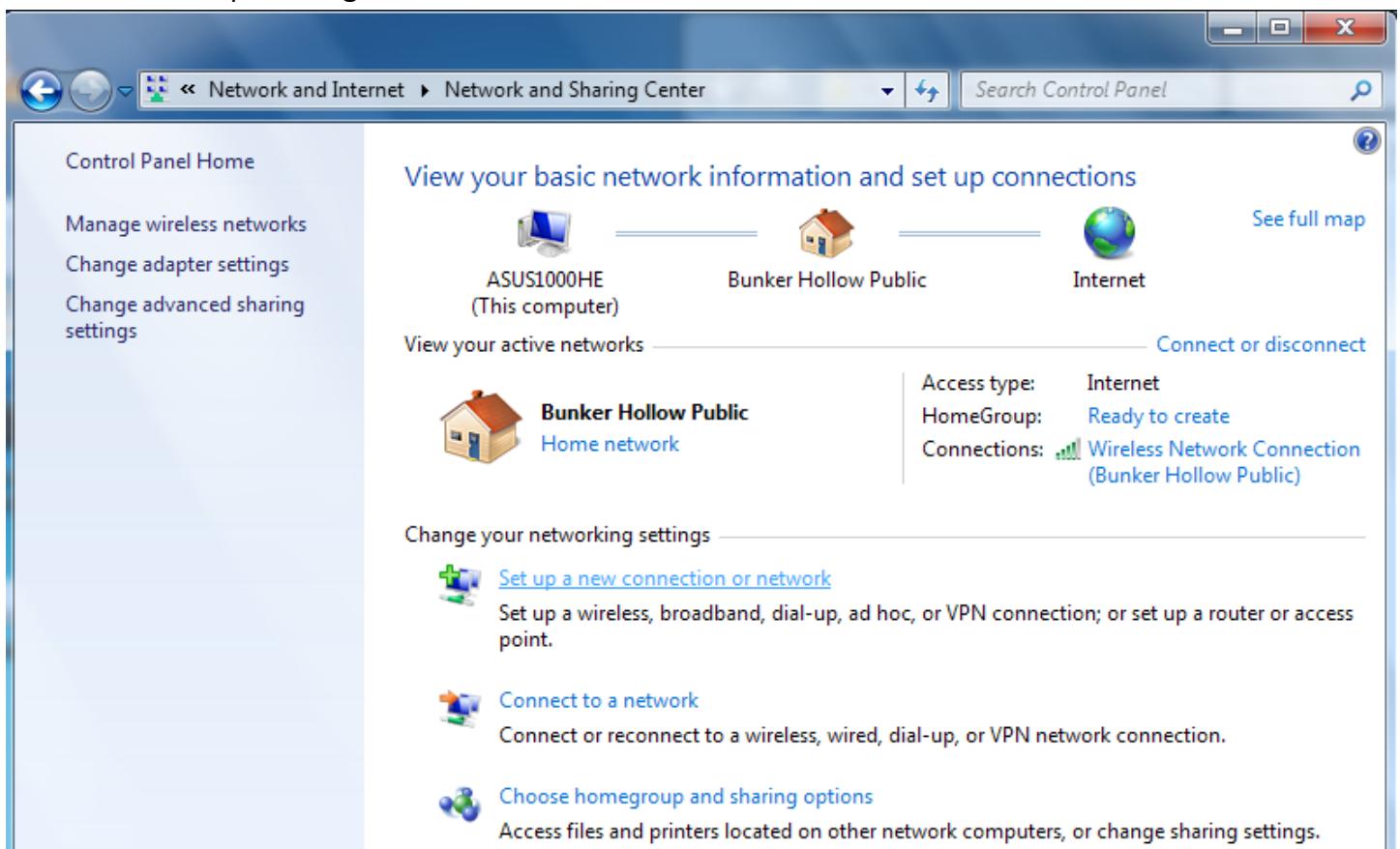
Coneção de um cliente usando Windows 7

Para criar uma conexão VPN L2TP em uma maquina usando o Windows 7:

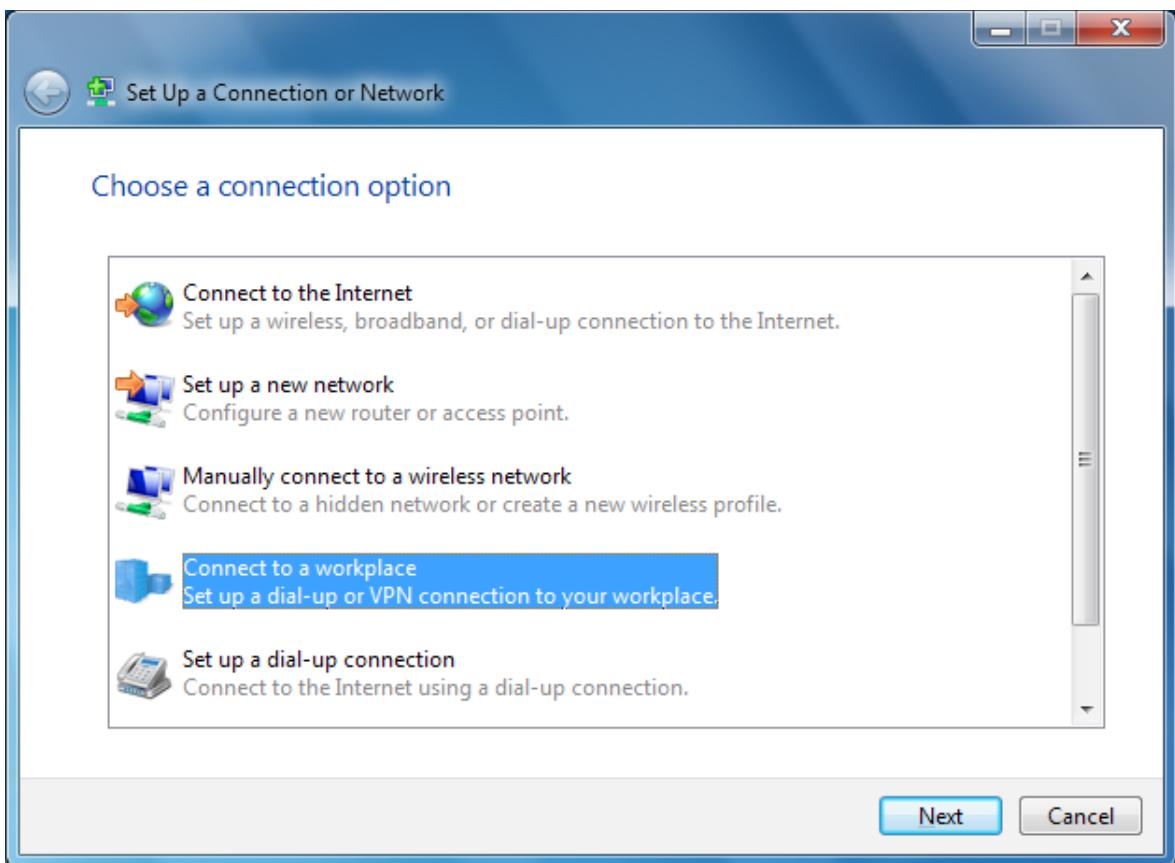
1. Abra o **Painel de Controle | Rede e Internet | Status de tarefas de rede**, abra o Central de Rede e compartilhamento



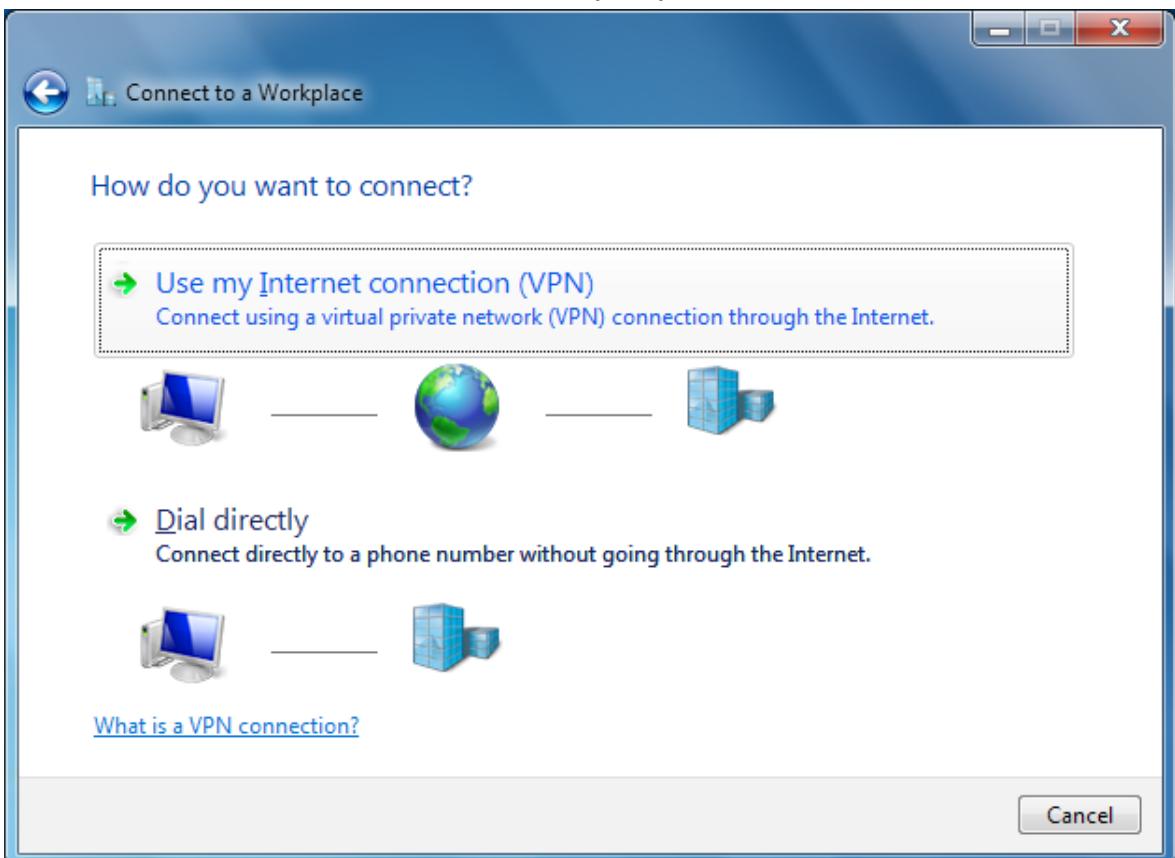
2. Clique **Configurar uma nova conexão de rede**



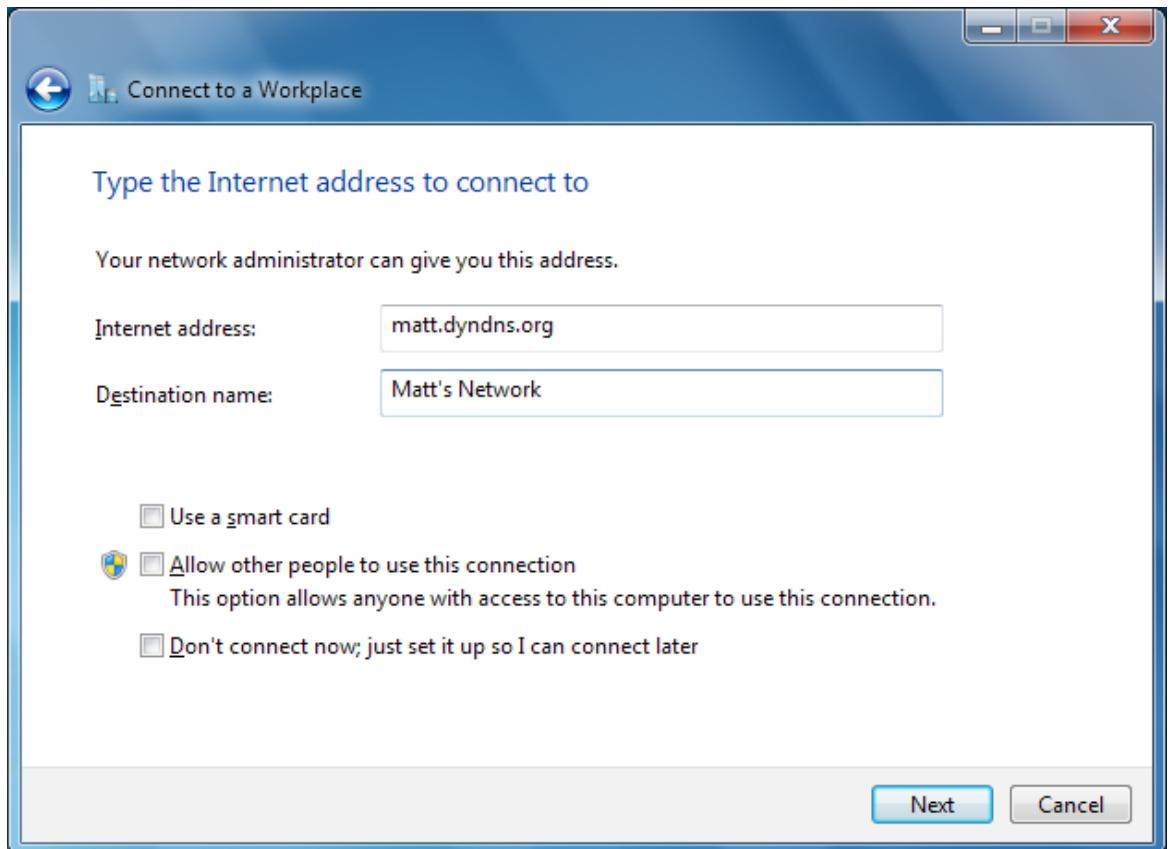
3. Escolha **Conectar a um local de trabalho**.



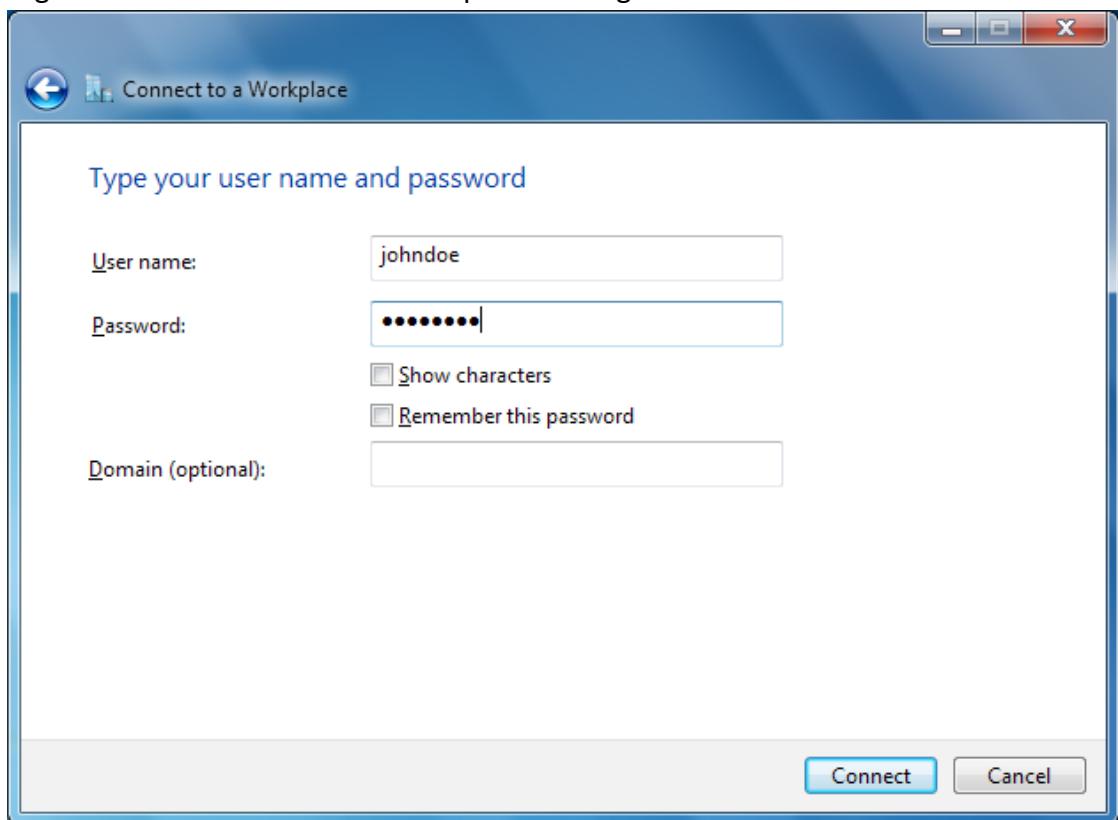
4. Escolha **Usar minha conexão com a internet (VPN)**:



5. Digite em **Endereço na Internet** o endereço do servidor da rede a qual você está querendo se conectar. Se o endereço L2TP que você configurou não está acessível diretamente, você terá que fazer um NAT no servidor direcionando o tráfego L2TP.



6. Digite o nome de **usuário** e **senha** que foi configurado antes:



7. Clique depois em **Conectar**, o Windows irá detectar automaticamente se o servidor está aceitando a conexão L2TP ou PPTP, e vai ser configurado de acordo com o selecionado.

Veja também...

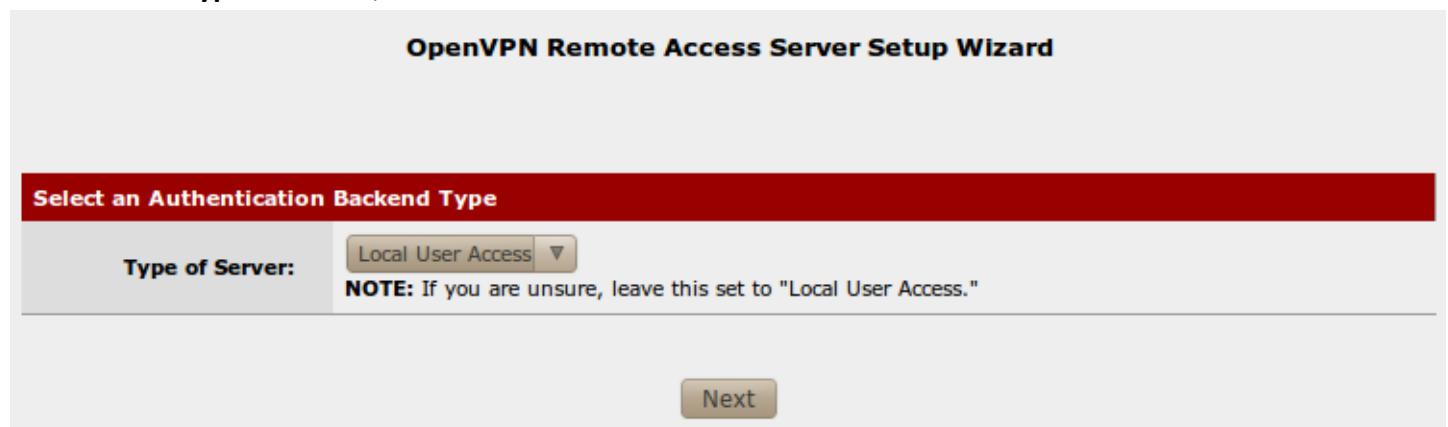
- Configurando NAT por Forward, capítulo 3 – Configuração Geral
- Criando VPN em um túnel IPSec
- Configurando o serviço OpenVPN
- Configurando o serviço PPTP VPN

Configurando serviço de OpenVPN

Aqui vamos descrever como configurar o PfSense para aceitar conexões OpenVPN.

Como fazê-lo...

1. Vá até **VPN | OpenVPN**.
2. Clique na aba **Wizards**.
3. Em **Type of Server**, selecione **Local User Access**.



4. Clique em **Next**.
5. Em **Descriptive Name**, coloque um nome para seu VPN, no exemplo nos usamos **MyCaCert**, se referindo ao certificado CA.
6. Em **Country Code** usamos no exemplo o **USA**.
7. Em **State or Province**, nós usamos no exemplo **New York**.
8. Em **City**, nós usamos no exemplo **New York**.
9. Em **Organization**, usamos no exemplo **Blue Key Consulting**.
10. No **e-mail** usamos como exemplo **contact@example.com**.
11. Clique em **Add new CA**.

OpenVPN Remote Access Server Setup Wizard

Create a New Certificate Authority (CA) Certificate

Descriptive name:	MyCaCert A name for your reference, to identify this certificate. This is the same as common-name field for other Certificates.
Key length:	2048 bit Size of the key which will be generated. The larger the key, the more security it offers, but larger keys are generally slower to use.
Lifetime:	3650 Lifetime in days. This is commonly set to 3650 (Approximately 10 years.)
Country Code:	US Two-letter ISO country code (e.g. US, AU, CA)
State or Province:	New York Full State or Province name, not abbreviated (e.g. Kentucky, Indiana, Ontario).
City:	New York City or other Locality name (e.g. Louisville, Indianapolis, Toronto).
Organization:	Blue Key Consulting Organization name, often the Company or Group name.
E-mail:	contact@example.com E-mail address for the Certificate contact. Often the e-mail of the person generating the certificate (i.e. You.)

Add new CA

12. Digite em **Descriptive name**, um nome o novo certificado do servidor, no exemplo usamos o mesmo **MyCaCert**. A criação desse certificado vai ficar quase idêntico ao criado anteriormente.
13. Em **Country Code** usamos no exemplo o **USA**.
14. Em **State or Province**, nós usamos no exemplo **New York**.
15. Em **City**, nós usamos no exemplo **New York**.
16. Em **Organization**, usamos no exemplo **Blue Key Consulting**.
17. No **e-mail** usamos como exemplo **contact@example.com**.
18. Clique em **Create new Certification**.

OpenVPN Remote Access Server Setup Wizard

Create a New Server Certificate

Descriptive name:	<input type="text" value="MyServerCert"/> MyServerCert A name for your reference, to identify this certificate. This is also known as the certificate's "Common Name."
Key length:	<input type="text" value="2048 bits"/> 2048 bits Size of the key which will be generated. The larger the key, the more security it offers, but larger keys are generally slower to use.
Lifetime:	<input type="text" value="3650"/> 3650 Lifetime in days. This is commonly set to 3650 (Approximately 10 years.)
Country Code:	<input type="text" value="US"/> US Two-letter ISO country code (e.g. US, AU, CA)
State or Province:	<input type="text" value="New York"/> New York Full State or Province name, not abbreviated (e.g. Kentucky, Indiana, Ontario).
City:	<input type="text" value="New York"/> New York City or other Locality name (e.g. Louisville, Indianapolis, Toronto).
Organization:	<input type="text" value="Blue Key Consulting"/> Blue Key Consulting Organization name, often the Company or Group name.
E-mail:	<input type="text" value="contact@example.com"/> contact@example.com E-mail address for the Certificate contact. Often the e-mail of the person generating the certificate (i.e. You.)

19. Em **Description** você coloca a descrição que você possa reconhecer futuramente, no exemplo nos usamos **My OpenVPN Connection**.

General OpenVPN Server Information

Interface:	<input type="text" value="wan"/> wan The interface where OpenVPN will listen for incoming connections (typically WAN.)
Protocol:	<input type="text" value="UDP"/> UDP Protocol to use for OpenVPN connections. If you are unsure, leave this set to UDP.
Local Port:	<input type="text" value="1194"/> 1194 Local port upon which OpenVPN will listen for connections. The default port is 1194. Leave this blank unless you need to use a different port.
Description:	<input type="text" value="My OpenVPN Connection"/> My OpenVPN Connection A name for this OpenVPN instance, for your reference. It can be set however you like, but is often used to distinguish the purpose of the service (e.g. "Remote Technical Staff").

20. Digite em **Tunner Network** a conotação em CIDR, isso vai ser uma faixa de IP não usada (que geralmente não é muito diferente da rede que você usa) como **192.168.4.0/24**.

21. Digite em **Local Network** a conotação em CIDR, que os clientes vão ser capazes de acessar, que geralmente é a rede interna LAN, **192.168.1.0/24**.
22. Especifique em **Concurrent Connections**, o numero máximo de clientes que irão se conectar.

Tunnel Settings	
Tunnel Network:	<input type="text" value="192.168.4.0/24"/> This is the virtual network used for private communications between this server and client hosts expressed using CIDR notation (eg. 10.0.8.0/24). The first network address will be assigned to the server virtual interface. The remaining network addresses can optionally be assigned to connecting clients. (see Address Pool)
Redirect Gateway:	<input type="checkbox"/> Force all client generated traffic through the tunnel.
Local Network:	<input type="text" value="192.168.1.0/24"/> This is the network that will be accessible from the remote endpoint, expressed as a CIDR range. You may leave this blank if you don't want to add a route to the local network through this tunnel on the remote machine. This is generally set to your LAN network.
Concurrent Connections:	<input type="text" value="100"/> Specify the maximum number of clients allowed to concurrently connect to this server.
Compression:	<input type="checkbox"/> Compress tunnel packets using the LZO algorithm.
Type-of-Service:	<input type="checkbox"/> Set the TOS IP header value of tunnel packets to match the encapsulated packet value.
Inter-Client Communication:	<input type="checkbox"/> Allow communication between clients connected to this server.
Duplicate Connections:	<input type="checkbox"/> Allow multiple concurrent connections from clients using the same Common Name. NOTE: This is not generally recommended, but may be needed for some scenarios.

23. Clique no botão **Next**.
24. Marque **Add a rule to permit traffic from clients on the Internet to the OpenVPN server process**.
25. Marque **Add a rule to allow all traffic from connected clients to pass across the VPN tunnel**:

OpenVPN Remote Access Server Setup Wizard

Firewall Rule Configuration

Firewall Rules control what network traffic is permitted. You must add rules to allow traffic to the OpenVPN server's IP and port, as well as allowing traffic from connected clients through the tunnel. These rules can be automatically added here, or configured manually after completing the wizard.

Traffic from clients to server

Firewall Rule: Add a rule to permit traffic from clients on the Internet to the OpenVPN server process.

Traffic from clients through VPN

OpenVPN rule: Add a rule to allow all traffic from connected clients to pass across the VPN tunnel.

Next

26. Clique no botao Next.

OpenVPN Remote Access Server Setup Wizard

Configuration Complete!

Your configuration is now complete.

To be able to export client configurations, browse to System->Packages and install the OpenVPN Client Export package.

Finish

27. Depois clique no botao Finish.

OpenVPN: Server

S L ?

Server Client Client Specific Overrides Wizards

Disabled	Protocol / Port	Tunnel Network	Description	
NO	UDP / 1194	192.168.4.0/24	My OpenVPN Connection	  

Additional OpenVPN servers can be added here.

Como ele funciona...

O serviço permite que usuários externos usem o OpenVPN para estabelecer uma conexão segura e criptografada em nossa rede. Os usuários se conectarão usando um cliente OpenVPN, e uma vez autenticado, o usuário terá acesso a rede como se estivesse no local fisicamente.

Algoritmos de Criptografia

Escolher o melhor algoritmo de criptografia é essencial para o melhor desempenho do seu hardware. Muitas placas de expansão VPN, como aquelas encontradas em Netgate usando Alix requerem placas AES-128-CBC. Verifique com seu fornecedor de hardware para obter mais detalhes.

Exportando Cliente OpenVPN

Há um pacote de instalação no PfSense chamado **OpenVPN Client Export Utility**, que simplifica o processo de configuração:

1. Vá até **System | Packages**
2. Clique na aba **Available Packages**.
3. Localize **OpenVPN Client Export Utility**, e clique no botão "+" para começar a instalação.

OpenVPN Client Export Utility	Security	BETA 0.5 platform: 2.0	No info, check the forum	Allows a pre-configured OpenVPN Windows Client or Mac OSX's Viscosity configuration bundle to be exported directly from pfSense.
-------------------------------	----------	---------------------------------	--------------------------------	--

4. O pacote depois de baixado será instalado automaticamente.

System: Package Manager: Install Package

The screenshot shows the pfSense Package Manager interface. At the top, there are tabs for "Available packages", "Installed packages", and "Package Installer". The "Package Installer" tab is selected. A progress bar at the top indicates the installation is complete. Below the progress bar, a message box displays the text: "OpenVPN Client Export Utility installation completed." The main window shows the log output of the package installation process:

```
Beginning package installation for OpenVPN Client Export Utility...
Downloading package configuration file... done.
Saving updated package information... done.
Downloading OpenVPN Client Export Utility and its dependencies...
Checking for package installation...
  Downloading http://files.pfsense.org/packages/8/All/zip-3.0.tbz ...
  (extracting)Loading package configuration... done.
Configuring package components...
Additional files... done.
Loading package instructions...
Integrated Tab items... done.
Custom commands...
Executing custom_php_install_command()...done.
Writing configuration... done.
Starting service.

Installation completed. Please check to make sure that the package is
configured from the respective menu then start the package.
```

5. O pacote depois de instalado será encontrado no menu **VPN | OpenVPN**.

Veja também...

- Criando VPN em um túnel IPSec

- Configurando o serviço PPTP VPN
- Configurando o serviço L2TP VPN

Configurando o serviço PPTP VPN

Aqui vamos descrever como configurar o PfSense para receber conexões PPTP VPN.

Como fazê-lo...

1. Vá até **VPN | PPTP | aba Configuration**
2. Marque **Enable PPTP server**
3. Escolha em **No. PPTP users**, o numero de clientes que irão se conectar
4. Em **Server address** digite um IP não usado para especificar o endereço para o servidor PPTP. O PPTP do servidor vai escutar esse endereço.
5. Em **Remote address range**, digite o inicio dos IPs dos clientes que irão se conectar, lembre-se de deixar uma quantidade de IP o suficiente referente ao que você colocou em **No. PPTP users**.

VPN: VPN PPTP

Configuration **Users**

Off

Redirect incoming PPTP connections to:

PPTP redirection
Enter the IP address of a host which will accept incoming PPTP connections.

Enable PPTP server

No. PPTP users Hint: 10 is TEN pptp clients

Server address
Enter the IP address the PPTP server should use on its side for all clients.

Remote address range
Specify the starting address for the client IP subnet.

PPTP DNS Servers

primary and secondary DNS servers assigned to PPTP clients

WINS Server

6. Marque **Require 128-bit encryption**.

Require 128-bit encryption
When set, only 128-bit encryption will be accepted. Otherwise 40-bit and 56-bit encryption will be accepted as well. Note that encryption will always be forced on PPTP connections (i.e. unencrypted connections will not be accepted).

Save

Note:
don't forget to add a firewall rule to permit traffic from PPTP clients!

7. Clique em **Save**.
8. Selecione a aba **Users**.
9. Clique no botão “+” para adicionar um usuário
10. Coloque o nome de usuário em **username** e a senha em **password**.
11. Clique em **Save**.

VPN: VPN PPTP: Users

Username	IP address
johndoe	

12. Vá até **Firewall | Rules**
13. Selecione a aba **PPTP VPN**
14. Clique no botão “+” para criar uma nova regra de firewall.
15. Selecione em **Destination** o **Lansubnet**.
16. Selecione em **Destination port range** a opção **any**.
17. Em **Description** digite uma descrição que você possa reconhecer futuramente, no exemplo usamos **Allow PPTP Clients to LAN**.
18. Clique em **Save**.

Firewall: Rules

ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
1	TCP	*	*	LAN net	*	*	none		Allow PPTP clients to LAN.

Legend:
 pass block
 pass (disabled) block (disabled)
 reject reject (disabled)
 log log (disabled)

19. Clique em **Apply Changes**.

Como ele funciona...

O serviço permite que usuários externos estabeleçam uma conexão segura e criptografada usando o PPTP. Os usuários irão se conectar a rede usando um cliente PPTP, uma vez autenticado, o usuário terá acesso a rede como se estivesse conectado no próprio local.

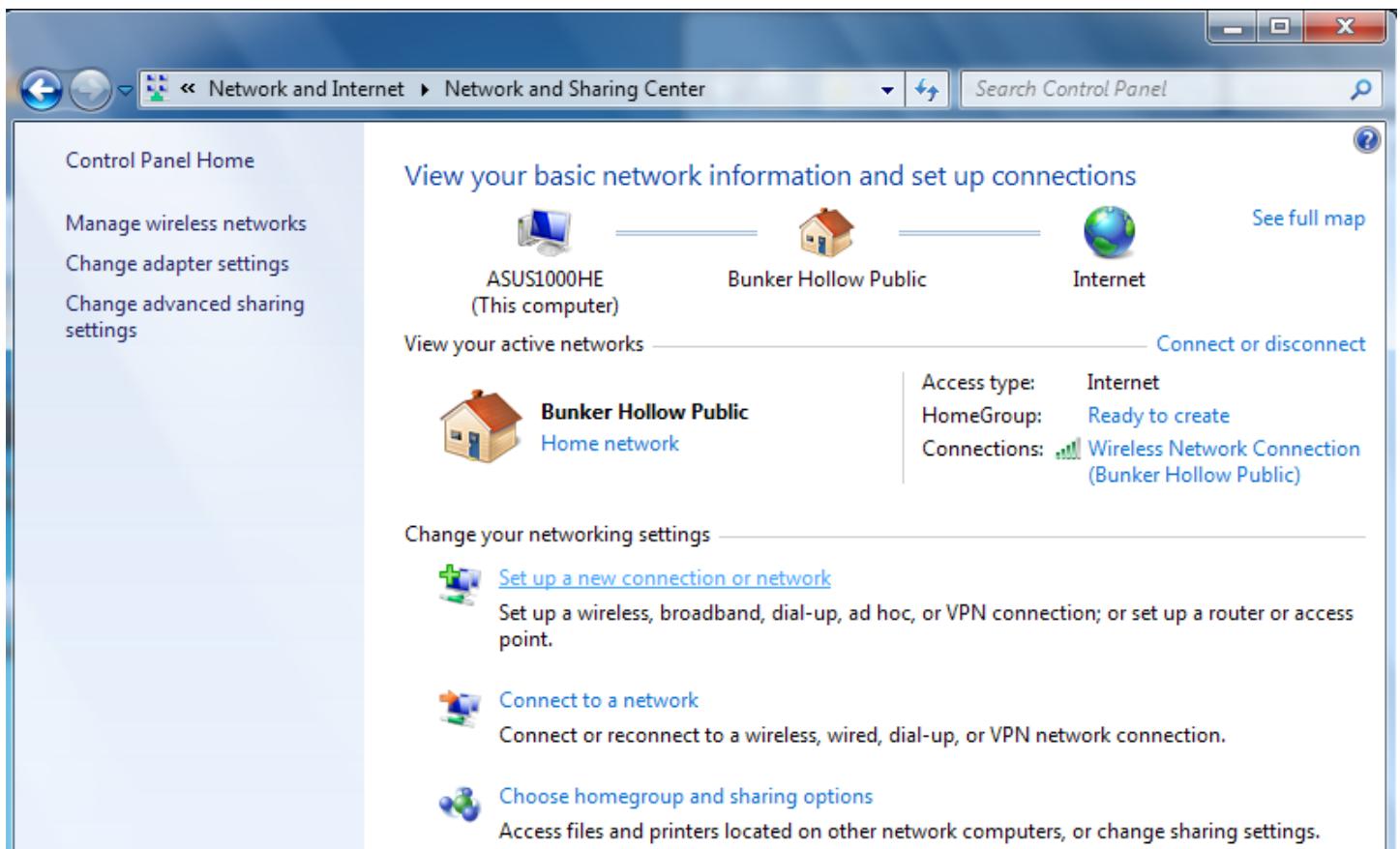
Coneção de um cliente usando Windows 7

Para criar uma conexão VPN PPTP em uma máquina usando o Windows 7:

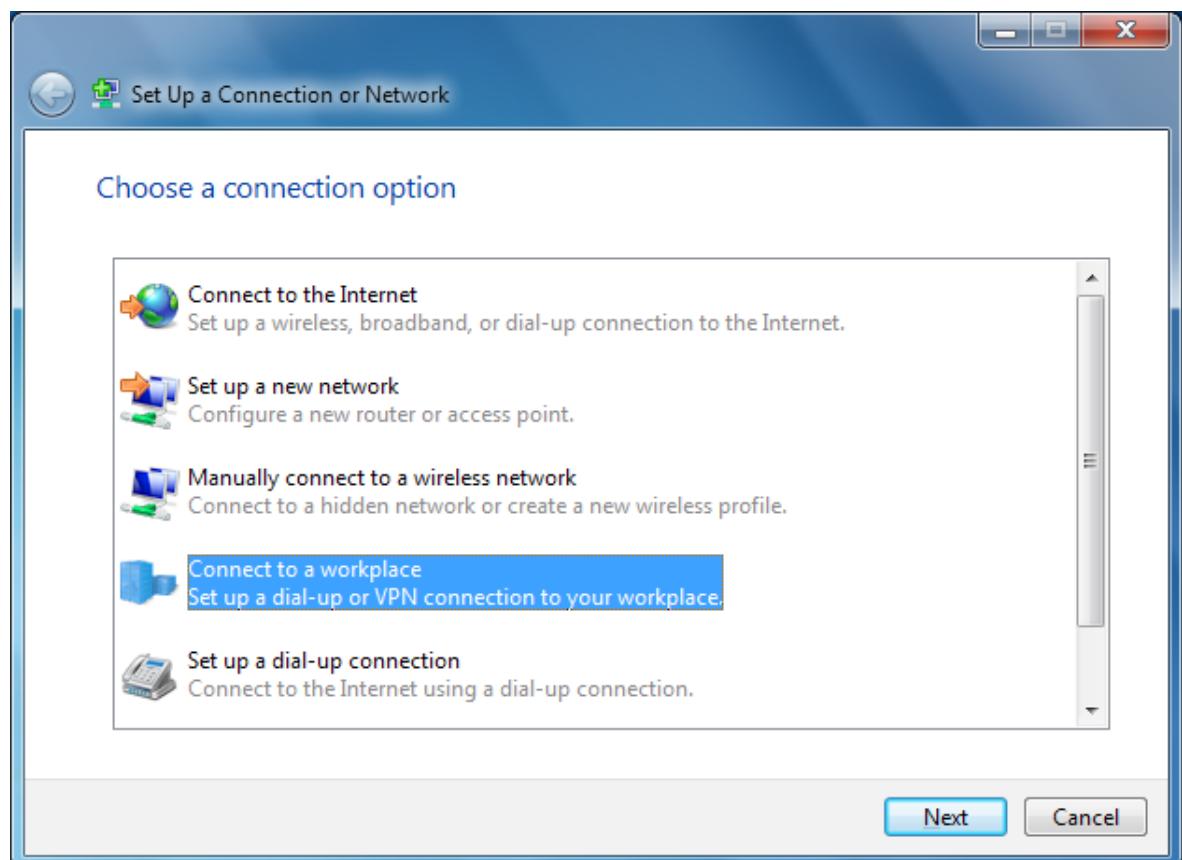
8. Abra o **Painel de Controle | Rede e Internet | Status de tarefas de rede**, abra o Central de Rede e compartilhamento



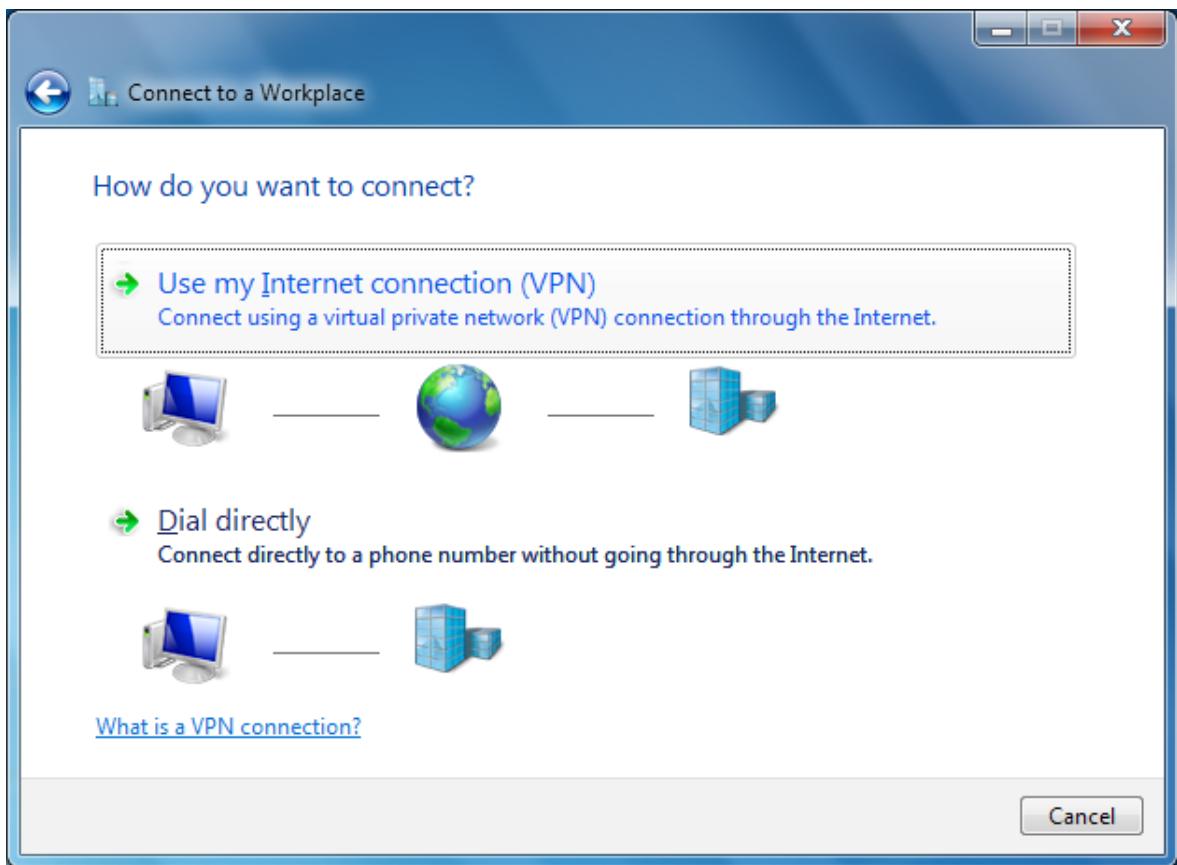
9. Clique **Configurar uma nova conexão de rede**



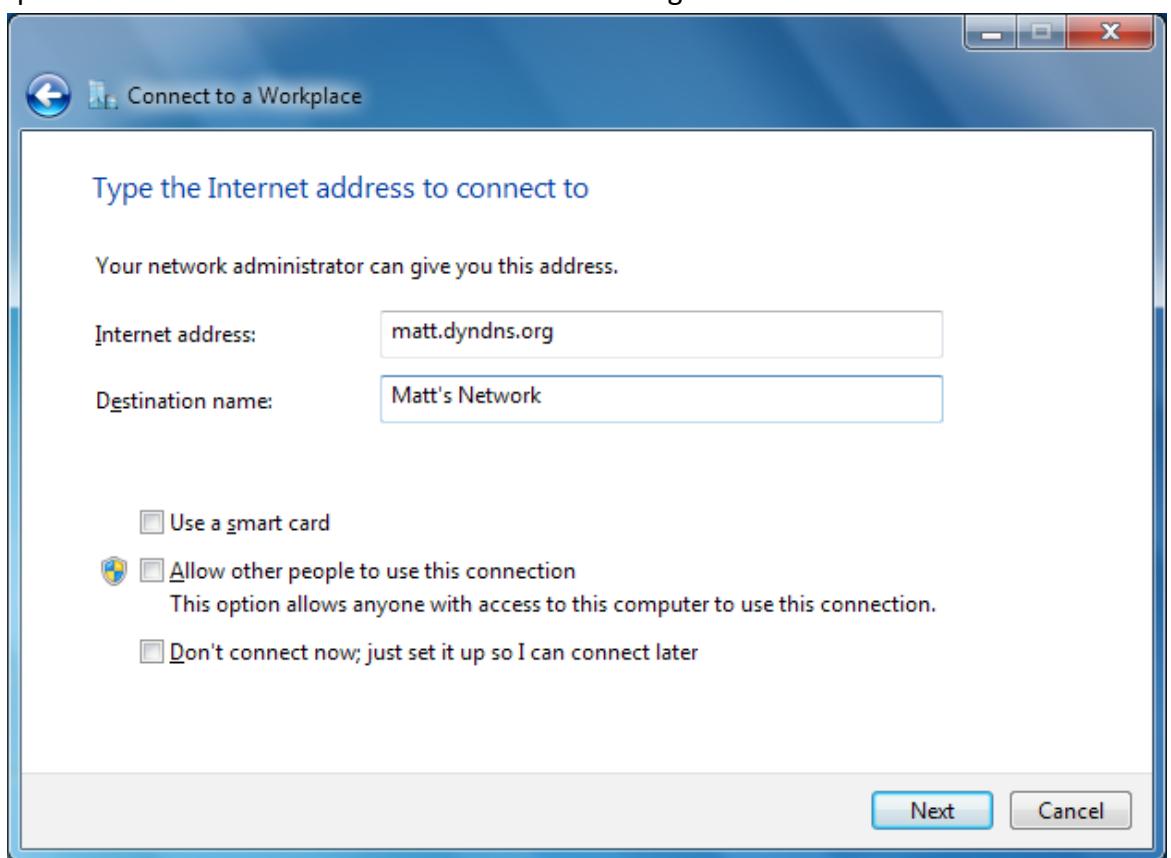
10. Escolha **Conectar a um local de trabalho**.



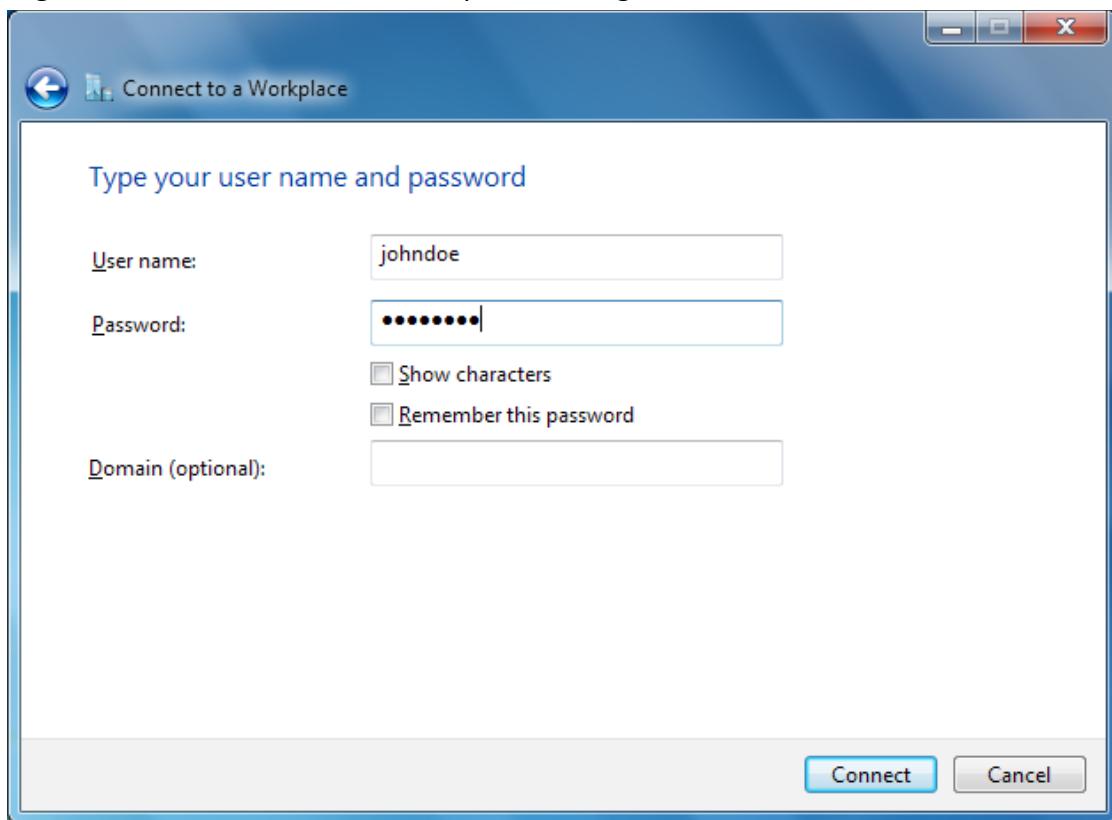
11. Escolha **Usar minha conexão com a internet (VPN)**:



12. Digite em **Endereço na Internet** o endereço do servidor da rede a qual você está querendo se conectar. Se o endereço L2TP que você configurou não está acessível diretamente, você terá que fazer um NAT no servidor direcionando o tráfego L2TP.



13. Digite o nome de **usuário** e **senha** que foi configurado antes:



Clique depois em **Conectar**, o Windows irá detectar automaticamente se o servidor está aceitando a conexão L2TP ou PPTP, e vai ser configurado de acordo com o selecionado.

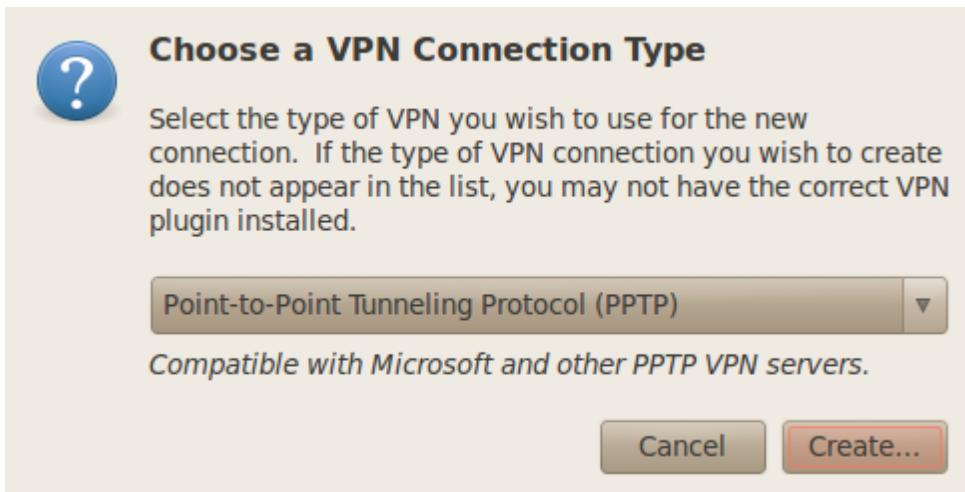
Conectando usando como cliente o Ubuntu 10.10

Execute os seguintes passos para criar uma conexão PPTP VPN em um cliente usando Ubuntu 10.10 (por não ter um computador com esse sistema operacional em português eu mantive os exemplos em inglês de acordo com as janelas de exemplo).

1. Abra **System | Preferences | Network Connections**
2. Selecione a aba **VPN** | Clique no botão **Add** para criar uma conexão VPN.



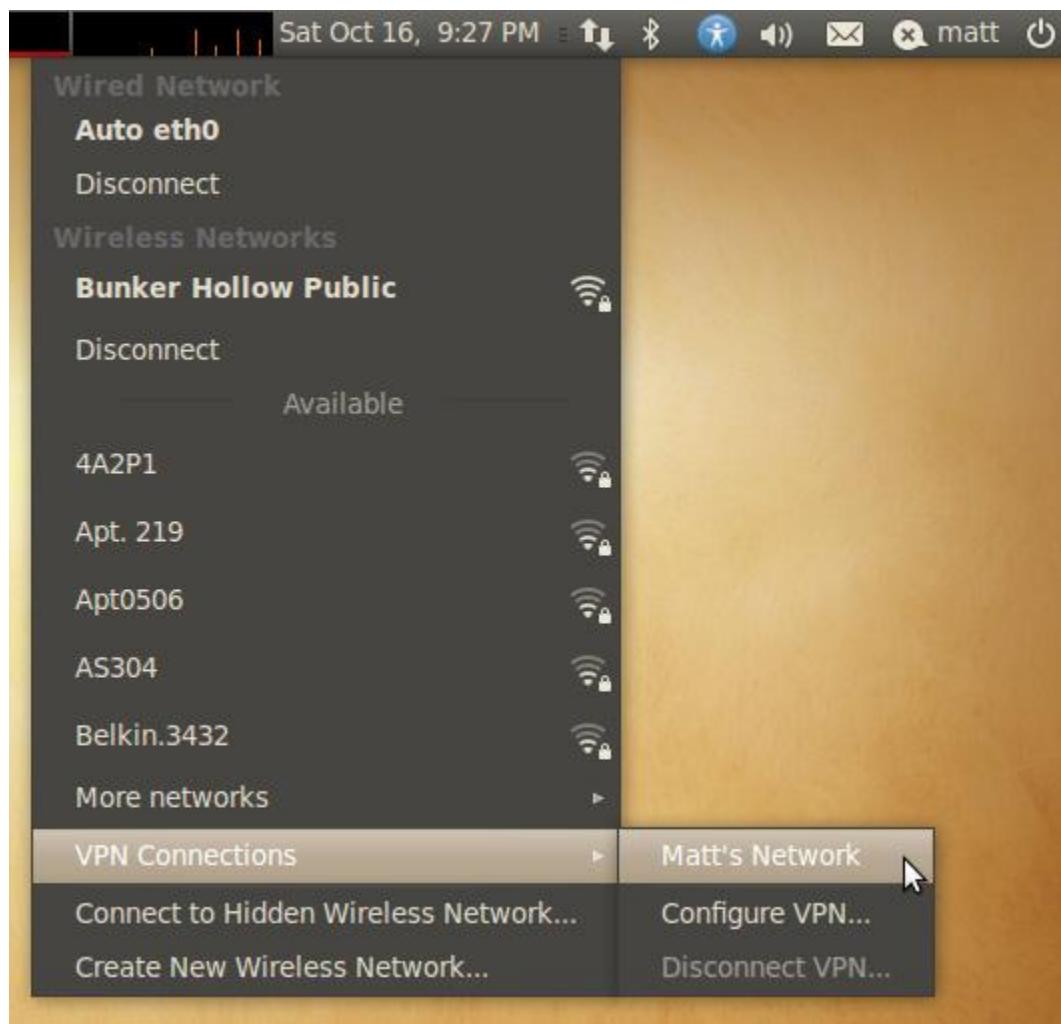
3. Selecione **PPTP** e clique em **Create...**



4. Em **Connection name** digite um nome que você possa identificar, no exemplo usamos **Matt's Network**.
5. Em **Gateway** digite o ip do servidor que você configurou o PPTP VPN. Se o IP não pode ser acessado diretamente, você terá que configurar o NAT com port Forward.



6. Cliquem **Apply**
7. Clique em **Close**.
8. Vá em **Network connection**, selecione no menu **VPN Connections | Matt's Network**



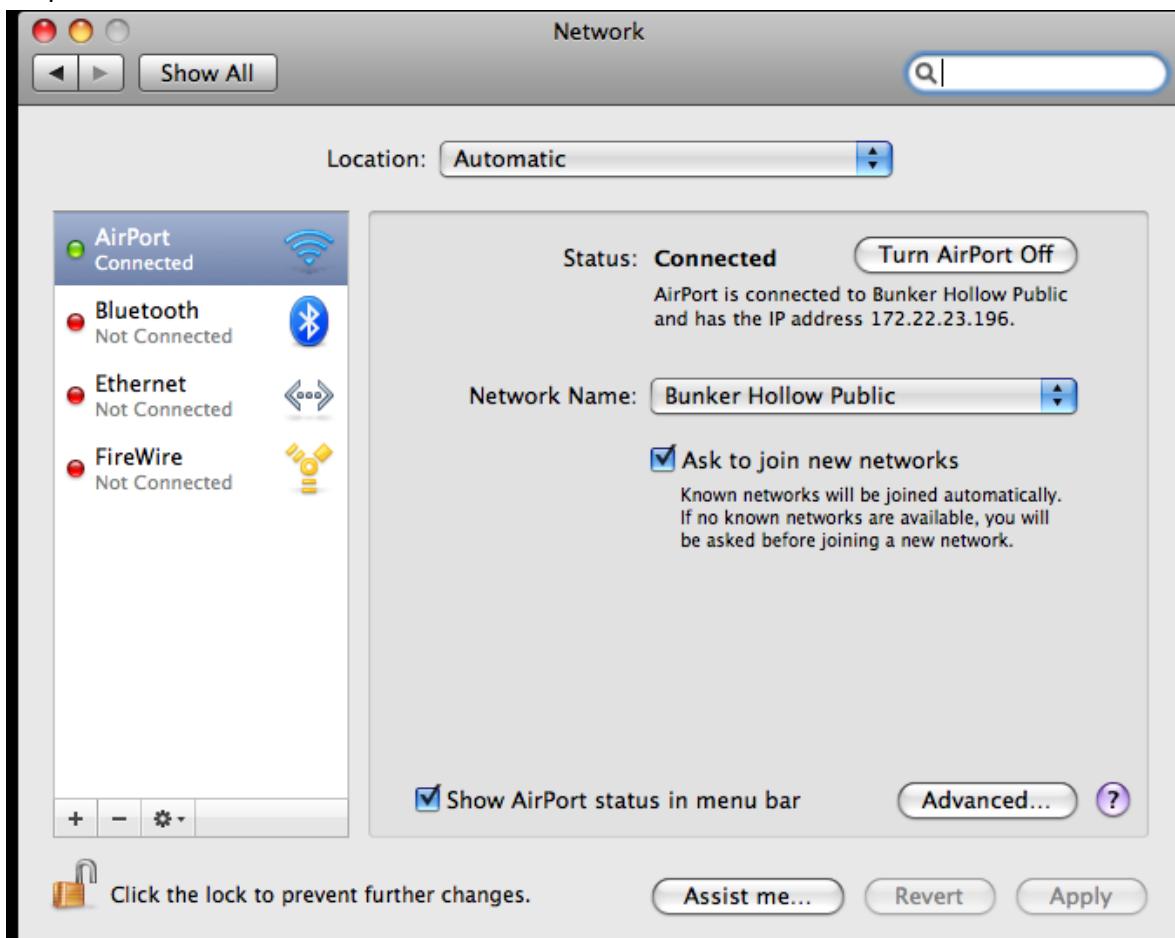
Conectando usando como cliente o Mac OSx

Execute os seguintes passos para criar uma conexão PPTP VPN em um cliente usando Mac OSx (por não ter um computador com esse sistema operacional em português eu mantive os exemplos em inglês de acordo com as janelas de exemplo).

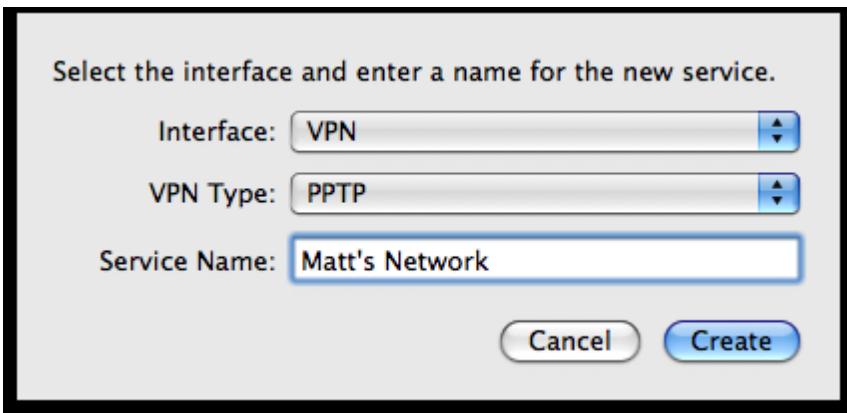
1. Abra **System Preferences**.



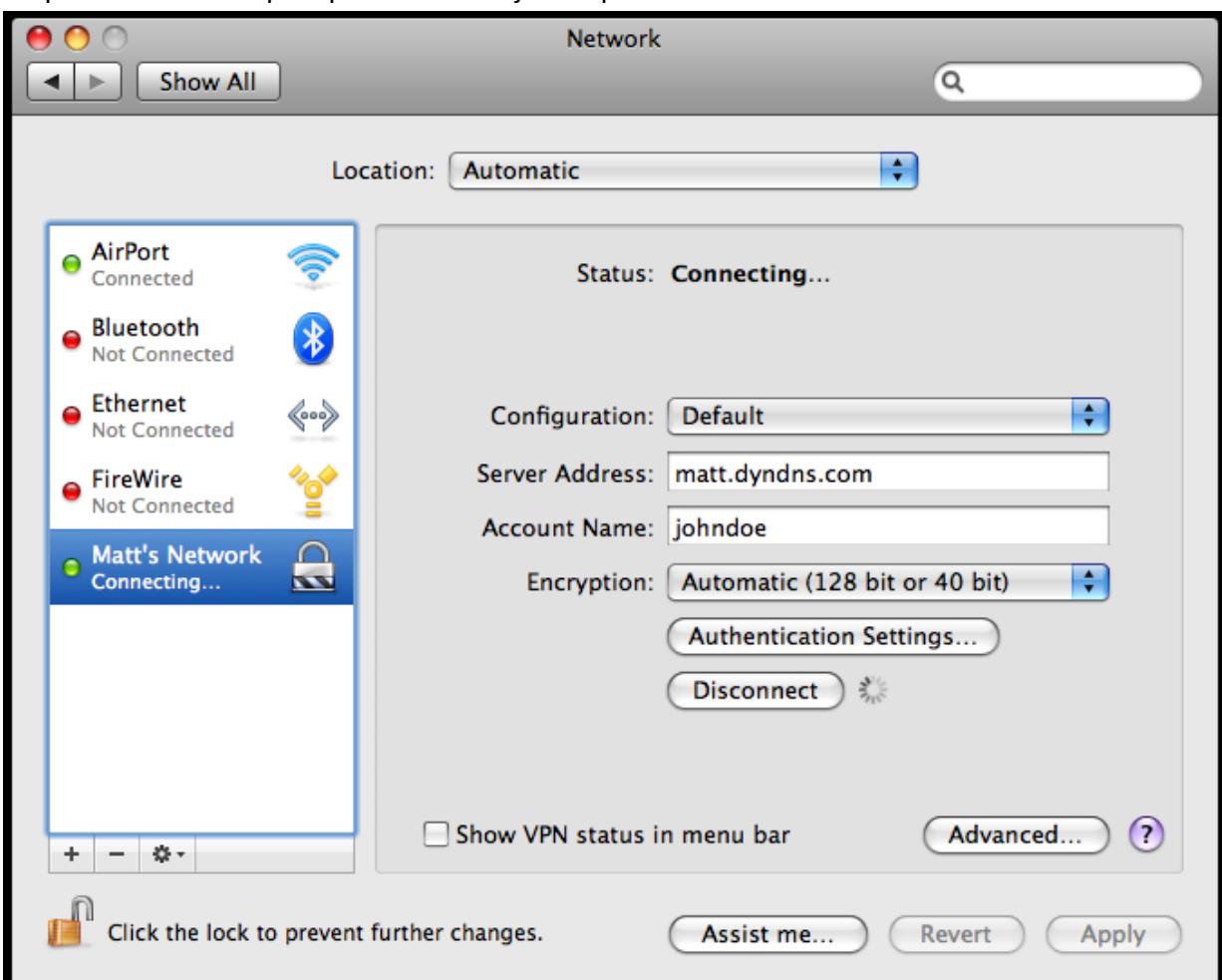
2. Clique em Network



3. Clique no botão “+” para adicionar uma nova conexão de rede
4. Selecione **VPN** em **Interface**.
5. Selecione **PPTP** em **VPN Type**.
6. Digite em **Service Name** um nome de descrição, no exemplo usamos **Matt's Network**.



7. Digite em **Server Address** o ip do servidor que você configurou o PPTP VPN. Se o IP não pode ser acessado diretamente, você terá que configurar um NAT port Forward.
8. Digite o nome de usuário cadastrado em **Account Name**.
9. Clique em **Connect** que aparecerá uma janela pedindo a senha



Veja também...

- Criando VPN em um túnel IPSec
- Configurando o serviço L2TP VPN
- Configurando o serviço OpenVPN
- Configurando o serviço PPTP VPN

5

Configurações Avançadas

Nesse capítulo, iremos abordar:

- Criando um IP Virtual
- Criando regra de NAT 1:1
- Criando uma regra de NAT outbound
- Criando Gateway
- Criando uma rota estática
- Configurando o Traffic Shaping (QoS, Qualidade do Serviço)
- Interfaces do tipo ponte
- Criando uma LAN Virtual
- Criando um Captive Portal

Introdução

A seguir vamos abordar recursos avançados de rede, que normalmente se encontram em classes empresariais. No entanto cada um desses recursos então disponíveis na ultima versão do PfSense.

Criando um IP Virtual

Aqui vamos descrever como configurar um endereço de IP virtual no PfSense.

Se preparando...

No PfSense você pode criar quatro tipos distintos de IPs virtuais:

- **Proxy ARP**
- **CARP**
- **Other**
- **AP Alias**

Um tipo comum de IP virtual é configurado como NAT 1:1, neste cenário o IP virtual do tipo **Other** é necessário, é o que vamos configurar agora:

Como fazê-lo...

1. Vá em **Firewall | Virtual IPs**
2. Clique no botão “+” e adicione um novo endereço de IP virtual.
3. Em **Type** escolha **Other**.
4. Em **Interface** escolha **WAN**
5. Em **IP address** digite o IP que você deseja virtualizar
6. Adicione uma descrição que você possa identificar posteriormente em **Description**.

Firewall: Virtual IP Address: Edit



Edit Virtual IP	
Type	<input type="radio"/> Proxy ARP <input type="radio"/> CARP <input checked="" type="radio"/> Other <input type="radio"/> IP Alias
Interface	WAN ▾
IP Address(es)	Type: Single address Address: <input type="text" value="66.77.88.99"/> / <input type="text" value="32"/>
Virtual IP Password	<input type="password"/> Enter the VHID group password.
VHID Group	<input type="text" value="1"/> Enter the VHID group that the machines will share
Advertising Frequency	<input type="text" value="0"/> The frequency that this machine will advertise. 0 = master. Anything above 0 designates a backup.
Description	<input type="text" value="My Other VIP."/> You may enter a description here for your reference (not parsed).
Save Cancel	

7. Clique em **Save**
8. Clique em **Apply Changes**

Firewall: Virtual IP Addresses



Virtual IP address	Type	Description				
66.77.88.99/32		My Other VIP.				

Note:
The virtual IP addresses defined on this page may be used in **NAT** mappings.
You can check the status of your CARP Virtual IPs and interfaces [here](#).

Como ele funciona...

O IP Virtual (vamos o chamar de VIP de agora em diante) do tipo **Other** tem as seguintes características:

- O tráfego só pode ser encaminhado para esse tipo de VIP; e o PfSense não pode usar esse tipo de VIP para os seus próprios serviços.
- O VIP pode ser usado em uma subrede diferente do que esta sendo usado pelo PfSense.
- O VIP não pode responder a pings.

Há mais...

Nós estamos configurando um VIP do tipo **Other**. Mas existem mais três tipos de endereços VIP que podem ser configurados no PfSense 2.0. Os quatro tipos de endereços VIP são semelhantes, mas mudam algumas propriedades, vamos ver a comparação:

- **CARP**
 - Pode ser usados e encaminhados pelo firewall
 - Pode usar o tráfego **Layer 2**.
 - Podem ser usados em cenários com balanceamento de carga e Fail-Over
 - Tem que estar na mesma subrede da interface
 - Ele vai responder a pings se configurado corretamente
- **Proxy ARP**
 - Só pode ser transmitida pelo firewall
 - Pode usar o tráfego **Layer 2**.
 - Pode estar em uma subrede diferente do que a interface
 - Não pode responder aos pings
- **Other**
 - Só pode ser transmitida pelo firewall
 - Pode estar em uma subrede diferente do que a interface
 - Não pode responder aos pings
- **IP Alias**
 - Novo no PfSense 2.0
 - Só pode ser usado ou encaminhado pelo firewall
 - Permite que os endereços IP sejam adicionados como IP extra na interface.

Configurando CARP como endereço VIP

1. Vá até **Firewall | Virtual IPs**
2. Clique no botão “+” para adicionar um novo endereço VIP
3. Em **Type** escolha **CARP**
4. Em **Interface** selecione **WAN**
5. Em **IP address** digite o IP que você deseja
6. Em **Virtual IP Password**, digite uma senha
7. Escolha um **VHID Group**
8. Escolha um **Advertising Frequency (0 para todos)**

9. Digite uma descrição que você possa identificar futuramente em **Description**.

Firewall: Virtual IP Address: Edit

Edit Virtual IP

Type	<input type="radio"/> Proxy ARP <input checked="" type="radio"/> CARP <input type="radio"/> Other <input type="radio"/> IP Alias
Interface	WAN ▾
IP Address(es)	Type: Single address Address: <input type="text"/> 69.116.129.1 / 32 ▾ <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	1 ▾ Enter the VHID group that the machines will share
Advertising Frequency	0 ▾ The frequency that this machine will advertise. 0 = master. Anything above 0 designates a backup.
Description	<input type="text"/> My CARP VIP. You may enter a description here for your reference (not parsed).

Save **Cancel**

10. Clique em **Save**

11. Clique em **Apply Changes**.

Firewall: Virtual IP Addresses

Virtual IPs **CARP Settings**

Virtual IP address	Type	Description				
66.77.88.99/32		My Other VIP.				
69.116.129.1/32 (vhid 1)		My CARP VIP.				

Note:
The virtual IP addresses defined on this page may be used in **NAT** mappings.
You can check the status of your CARP Virtual IPs and interfaces [here](#).

Configurando o Proxy ARP como endereço VIP

1. Vá em Firewall | Virtual IPs
2. Clique no botão “+” para adicionar um novo endereço VIP
3. Em **Type** escolha **Proxy ARP**.
4. Em **Interface** selecione **WAN**
5. Selecione **Single Address** em **Type**.
6. Em **Address** digite o IP.

7. Digite uma descrição em **Description**.

Firewall: Virtual IP Address: Edit

Edit Virtual IP

Type	<input checked="" type="radio"/> Proxy ARP <input type="radio"/> CARP <input type="radio"/> Other <input type="radio"/> IP Alias
Interface	WAN
IP Address(es)	Type: Single address Address: <input type="text"/> 55.44.33.22 / 32 <small>This is a CIDR block of proxy ARP addresses.</small>
Virtual IP Password	<input type="password"/> Enter the VHID group password.
VHID Group	<input type="text"/> 1 Enter the VHID group that the machines will share
Advertising Frequency	<input type="text"/> 0 The frequency that this machine will advertise. 0 = master. Anything above 0 designates a backup.
Description	<input type="text"/> My Proxy ARP VIP. You may enter a description here for your reference (not parsed).

Save **Cancel**

8. Clique em **Save**

9. Clique em **Apply Changes**.

Firewall: Virtual IP Addresses

Virtual IPs **CARP Settings**

Virtual IP address	Type	Description			
66.77.88.99/32	IP	My Other VIP.			
69.116.129.1/32 (vhid 1)	CARP	My CARP VIP.			
55.44.33.22/32	PARP	My Proxy ARP VIP.			

Note:
The virtual IP addresses defined on this page may be used in NAT mappings.
You can check the status of your CARP Virtual IPs and interfaces [here](#).

Configurando o IP Alias como endereço VIP

1. Vá em **Firewall | Virtual IPs**
2. Clique no botão “+” para adicionar um novo endereço VIP
3. Em **Type** escolha **IP Alias**
4. Em **Interface** escolha **WAN**.
5. Em **IP address** digite o IP

6. Digite uma descrição em **Description**.

Firewall: Virtual IP Address: Edit

Edit Virtual IP

Type	<input type="radio"/> Proxy ARP <input type="radio"/> CARP <input type="radio"/> Other <input checked="" type="radio"/> IP Alias
Interface	WAN
IP Address(es)	Type: Single address Address: <input type="text" value="22.33.44.55"/> / <input type="text" value="32"/> This must be the network's subnet mask. It does not specify a CIDR range.
Virtual IP Password	<input type="password"/> Enter the VHID group password.
VHID Group	<input type="text" value="1"/> Enter the VHID group that the machines will share
Advertising Frequency	<input type="text" value="0"/> The frequency that this machine will advertise. 0 = master. Anything above 0 designates a backup.
Description	<input type="text" value="My IP Alias VIP."/> You may enter a description here for your reference (not parsed).

Save **Cancel**

7. Clique em **Save**.

8. Clique em **Apply Changes**.

Firewall: Virtual IP Addresses

Virtual IPs **CARP Settings**

Virtual IP address	Type	Description		
66.77.88.99/32		My Other VIP.		
69.116.129.1/32 (vhid 1)		My CARP VIP.		
55.44.33.22/32		My Proxy ARP VIP.		
22.33.44.55/32		My IP Alias VIP.		

Note:
The virtual IP addresses defined on this page may be used in NAT mappings.
You can check the status of your CARP Virtual IPs and interfaces [here](#).

Veja também...

- Criando regra de NAT 1:1
- Criando uma regra de NAT outbound
- Criando uma rota estática
- Criando uma LAN Virtual

Configurando regra de NAT 1:1

Aqui vamos descrever como configurar uma regra de NAT 1:1. A regra NAT 1:1 é usada quando você quiser associar um endereço de IP público com uma máquina da rede interna. Tudo que for destinado ao IP público vai ser encaminhado para máquina da rede interna.

Como fazê-lo...

1. Vá até **Firewall | Virtual IP**
2. Na aba **Virtual IPs**, clique no botão “+” para adicionar um novo VIP.
3. Em **Type** selecione **Proxy ARP**.
4. Em **Interface** selecione **WAN**
5. Na opção **IP address**, em **Type** selecione **Single Address**, e em **Address** digite o ip externo que você deseja associar a uma máquina da rede interna.
6. Adicione uma descrição que você possa reconhecer mais tarde em **Description**, no exemplo nos usamos **My public IP address**.

Firewall: Virtual IP Addresses



The screenshot shows the 'Virtual IPs' tab selected in the Firewall interface. A single entry is listed:

Virtual IP address	Type	Description
92.44.66.77/32	Proxy ARP	My public IP address.

Note:
The virtual IP addresses defined on this page may be used in NAT mappings.
You can check the status of your CARP Virtual IPs and interfaces [here](#).

7. Clique em **Save**.
8. Clique em **Apply Changes**.
9. Vá em **Firewall | NAT**.
10. Selecione a aba **1:1**
11. Clique no botão “+” para adicionar uma regra de NAT 1:1
12. Em **Interface** selecione **WAN**
13. Em **Source** selecione **any**
14. Em **Destination**, especifique o computador interno, no caso vamos usar o Alias.
15. Digite em **External Subnet** o seu ip público
16. Em **Description**, adicione uma descrição que você possa reconhecer posteriormente, no exemplo usamos **Forward all external requests to Webserver1**.
17. Em **NAT Preflection** deixe **Disabled**.

Firewall: NAT: 1:1: Edit

?

Edit NAT 1:1 entry	
Disabled	<input type="checkbox"/> Disable this rule Set this option to disable this rule without removing it from the list.
Interface	WAN <input type="button" value="▼"/> Choose which interface this rule applies to. Hint: in most cases, you'll want to use WAN here.
Source	<input type="checkbox"/> not Use this option to invert the sense of the match. Type: any <input type="button" value="▼"/> Address: <input type="text"/> / <input type="text" value="31"/> Enter the internal (LAN) subnet for the 1:1 mapping. The subnet size specified for the external subnet also applies to the internal subnet (they have to be the same).
Destination	<input type="checkbox"/> not Use this option to invert the sense of the match. Type: Single host or alias <input type="button" value="▼"/> Address: Webserver1 <input type="button" value="▼"/>
External subnet	92.44.66.77
Description	 Forward all external requests to Webserver1. You may enter a description here for your reference (not parsed).
NAT reflection	disable <input type="button" value="▼"/>

Save **Cancel**

18. Clique em **Save**.

19. Clique em **Apply Changes**.

Como ele funciona...

Uma vez que é feita uma relação de NAT 1:1 estabelecida, todo o tráfego será encaminhado para o endereço de IP internou ou subrede, como se a máquina interna fosse diretamente configurado com o IP público. Isso é muito mais fácil do que criar uma regra de Port Forward se todo o tráfego de entrada e saída tiver destinado a máquina.

Há mais...

Como muitos recursos avançados de rede, o relacionamento bem sucedido do NAT 1:1 requer o uso de VIPs.

Veja também...

- Criando um IP Virtual

Criando uma regra de NAT outbound

Aqui vamos descrever como criar uma regra de NAT outbound

Se preparando...

Uma regra de NAT outbound define como traduzir o que um tráfego de rede esta deixando. Isso pode parecer um conceito difícil de entender na primeira vez, porque a maioria dos cenários de rede em geral só então preocupados em saber o local de onde os pacotes estão vindos, e não se preocupam em saber como eles saem.

Vamos descrever agora como usar uma regra de NAT outbound para resolver um cenário comum que envolve o nateamento para uma maquina com varias interfaces. Vamos supor que temos um único servidor de destino com duas interfaces, LAN e DMZ, e o firewall PfSense protege essas duas interfaces. Usando a velha regra de Port Forward, encaminhando solicitações HTTP para o servidor em sua interface DMZ, o que é bom. No entanto, quando tentamos encaminhar solicitações SSH para a interface LAN do servidor, o tráfego chega corretamente, mas tenta responder através da rede DMZ. Isso não é reconhecido como valido pelo firewall e fica dando tempo perdido quando se tenta conectar.

A solução e lhe dar com os pedidos SSH usando uma regra de NAT outbound junto com uma regra de NAT 1:1, como vamos descrever.

Como fazê-lo...

1. Vá a **Firewall | Virtual IPs**
2. Na aba **Virtual IPs**, clique no botão “+” para adicionar um novo VIP.
3. Em **Type** selecione **Proxy ARP**
4. Em **Interface** selecione **WAN**
5. Na opção **IP address**, em **Type** selecione **Single Address**, e em **Address** digite o ip externo que você deseja associar a uma maquina da rede interna.
6. Adicione uma descrição que você possa reconhecer mais tarde em **Description**, no exemplo nos usamos **My public IP address**.
7. Clique em **Save**
8. Clique em **Apply Changes**

Firewall: Virtual IP Addresses

?

Virtual IP address	Type	Description
92.44.66.77/32	CARP	My public IP address.

Note:
The virtual IP addresses defined on this page may be used in NAT mappings.
You can check the status of your CARP Virtual IPs and interfaces [here](#).

9. Vá até **Firewall | NAT**
10. Clique na aba **Outbound**
11. Selecione o modo **Automatic outbound NAT rule generation (IPsec passthrough included)**.
12. Clique no botão “+” para adicionar um novo mapeamento de NAT outbound.
13. Escolha **Interface** que a maquina vai responder, no caso é a LAN.
14. Em **Source** especifique **any**
15. Em **Destination** ponha o endereço do servidor que ira responder.
16. Deixe o **Translation** para tratar da **Interface Address** e especificar a porta **22** para responder os pedidos de SSH.
17. Escreva em **Description** a descrição para você identificar futuramente, no exemplo usamos **Outbound NAT for WAN Clients to Server1 SSH**.
18. Clique em **Save**.
19. Clique em **Apply Changes**.

Firewall: NAT: Outbound

?

Mode: **Automatic outbound NAT rule generation (IPsec passthrough included)** **Manual Outbound NAT rule generation (AON - Advanced Outbound NAT)** **Save**

Mappings:

Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description
LAN	any	*	192.168.1.200/32	*	*	22	NO	Outbound NAT for WAN Clients to Server1 SSH

Note:
If advanced outbound NAT is enabled, no outbound NAT rules will be automatically generated any longer. Instead, only the mappings you specify below will be used. With advanced outbound NAT disabled, a mapping is automatically created for each interface's subnet (except WAN). If you use target addresses other than the WAN interface's IP address, then depending on the way your WAN connection is setup, you may also need a [Virtual IP](#).

20. Vá até **Firewall | NAT**
21. Clique na aba **1:1**
22. Clique no botão “+” para adicionar um mapeamento NAT 1:1
23. Em **Interface** escolha **WAN**.
24. Em **Source** escolha **any**.
25. Especifique em **Destination**, **Single Host** ou **Alias**, e fornecer o endereço IP do servidor que esta recebendo as solicitações.
26. Especifique o VIP que criamos anteriormente em **External subnet**.
27. Em **Description** digite uma descrição que possa reconhecer no futuro, no exemplo colocamos **1:1 NAT Public IP to Server1**.
28. Clique em **Save**
29. Clique em **Apply Changes**.

Firewall: NAT: 1:1

?

Interface	External IP	Source IP	Destination IP	Description
WAN	92.44.66.77	*	192.168.1.200	1:1 NAT Public IP to Server1

Note:
Depending on the way your WAN connection is setup, you may also need a Virtual IP.
If you add a 1:1 NAT entry for any of the interface IPs on this system, it will make this system inaccessible on that IP address. i.e. if you use your WAN IP address, any services on this system (IPsec, OpenVPN server, etc.) using the WAN IP address will no longer function.

30. Vá a **Firewall | Rules**
31. Clique na aba **WAN**.
32. Clique no botão “+” para adicionar uma nora regra de firewall.
33. Em **Source** escolha **any**
34. Em **Source port range** escolha **any**.
35. Em **Destination** selecione ou **Singles host** ou **Alias** especificando o endereço de IP do servidor que está lidando com as solicitações.
36. Em **Destination port range** selecione **SSH**.
37. Em **Description** digite uma descrição qualquer que você possa reconhecer mais tarde, no exemplo usamos **Allow WAN Clients to Server1 SSH**.
38. Clique em **Save**.
39. Clique em **Apply Changes**.

Firewall: Rules

S L ?

Floating WAN LAN DMZ

ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
X	*	RFC 1918 networks	*	*	*	*	*		Block private networks
X	*	Reserved/not assigned by IANA	*	*	*	*	*	*	Block bogon networks
▶	TCP	*	*	192.168.1.200	22 (SSH)	*	none		Allow WAN Clients to Server1 SSH

Actions:

Legend: pass block reject log
 pass (disabled) block (disabled) reject (disabled) log (disabled)

Hint:
Rules are evaluated on a first-match basis (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you'll have to pay attention to the rule order. Everything that isn't explicitly passed is blocked by default.
You may drag and drop rules using your mouse to reorder the rule ordering.

Como ele funciona...

A regra de outbound que criamos avisa ao PfSense para direcionar o tráfego de saída através da interface LAN, independentemente de qual interface ela entrou. Isso vai permitir que o tráfego SSH encontrasse o caminho de casa mesmo se o gateway padrão do servidor estiver em contra interface, no caso (DMZ). Enquanto isso as solicitações HTTP que foram configuradas através do Port Forwarding continuam funcionando perfeitamente.

Veja também...

- Criando um IP Virtual
- Criando regra de NAT 1:1
- Criação de regras em Nat port Forward

Criando um Gateway

Aqui vamos descrever como criar um gateway no PfSense.

Se preparando...

Em geral, as redes com uma única ligação WAN, não é necessário mudar as configurações de gateway; o padrão criado pelo próprio PfSense automaticamente já é o suficiente. No entanto, as redes que possuem

mais de uma conexão de internet ou tira proveito de algumas funcionalidades avançadas (por exemplo, rotas estáticas) terá que definir um gateway personalizado.

Como fazê-lo...

1. Vá a **System | Routing**
2. Clique na aba **Gateways**
3. Clique no botão “+” para adicionar um novo gateway
4. Selecione a **Interface** do novo gateway
5. Em **Name** você vai especificar um nome para esse gateway (não pode ser espaço)
6. Em **Gateway** especifique o IP do gateway, esse IP tem que ser reconhecido pela interface que você escolheu na etapa 4.
7. Em **Monitor IP** você pode atribuir um IP alternativo ou deixar em branco mesmo, fazendo isso o sistema irá colocar o mesmo IP do gateway como monitor IP.
8. Em **Description** você vai colocar uma descrição para identificar qual gateway você criou, no exemplo usamos **My New Gateway**.

System: Gateways: Edit gateway

S ?

Edit gateway	
Interface	<input type="button" value="DMZ"/> Choose which interface this gateway applies to.
Name	<input type="text" value="MyNewGateway"/> <small>Gateway name</small>
Gateway	<input type="text" value="192.168.2.100"/> <small>Gateway IP address</small>
Default Gateway	<input type="checkbox"/> Default Gateway This will select the above gateway as the default gateway
Monitor IP	<input type="text" value="192.168.2.100"/> Alternative monitor IP Enter an alternative address here to be used to monitor the link. This is used for the quality RRD graphs as well as the load balancer entries. Use this if the gateway does not respond to ICMP echo requests (pings).
Advanced	<input type="button" value="Advanced"/> - Show advanced option
Description	<input type="text" value="My new gateway."/> You may enter a description here for your reference (not parsed).

Save

Cancel

9. Clique em **Save**.
10. Clique em **Apply Changes**.

System: Gateways

S ?

Name	Interface	Gateway	Monitor IP	Description
GW_WAN (default)	WAN	dynamic	dynamic	Interface wan Dynamic Gateway
MyNewGateway	DMZ	192.168.2.100	192.168.2.100	My new gateway.

Como ele funciona...

Um gateway é um “portal” que liga duas redes. O gateway eh o que gera tráfego entre a LAN e a internet. Se tivermos varias conexões WAN (ou seja, múltiplas conexões para internet) seria necessário definir um gateway para cada um.

Há mais...

Vamos ver agora como criar gateways para fazer rotas estáticas. Uma rota estática é um caminho feito de uma rede para outra, o todo o tráfego entre essas duas redes devem passar por um gateway.

Grupos de Gateway

O PfSense 2.0 implemente um novo conceito chamado Grupos de Gateway. O grupo de gateway é uma junção de vários gateways que podem ser tratados como uma unidade a partir de varias outras funcionalidades no sistema.

Grupos de gateway ira aparecer na porta de entrada em um menu drop-down, como em uma definição de regra de firewall.

Veja também...

- Criando regras de firewall, capítulo 3 – Configurações Gerais
- Configurando interface WAN, capítulo 1 – Configurações Iniciais
- Criando rotas estáticas

Criando rotas estáticas

Aqui vamos descrever como criar uma rota estática no PfSense.

Se preparando...

As rotas estáticas servem para acessar redes que não são acessíveis através do gateway padrão WAN, mas pode ser alcançado indiretamente através de uma interface diferente. Um exemplo comum pode ser usado em uma grande empresa com vários escritórios que usam uma impressora compartilhada, é só preciso

criar uma rota estática. Podemos usar o PfSense para criar essa rota estática para uma rede interna, em vez de configurar uma rota estática em cada pc.

Como fazê-lo...

1. Vá até **System | Routing**.
2. Clique na aba **Gateways**
3. Clique no botão “+” para adicionar um novo gateway
4. Selecione em **Interface** onde vai ficar o novo gateway
5. Digite em **Name** o nome do seu gateway (não pode ter espaço)
6. Digite em **IP Address** o IP do gateway, esse IP tem que ser reconhecido pela interface selecionada anteriormente.
7. Em **Monitor IP** você pode atribuir um IP alternativo ou deixar em branco mesmo, fazendo isso o sistema irá colocar o mesmo IP do gateway como monitor IP.
8. Em **Description** você vai colocar uma descrição para identificar qual gateway você criou, no exemplo usamos **My New Gateway**.
9. Clique em **Save**
10. Clique em **Apply Changes**

System: Gateways

S ?

Gateways	Routes	Groups		
Name	Interface	Gateway	Monitor IP	Description
GW_WAN (default)	WAN	dynamic	dynamic	Interface wan Dynamic Gateway
MyNewGateway	DMZ	192.168.2.100	192.168.2.100	My new gateway.

11. Vá em **System | Routing**
12. Clique na aba **Routes**
13. Clique no botão “+” para adicionar uma nova rota
14. Em **Destination network** digite o endereço de IP da rede de destino
15. Em **Gateway** escolha o que criamos a cima.
16. Em **Description** escreva algo para descrever a regra, no exemplo usamos **Static route for shared printer network**.

System: Static Routes: Edit route

?

Edit route entry

Destination network	<input type="text" value="192.168.2.0"/> / <input type="text" value="24"/> <input type="button" value="▼"/>
Destination network for this static route	
Gateway	<input type="text" value="MyNewGateway - 192.168.2.100"/> <input type="button" value="▼"/>
Choose which gateway this route applies to or add a new one.	
Description	<input type="text" value="Static route for shared printer network."/> You may enter a description here for your reference (not parsed).

17. Clique em Save.

18. Clique em Apply Changes.

System: Static Routes

S ?

Gateways Routes Groups

Network	Gateway	Interface	Description
192.168.2.0/24	MyNewGateway - 192.168.2.100	DMZ	Static route for shared printer network.

Note: Do not enter static routes for networks assigned on any interface of this firewall. Static routes are only used for networks reachable via a different router, and not reachable via your default gateway.

Como ele funciona...

Ao definir uma rota estática, temos um caminho traçado para nossa rede de impressora compartilhada. Nós podemos acessar agora esta rede através da rota estática criada, e oferecer uma porta de entrada para outros usuários do firewall.

Veja também...

➤ Criando Gateway

Configurando o Traffic Shaping (QoS, Qualidade do Serviço)

Aqui vamos descrever como configurar o controle de banda no PfSense

Se preparando...

O Traffic Shaping, também conhecido como QoS, é a priorização e otimização de pacotes de rede. Priorizando os pacotes de rede de certos tipos de tráfego em relação a outros. Limita o pacote de rede fixando

certos limites de velocidade de certos tipos de tráfego para certos momentos. Um administrador pode querer priorizar os pacotes de VoIP sobre todos os outros para garantir que chamadas telefônicas não vão ser descartadas ou interrompidas devido ao alto tráfego de rede. Além disso, podemos também limitar o rendimento do VoIP para 100kbps. Esse é um exemplo tipo de ambiente que roda VoIP.

A seguir vamos usar o PfSense para moldar os acessos externos usando o Desktop Remoto do próprio Windows (MSRDP) que entram em nossa rede. Assim podemos nos assegurar que podemos administrar nossos servidores remotamente mesmo se o tráfego de rede estiver muito alto.

Como fazê-lo...

1. Vá a **Firewall | Traffic Shaper**
2. Clique na aba **Wizards**
3. Na coluna **Wizard functions**, clique no link referente a **Single WAN multi LAN**.

Firewall: Traffic Shaper: Wizards

S ?

Wizard function	Wizard Link
Single Lan multi Wan	traffic_shaper_wizard.xml
Single Wan multi Lan	traffic_shaper_wizard_multi_lan.xml
Multiple Lan/Wan	traffic_shaper_wizard_multi_all.xml
Dedicated Links	traffic_shaper_wizard_dedicated.xml

4. Em **Enter number of LAN type connections** digite o numero de Lans, no nosso caso tem LAN e DMZ, então colocamos numero **2**.

This wizard will guide you through setting up the pfSense traffic shaper for the situation where you have 1 WAN connection and multiple LAN connections. Please be aware that Custom Bandwidths should not exceed 30% of the Interface/link bandwidth. Keep this in mind during the wizard.

Enter number of LAN type connections:	<input type="text" value="2"/> 2 Number of local(LAN) interfaces you have
<input type="button" value="Next"/>	

5. Em **Link Upload** digite a velocidade que o seu provedor de internet forneceu para upload, no exemplo usamos 2.000Kbps (2Mbps), se você tiver duvida faça um teste em sites de velocidade, como por exemplo: <http://speedtest.net/>
6. Em **Link Download** digite a velocidade que o seu provedor de internet forneceu para download, no exemplo usamos 15.000Kbps (15Mbps), se você tiver duvida faça um teste em sites de velocidade, como por exemplo: <http://speedtest.net/>

pfSense Traffic Shaper Wizard

Setup WAN(upload) scheduler

Upload Scheduler: Queueing discipline to apply on the upload of this link.

Setup link speed details

Link Upload: Kbit/s Upload bandwidth on this connection.

Link Download: Kbit/s Download bandwidth on this connection.

Setup connection speed and scheduler information for LAN interface #1

LAN interface: Interface of this connection.

LAN Scheduler: Queueing discipline to apply on the upload of this connection.

Setup connection speed and scheduler information for LAN interface #2

LAN interface: Interface of this connection.

LAN Scheduler: Queueing discipline to apply on the upload of this connection.

7. A pagina seguinte é usada especificamente para configurar a priorização de tráfego de VoIP, você pode pular essa etapa clicando em **Next**.

pfSense Traffic Shaper Wizard

Enable: This will raise the priority of VOIP traffic above all other traffic. Prioritize Voice over IP traffic

VOIP specific settings

Provider: Choose Generic if your provider isn't listed.

Address: (Optional) If this is chosen, the provider field will be overridden. This allows you to just provide the IP address of the VOIP adaptor to prioritize. NOTE: You can also use a Firewall Alias in this location.

Download Speed: % The limit you want to apply.

Upload Speed: % The limit you want to apply.

8. Na próxima pagina se chama **PenaltyBox**, nos permite limitar a velocidade de um determinado endereço de IP ou Alias. Isso é muito útil, mas não vamos ter a necessidade de usar essa função no momento, você pode ignorar clica em **Next**.

pfSense Traffic Shaper Wizard

Enable: This will lower the priority of traffic from this IP or alias. Penalize IP or Alias

Next

PenaltyBox specific settings

Address: [REDACTED] This allows you to just provide the IP address of the computer(s) to penalize. NOTE: You can also use a Firewall Alias in this location.

Bandwidth: % The limit you want to apply.

Next

9. Essa próxima pagina se chama **Peer to Peer (P2P) Networking**, você pode diminuir a prioridade de tráfego P2P, nessa pagina a cerca de 20 opções de rede P2P mais populares para ser limitado o tráfego. Como não nos interessa essa parte no momento então clique em **Next**.

pfSense Traffic Shaper Wizard

Enable: This will lower the priority of P2P traffic below all other traffic. Please check the items that you would like to prioritize lower than normal traffic. Lower priority of Peer-to-Peer traffic

Next

p2p Catch all

p2pCatchAll: When enabled, all uncategorized traffic is fed to the p2p queue.

Bandwidth: % The limit you want to apply.

Enable/Disable specific P2P protocols

Aimster: Aimster and other P2P using the Aimster protocol and ports

BitTorrent: BitTorrent and other P2P using the Torrent protocol and ports

RuddyShare: RuddyShare and other P2P using the RuddyShare protocol and ports

10. Nessa próxima pagina **Network Games**, você pode configurar o tráfego de rede liberada aos jogos online, nessa pagina a cerca de 20 jogos mais populares online para ser priorizado. Como não nos interessa essa parte no momento então clique em **Next**.

pfSense Traffic Shaper Wizard

Enable: This will raise the priority of gaming traffic to higher than most traffic. Prioritize network gaming traffic

Next

Enable/Disable specific games

BattleNET:	<input type="checkbox"/> Battle.net - Virtually every game from Blizzard publishing should match this. This includes the following game series: Starcraft, Diablo, Warcraft. Guild Wars also uses this port.
Battlefield2:	<input type="checkbox"/> Battlefield 2 - this game uses a LARGE port range, be aware that you may need to manually rearrange the resulting rules to correctly prioritize other traffic.
CallOfDuty:	<input type="checkbox"/> Call Of Duty (United Offensive)
Counterstrike:	<input type="checkbox"/> Counterstrike_The ultimate 1st person shooter

11. Na página final **Other Applications**, nos permite mordar outros tipos comuns de tráfego. Vamos ter que clicar na opção **Enable**, para permitir o uso dessa aplicação, em **MSRDP** vamos selecionar **Higher priority**, os outros vamos deixar como **Default**, e clique em **Next**.

pfSense Traffic Shaper Wizard

Enable: This will help raise or lower the priority of other protocols higher than most traffic. Other networking protocols

Next

Remote Service / Terminal emulation

MSRDP:	Higher priority ▾ Microsoft Remote Desktop Protocol
VNC:	Default priority ▾ Virtual Network Computing
AppleRemoteDesktop:	Default priority ▾ Apple Remote Desktop
PCAnywhere:	Default priority ▾ Symantec PC Anywhere

Messengers

IRC:	Default priority ▾ Internet Relay Chat
Jabber:	Default priority ▾ Jabber instant messenger

12. Clique em **Finish** para aplicar a nova configuração.

After pressing Finish the system will load the new profile.

Please note that this may take a moment.

**Also note that the traffic shaper is stateful meaning that only new connections will be shaped.
If this is an issue please reset the state table after loading the profile.**

pfSense Traffic Shaper Wizard

Finish

Como ele funciona...

Usando o Wizard do Traffic Shaping, nós definimos um conjunto de regras que prioriza o tráfego do MSRDP acima de qualquer outro. Mesmo que a rede esteja com tráfego pesado, seja com uso da web, VoIP ou quantos mais tiver, nossa conexão MSRDP sempre ficará estável e interrupta, já que foi priorizado.

Interfaces do tipo ponte (bridge)

Aqui vamos descrever como fazer uma ponte juntando duas interfaces no PfSense. Pontes permitem unir duas redes. Por exemplo, o administrador pode fazer uma ponte de rede entre uma rede com fio e uma rede sem fio.

Como fazê-lo...

1. Vá a **Interfaces | (assign)**
2. Clique na aba **Bridge**
3. Clique no botão “+” para adicionar uma nova ponte
4. Em **Member Interfaces**, selecione as interfaces com o Ctrl pressionado.
5. Em **Description** você vai digitar uma identificação que possa reconhecer posteriormente, no exemplo nos usamos **LAN DMZ Bridge**.

Firewall: Bridge: Edit

?

Bridge configuration

Member interfaces	WAN LAN DMZ
Interfaces participating in the bridge.	
Description	LAN DMZ Bridge
<input type="button" value="Show advanced options"/>	
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

6. Clique em **Save**

Interfaces: Bridge

?

Interface	Members	Description
BRIDGE0	LAN, DMZ	LAN DMZ Bridge

Note:
Here you can configure bridging of interfaces.

Como ele funciona...

A ponte combina duas interfaces no firewall em uma rede única de **Layer-2**. A LAN e DMZ estão agora ligados.

Há mais...

Clique em **Show advanced options**, para configurar qualquer uma dessas seguintes opções:

- RSTP/STP: Abilite para abrir a arvore de opções:
 - Protocol
 - STP Interfaces
 - Valid time
 - Forward time
 - Hello time
 - Priority
 - Hold count
 - Interface priority
 - Path cost
- Cache size
- Cache entry expire time
- Span port
- Edge ports
- Auto Edge ports
- PTP ports
- Auto PTP ports
- Sticky ports
- Private ports

Veja também...

- Identificando e atribuindo interfaces, capítulo 1 – Configuração Inicial.

Criando LAN Virtual

Aqui vamos descrever como criar uma LAN Virtual no PfSense.

Se preparando...

A VLAN permite q um único interruptor físico possa hospedar varias camadas de rede, separando as portas com tags VLAN. A tag de VLAN define uma rede virtual separada. O PfSense pode anexar em cada VLAN, definindo tags nas interfaces do firewall.

Como fazê-lo...

1. Vá até **Interface | (assign)**
2. Clique na aba **VLANs**
3. Clique no botão “+” para adicionar uma nova VLAN
4. Na opção **Parent Interface**. Se refere a uma atribuição de uma interface de referencia (observe na figura a baixo). Neste caso a **DMZ** foi atribuída como **vr2** então vamos selecionar ela.

Interfaces: Assign network ports

S ?

Interface	Network port
WAN	vr1 (00:0d:b9:1e:f6:9d) ▾
LAN	vr0 (00:0d:b9:1e:f6:9c) ▾
DMZ	vr2 (00:0d:b9:1e:f6:9e) ▾

Interfaces that are configured as members of a lagg(4) interface will not be shown.

5. Na opção **VLAN tag**, ponha um valor entre 1-4094
6. Em **Description**, ponha um nome para referencia nos usamos **My DMZ virtual LAN**.

Firewall: VLAN: Edit

?

VLAN configuration	
Parent Interface	vr2 (00:0d:b9:1e:f6:9e) ▾ Only VLAN capable interfaces will be shown.
VLAN tag	99 802.1Q VLAN tag (between 1 and 4094)
Description	My DMZ virtual LAN. You may enter a description here for your reference (not parsed).

Save **Cancel**

7. Clique em **Save**.

Interfaces: VLAN

?

The screenshot shows a table with three columns: Interface, VLAN tag, and Description. The first row contains 'vr2' in the Interface column, '99' in the VLAN tag column, and 'My DMZ virtual LAN.' in the Description column. To the right of the table are three icons: a pencil for edit, a delete 'x', and a plus sign for add.

Interface	VLAN tag	Description
vr2	99	My DMZ virtual LAN.

Note:
Not all drivers/NICs support 802.1Q VLAN tagging properly. On cards that do not explicitly support it, VLAN tagging will still work, but the reduced MTU may cause problems. See the pfSense handbook for information on supported cards.

Como ele funciona...

Todos os pacotes destinados ou originados de VLAN serão marcados com a tag VLAN. É assim que o PfSense diferencia ele dos outros tráfegos, garantindo que esse tráfego vá para o lugar certo.

Veja também...

- Identificando e atribuindo interfaces, capítulo 1 – Configuração Inicial.

Criando um Captive Portal

Aqui vamos descrever como criar um Captive Portal no PfSense.

Se preparando...

O **Captive Portal** é uma página web que é exibida ao usuário antes de navegar na web. Isso geralmente é visto em ambientes comerciais como Wi-Fi Hotspot onde você deve pagar pelo serviço antes de navegar na web. Em outros cenários o **Captive Portal** é usado para autenticação do usuário.

Nessa explicação vamos configurar o PfSense para mostrar um **Captive Portal** de autenticação antes que o usuário navegue na web pela DMZ.

Como fazê-lo...

1. Vá a **Services | Captive Portal**
2. Na aba **Captive Portal**, clique em **Enable Captive Portal**.
3. Em **Interface** escolha a interface que deseja usar o serviço , no nosso exemplo vamos usar o DMZ.
4. Em **Idle timeout**, nós selecionamos **10** minutos, clientes que passarem mais tempo sem atividade no computador, assim que ele acessar de novo vai pedir o usuário e senha.
5. Em **Hard timeout**, nós usamos **60** minutos, clientes que estão navegando ou não no computador depois de 60 minutos vai aparecer uma tela de usuário e senha para ser digitado, você pode deixar em branco para desabilitar essa opção.
6. Clique em **Enable logout popup window**, para q os usuários possam deslogar quando terminar.
7. Em **Redirection URL**, você pode fazer com que o cliente assim que se logar seja direcionado a uma página que você escolher, no exemplo nos usamos <http://www.google.com>

Services: Captive portal

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

Enable captive portal

Interfaces



Select the interface(s) to enable for captive portal.

Maximum concurrent connections per client IP address (0 = no limit)
This setting limits the number of concurrent connections to the captive portal HTTP(S) server. This does not set how many users can be logged in to the captive portal, but rather how many users can load the portal page or authenticate at the same time! Default is 4 connections per client IP address, with a total maximum of 16 connections.

Idle timeout minutes
Clients will be disconnected after this amount of inactivity. They may log in again immediately, though. Leave this field blank for no idle timeout.

Hard timeout minutes
Clients will be disconnected after this amount of time, regardless of activity. They may log in again immediately, though. Leave this field blank for no hard timeout (not recommended unless an idle timeout is set).

Logout popup window **Enable logout popup window**
If enabled, a popup window will appear when clients are allowed through the captive portal. This allows clients to explicitly disconnect themselves before the idle or hard timeout occurs.

Redirection URL
If you provide a URL here, clients will be redirected to that URL instead of the one they initially tried to access after they've authenticated.

8. Em **Authentication**, escolha **Local User Manager**.



9. Clique em **Save**.

10. Vá até **System | User Manager**

11. Clique na aba **User**

12. Clique na aba “+” para adicionar um novo usuário

13. Em **Username** digite o nome de usuário

14. Em **Password** digite uma senha desejada duas vezes.

15. Em **Full Name** ponha o nome completo do usuário

System: User Manager

?

Users Groups Settings Servers

Defined by	USER
Disabled	<input type="checkbox"/>
Username	User1
Password	<input type="password"/> <input type="password"/>
	(confirmation)
Full name	Captive portal user1 User's full name, for your own information only
Expiration date	 Leave blank if the account shouldn't expire, otherwise enter the expiration date in the following format: mm/dd/yyyy

16. Clique em **Save**

System: User Manager

?

Users Groups Settings Servers

Username	Full name	Disabled	Groups	
admin	System Administrator	<input type="checkbox"/>	admins	
User1	Captive portal user1	<input type="checkbox"/>		

Additional webConfigurator users can be added here. User permissions can be assigned directly or inherited from group memberships. An icon that appears grey indicates that it is a system defined object. Some system object properties can be modified but they cannot be deleted.

Como ele funciona...

Através de uma criação do **Captive Portal** na DMZ, todo usuário que tentar navegar na web terá que primeiro se autenticar como na imagem abaixo. Uma vez autenticado, ele será direcionado para pagina do Google, onde pode navegar na web obedecendo as regras de tempo predefinidas, onde terão que se autenticar novamente.

pfSense captive portal

Welcome to the pfSense Captive Portal! This is the default page since a custom page has not been defined.

Username:

Password:

Há mais...

Todas as três paginas do **Captive Portal** (login, logout e erro) podem ser personalizadas para atender o padrão da organização onde foi implementado o sistema. A maneira mais fácil de ser feito isso é salvando cada pagina como um arquivo edita-lo a sua maneira (sem mudar onde o usuário vai colocar suas credenciais), e depois envia-lo usando as opções na parte inferior da pagina do serviço Captive Portal.

Portal page contents	<input type="text"/> Browse...
<p>Upload an HTML/PHP file for the portal page here (leave blank to keep the current one). Make sure to include a form (POST to "") with a submit button (name="accept") and a hidden field with name="redirurl" and value"". Include the "auth_user" and "auth_pass" and/or "auth_voucher" input fields if authentication is enabled, otherwise it will always fail. Example code for the form:</p> <pre><form method="post" action="\$PORTAL_ACTIONS\$> <input name="auth_user" type="text"> <input name="auth_pass" type="password"> <input name="auth_voucher" type="text"> <input name="redirurl" type="hidden" value="\$PORTAL_REDIRURL\$"> <input name="accept" type="submit" value="Continue"> </form></pre>	
Authentication error page contents	<input type="text"/> Browse...
<p>The contents of the HTML/PHP file that you upload here are displayed when an authentication error occurs. You may include "\$PORTAL_MESSAGE\$", which will be replaced by the error or reply messages from the RADIUS server, if any.</p>	
Logout page contents	<input type="text"/> Browse...
<p>The contents of the HTML/PHP file that you upload here are displayed on authentication success when the logout popup is enabled.</p>	
Save	
<p>Note: Changing any settings on this page will disconnect all clients! Don't forget to enable the DHCP server on your captive portal interface! Make sure that the default/maximum DHCP lease time is higher than the timeout entered on this page. Also, the DNS forwarder needs to be enabled for DNS lookups by unauthenticated clients to work.</p>	

6

Redundância, Balanceamento de carga, e Failover

Nesse capítulo, iremos abordar:

- Configurando múltiplas interfaces WAN
- Configurando o balanceamento de carga em uma multi-WAN
- Configurando o Failover em uma multi-WAN
- Configurando um servidor de web com balanceamento de carga
- Configurando um servidor web com Failover
- Configurando um firewall CARP com Failover

Introdução

Redundância, balanceamento de carga e Failover são alguns dos mais avançados recursos de rede usados no momento. Alguns desses serviços são necessários em empresas de grande porte, alguns firewalls e roteadores não são capazes de fazer isso. É claro que o PfSense suporta todos eles.

Redundância de varias interfaces WAN (multi-WAN) fornece um firewall único para varias conexões de internet. O PfSense pode ser configurado para equilíbrio de carga ou Failover de interface multi-WAN. Balanceamento de carga vai dividir o tráfego entre as interfaces de internet, quanto o Failover faz com que se uma interface caia a outra assume 100% do tráfego, não fazendo a internet da rede parar.

O balanceamento de carga do PfSense permite tipos de tráfego específicos (como tráfego na web) serem distribuídos entre os servidores. A capacidade de criar sua própria webfarm é feito direto no PfSense!

Redundância de firewall permite que o sistema sobreviva se a maquina do firewall PfSense venha a ser desligada. Para isso usamos uma configuração CARP, o PfSense pode configurar um Failover para passar o acesso automaticamente para um firewall de backup.

Configurando múltiplas interfaces WAN

Aqui vamos descrever como configurar múltiplas interfaces WAN no PfSense.

Se preparando...

Um sistema de PfSense com uma única interface WAN é quase plug-and-play desde um gateway até um DNS padrão. No entanto algumas descrições nesse capítulo requer múltiplas conexões de WANs e os gateways devem ser configurados manualmente. As descrições a seguir vão ver como configurar duas interfaces WAN que podem ser usadas mais tarde como balanceamento de carga redundante e Failover.

As seguintes interfaces não se configuradas com endereços de IPs privados para fins de exemplo, mas uma configuração real exigiria que cada interface WAN fosse configurada corretamente de acordo com as informações fornecidas por cada provedor.

Como fazê-lo...

1. Vá a **System | Routing**
2. Selecione a aba **Gateways**
3. Tome nota que o gateway da nossa interface padrão WAN existente foi criada automaticamente, por isso ela está definida como **default**, que geralmente é definida como **dynamics**.

System: Gateways

S ?

Name	Interface	Gateway	Monitor IP	Description
GW_WAN (default)	WAN	dynamic	dynamic	Interface wan Dynamic Gateway

4. Clique no botão “+” para adicionar um novo gateway
5. Em **Interface** escolha a conexão já existente WAN
6. Em **Name** digite um nome para o gateway
7. Em **Gateway** digite o gateway da interface
8. Marque **Default Gateway**
9. Em **Description** digite uma descrição para seu gateway, no exemplo nós usamos **WAN Gateway**.

System: Gateways: Edit gateway

S ?

Edit gateway

Interface	<input style="border: none; width: 50px; height: 20px; padding: 0; margin-right: 10px;" type="button" value="WAN"/> <input style="border: none; width: 20px; height: 20px; padding: 0;" type="button" value="▼"/> Choose which interface this gateway applies to.
Name	<input style="border: 1px solid #ccc; width: 150px; height: 20px; margin-right: 10px;" type="text" value="WANGateway"/> Gateway name
Gateway	<input style="width: 150px; height: 20px; margin-bottom: 5px;" type="text" value="172.16.1.1"/> Gateway IP address
Default Gateway	<input checked="" type="checkbox"/> Default Gateway This will select the above gateway as the default gateway
Monitor IP	<input style="width: 150px; height: 20px; margin-bottom: 5px;" type="text" value="172.16.1.1"/> Alternative monitor IP Enter an alternative address here to be used to monitor the link. This is used for the quality RRD graphs as well as the load balancer entries. Use this if the gateway does not respond to ICMP echo requests (pings).
Advanced	<input style="border: none; width: 100px; height: 20px; padding: 0; margin-right: 10px;" type="button" value="Advanced"/> - Show advanced option
Description	<input style="border: 1px solid #ccc; width: 150px; height: 20px; margin-bottom: 5px;" type="text" value="WAN Gateway"/> You may enter a description here for your reference (not parsed).

Save

Cancel

10. Clique em **Save**.

System: Gateways

S ?

Gateways **Routes** **Groups**

Name	Interface	Gateway	Monitor IP	Description
GW_WAN	WAN	dynamic	172.16.1.1	Interface wan Dynamic Gateway
WANGateway (default)	WAN	172.16.1.1	172.16.1.1	WAN Gateway

11. Clique no botão “+” para adicionar um novo Gateway

12. Na opção **Interface** escolha a nova interface WAN.

13. Em **Name** digite um nome para o gateway

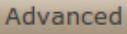
14. Em **Gateway** digite o gateway da interface

15. Em **Description** digite uma descrição para seu gateway, no exemplo nós usamos **WAN2 Gateway**.

System: Gateways: Edit gateway

S ?

Edit gateway

Interface	WAN2 	Choose which interface this gateway applies to.
Name	 WAN2Gateway	Gateway name
Gateway	 172.16.2.1	Gateway IP address
Default Gateway	<input type="checkbox"/> Default Gateway This will select the above gateway as the default gateway	
Monitor IP	172.16.2.1	Alternative monitor IP Enter an alternative address here to be used to monitor the link. This is used for the quality RRD graphs as well as the load balancer entries. Use this if the gateway does not respond to ICMP echo requests (pings).
Advanced	 - Show advanced option	
Description	 WAN2 Gateway You may enter a description here for your reference (not parsed).	

Save

Cancel

16. Clique em **Save**

17. Clique em **Apply Changes**

System: Gateways

S ?

Gateways **Routes** **Groups**

Name	Interface	Gateway	Monitor IP	Description	
GW_WAN	WAN	dynamic	172.16.1.1	Interface wan Dynamic Gateway	      
WANGateway (default)	WAN	172.16.1.1	172.16.1.1	WAN Gateway	      
WAN2Gateway	WAN2	172.16.2.1	172.16.2.1	WAN2 Gateway	      

18. Vá a **Interfaces | WAN**

19. Em **Type** escolha **Static**

20. Em **IP Address** digite o IP da WAN

21. Em **Gateway** selecione o gateway que você criou referente à WAN

22. Marque **Block private networks**

23. Marque **Block bogon networks**

Static IP configuration

IP address	<input type="text" value="172.16.1.2"/> / 24 ▾
Gateway	<input type="text" value="WANGateway - 172.16.1.1"/> ▾
If this Interface Is an Internet connection, select an existing Gateway from the list or add a new one.	

Private networks

Block private networks
When set, this option blocks traffic from IP addresses that are reserved for private networks as per RFC 1918 (10/8, 172.16/12, 192.168/16) as well as loopback addresses (127/8). You should generally leave this option turned on, unless your WAN network lies in such a private address space, too.

Block bogon networks
When set, this option blocks traffic from IP addresses that are reserved (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and obviously should not appear as the source address in any packets you receive.

Save **Cancel**

24. Clique em **Save**
25. Vá á **Interfaces | WAN2**
26. Em **Type** escolha **Static**

General configuration

Enable	<input checked="" type="checkbox"/> Enable Interface
Description	<input type="text" value="WAN2"/> Enter a description (name) for the interface here.
Type	<input type="button" value="Static"/> ▾

27. Em **IP address** digite o IP da WAN2
28. Em **Gateway**, selecione o gateway criado referente a WAN2
29. Marque **Block private networks**
30. Marque **Block bogon networks**

Static IP configuration

IP address	<input type="text" value="172.16.2.2"/> / 24 ▾
Gateway	<input type="text" value="WAN2Gateway - 172.16.2.1"/> ▾
If this Interface Is an Internet connection, select an existing Gateway from the list or add a new one.	

Private networks

Block private networks
When set, this option blocks traffic from IP addresses that are reserved for private networks as per RFC 1918 (10/8, 172.16/12, 192.168/16) as well as loopback addresses (127/8). You should generally leave this option turned on, unless your WAN network lies in such a private address space, too.

Block bogon networks
When set, this option blocks traffic from IP addresses that are reserved (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and obviously should not appear as the source address in any packets you receive.

Save **Cancel**

31. Clique em **Save**

32. Clique em **Apply Changes**

Como ele funciona...

Apenas a primeira interface WAN que é criada pelo PfSense, vai ter seu gateway padrão gerado automaticamente. Ao criar um gateway manualmente para interface WAN, como acabamos de fazer, então agora podemos continuar com o capítulo fazendo para configurar os recursos de redundância.

Há mais...

Lembre-se sempre de marcar as opções de **Block private networks** e **Block bogon networks** nas redes de internet.

Veja também...

- Configurando a Interface, capítulo 1 – Configuração Inicial.
- Criando gateway, capítulo 5 – Configurações avançadas.
- Configurando multi-WAN com balanceamento de carga
- Configurando multi-WAN com Failover

Configurando multi-WAN com balanceamento de carga

Aqui vamos descrever como configurar o balanceamento de carga em um único sistema PfSense.

Se preparando...

Ao longo dessas instruções, vamos configurar o balanceamento de carga de duas interfaces WAN separadas. Então terá que se certificar primeiro se as duas interfaces estão corretamente configuradas seguindo pela instrução mais a cima.

Toda vez que um balanceamento de carga entra em vigor, o Failover automaticamente também entra. Mas se quiséssemos ativar somente o Failover, na próxima etapa vamos descrever como fazer.

Como fazê-lo...

1. Vá a **System | Routing**
2. Selecione a aba **Groups**
3. Em **Group name** digite um nome (esse nome vai ser o nome do seu gateway, e não pode ter espaço) no exemplo usamos **LoadBalancedGroup**
4. Em **Gateway Priority** em ambos os gateways selecione **Tier1**
5. Em **Trigger Level**, selecione **Member Down**
6. Em **Description** digite uma descrição para seu balanceamento.

System: Gateways: Edit gateway

S ?

Edit gateway entry

Group Name	<input type="text" value="LoadBalancedGroup"/> LoadBalancedGroup Group Name									
Gateway Priority	<table border="1"><tr><td>Never</td><td>▼</td><td>GW_WAN - Interface wan Dynamic Gateway</td></tr><tr><td>Tier 1</td><td>▼</td><td>WANGateway - WAN Gateway</td></tr><tr><td>Tier 1</td><td>▼</td><td>WAN2Gateway - WAN2 Gateway</td></tr></table>	Never	▼	GW_WAN - Interface wan Dynamic Gateway	Tier 1	▼	WANGateway - WAN Gateway	Tier 1	▼	WAN2Gateway - WAN2 Gateway
Never	▼	GW_WAN - Interface wan Dynamic Gateway								
Tier 1	▼	WANGateway - WAN Gateway								
Tier 1	▼	WAN2Gateway - WAN2 Gateway								
Link Priority The priority selected here defines in what order failover and balancing of links will be done. Multiple links of the same priority will balance connections until all links in the priority will be exhausted. If all links in a priority level are exhausted we will use the next available link(s) in the next priority level.										
Trigger Level	<input type="text" value="Member Down"/> Member Down When to trigger exclusion of a member									
Description	<input type="text" value="Round-robin effect for gateways on the same tier."/> Round-robin effect for gateways on the same tier. You may enter a description here for your reference (not parsed).									

Save **Cancel**

7. Clique em **Save**
8. Clique em **Apply Changes**

System: Gateway Groups

S ?

Gateways Routes Groups

Group Name	Gateways	Priority	Description	
LoadBalancedGroup	WANGATEWAY WAN2GATEWAY	Tier 1 Tier 1	Round-robin effect for gateways on the same tier.	   

9. Vá até **System | Routing**
10. Edite o WAN gateway
11. Em **Monitor IP** você pode especificar um endereço de IP externo. Eu particularmente coloco o endereço `http://www.google.com.br`, mas você pode especificar o endereço a sua escolha, pode ser um mais perto do seu firewall (algum ip dentro da rede do seu provedor por exemplo).
12. Clique em **Save**.
13. Edite o Wan2 gateway
14. Em **Monitor IP** você pode especificar um endereço de IP externo. Eu particularmente coloco o endereço `http://www.google.com.br`, mas você pode especificar o endereço a sua escolha, pode ser um mais perto do seu firewall (algum ip dentro da rede do seu provedor por exemplo).
15. Clique em **Save**.
16. Clique em **Apply Changes**.

System: Gateways

S ?

Gateways Routes Groups

Name	Interface	Gateway	Monitor IP	Description
GW_WAN	WAN	dynamic	172.16.1.1	Interface wan Dynamic Gateway
WANGateway (default)	WAN	172.16.1.1	173.194.33.104	WAN Gateway
WAN2Gateway	WAN2	172.16.2.1	98.137.149.56	WAN2 Gateway



17. Vá até Firewall | Rules

18. Clique no botão “+” para adicionar uma nova regra de firewall na aba **LAN**
19. Em ação selecione **Pass**
20. Em **Interface** selecione **LAN**
21. Em **Protocol** selecione **any**
22. Em **Source** selecione **Lan Subnet**
23. Em **Destination** selecione **any**
24. Em **Description** digite uma descrição
25. Em **Advanced Features**, na opção **Gateway** clique em **Advanced** e irá aparecer um menu com a lista de gateways criados
26. Em **gateway** selecione o gateway que criamos logo a cima com o nome **LoadBalancedGroup**
27. Clique em **Save**
28. Clique em **Apply Changes**

Firewall: Rules

S L ?

Floating WAN LAN WAN2

ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
1	*	LAN net	*	*	*	LoadBalancedGroup	none		Load balance all of our traffic.

pass
 pass (disabled)

block
 block (disabled)

reject
 reject (disabled)

log
 log (disabled)

Hint:

Rules are evaluated on a first-match basis (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you'll have to pay attention to the rule order. Everything that isn't explicitly passed is blocked by default.

You may drag and drop rules using your mouse to reorder the rule ordering.

Como ele funciona...

Todo o tráfego de internet que passar pela LAN vai passar pelo nosso gateway. As duas WANs configuradas vão ter o mesmo nível de prioridade vai alternar entre si simultaneamente.

Além disso, nós também configuramos o **IP Monitor**, com isso o PfSense saberá quando um gateway perde a conexão com a internet, então o balanceamento de carga exclui esse link deixando o outro ou os outros funcionando, quem faz isso é o Failover, que entra em vigor automaticamente.

Há mais...

Nós definimos o **Trigger Level**, como **Member Down**, mas há varias outras opções:

- **Member Down**: É acionado quando o endereço que colocamos em **IP monitor** deixa de responder aos pings.
- **Packet Loss**: É acionado quando os pacotes que viajam entre um dos gateways são perdidos.
- **High Latency**: É ativado quando os pacotes que viajam entre um dos gateways ficam com uma instabilidade muito alta.
- **Packet Loss or High Latency**: É acionado quando os pacotes que viajam entre um dos gateways ficam com perda ou instável.

Veja também...

- Configurando múltiplas interfaces WAN

Configurando o Failover em uma multi-WAN

Aqui vamos descrever como configurar o Failover em uma multi-WAN usando somente um sistema PfSense.

Se preparando...

Ao longo dessa descrição, vamos configurar o Failover para nossas duas interfaces WAN separadas. Então terá que se certificar primeiro se as duas interfaces estão corretamente configuradas se guiando pela instrução anteriormente dita.

Como fazê-lo...

1. Vá a **System | Routing**
2. Selecione a aba **Groups**
3. Em **Group name** digite um nome (esse nome vai ser o nome do seu gateway, e não pode ter espaço) no exemplo usamos **FailoverGroup**
4. Em **Gateway Priority** selecione seu WAN Gateway como **Tier 1**.
5. Em **Gateway Priority** selecione seu WAN2 Gateway como **Tier 2**.
6. Em **Trigger Level** selecione **Member Down**
7. Em **Description** digite uma descrição para seu Failover.

System: Gateways: Edit gateway

S ?

Edit gateway entry

Group Name	FailoverGroup Group Name
Gateway Priority	<input type="button" value="Never"/> GW_WAN - Interface wan Dynamic Gateway <input type="button" value="Tier 1"/> WANGateway - WAN Gateway <input type="button" value="Tier 2"/> WAN2Gateway - WAN2 Gateway
Link Priority The priority selected here defines in what order failover and balancing of links will be done. Multiple links of the same priority will balance connections until all links in the priority will be exhausted. If all links in a priority level are exhausted we will use the next available link(s) in the next priority level.	
Trigger Level	<input type="button" value="Member Down"/> When to trigger exclusion of a member
Description	Failover for WAN down. You may enter a description here for your reference (not parsed).

8. Clique em **Save**
9. Clique em **Save Changes**

System: Gateway Groups

S ?

Gateways Routes Groups

Group Name	Gateways	Priority	Description	
FailoverGroup	WANGATEWAY WAN2GATEWAY	Tier 1 Tier 2	Failover for WAN down.	

10. Vá até **System | Routing**
11. Edite o WAN gateway
12. Em **Monitor IP** você pode especificar um endereço de IP externo. Eu particularmente coloco o endereço `http://www.google.com.br`, mas você pode especificar o endereço a sua escolha, pode ser um mais perto do seu firewall (algum ip dentro da rede do seu provedor, por exemplo).
13. Clique em **Save**.
14. Edite o Wan2 gateway
15. Em **Monitor IP** você pode especificar um endereço de IP externo. Eu particularmente coloco o endereço `http://www.google.com.br`, mas você pode especificar o endereço a sua escolha, pode ser um mais perto do seu firewall (algum ip dentro da rede do seu provedor, por exemplo).
16. Clique em **Save**.
17. Clique em **Apply Changes**.

System: Gateways

S ?

Gateways	Routes	Groups		
GW_WAN	WAN	dynamic	172.16.1.1	Interface wan Dynamic Gateway
WANGateway (default)	WAN	172.16.1.1	173.194.33.104	WAN Gateway
WAN2Gateway	WAN2	172.16.2.1	98.137.149.56	WAN2 Gateway

18. Vá até Firewall | Rules

19. Clique no botão “+” para adicionar uma nova regra de firewall na aba **LAN**
20. Em ação selecione **Pass**
21. Em **Interface** selecione **LAN**
22. Em **Protocol** selecione **any**
23. Em **Source** selecione **Lan Subnet**
24. Em **Destination** selecione **any**
25. Em **Description** digite uma descrição
26. Em **Advanced Features**, na opção **Gateway** clique em **Advanced** e irá aparecer um menu com a lista de gateways criados
27. Em **gateway** selecione o gateway que criamos logo a cima com o nome **FailoverGroup**
28. Clique em **Save**
29. Clique em **Apply Changes**

Firewall: Rules

S L ?

Floating	WAN	LAN	WAN2							
ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	*	LAN net	*	*	*	FailoverGroup	none		Failover for WAN down.	
	*	*	*	*	*	FailoverGroup	none		Failover for WAN down.	

pass block reject
 pass (disabled) block (disabled) reject (disabled)

log log (disabled)

Hint:

Rules are evaluated on a first-match basis (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you'll have to pay attention to the rule order. Everything that isn't explicitly passed is blocked by default.

You may drag and drop rules using your mouse to reorder the rule ordering.

Como ele funciona...

Todo o tráfego da nossa LAN vai passar pelo gateway que acabamos de criar. Consiste em um gateway de dois níveis de prioridades separadas, a rede funcionara pelo gateway **Tier 1**, quando esse gateway por algum motivo ficar off, então o gateway **Tier 2** assume o lugar do gateway principal, e quando **Tier 1** voltar ao normal, os dois gateways voltam para a posição inicial.

Há mais...

Nós definimos o **Trigger Level**, como **Member Down**, mas há varias outras opções:

- **Member Down**: É acionado quando o endereço que colocamos em **IP monitor** deixa de responder aos pings.
- **Packet Loss**: É acionado quando os pacotes que viajam entre um dos gateways são perdidos.
- **High Latency**: É ativado quando os pacotes que viajam entre um dos gateways ficam com uma instabilidade muito alta.
- **Packet Loss or High Latency**: É acionado quando os pacotes que viajam entre um dos gateways ficam com perda ou instável.

Veja também...

- Configurando múltiplas interfaces WAN
- Configurando o balanceamento de carga em uma multi-WAN

Configurando um servidor web com balanceamento de carga

Aqui vamos descrever um pequeno serviço de web com平衡ador de carga no PfSense.

Se preparando...

O平衡ador de carga permite que o PfSense distribua certos tipos de tráfego para varias maquinas na rede. Um uso comum desse recurso é para distribuir solicitações HTTP de entrada para vários servidores web, a seguir vamos descrever como configurar o平衡ador de carga para criar um serviço de web priorizado.

Como fazê-lo...

1. Vá á **Services | Load Balancer**
2. Na aba **Monitor**
3. Clique no botão “+” para adicionar um novo Monitor.
4. Em **Name** digite um nome para seu monitor
5. Em **Description** digite uma descrição para identificar seu monitor
6. Em **Type** selecione **HTTP**.
7. na opção **Host**, aqui vamos digitar um endereço de IP que não é usado na rede, para ser o IP do servidor virtual. O servidor virtual vai ser configurado para passar os pedidos para os servidores reais de web, esse IP é o que vai ser monitorado

8. Em **HTTP Code** selecione **200 OK**.

Services: Load Balancer: Monitor: Edit

S L ?

Edit Load Balancer - Monitor entry

Name	WebfarmMonitor
Description	Monitor the webfarm pool.
Type	HTTP
HTTP <div style="display: flex; justify-content: space-between;"> <div style="flex: 1;"> Path: / Host: 192.168.1.200 <small>Hostname for Host: header if needed.</small> </div> <div style="flex: 1; text-align: right;"> HTTP Code: 200 OK </div> </div>	
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

9. Clique em **Save**

10. Clique em **Apply Changes**.

Services: Load Balancer: Monitor

S L ?

Pools	Virtual Servers	Monitors						
		<table border="1"> <thead> <tr> <th>Name</th><th>Type</th><th>Description</th></tr> </thead> <tbody> <tr> <td>WebfarmMonitor</td><td>http</td><td>Monitor the webfarm pool.</td></tr> </tbody> </table>	Name	Type	Description	WebfarmMonitor	http	Monitor the webfarm pool.
Name	Type	Description						
WebfarmMonitor	http	Monitor the webfarm pool.						

11. Clique na aba **Pools**.

12. Clique no botão “+” para adicionar um novo pool

13. Selecione um nome em **Name**

14. Em **Mode** selecione **Load Balance**

15. Em **Description** digite uma descrição pro pool que você acabou de criar

16. Em **Port** selecione **80** (pois estamos criando um balanceador de carga de um servidor web)

17. Em **Monitor** selecione o monitor que você acabou de criar com o nome **WebfarmMonitor**.

18. Em **Server IP Address** digite cada ip dos servidores web e clique em **Add to pool**.

Services: Load Balancer: Pool: Edit

S L ?

Add/edit Load Balancer - Pool entry

Name	WebfarmPool
Mode	Load Balance ▾
Description	Webfarm pool for www.mydomain.com
Port	80 This is the port your servers are listening on.

Add item to pool

Monitor	WebfarmMonitor ▾
Server IP Address	<input type="text"/> Add to pool

Current Pool Members

Members	Pool Disabled	Enabled (default)
	<input type="button" value="▲"/> > <input type="button" value="▼"/>	192.168.1.201 192.168.1.202
	<input type="button" value="Remove"/>	<input type="button" value="Remove"/>

19. Clique em **Save**

20. Clique em **Apply Changes**

Services: Load Balancer: Pool

S L ?

Pools	Virtual Servers	Monitors				
Name	Mode	Servers	Port	Monitor	Description	
WebfarmPool	loadbalance	192.168.1.201 192.168.1.202	80	WebfarmMonitor	Webfarm pool for www.mydomain.com	

21. Clique na aba **Virtual Servers**

22. Clique no botão “+” para adicionar um novo servidor virtual

23. Em **Name** digite um nome para o seu servidor virtual

24. Em **Description** digite uma descrição para o seu servidor

25. Em **IP address** digite o IP que você cadastrou em **Monitor**.

26. Em **Port** digite a porta que você quer usar no caso é **80** já que é um servidor de web

27. Em **Virtual Server Pool** selecione o pool que você criou, **WebfarmPool**

Services: Load Balancer: Virtual Server: Edit

S L ?

Edit Load Balancer - Virtual Server entry

Name	WebfarmVirtualServer
Description	Virtual webserver for www.mydomain.com
IP Address	192.168.1.200
This is normally the WAN IP address that you would like the server to listen on. All connections to this IP and port will be forwarded to the pool cluster.	
Port	80
This is the port that the clients will connect to. All connections to this port will be forwarded to the pool cluster.	
Virtual Server Pool	WebfarmPool ▾
Fall Back Pool	none ▾
NOTE: This is the server that clients will be redirected to if *ALL* servers in the pool are offline.	
Submit	Cancel

Note: Don't forget to add a firewall rule for the virtual server/pool after you're finished setting it up.

28. Clique em **Submit**

29. Clique em **Apply Changes**

Services: Load Balancer: Virtual Servers

S L ?

Pools	Virtual Servers	Monitors					
Name	Mode	IP Address	Port	Pool	Fall Back Pool	Description	
WebfarmVirtualServer	redirect_mode	192.168.1.200	80	WebfarmPool	none	Virtual webserver for www.mydomain.com	   

Como ele funciona...

Nessas descrições, temos configurado o PfSense para dividir o tráfego de entradas de HTTP (porta 80) entre os dois servidores web separados. O pool define a localização do servidor web e o modo que o balanceamento de carga é feito (ao contrario do Failover). Nossa servidor virtual define o endereço de IP, vamos utilizar o nosso NAT e regras de firewall para ouvir os pedido HTTP, e o servidor virtual vai saber dividir corretamente as requisições atribuídas pelo Pool. O monitor irá verificar o estado o pool periodicamente fazendo um pedido de web. Uma vez que o pedido é direcionado ao endereço de IP do servidor virtual, vai ser desligado o pool, se qualquer um dos dois servidores não responder com o status **200 OK**. Uma vez que isso acontecer o pool vai definir o Failover também.

Há mais...

Sticky connections podem ser usados para garantir que o cliente sempre vai fazer pedidos para o mesmo servidor durante um período de tempo. Se o próximo pedido for feito após o time out do **Sticky connections**, ele vai ser manuseado por qualquer um dos dois servidores.

Os desenvolvedores geralmente precisam desse recurso para garantir a integridade dos dados específicos do servidor (cache InMemory), mas não é tão confiável do que usar a sessão de armazenamento compartilhado.

Veja também...

- Criando regras de NAT port Forward, capítulo 3 – Configuração Geral
- Criando regras de Firewall, capítulo 3 – Configuração Geral
- Configurando servidor web com Failover

Configurando um servidor web com Failover

Aqui vamos descrever como fazer um pequeno servidor web com a função de Failover.

Se preparando...

O balanceador de carga também permite que o PfSense envie o tráfego para um servidor Failover quando cair a conexão.

Como fazê-lo...

1. Vá a **Services | Load Balancer**
2. Clique na aba **Monitor**
3. Clique no botão “+” para adicionar um novo monitor
4. Em **name** digite um nome para o seu monitor
5. Em **Description** digite uma descrição que você possa reconhecer seu monitor
6. Na opção **type** selecione **HTTP**
7. Em **host** digite o IP do seu servidor primário de web
8. Na opção **HTTP code** selecione **200 OK**

Services: Load Balancer: Monitor: Edit

S L ?

Edit Load Balancer - Monitor entry							
Name	WebserverMonitor						
Description	Monitor the primary webserver.						
Type	HTTP						
HTTP	<table border="1"><tr><td>Path</td><td>/</td></tr><tr><td>Host</td><td>192.168.1.201 Hostname for Host: header if needed.</td></tr><tr><td>HTTP Code</td><td>200 OK</td></tr></table>	Path	/	Host	192.168.1.201 Hostname for Host: header if needed.	HTTP Code	200 OK
Path	/						
Host	192.168.1.201 Hostname for Host: header if needed.						
HTTP Code	200 OK						
Save Cancel							

9. Clique em **Save**

10. Clique em **Apply Change**

Services: Load Balancer: Monitor

S L ?

Name	Type	Description	
WebserverMonitor	http	Monitor the primary webserver.	   

11. Clique na aba **Pools**.

12. Clique no botão “+” para adicionar um novo pool

13. Em **name** digite um nome para o pool

14. Em **mode** selecione **Manual Failover**.

15. Digite uma descrição para o seu pool em **Description**

16. Em **port** selecione **80** (já que estamos criando um Failover para servidor web)

17. Em **Monitor** selecione o monitor que você acabou de criar com o nome **WebFailoverMonitor**.

18. Em **Server IP Address** digite o ip do seu servidor web primário, e clique em **Add pool**, se você reparar o ip vai para lista de **Enable (default)**

19. Depois digite novamente em **Server IP Address**, só que agora você vai digitar o IP do servidor web de backup, e clique em **Add pool**, se você reparar o IP vai para lista de **Pool Disabled**.

Services: Load Balancer: Pool: Edit

S L ?

Add/edit Load Balancer - Pool entry

Name	WebFailoverPool
Mode	Manual Failover
Description	Web failover pool for www.mydomain.com
Port	80 This is the port your servers are listening on.

Add item to pool

Monitor	WebserverMonitor
Server IP Address	<input type="text"/> Add to pool

Current Pool Members

Members	Pool Disabled	Enabled (default)
	192.168.1.202	192.168.1.201
	>	<
	Remove	Remove

Save **Cancel**

20. Clique em **Save**

21. Clique em **Apply Changes**

Services: Load Balancer: Pool

S L ?

Pools	Virtual Servers	Monitors
WebFailoverPool	failover 192.168.1.201 80 WebserverMonitor	Web failover pool for www.mydomain.com

22. Clique na aba **Virtual Server**.

23. Clique no botão “+” para adicionar um novo servidor virtual

24. Em **Name** digite um nome para o seu servidor virtual

25. Digite em **Description** uma descrição para o seu servidor virtual

26. Em **IP address** digite um IP que não tiver uso na sua rede

27. Em **port** selecione **80** (já que estamos criando um Failover para servidor web)

28. Em **Virtual Server Pool** selecione o Pool que você acabou de criar, no exemplo é o **WebFailoverPool**.

Services: Load Balancer: Virtual Server: Edit

S L ?

Edit Load Balancer - Virtual Server entry

Name	WebVirtualServer
Description	Virtual webserver for www.mydomain.com
IP Address	192.168.1.200 <small>This is normally the WAN IP address that you would like the server to listen on. All connections to this IP and port will be forwarded to the pool cluster.</small>
Port	80 <small>This is the port that the clients will connect to. All connections to this port will be forwarded to the pool cluster.</small>
Virtual Server Pool	WebFailoverPool ▾
Fall Back Pool	none ▾ NOTE: This is the server that clients will be redirected to if *ALL* servers in the pool are offline.

Submit **Cancel**

Note: Don't forget to add a firewall rule for the virtual server/pool after you're finished setting it up.

29. Clique em **Submit**

30. Clique em **Apply Changes**

Services: Load Balancer: Virtual Servers

S L ?

Pools	Virtual Servers	Monitors				
Name	Mode	IP Address	Port	Pool	Fall Back Pool	Description
WebVirtualServer	redirect_mode	192.168.1.200	80	WebFailoverPool	none	Virtual webserver for www.mydomain.com

Como ele funciona...

Ao longo dessas descrições, explicamos como configurar o PfSense para redirecionar o tráfego automaticamente do servidor web primário para o servidor web de backup se o primário ficar off por algum motivo. O pool define a localização dos servidores web e o modo Failover (que é o contrario de balanceamento de carga). E o servidor virtual define o endereço de IP, e vamos utilizar o NAT e regras de firewall para ouvir os pedidos HTTP, o servidor virtual para o pool que definimos. O monitor verifica o status do servidor principal periodicamente fazendo pedidos web. Se a resposta voltar 200 OK, o pool vai usar o tráfego do servidor primário, caso contrario ele vai direcionar o tráfego para o servidor de backup.

Veja também...

- Criando NAT de port forward, capítulo – 3, Configuração Geral
- Criando regras de firewall, capítulo – 3, Configuração Geral
- Configurando servidor web com balanceamento de carga

Configurando um firewall CARP com Failover

Aqui vamos aprender como configurar dois firewalls PfSense para Failover

Se preparando...

Redundância de hardware precisa de um hardware adicional claro. Para configurar um Failover de firewall, vamos precisar de duas máquinas PfSense. Cada máquina também precisa de uma interface adicional dedicado ao processo de sincronização (vamos chamar de pfsync). Agora vamos demonstrar como usar duas máquinas separadas com PfSense, cada uma com três interfaces (WAN, LAN e pfsync)

As seguintes interfaces serão configuradas com endereços de IPs privados para o exemplo, mas em uma configuração real exigiria para cada interface WAN ser configurada corretamente de acordo com as informações fornecidas pelo provedor.

Como fazê-lo...

1. Configure a interface da nossa primeira maquina, o PfSense primário com as seguintes informações:
 - **WAN:** 192.168.111.2
 - **SYNC:** 192.168.222.2
 - **LAN:** 192.168.1.2
2. Configure a interface da nossa segunda maquina, o PfSense secundário com as seguintes informações:
 - **WAN:** 192.168.111.3
 - **SYNC:** 192.168.222.3
 - **LAN:** 192.168.1.3
3. Em ambas as maquinas, adicione no firewall a regra de tráfego livre na interface SYNC:
 1. Vá a **Firewall | Rules**
 2. Clique na aba **Interface SYNC**
 3. Clique no botão “+” adicionando uma nova regra de firewall
 4. Em **Protocol** selecione **any** e digite uma descrição em **Description**

Firewall: Rules: Edit

S L ?

Edit Firewall rule	
Action	<input type="button" value="Pass"/> <input type="button" value="▼"/> Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.
Disabled	<input type="checkbox"/> Disable this rule Set this option to disable this rule without removing it from the list.
Interface	<input type="button" value="SYNC"/> <input type="button" value="▼"/> Choose on which interface packets must come in to match this rule.
Protocol	<input type="button" value="any"/> <input type="button" value="▼"/> Choose which IP protocol this rule should match. Hint: in most cases, you should specify TCP here.
Description	 Allow all traffic on SYNC interface. You may enter a description here for your reference.

5. Clique em **Save**
6. Clique em **Apply Changes**

Firewall: Rules

S L ?

Floating	WAN	LAN	SYNC						
ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
<input type="checkbox"/>	*	*	*	*	*	*	none		Allow all traffic on SYNC interface.

Actions:

Legend: pass pass (disabled) block block (disabled) reject reject (disabled) log log (disabled)

Hint:

Rules are evaluated on a first-match basis (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you'll have to pay attention to the rule order. Everything that isn't explicitly passed is blocked by default.
You may drag and drop rules using your mouse to reorder the rule ordering.

7. Na máquina PfSense secundário precisamos habilitar a sincronização CARP, e configura-lo apenas como backup:
 1. Vá a **Firewall | Virtual IPs**
 2. Clique na aba **CARP Settings**
 3. Marque **Synchronize Enabled**.
 4. Em **Synchronize Interface** selecione **SYNC**

Services: CARP Settings: Edit

?

Virtual IPs	CARP Settings
Synchronize Enabled <input checked="" type="checkbox"/>	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. NOTE: Clicking save will force a configuration sync!
Synchronize Interface	If Synchronize State 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.

8. Clique em **Save**
9. Nós acabamos de configurar o firewall de backup
10. Na máquina PfSense primário precisamos habilitar a sincronização CARP, e configura-lo para atuar como firewall principal:
 1. Vá em **Firewall | Virtual IPs**
 2. Clique na aba **CARP Settings**
 3. Marque **Synchronize Enabled**

4. Na opção **Synchronize Interface** selecione **SYNC**

Services: CARP Settings: Edit



Virtual IPs **CARP Settings**

Synchronize Enabled 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.
NOTE: Clicking save will force a configuration sync!

Synchronize Interface If Synchronize State 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.

11. Marque a opção **Synchronize rules**

Synchronize rules When this option is enabled, this system will automatically sync the firewall rules to the other CARP host when changes are made..

12. Marque a opção **Synchronize nat**

Synchronize nat When this option is enabled, this system will automatically sync the NAT rules over to the other CARP host when changes are made.

13. Marque a opção **Synchronize Virtual IPs**

Synchronize Virtual IPs When this option is enabled, this system will automatically sync the CARP Virtual IPs to the other CARP host when changes are made.

14. Em **Synchronize to IP** digite o IP do servidor secundário

15. Em **Remote System Password** digite a senha do pfSense secundário

Synchronize to IP Enter the IP address of the firewall you are synchronizing with.

Remote System Password Enter the webConfigurator password of the system that you would like to synchronize with.

Save **Cancel**

16. Clique em **Save**

17. Vamos agora configurar um VIP para interface WAN no PfSense primário

1. Vá a **Firewall | Virtual IPs**
2. Clique na aba **Virtual IPs**
3. Clique no botão “+” para adicionar um novo VIP
4. Em **type** selecione **CARP**.
5. Em **Interface** selecione **WAN**

6. Em **IP address** digite um endereço de IP único da WAN que será usado durante todo o sistema, independente do sistema primário ou secundário estar funcionando.
7. Em **Virtual IP Password** digite uma senha
8. Em **VHID Group** deixe a opção **1**
9. Em **Advertising Frequency** deixe a opção **0**
10. Em **Description** digite uma descrição qualquer

Firewall: Virtual IP Address: Edit

Edit Virtual IP

Type	<input type="radio"/> Proxy ARP <input checked="" type="radio"/> CARP <input type="radio"/> Other <input type="radio"/> IP Alias
Interface	WAN
IP Address(es)	Type: Network Address: <input type="text" value="192.168.111.1"/> / <input type="text" value="24"/> This must be the network's subnet mask. It does not specify a CIDR range.
Virtual IP Password	<input type="password"/> Enter the VHID group password.
VHID Group	<input type="button" value="1"/> Enter the VHID group that the machines will share
Advertising Frequency	<input type="button" value="0"/> The frequency that this machine will advertise. 0 = master. Anything above 0 designates a backup.
Description	<input type="text" value="WAN VIP for our CARP configuration."/> You may enter a description here for your reference (not parsed).
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

11. Clique em **Save**
12. Clique em **Apply Changes**

Firewall: Virtual IP Addresses

Virtual IPs **CARP Settings**

Virtual IP address	Type	Description	
192.168.111.1/24 (vhid 1)		WAN VIP for our CARP configuration.	

Note:
 The virtual IP addresses defined on this page may be used in NAT mappings.
 You can check the status of your CARP Virtual IPs and interfaces [here](#).

18. Vamos agora configurar um VIP para interface LAN no PfSense primário
 01. Vá a **Firewall | Virtual IPs**
 02. Clique na aba **Virtual IPs**
 03. Clique no botão “+” para adicionar um novo VIP

04. Em **Type** selecione **CARP**.
05. Em **Interface** selecione **LAN**
06. Em **IP address** digite um endereço de IP único da LAN que será usado como gateway nos clientes da rede, independente do sistema primário ou secundário estar funcionando.
07. Em **Virtual IP Password** digite uma senha
08. Em **VHID Group** deixe a opção **2**
09. Em **Advertising Frequency** deixe a opção **0**
10. Em **Description** digite uma descrição qualquer

Firewall: Virtual IP Address: Edit

[?](#)

Edit Virtual IP	
Type	<input type="radio"/> Proxy ARP <input checked="" type="radio"/> CARP <input type="radio"/> Other <input type="radio"/> IP Alias
Interface	LAN ▼
IP Address(es)	Type: Network  192.168.1.1 / 24 <small>This must be the network's subnet mask. It does not specify a CIDR range.</small>
Virtual IP Password	 <small>Enter the VHID group password.</small>
VHID Group	2 ▼ <small>Enter the VHID group that the machines will share</small>
Advertising Frequency	0 ▼ <small>The frequency that this machine will advertise. 0 = master. Anything above 0 designates a backup.</small>
Description	 LAN VIP for our CARP configuration. <small>You may enter a description here for your reference (not parsed).</small>
Save Cancel	

11. Clique em **Save**
12. Clique em **Apply Changes**

Firewall: Virtual IP Addresses

[Virtual IPs](#) [CARP Settings](#) [?](#)

Virtual IP address	Type	Description		 	 
192.168.111.1/24 (vhid 1)	 ARP	WAN VIP for our CARP configuration.		 	 
192.168.1.1/24 (vhid 2)	 ARP	LAN VIP for our CARP configuration.		 	 

Note:
The virtual IP addresses defined on this page may be used in NAT mappings.
You can check the status of your CARP Virtual IPs and interfaces [here](#).

Como ele funciona...

Aqui foi descrito como criar um PfSense Failover usando CARP. Os dois firewalls se sincronizam constantemente as regras, NAT e configurações de IPs, de modo que se o servidor principal pare ou por algum motivo fique off, o outro assume seu lugar automaticamente.

O truque para a sincronização é a configuração do **Advertising Frequency** entre o IP virtual de cada interface. O servidor principal tem um **Advertising Frequency** definido como **0**, então quando as configurações se sincronizam, a **Advertising Frequency** é incrementado para o servidor de backup (ou seja, o **Advertising Frequency** é **1**). E é assim que o PfSense consegue distinguir as máquinas e as configurações de sincronização.

Veja também...

- Criando NAT de port forward, capítulo – 3, Configuração Geral
- Criando regras de firewall, capítulo – 3, Configuração Geral
- Criando VIP, capítulo – 5, Configurações Avançadas

7

Serviços e Manutenção

Nesse capítulo, iremos abordar:

- Habilitando OLSR
- Habilitando PPPoE
- Habilitando RIP
- Habilitando SNMP
- Habilitando UPnP e NAT-PMP
- Habilitando OpenNTPD
- Habilitando Wake On Lan (WOL)
- Habilitando o log externo (syslog server)
- Usando o PING
- Usando o tracerout
- Fazer backup do arquivo de configuração
- Restaurando o arquivo de configuração
- Configurando o backup automático do arquivo de configuração
- Atualização do firmware do PfSense

Introdução

O PfSense oferece uma infinidade de serviços modernos e funcionais. Nesse capítulo vamos descrever os serviços mais usados em relação à manutenção, descrevendo a funcionalidade e como usar cada um deles.

Na primeira metade desse capítulo vamos descrever como usar os serviços de rede mais populares, desde SNMP, até como usar o ping e o tracerout, descrevendo como usar essas ferramentas indispensáveis, que já vem embutidas na interface WEB do PfSense. Na outra metade do capítulo vamos descrever um serviço essencial que é o sistema de backup, restauração e atualização do PfSense.

Habilitando o OLSR

O OLSR (**Optimized Link State Routing**), é um protocolo de roteamento de IP, otimizando a rede sem fio. É quando uma rede é constituída por dois ou mais nós, mas o que torna esse sistema único é a maneira

que esses nós se comunicam uns com os outros. Os nós têm múltiplas rotas em toda a rede, aumentando a confiabilidade focando em falhas individuais em cada nó.

Aqui vamos descrever como habilitar o serviço de **OLSR (Optimized Link State Routing)**.

Como fazê-lo...

1. Vá a **Services | OLSR**
2. Marque **Enable OLSR**.
3. Escola a interface (você pode selecionar varias interfaces com o botão Ctrl pressionado)
4. Clique em **Save**

OLSRD

The screenshot shows the 'OLSRD Settings' configuration page. It includes fields for enabling OLSR, setting link quality level, selecting interfaces (WAN, LAN, DMZ), and a note about selecting multiple interfaces using the CTRL or COMMAND key.

OLSRD Settings

Enable OLSR Enables the dynamic mesh linking daemon

Link Quality Level

Interfaces WAN LAN DMZ
Select the interfaces that OLSR will bind to. You can use the CTRL or COMMAND key to select multiple interfaces.

Como ele funciona...

O OLSR pode ser configurado na WebGUI do PfSense. O OLSR é muito usado para aumentar a confiabilidade em serviços portáteis como acesso wireless, em serviços ad-hoc.

Há mais...

Habilitando o HTTPInfo nós permite visualizar e controlar o estado da nossa rede OLSR:

1. Vá a **Services | OLSR**
2. Marque **Enable HTTPInfo Plugin**.
3. Digite em **HTTPInfo Port** a porta que você vai ter acesso ao HTTPInfo
4. Em **Allowed Host(s)**, digite o ip que você vai querer ter acesso ao HTTPInfo
5. Em **Allowed Host(s) Subnet** digite a mascara de subrede desse ip
6. Clique em **Save**.

The screenshot shows the 'HTTPInfo Plugin' configuration page. It includes fields for enabling the plugin, setting the port (54321), specifying allowed hosts (192.168.1.1), and defining the subnet mask (255.255.255.0).

Enable HTTPInfo Plugin Enables the OLSR stats web server

HTTPInfo Port Port that HTTPInfo will listen on

Allowed host(s) Hosts that are allowed to access the HTTPInfo web service.

Allowed host(s) subnet Enter the subnet mask in form 255.255.255.0

7. Abra qualquer navegador para ter acesso ao HTTPInfo:

<http://192.168.1.1:54321/>

olsr.org OLSR daemon

Variables

Main address: 192.168.1.1	IP version: 4	Debug level: 2	FIB Metrics: flat
Pollrate: 0.05	TC redundancy: 2	MPR coverage: 3	NAT threshold: 1.000000
Fisheye: Disabled	TOS: 0x0010	RtTable: 0x00fe/254	RtTableDefault: 0x0000/0
LQ extension: Enabled	LQ level: 2	LQ aging: 0.100000	Willingness: 3

Interfaces

vr0		
IP: 192.168.1.1	MASK: 255.255.255.0	BCAST: 192.168.1.255
MTU: 1472	WLAN: No	STATUS: UP

Olsrd is configured to run even if no interfaces are available

Plugins

Name	Parameters
/usr/local/lib/olsrd_httpinfo.so.0.1	KEY, VALUE

Announced HNA entries

(C)2005 Andreas Tønnesen
<http://www.olsr.org>

Habilitando o PPPoE

PPPoE significa **Point-to-Point Protocol over Ethernet**, eh um protocol de rede que permite encapsular Protocolo Point-to-Point (PPP) dentro dos frames da interface. PPPoE permite que dois clientes remotos possam ligar-se e passar dados entre si.

Aqui vamos descrever como habilitar o PPPoE no PfSense.

Como fazê-lo...

1. Vá a **Services | PPPoE Server**
2. Clique no botão “+” para adicionar uma nova estancia de PPPoE.
3. Marque **Enable PPPoE Server**
4. Em **Interface** selecione a interface que você deseja configurar
5. Em **Subnet Mask** selecione a mascara de subrede

6. Em **No. PPPoE Users** selecione o numero máximo de clientes que irão se conectar
7. Em **Server Address** digite um IP não usado que o PfSense vai servir para os clientes se conectarem.
8. Em **Remote Address Range** definir de que faixa de IP vai ser usado para ter acesso ao PPPoE, levando em consideração o numero de clientes que você definiu na etapa 6.
9. Em **Description** digite uma descrição para seu serviço de PPPoE
10. Em **DNS Servers** digite um conjunto de DNS ou deixe em branco para aceitar o padrão
11. Em **User(s)**, clique no botão "+" para adicionar um novo usuário. Digite o nome de usuário em **username**, a senha em **password** e o **IP**

User (s)	Username	Password	IP
	johndoe	•••••••	192.168.200.1
	janedoe	•••••••	192.168.200.2

12. Clique em **Save**.

Services: PPPoE Server: Edit

PPPoE server configuration

Off

Enable PPPoE server

Interface

Subnet netmask
Hint: 24 is 255.255.255.0

No. PPPoE users
Hint: 10 is ten PPPoE clients

Server address
Enter the IP address the PPPoE server should use on its side for all clients.

Remote address range
Specify the starting address for the client IP address subnet.

Description

DNS servers

If entered they will be given to all PPPoE clients, else LAN DNS and one WAN DNS will go to all clients

13. Clique em **Apply Changes**

VPN: PPPoE

Interface	Local ip	Number of users	Description	
WAN	192.168.1.200	10	My PPPoE Server.	

Como ele funciona...

O serviço PPPoE é usado geralmente para preencher lacunas entre conexões PPP(dial-up) e conexões Ethernet (banda-larga). Muitos provedores de internet que usam sistema de dial-up e querem usar esse tipo de autenticação para serviço de banda larga (PPPoE) e esse sistema faz exatamente isso.

Habilitando RIP

RIP significa **Routing Information Protocol**, protocolo de roteamento dinâmico para redes locais e largas áreas de rede.

Aqui vamos mostrar como habilitar o serviço de RIP no PfSense

Como fazê-lo...

1. Vá á **Services | RIP**
2. Marque **Enable RIP**
3. Selecione a interface (você pode selecionar mais de uma interface clicando nelas com o ctrl pressionado)
4. Selecione a versão do RIP em **RIP Version**
5. Se você selecionou o a versão 2 então digite uma senha em **RIPv2 password**
6. Clique em **Save**

Services: RIP



ROUTED Settings

Enable RIP	<input checked="" type="checkbox"/> Enables the Routing Information Protocol daemon
Interfaces	WAN LAN (selected) DMZ
Select the interfaces that RIP will bind to. You can use the CTRL or COMMAND key to select multiple interfaces.	
RIP Version	RIP Version 2
Select which RIP version the daemon will listen/advertise using.	
RIPv2 password	MyRipPassword
Specify a RIPv2 password. This password will be sent in the clear on all RIPv2 responses received and sent.	
Save	

Como ele funciona...

O protocolo RIP foi o primeiro protocolo de roteamento dinâmico que foi criado tem o objetivo de compartilhar informações de roteamento entre hosts Unix. O protocolo RIP transmite uma tabela de roteamento completo em todas as interfaces ativas em um período de geralmente 30 segundos.

Habilitando o SNMP

O SNMP significa (**Simple Network Management Protocol**), um protocolo padrão de SNMP permite que os clientes consultem informações de status de máquinas que também suportam SNMP.

Aqui vamos descrever como habilitar o serviço de SNMP.

Como fazê-lo...

1. Vá á **Services | SNMP**
2. Marque **Enable SNMP Daemon**
3. Em **Polling Port** você pode selecionar uma porta, mas a padrão é UDP 161
4. Em **System Location** digite o local que você está configurando
5. Em **System Contact** digite o nome de um contato, pode ser o seu mesmo.
6. Em **Read Community String** é uma senha comunitária que os clientes autorizados a consultar informações SNMP têm que digitar a partir de suas máquinas.

Services: SNMP

SNMP Daemon	
Polling Port	<input type="text" value="161"/> Enter the port to accept polling events on (default 161)
System location	<input type="text" value="Home Office"/>
System contact	<input type="text" value="Matt Williamson"/>
Read Community String	<input type="text" value="MySecretString"/> The community string is like a password, restricting access to querying SNMP to hosts knowing the community string. Use a strong value here to protect from unauthorized information disclosure.

7. Em **SNMP Modules** selecione os módulos que você deseja consultar

Modules	
SNMP Modules	<input checked="" type="checkbox"/> MibII <input checked="" type="checkbox"/> Netgraph <input checked="" type="checkbox"/> PF <input checked="" type="checkbox"/> Host Resources

8. Clique em **Save**

Como ele funciona...

Ao habilitar o SNMP no PfSense os administradores podem consultar informações sobre o sistema vital do cliente SNMP de sua escolha.

Há mais...

SNMP traps, são enviados pelo SNMP (como o PfSense) para os servidores especificados quando ocorre um evento significativo, Servidores de SNMP trap, decidem como processa e manipular tal evento, como e-mails de uma rede de administrador. SNMP Trap é útil para administradores de rede que precisam receber alertas rapidamente, ao invés de esperar pelo ciclo de pooling que tem um potencial muito longo então pode demorar muito.

Especificando um SNMP trap no servidor PfSense:

1. Vá á **Services | SNMP**
2. Marque **Enable SNMP Traps**
3. Digite o nome do seu SNMP trap em **Trap Server Name**
4. Digite a porta em **Trap Server Port**
5. Digite uma string em **SNMP Trap String**

SNMP Traps	
Trap server	<input type="text" value="trapserver1.mydomain.com"/> <small>Enter trap server name</small>
Trap server port	<input type="text" value="162"/> <small>Enter the port to send the traps to (default 162)</small>
Enter the SNMP trap string	<input type="text" value="MyTrapServerString"/> <small>Trap string</small>

6. Clique em **Save**

Veja também...

- Documentação sobre SNMP
http://doc.pfsense.org/index.php/SNMP_Daemon

Habilitando UPnP e NAT-PMP

UPnP e NAT-PMP são implementações totalmente diferentes dos já vistos, ela automatiza o mapeamento de portas NAT. Esses protocolos são projetados para permitir que clientes possam configurar automaticamente as regras de port Forward de um roteador ou firewall. Um exemplo comum de permissão UPnP , quando um Xbox 360 possa se conectar ao Xbox Live.

Geralmente os protocolos UPnP são usados em sistemas da Microsoft, enquanto o NAT-PMP são usados em sistemas da Apple.

Aqui vamos descrever como habilitar o UPnP e NAT-PMP no PfSense.

Como fazê-lo...

1. Vá á **Services | UPnP e NAT-PMP**

2. Marque **Enable UPnP & NAT-PMP**
3. Marque ou **Allow UPnP Port Mapping**, ou **Allow NAT-PMP Port Mapping** ou os dois.
4. Em **Interfaces** selecione a interface (se quiser selecionar mais de uma selecione a outra pressionando o botão Ctrl)

Services: UPnP & NAT-PMP



UPnP & NAT-PMP Settings

Enable UPnP & NAT-PMP	<input checked="" type="checkbox"/>
Allow UPnP Port Mapping	<input checked="" type="checkbox"/>
This protocol is often used by Microsoft-compatible systems.	
Allow NAT-PMP Port Mapping	<input type="checkbox"/>
This protocol is often used by Apple-compatible systems.	
Interfaces (generally LAN)	<input type="checkbox"/> WAN <input checked="" type="checkbox"/> LAN <input type="checkbox"/> PUB
You can use the CTRL or COMMAND key to select multiple interfaces.	

5. Clique em **Save**

Como ele funciona...

Ativando o UPnP e NAT-PMP permite que dispositivos compatíveis possam funcionar corretamente em uma determinada rede sem a necessidade de definir alguma regra ou port Forwarding.

Há mais...

Há mais recursos opcionais disponíveis em serviços UPnP e NAT-PMP no PfSense:

- Em **Maximum Download Speed** você pode definir que velocidade de download seus dispositivos usando o serviço UPnP e NAT-PMP pode usar
- Em **Maximum Upload Speed** você pode definir que velocidade de upload seus dispositivos usando o serviço UPnP e NAT-PMP pode usar
- Em **Override the WAN Address** você pode especificar qual IP pode substituir a WAN
- Em **Traffic Shaping Queue** você pode colocar um shaping já configurado

Maximum Download Speed (Kbits/second)	<input type="text"/> 1500
Maximum Upload Speed (Kbits/second)	<input type="text"/> 500
Override WAN address	<input type="text"/>
Traffic Shaping Queue	<input type="text"/>

- Marque **Enable Log Packets** para habilitar os logs usados por clientes UPnP e NAT-PMP
- Marcando o **System Uptime** você vai estar substituindo o uptime do serviço de UPnP e NAT-PMP pelo uptime do próprio sistema
- Marcando o **Default Deny Access** você vai estar negando todo o acesso vindo do UPnP e NAT-PMP

Log packets handled by UPnP & NAT-PMP rules?	<input checked="" type="checkbox"/>
Use system uptime instead of UPnP & NAT-PMP service uptime?	<input type="checkbox"/>
By default deny access to UPnP & NAT-PMP?	<input type="checkbox"/>

- Em **User specified permissions** você pode especificar até quatro usuários com permissões.

User specified permissions 1	 Format: [allow or deny] [ext port or range] [int ipaddr or ipaddr/cdir] [int port or range] Example: allow 1024-65535 192.168.0.0/24 1024-65535
User specified permissions 2	 Format: [allow or deny] [ext port or range] [int ipaddr or ipaddr/cdir] [int port or range]
User specified permissions 3	 Format: [allow or deny] [ext port or range] [int ipaddr or ipaddr/cdir] [int port or range]
User specified permissions 4	 Format: [allow or deny] [ext port or range] [int ipaddr or ipaddr/cdir] [int port or range]

Aviso de Segurança

Permitindo que dispositivos possam modificar suas regras de firewall, isso contém uma série de implicações de segurança. O firewall da Microsoft o sistema ISA (TMG é o mais recente) não apoia esses protocolos. Se você precisar habilitar esses serviços esteja ciente dos riscos. Você teria que dedicar uma interface separada para esse serviço (o tráfego é arriscado de mais). Você pode ver nas imagens que eu só habilito o UPnP na interface pública. Essa interface se trata como insegura mas é útil para jogos e que clientes naveguem na web livremente.

- Documentação sobre UPnP no PfSense
http://doc.pfsense.org/index.php/What_is_UPNP%3F
- Artigo sobre UPnP no Wikipedia
http://en.wikipedia.org/wiki/Universal_Plug_and_Play
- Artigo sobre NAT-PMP no Wikipédia
http://en.wikipedia.org/wiki/NAT_Port_Mapping_Protocol

Habilitando o OpenNTPD

O serviço vai atender as solicitações OpenNTPD, data e hora para os clientes solicitarem. Aqui vamos descrever como ativar o serviço OpenNTPD no PfSense.

Como fazê-lo...

1. Vá à **Services | OpenNTPD**
2. Marque **Enable** para habilitar o serviço NTPD
3. Em **Interface** selecione a interface para usar o serviço NTPD (você pode marcar mais de uma interface)

NTP server



The screenshot shows the 'NTP server' configuration page. At the top, there is a checked checkbox labeled 'Enable' with the instruction 'Check this to enable the NTP server.' Below it, a dropdown menu titled 'Interface' lists 'WAN', 'LAN', 'PUB', and 'DMZ'. A note below the dropdown says 'Select the interface(s) the NTP server will listen on.' At the bottom right of the form is a 'Save' button.

4. Clique em **Save**

Como ele funciona...

O OpenNTPD é uma implementação open-source do serviço **Network Time Protocol**. Dispositivos dentro de sua rede podem agora consultar o firewall PfSense com NTP e receber dados no tempo exato partir dele.

O cliente pode levar algumas horas para se tornar totalmente sincronizada com o serviço OpenNTPD, terá que ser paciente.

Veja também...

- Documentação sobre o PfSense NTPD
http://doc.pfsense.org/index.php/NTP_Server_%28OpenNTPD%29
- OpenNTPD.org
<http://www.openntpd.org/>
- Wikipedia OpenNTPD Article
<http://en.wikipedia.org/wiki/OpenNTPD>

Habilitando o Wake-On-Lan (WOL)

O PfSense pode enviar um pacote Wake-On-lan (também conhecido como pacote mágico) para que um dispositivo compatível possa ser “acordado”. Aqui vamos aprender como usar esse recurso no PfSense.

Como fazê-lo...

1. Vá a **Services | Wake on LAN**
2. Em **Interface**, selecione a interface onde estão os dispositivos que você deseja acordar.
3. Em **MAC address** digite o endereço MAC do dispositivo

Services: Wake on LAN

?

Wake on LAN	
Interface	<input type="button" value="LAN"/> <input type="button" value="▼"/>
Choose which interface the host to be woken up is connected to.	
MAC address	<input type="text" value="90:84:0d:9d:fc:57"/> <input type="button" value="Edit"/>
Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx	
<input type="button" value="Send"/>	

4. Clique em **Send**

Services: Wake on LAN

?

Wake on LAN	
Interface	<input type="button" value="LAN"/> <input type="button" value="▼"/>
Choose which interface the host to be woken up is connected to.	
MAC address	<input type="text" value="90:84:0d:9d:fc:57"/> <input type="button" value="Edit"/>
Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx	
<input type="button" value="Send"/>	

! Sent magic packet to 90:84:0d:9d:fc:57.

Como ele funciona...

O serviço Wake-on-LAN vai enviar “pacotes mágicos” para qualquer dispositivo ligado a rede que suportem esse recurso configurados para Wake-on-LAN. Quando um dispositivo configurado corretamente recebe um pacote magico, o computador vai ligar.

Vale ressaltar que em computadores mais antigos, tem que ser configurado corretamente essa opção na bios e conectar um cabo especial na placa mãe.

Há mais...

Você pode armazenar o endereço MAC de todas as maquinas de sua rede:

1. Vá á **Services | Wake on LAN**
2. Clique no botão “+” para adicionar um endereço de MAC para usar o serviço WOL.
3. Em **Interface** selecione a interface onde está ligado o dispositivo
4. Em **MAC address** digite o endereço MAC do computador ou dispositivo
5. Em **Description** digite uma descrição para o dispositivo

Services: Wake on LAN: Edit

?

Edit WOL entry

Interface	LAN
Choose which interface this host is connected to.	
MAC address	90:84:0d:9d:fc:57
Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx	
Description	Matt's Desktop
You may enter a description here for your reference (not parsed).	
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

6. Clique em **Save**

Interface	MAC address	Description	
LAN	90:84:0d:9d:fc:57	Matt's Desktop	 
LAN	00:26:08:ae:b3:3a	Matt's Laptop	 

7. Clique no **MAC address** do dispositivo que você quer mandar o pacote magico

Services: Wake on LAN

?

 Sent magic packet to 00:26:08:ae:b3:3a.

Wake on LAN

Interface	WAN
Choose which interface the host to be woken up is connected to.	
MAC address	
Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx	
<input type="button" value="Send"/>	

Wake all clients at once: 

Or Click the MAC address to wake up an individual device:

Interface	MAC address	Description	
LAN	90:84:0d:9d:fc:57	Matt's Desktop	 
LAN	00:26:08:ae:b3:3a	Matt's Laptop	 

Note:

This service can be used to wake up (power on) computers by sending special "Magic Packets". The NIC in the computer that is to be woken up must support Wake on LAN and has to be configured properly (WOL cable, BIOS settings).

Enviar pacote magico a todos

Em vez de acordar cada cliente um por um, você pode acordar todos de uma só vez, basta clicar no botão “Wake all clients”

Services: Wake on LAN



Wake on LAN

Interface	WAN	Choose which interface the host to be woken up is connected to.
MAC address	<input type="text" value="90:84:0d:9d:fc:57"/>	Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx
<input type="button" value="Send"/>		

Wake all clients at once:

Or Click the MAC address to wake up an individual device:

Interface	MAC address	Description					
LAN	90:84:0d:9d:fc:57	Matt's Desktop					
LAN	00:26:08:ae:b3:3a	Matt's Laptop					

Note:

This service can be used to wake up (power on) computers by sending special "Magic Packets". The NIC in the computer that is to be woken up must support Wake on LAN and has to be configured properly (WOL cable, BIOS settings).

Veja também...

- Documentação do PfSense Wake-on-LAN
http://doc.pfsense.org/index.php/Wake_on_LAN
- Artigo no Wikipedia Wake-on-LAN
<http://en.wikipedia.org/wiki/Wake-on-LAN>

Habilitando log externo (syslog server)

O **syslog** é um sistema padronizado para registrar todo o tipo de informação. Cliente syslog e implementações de servidores existem para todos os principais sistemas operacionais

A maioria das distribuições Linux já executa o serviço syslog, de modo que configurar um servidor centralizado é só questão de decidir qual máquina usar, configurar uma máquina para executar dados do syslog na rede, e depois configurar todas as máquinas direcionando mensagens de syslog para o servidor.

Aqui vamos descrever como configurar o PfSense para escrever os logs para um servidor syslog na rede.

Se preparando...

Para ligar uma maquina Windows em um servidor de syslog centralizado, dê uma olhada no Servidor de Kiwi Syslog e log viewer

Como fazê-lo...

1. Vá á **Status | System Logs**
2. Clique na aba **Settings**.
3. Marque **Enable syslog'ing to remote syslog server**
4. Em **remote syslog servers** você pode digitar até três servidores de log remoto
5. Marque **Everything** para gravar todas as mensagens, ou marque apenas o que lhe interessar.

The screenshot shows the 'Enable syslog'ing to remote syslog server' configuration page. At the top, there is a checked checkbox labeled 'Enable syslog'ing to remote syslog server'. Below it, under 'Remote syslog servers', there is a list of three servers: 'Server 1' with IP '192.168.1.231', 'Server 2', and 'Server 3'. A note below says 'IP addresses of remote syslog servers'. Underneath the servers, there is a list of event types with checkboxes: 'system events', 'firewall events', 'DHCP service events', 'Portal Auth', 'PPTP VPN events', and 'Everything'. The 'Everything' checkbox is checked. At the bottom of the page is a large 'Save' button and a note: 'Note: syslog sends UDP datagrams to port 514 on the specified remote syslog server. Be sure to set syslogger on the remote server to accept syslog messages from pfSense.'

6. Clique em **Save**

Como ele funciona...

Ao escrever os logs para um servidor externo syslog, isso pode ter um efeito muito positivo sobre o PfSense já que não consome muita memoria e espaço em disco.

Há mais...

Se você não configurar um servidor de log externo, você tem as seguintes opções de registro interno disponíveis no PfSense:

- Mostrar logs de entrada em ordem inversa (as mais recentes ficam no topo)
- Numero de entrada de logs
- Log de pacotes bloqueados na regra padrão
- Mostra logs de filtros
- Desabilita a gravação de arquivos de log do disco para memoria RAM

Status: System logs: Settings

?

The screenshot shows the 'System logs: Settings' page of the PfSense web interface. At the top, there is a navigation bar with tabs: System, Firewall, DHCP, Portal Auth, IPsec, PPP, VPN, Load Balancer, OpenVPN, OpenNTPD, and Settings. The 'Settings' tab is currently selected. Below the navigation bar, there is a checkbox labeled 'Show log entries in reverse order (newest entries on top)'. A text input field shows 'Number of log entries to show:' with the value '50'. There are three main configuration sections: 1) 'Log packets blocked by the default rule' (checkbox checked, hint: packets that are blocked by the implicit default block rule will not be logged anymore if you uncheck this option. Per-rule logging options are not affected). 2) 'Show raw filter logs' (checkbox unchecked, hint: If this is checked, filter logs are shown as generated by the packet filter, without any formatting. This will reveal more detailed information). 3) 'Disable writing log files to the local RAM disk' (checkbox unchecked).

Veja também...

- Documentação de Configuração de Log no PfSense
http://doc.pfsense.org/index.php/Log_Settings
- Artigo no Wikipédia sobre Syslog
<http://en.wikipedia.org/wiki/Syslog>
- Kiwi Syslog Server and Log Viewer
<http://www.kiwisyslog.com/>

Usando o ping

O PfSense habilita o serviço de ping que está incluso em quase todos os sistemas operacionais. Isso pode ser útil para os administradores fazerem teste de ping do PfSense para outra máquina qualquer a partir de qualquer interface especificada. Aqui vamos descrever como configurar o serviço de ping do PfSense.

Como fazê-lo...

1. Vá em **Diagnostics | Ping**
2. Em **Host** digite o endereço de IP ou o host do qual você quer fazer o teste
3. Em **Interface** selecione a interface da qual o host ou o endereço de IP está ligado
4. Em **count** selecione a quantidade de pacotes que você quer fazer o teste

Diagnostics: Ping

?

Ping

Host	192.168.1.101
Interface	LAN ▾
Count	3 ▾
Ping	

5. Clique no botão **Ping**

Diagnostics: Ping

?

Ping

Host	192.168.1.101
Interface	LAN ▾
Count	3 ▾
Ping	

Ping output:

```
PING 192.168.1.101 (192.168.1.101) from 192.168.1.1: 56 data bytes
64 bytes from 192.168.1.101: icmp_seq=0 ttl=64 time=0.433 ms
64 bytes from 192.168.1.101: icmp_seq=1 ttl=64 time=0.441 ms
64 bytes from 192.168.1.101: icmp_seq=2 ttl=64 time=0.405 ms
```

```
-- 192.168.1.101 ping statistics --
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.405/0.426/0.441/0.015 ms
```

Como ele funciona...

O utilitário ping permite aos administradores fazer teste de ping de qualquer interface, para qualquer interface. O ping é uma ferramenta indispensável e ter ela na interface web do PfSense é uma ótima função.

Veja também...

- Documentação do PfSense sobre Ping e Host
http://doc.pfsense.org/index.php/Ping_Host
- Artigo no Wikipédia sobre Ping
<http://en.wikipedia.org/wiki/Ping>

Usando traceroute

O PfSense usa o serviço de traceroute incluso em quase todos os sistemas operacionais. Isso pode ser útil para administradores que querem realizar um traceroute ad-hoc

Vamos descrever agora como usar o utilitário traceroute do PfSense

Como fazê-lo...

1. Vá á **Diagnostics | Traceroute**
2. Em **host** digite o IP ou o host que você deseja traçar a rota
3. Em **Maximum number of hops** você pode especificar a quantidade de saltos que o traceroute pode fazer
4. Você pode marcar o **Use ICMP** se quiser

Diagnostics: Traceroute

?

Traceroute	
Host	<input type="text" value="google.com"/>
Maximum number of hops	<input type="text" value="18"/> ▾
Use ICMP	<input type="checkbox"/>
Traceroute	

Note:Traceroute may take a while to complete. You may hit the Stop button on your browser at any time to see the progress of failed traceroutes.

5. Clique no botão **traceroute**

Diagnostics: Traceroute

?

Traceroute	
Host	<input type="text" value="google.com"/>
Maximum number of hops	<input type="text" value="18"/> ▾
Use ICMP	<input type="checkbox"/>
Traceroute	

Note: Traceroute may take a while to complete. You may hit the Stop button on your browser at any time to see the progress of failed traceroutes.

Traceroute output:

```
1 10.240.176.13 (10.240.176.13) 9.819 ms 6.781 ms 5.817 ms
2 dstswr2-vlan2.rh.nbrgnj.cv.net (67.83.246.162) 7.783 ms 8.320 ms 6.748 ms
3 rtr2-ge1-14.mhe.prnynj.cv.net (67.83.246.133) 9.923 ms 9.245 ms 9.716 ms
4 64.15.2.81 (64.15.2.81) 12.427 ms 11.448 ms 10.172 ms
5 64.15.0.249 (64.15.0.249) 12.698 ms
   64.15.0.145 (64.15.0.145) 11.861 ms 11.655 ms
6 * * *
7 72.14.238.232 (72.14.238.232) 12.564 ms 11.508 ms 14.527 ms
8 216.239.48.92 (216.239.48.92) 13.084 ms 11.738 ms 9.703 ms
9 lga15s16-in-f104.1e100.net (173.194.35.104) 10.809 ms 13.138 ms 11.576 ms
```

Note: Multi-wan is not supported from this utility currently.

Como ele funciona...

O utilitário traceroute permite aos administradores realizar um rastreamento de rotas diretamente pela interface web.

O traceroute pode levar um tempo longo para ser concluído. Você pode clicar em cancelar a qualquer momento.

Veja também...

- Documentação do PfSense sobre Traceroute
<http://doc.pfsense.org/index.php/Traceroute>
- Artigo no Wikipédia sobre o Traceroute
<http://en.wikipedia.org/wiki/Traceroute>

Fazer backup do arquivo de configuração

Fazer backup dos arquivos de configuração é uma parte essencial de qualquer administrador. Aqui vamos descrever como fazer o backup do arquivo de configuração no PfSense.

Se preparando...

Os arquivos de configuração do PfSense são armazenados em um formato de texto simples XML por padrão. Mas também tem a opção de ser criptografado.

Como fazê-lo...

1. Vá á **Diagnostics | Backup/Restore**
2. Clique na aba **Backup/Restore**
3. Em **Backup área** selecione **All**. Para obter o backup de toda a lista de opções, se você quiser fazer backup de algumas opções somente, confira a baixo a lista de **Áreas de backup**.
4. Deixe **Do not backup package information** desmarcado, se você marcar não será salvo a lista de pacotes instalados no seu PfSense.
5. Deixe **Do not backup RRD data** marcado, se você deixar desmarcado vai ser salvo todo o histórico de tráfego feito pelo PfSense, e com isso o arquivo vai ficar muito grande, e não é o caso.

Diagnostics: Backup/restore



Config History **Backup/Restore**

Backup configuration

Click this button to download the system configuration in XML format.

Backup area: **ALL** ▾

Do not backup package information.
 Encrypt this configuration file.
 Do not backup RRD data (NOTE: RRD Data can consume 4+ megabytes of config.xml space!)

Download configuration

6. Clique em **Download configuration**.
7. Selecione o local que você vai querer salvar.

You have chosen to open
...ig-pfsense.bunkerhollow.com-20101205144603.xml
which is a: XML document
from: <http://pfsense.bunkerhollow.com>

What should Firefox do with this file?

Open with **Firefox Web Browser (default)** ▾
 Save File
 Do this automatically for files like this from now on.

Cancel **OK**

Como ele funciona...

O PfSense permite que um administrador possa transferir configurações feitas no PfSense inteiro em um arquivo único no formato XML, para qualquer lugar do teu computador ou rede.

Há mais...

Algumas senhas configuradas no PfSense vão aparecer no arquivo em texto puro! Se isso pode ser uma preocupação então na hora que você for fazer o backup, deixe marcada a opção **Encrypt this configuration file**, e então digite uma senha em **Password**.

Diagnostics: Backup/restore

?

The screenshot shows the 'Backup configuration' section of the 'Backup/Restore' tab in the 'Diagnostics' menu. A red header bar at the top says 'Backup configuration'. Below it, a message says 'Click this button to download the system configuration in XML format.' A dropdown menu labeled 'Backup area:' has 'ALL' selected. There are three checkboxes: one unchecked 'Do not backup package information.', one checked 'Encrypt this configuration file.', and one checked 'Do not backup RRD data (NOTE: RRD Data can consume 4+ megabytes of config.xml space!)'. Below these are two password input fields, each showing a lock icon and several dots. A large 'Download configuration' button is at the bottom.

Áreas de backup

Na versão atual do PfSense 2.0 que o livro foi lançado, as seguintes áreas para backup estão disponíveis:

- ALL
- Aliases
- DNS Forwarder
- DHCP Server
- Firewall Rules
- Interface
- IPSec
- NAT
- Package Manager
- PPTP Server
- Scheduled Tasks
- Syslog
- System
- System Tunables

- SNMP Server

Veja também...

- Documentação sobre configuração no PfSense sobre Backup/Restore
http://doc.pfsense.org/index.php/Configuration_Backup_and_Restore

Restaurando o backup do arquivo de configuração

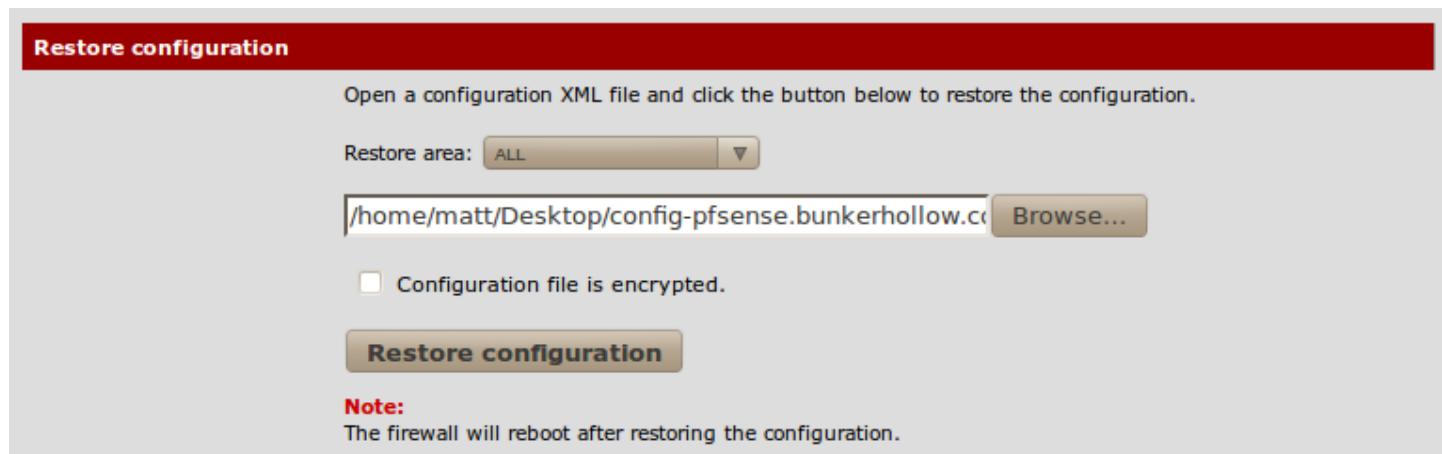
Aqui vamos descrever como restaurar o arquivo de backup das configurações salvas.

Se preparando...

Restauração de arquivos de configuração é uma parte essencial na administração de um PfSense. Os arquivos de configuração são armazenados em um formato de texto simples XML padrão, mas também pode ser criptografado se for marcado no instante que for feito do backup.

Como fazê-lo...

1. Vá a **Diagnostics | Backup/Restore**
2. Clique na aba **Backup/Restore**
3. Em **Restore área** selecione **All**. Para obter a restauração de toda a lista de opções, se você quiser fazer a restauração de algumas opções somente, confira a baixo a lista de **Áreas de restauração**.



The screenshot shows the 'Restore configuration' page. At the top, a red header bar reads 'Restore configuration'. Below it, a message says 'Open a configuration XML file and click the button below to restore the configuration.' A dropdown menu labeled 'Restore area:' is set to 'ALL'. A text input field contains the path '/home/matt/Desktop/config-pfsense.bunkerhollow.com'. To its right is a 'Browse...' button. Below the input field is a checkbox labeled 'Configuration file is encrypted.' A large brown button at the bottom is labeled 'Restore configuration'. Underneath the button, a note states: 'Note: The firewall will reboot after restoring the configuration.'

4. Clique em **Restore configuration** e espere o PfSense reiniciar.

Diagnostics: Backup/restore

?



A red message box appears with a yellow exclamation mark icon. The text inside says: 'The firewall configuration has been changed. The firewall is now rebooting.' In the bottom right corner of the box is a 'Close' button.

Como ele funciona...

O PfSense permite que um administrador possa restaurar as configurações feitas no PfSense a partir de um arquivo XML.

Há mais...

Se o arquivo de configuração foi criptografado na hora do backup, não esqueça de deixar marcada a opção **Configuration file is encrypted**, e digite a senha que foi digitada na hora do backup em **Password**.

Restore configuration

Open a configuration XML file and click the button below to restore the configuration.

Restore area: ▾

Configuration file is encrypted.

Password :

confirm :

Note:
The firewall will reboot after restoring the configuration.

Áreas de restauração

Na versão atual do PfSense 2.0 que o livro foi lançado, as seguintes áreas para restauração estão disponíveis:

- ALL
- Aliases
- Captive Portal
- Captive Portal Vouchers
- DNS Forwarder
- DHCP Server
- Firewall Rules
- Interface
- IPSec
- NAT
- OpenVPN
- Package Manager
- PPTP Server
- Scheduled Tasks
- Static Routes
- Syslog
- System
- System Tunables

- SNMP Server
- Traffic Shaper
- VLANs
- Wake on LAN

Veja também...

- Documentação sobre configuração no PfSense sobre Backup/Restore
http://doc.pfsense.org/index.php/Configuration_Backup_and_Restore

Configurando o backup automático do arquivo de configuração

Aqui vamos descrever como configurar o backup automático do arquivo de configuração do PfSense

Se preparando...

Os usuários com uma assinatura de suporte PfSense pode configurar um backup automatizado para servidores PfSense externo usando suas credenciais de login no portal.pfsense.org. Atualmente somente assinantes pagos podem ter suporte a esse recurso.

Como fazê-lo...

1. Vá a **Diagnostics | AutoConfigBackup**
2. Clique na aba **Settings**
3. Digite seu nome de usuário em **Subscription Username**
4. Digite sua senha em **Subscription Password**
5. Confirme sua senha em **Subscription Password**
6. Digite sua senha criptografada em **Encryption Password**
7. Confirme sua senha criptografada **Encryption Password**

Diagnostics: Auto Configuration Backup

?

Settings Restore Backup now Stats

Subscription Username	<input type="text" value="johndoe"/>	Enter the subscription username for portal.pfsense.org
Subscription Password	<input type="password"/>	Enter the password for portal.pfsense.org
Enter Password again	<input type="password"/>	
Encryption Password	<input type="password"/>	This password will be used to encrypt config.xml before sending to portal.pfsense.org. Do not share the password and keep it safe!
Encryption Password again	<input type="password"/>	Enter the encryption password again.
Test connection	<input type="checkbox"/>	Check this box to test the connection to portal.pfsense.org.

Change

8. Clique em **Save**

Como ele funciona...

Backups automatizados podem agora ser armazenados de forma segura em um conjunto de servidores externos. Isso é conveniente quando que o administrador tenha um local externo para backup das configurações.

Veja também...

- Documentação do PfSense sobre automatização de Configuração de Backup
<http://doc.pfsense.org/index.php/AutoConfigBackup>
- PfSense Portal Premium
<https://portal.pfsense.org/>

Atualização do firmware do PfSense

Aqui vamos descrever como atualizar o firmware do PfSense.

Se preparando...

Temos que fazer o backup do PfSense antes de começar a atualização.

Como fazê-lo...

1. Vá a **System | Firmware**
2. Clique na aba **Auto Update**

3. Clique em **Invoke Auto Upgrade**

System: Firmware: Auto Update

The screenshot shows the 'Auto Update' tab selected in the navigation bar. A message box displays the following information:

A new version is now available
Current version: 2.0-BETA4
NanoBSD Size : 1g
Built On: Sat Dec 4 02:44:21 EST 2010
New version: Sun Dec 5 07:23:23 EST 2010
Update source: http://snapshots.pfsense.org/FreeBSD_RELENG_8_1/i386/pfSense_HEAD/.updaters/

Below the message box is a button labeled 'Invoke Auto Upgrade'.

4. Observe o Status do download

Diagnostics: Firmware: Auto Update

The screenshot shows the 'Auto Update' tab selected in the navigation bar. A message box displays the following information:

Downloading updates...
Auto Update Download Status

Current Version : 2.0-BETA4
Latest Version : Sun Dec 5 07:23:23 EST 2010
File size : 62090020
Downloaded : 11027937
Percent : 18%

5. Quando o download estiver completo, o PfSense irá atualizar e reiniciar

Diagnostics: Firmware: Auto Update

The screenshot shows the 'Auto Update' tab selected in the navigation bar. A message box displays the following information:

Downloading updates...
pfSense is now upgrading.
The firewall will reboot once the operation is completed.

6. No primeiro login após o sistema ter reiniciado, vamos ser redirecionado para a página **Package Manager**.

System: Package Manager: Install Package

?

```
All packages reinstalled.

Removing package...
Removing AutoConfigBackup components...
    Configuration... done.
Beginning package installation for AutoConfigBackup...
Downloading package configuration file... done.
Saving updated package information... done.

Loading package configuration... done.
    Configuring package components...
        Additional files... done.
Loading package instructions...
    Menu items... done.
    Integrated Tab items... done.
Custom commands...
    Executing custom_php_resync_config_command()...done.
Writing configuration... done.
Starting service.

All packages reinstalled.
```

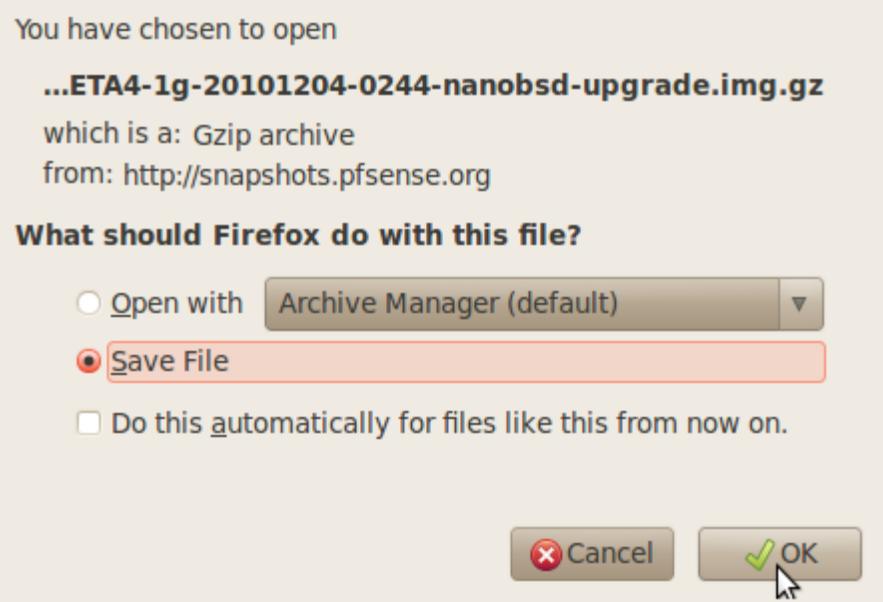
Como ele funciona...

O PfSense entrará em contato com um serviço web <http://pfsense.org/> pra fazer a verificação do firmware mais recente, e baixar se necessário.

Há mais...

O PfSense também permite a atualização do firmware manual, que vamos descrever mais a baixo:

1. Fazer o download da versão mais recente em <http://pfsense.org/>



2. Vá á **System | Firmware**
3. Clique na aba **Manual Update**

System: Firmware

Manual Update **Auto Update** **Updater Settings**

Invoke pfSense Manual Upgrade

Click "Enable firmware upload" below, then choose the image file (pfSense-*.img.gz) to be uploaded.
Click "Upgrade firmware" to start the upgrade process.

Enable firmware upload

Warning:
DO NOT abort the firmware upgrade once it has started. The firewall will reboot automatically after storing the new firmware. The configuration will be maintained.

4. Clique no botão **Enable firmware upload**
5. Clique em **Browse** para selecionar o local onde se encontra o arquivo baixado

System: Firmware

?

Manual Update Auto Update Updater Settings

Invoke pfSense Manual Upgrade

Click "Enable firmware upload" below, then choose the image file (pfSense-*.img.gz) to be uploaded.
Click "Upgrade firmware" to start the upgrade process.

Disable firmware upload

Firmware image file: **Browse...**

NOTE: You must upload a .img.gz image, not an uncompressed image!

Upgrade firmware

Warning:

DO NOT abort the firmware upgrade once it has started. The firewall will reboot automatically after storing the new firmware. The configuration will be maintained.

6. Clique em **Upgrade firmware**

System: Firmware

?



The firmware is now being updated. The firewall will reboot automatically.

Close

Atualização em andamento

Qualquer tentativa de acessar qualquer opção na hora que o sistema está sendo atualizado você será redirecionado para uma pagina igual que vamos mostrar logo a baixo:

System: Firmware: Manual Update

?

An upgrade is currently in progress.

The firewall will reboot when the operation is complete.



Close

Atalho para atualização do sistema

Quando uma nova versão do PfSense fica disponível, uma notificação chamada **Update available** vai aparecer na tela **Status Dashboard** na pagina inicial do PfSense.

The screenshot shows the PfSense Status Dashboard. At the top, there's a navigation bar with links to System, Interfaces, Firewall, Services, and other status pages. Below the navigation is the title "Status: Dashboard". Underneath the title is a toolbar with icons for system status, configuration, and help. A main content area contains a table titled "System Information". The table has two rows: "Name" (pfSense.bunkerhollow.com) and "Version" (2.0-BETA4 (i386), built on Sat Dec 4 02:44:21 EST 2010). In the "Version" row, there is a red link "Update available. Click Here to view update." with a cursor icon pointing at it. There are also close and minimize buttons in the top right corner of the table header.

System Information	
Name	pfSense.bunkerhollow.com
Version	2.0-BETA4 (i386) built on Sat Dec 4 02:44:21 EST 2010

Veja também...

- Fazer backup do arquivo de configuração
- Documentação do PfSense sobre atualização do Firmware
http://doc.pfsense.org/index.php/Firmware_Updates

A

Monitoramento e Registros

Nesse capítulo, iremos abordar:

- Personalizar a tela de Status Dashboard
- Monitoramento de tráfego em tempo real
- Configurando SMTP de e-mail de notificação
- Vendo os logs do sistema
- Configurando um servidor de syslog externo
- Visualizações de gráficos RRD
- Visualizações de mapeamentos DHCP
- Monitoramento de filtro de pacotes com PflInfo
- Monitoramento de tráfego com PfTop
- Monitoramento da atividade do sistema

Introdução

Uma vez que o PfSense está instalado e funcionando, é importante compreender a maneira correta de monitoramento do sistema. Aprender a usar o monitor de Status e ferramentas de medição construídas pelo próprio PfSense vai tornar a vida de um administrador muito mais fácil. Vamos descrever a seguir como monitorar e visualizar a maioria dos recursos disponíveis dentro do PfSense.

Personalizar a tela de Status Dashboard

Aqui vamos descrever como personalizar e configurar a tela de **Status Dashboard**

Como fazê-lo...

1. Vá á **Status | Dashboard**
2. Clique no botão “+” para adicionar um novo widget

Status: Dashboard

?

The screenshot shows the 'Status: Dashboard' interface. On the left, a sidebar titled 'Available Widgets' lists various monitoring options like Captive Portal Status, Carp Status, Gateways, Gmirror Status, Installed Packages, Interface Statistics, Interfaces, Ipsec, Load Balancer Status, Firewall Logs, OpenVPN, Picture, Rss, Services Status, System Information, Traffic Graphs, and Wake On Lan. Below this is a 'Current date/time' section showing 'Sun Jan 9 14:29:07 EST 2011'. On the right, there's a 'Traffic Graphs' section with three tabs: 'Current WAN Traffic', 'Current LAN Traffic', and 'Current PUB Traffic'. The 'Current WAN Traffic' tab is active, displaying traffic statistics (In: 481 Kbps, Out: 485 Kbps) and a graph showing traffic over time. The graph has a red line representing the current traffic level, with horizontal grid lines at 200, 400, and 600 Kbps.

3. Clique no botão “chave” para fazer configurações especiais do widget

This screenshot shows the configuration dialog for the 'Traffic Graphs' widget. It includes a 'Save Settings' button, a 'Refresh Interval' dropdown set to '10 Seconds', and a note about increasing CPU utilization if the interval is changed. The 'Current WAN Traffic' tab is selected, showing traffic stats (In: 504 Kbps, Out: 491 Kbps) and a graph. The graph has a red line representing the current traffic level, with horizontal grid lines at 200, 400, and 600 Kbps. Below the WAN traffic are tabs for 'Current LAN Traffic' and 'Current PUB Traffic', both of which have checkboxes next to them.

4. Clique no botão “minimizar” para recolher o widget, ou clique no botão “fechar” para remover o widget da tela.
5. Você pode clicar no título do widget e arrastar para mudar sua posição na tela

The screenshot shows the PfSense 2.0 Status Dashboard. At the top, there are icons for a plus sign, a question mark, and a gear, followed by a "Save Settings" button. Below these are two main sections: "System Information" and "Services Status".

System Information: Shows basic system details like RAM, CPU, and disk usage.

Services Status: A table listing services with their descriptions and status. All listed services are running:

Service	Description	Status
dnsmasq	DNS Forwarder	Running
ntpd	NTP clock sync	Running
dhcpcd	DHCP Service	Running
miniupnpd	UPnP Service	Running

Traffic Graphs: This section displays real-time traffic graphs for WAN, LAN, and PUB interfaces. The WAN graph shows current traffic levels of 526 Kbps (In) and 487 Kbps (Out). The LAN and PUB graphs show their respective interface details and connection speeds.

6. Clique em **Save Settings**
7. Clique em **Apply Changes**

Como ele funciona...

O painel de status entre muitos outros novos recursos são adicionados no PfSense 2.0.

Personalizando o painel para mostrar as informações que somente lhe interessa, a administração fica muito mais fácil. Se configurado corretamente, o painel de status fica sendo a única pagina que você precisa acessar para realizar muitas tarefas comuns.

Há mais...

Muito dos widgets disponíveis no painel de status tem um item correspondente a ele no menu **Status**

Monitoramento de tráfego em tempo real

Vamos configurar o monitoramento de entrada e saída de tráfego em tempo real no PfSense.

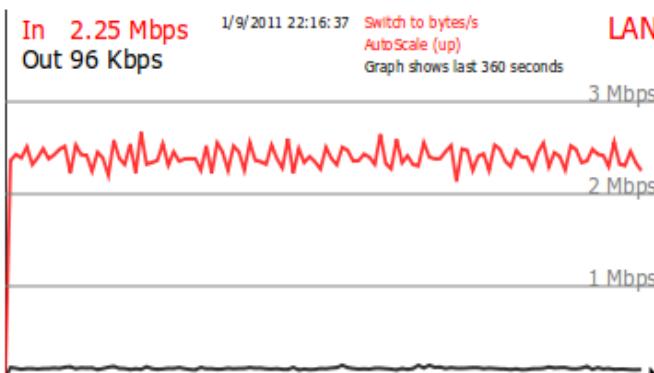
Como fazê-lo...

1. Vá a **Status | Traffic Graph**
2. Em **Interface** selecione a interface que você deseja monitorar

Status: Traffic Graph

?

Interface: LAN ▾



Host IP	Bandwidth In	Bandwidth Out
172.22.22.202	90.24k Bits/sec	2.17M Bits/sec

Note: the [Adobe SVG Viewer](#), [Firefox 1.5 or later](#) or other browser supporting SVG is required to view the graph.

Como ele funciona...

O **Traffic graph** mostra o tráfego de informações em tempo real do que passa da interface para interface. E a tabela a direito do tráfego mostra as informações de tráfego de cada dispositivo conectado que esteja usando na rede.

Seu navegador deve suportar gráficos SVG, eu recomendo o Mozilla Firefox que já vem instalado de padrão no navegador, mas se você preferir usar outro navegador você deve instalar o Adobe SVG Viewer.

Veja também...

- Documentação sobre Traffic Graph no PfSense
http://doc.pfsense.org/index.php/Traffic_Graph
- Adobe SVG Viewer
<http://www.adobe.com/svg/viewer/install/>

Configurando SMTP de e-mail de notificação

Aqui vamos descrever como configurar o SMTP para envio de e-mails de notificação

Se preparando...

Enviar e-mails do PfSense requer acesso a um servidor SMTP

Como fazê-lo...

1. Vá à **System | Advanced**
2. Clique na aba **Notifications**
3. Digite o IP ou o host do servidor de SMTP em **IP Address of the E-Mail server**

4. Digite a porta que o servidor de SMTP usa em **SMTP Port of the E-Mail server**
5. Digite o e-mail que você está usando como remetente em **From e-Mail address**
6. Digite o e-mail que você quer mandar as notificações em **Notification E-Mail address**
7. Digite o nome de usuário que você usa para logar no e-mail de remetente em **Notification E-Mail auth username**
8. Digite a senha que você usa para logar no usuário digita a cima em **Notification E-Mail auth password**

SMTP E-Mail

IP Address of E-Mail server	<input type="text" value="smtp.mydomain.com"/>	This is the IP address of the SMTP E-Mail server that will be used to send notifications to.
SMTP Port of E-Mail server	<input type="text" value="25"/>	This is the port of the SMTP E-Mail server, typically 25 or 587 (submission).
From e-mail address	<input type="text" value="johndoe@mydomain.com"/>	This is the e-mail address that will appear in the from field.
Notification E-Mail address	<input type="text" value="me@mydomain.com"/>	Enter the e-mail address that you would like email notifications sent to.
Notification E-Mail auth username (optional)	<input type="text" value="johndoe"/>	Enter the e-mail address username for SMTP authentication.
Notification E-Mail auth password	<input type="password" value="*****"/>	Enter the e-mail address password for SMTP authentication.

9. Clique em **Save**
10. Clique em **Apply Changes**

Como ele funciona...

O PfSense enviará uma notificação por e-mail utilizando as informações fornecidas para notificar os administradores de eventos significativos do sistema

Há mais...

Uma vez que nossas configurações são salvas, um teste de e-mail é enviado automaticamente. Se você não receber o teste de e-mail, verifique os logs do sistema para maiores informações. Vá à **Status | System Logs** | na aba **System** procure por algo relacionado a e-mails.

Status: System logs: System

?

System Firewall DHCP Portal Auth IPsec PPP VPN Load Balancer OpenVPN OpenNTPD Settings	
Last 50 system log entries	
Jan 9 15:47:36	php: /system_advanced_notifications.php: Could not send the message to me@mydomain.com -- Error: could not connect to the host "smtp.mydomain.com": ??
Jan 9 15:46:36	check_reload_status: syncing firewall
Jan 9 15:14:40	check_reload_status: syncing firewall
Jan 9 15:13:35	sshlockout[47037]: sshlockout/webConfigurator v3.0 starting up

Vendo os logs do sistema

Aqui vamos descrever como visualizar os logs de evento do PfSense

Como fazê-lo...

1. Vá á **Status | System logs**
2. Clique na aba **Settings**
3. Deixe marcado **Show log entries in reverse order (newest entries on top)**.
4. Clique em **Save**
5. Clique na aba **DHCP** por exemplo para visualizar eventos mais recentes do DHCP

Status: System logs: DHCP

?

System Firewall DHCP Portal Auth IPsec PPP VPN Load Balancer OpenVPN OpenNTPD Settings	
Last 50 DHCP service log entries	
Jan 9 16:53:44	dhcpd: DHCPACK on 172.22.23.192 to 00:26:08:ae:b3:3a (Alexs-iPhone) via em2
Jan 9 16:53:44	dhcpd: DHCPREQUEST for 172.22.23.192 from 00:26:08:ae:b3:3a (Alexs-iPhone) via em2
Jan 9 16:53:43	dhcpd: DHCPACK on 172.22.23.197 to 90:84:0d:9d:fc:57 (Matts-iPhone) via em2
Jan 9 16:53:43	dhcpd: DHCPREQUEST for 172.22.23.197 from 90:84:0d:9d:fc:57 (Matts-iPhone) via em2
Jan 9 16:49:24	dhcpd: DHCPACK on 172.22.22.206 to 00:1b:a9:26:b8:90 via em3
Jan 9 16:49:24	dhcpd: DHCPREQUEST for 172.22.22.206 from 00:1b:a9:26:b8:90 via em3

Como ele funciona...

O PfSense registra eventos significativos e registra-los internamente. O menu **System logs** permite ver os logs gerados para ajudar a solucionar uma variedade de questões administrativas.

Nas seguintes seções descrevem como configurar os pontos de vista alternativos fornecidos pelo log de eventos do firewall.

Há mais...

As informações de log são coletadas e exibidas para os seguintes serviços:

- System
- Firewall
- DHCP

- Portal Auth
- IPSec
- PPP
- VPN
- Load Balancer
- OpenVPN
- OpenNTPD

Se o registro dos logs é feito em um servidor de log externo, não haverá nenhum dado nessa página.

Exibição normal de log do Firewall

Essa é a tela normal de visualização de log do Firewall

Status: System logs: Firewall

Last 50 firewall log entries. Max(50)						
Act	Time	If	Source	Destination	Proto	
✖	Jan 9 16:57:51	WAN	ℹ️ 69.178.94.80:26040	ℹ️ + :51413	UDP	
✖	Jan 9 16:57:50	WAN	ℹ️ 74.41.254.202:49736	ℹ️ + :47241	TCP:S	
✖	Jan 9 16:57:50	WAN	ℹ️ 80.183.1.94:17215	ℹ️ + :3929	TCP:RA	
✖	Jan 9 16:57:50	WAN	ℹ️ 91.144.113.245:50793	ℹ️ + :51413	UDP	
✖	Jan 9 16:57:50	WAN	ℹ️ 92.255.251.75:54356	ℹ️ + :52472	UDP	
✖	Jan 9 16:57:48	WAN	ℹ️ 69.178.94.80:26040	ℹ️ + :51413	UDP	

Exibição dinâmica de log do Firewall

Essa é a tela dinâmica de visualização de log do Firewall

Diagnostics: System logs: Firewall

?

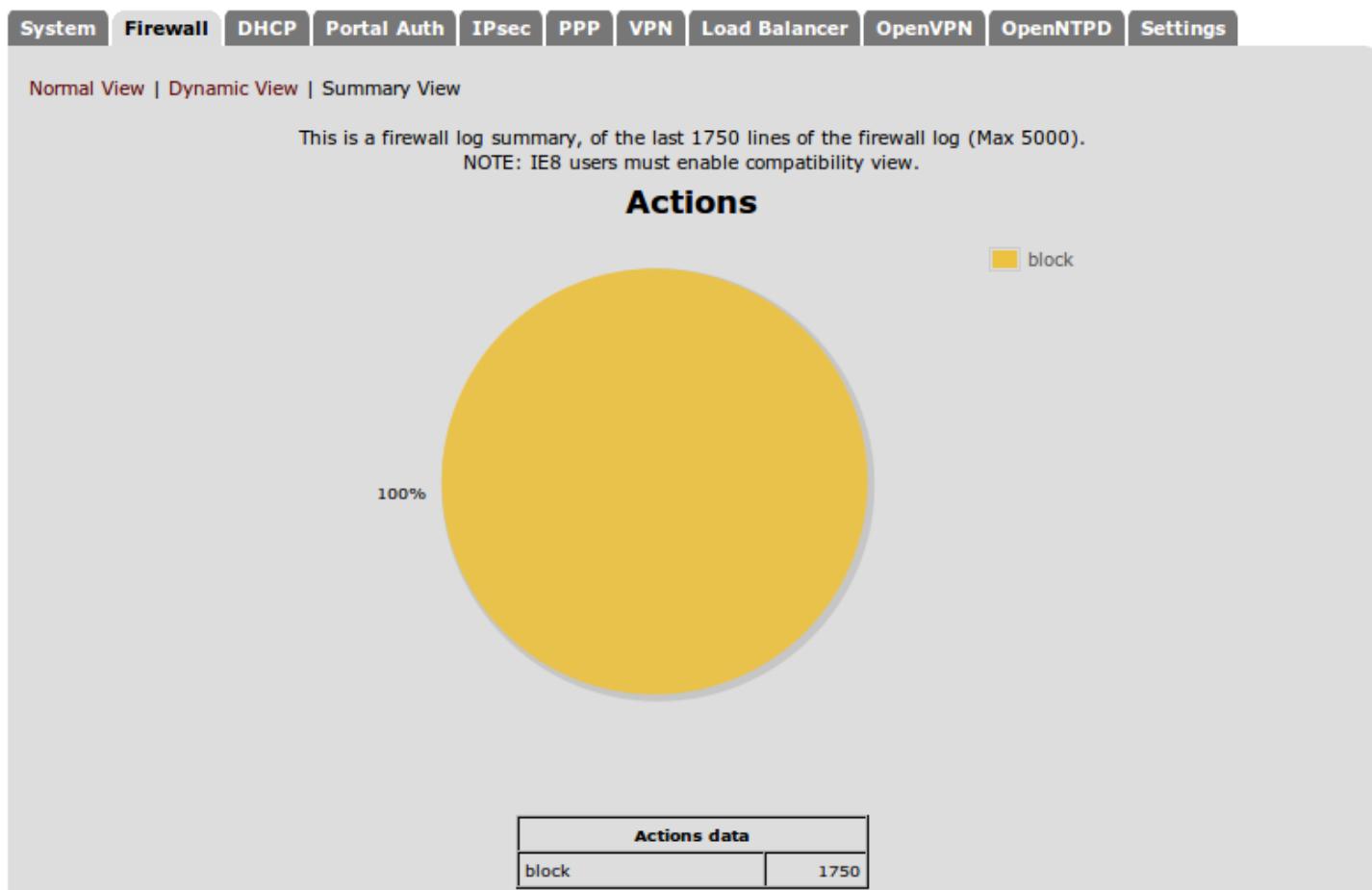
System							Firewall	DHCP	Portal Auth	IPsec	PPP	VPN	Load Balancer	OpenVPN	OpenNTPD	Settings																																
Normal View Dynamic View Summary View																																																
Last 50 records; Pause: <input type="button" value="■"/>																																																
<table border="1"><thead><tr><th>Act</th><th>Time</th><th>If</th><th>Source</th><th>Destination</th><th>Proto</th></tr></thead><tbody><tr><td>X</td><td>Jan 9 17:02:49</td><td>WAN</td><td>68.80.155.72:28286</td><td>:51413</td><td>UDP</td></tr><tr><td>X</td><td>Jan 9 17:02:49</td><td>WAN</td><td>78.30.158.253:12608</td><td>:51413</td><td>UDP</td></tr><tr><td>X</td><td>Jan 9 17:02:49</td><td>WAN</td><td>217.16.128.36:44043</td><td>:20942</td><td>UDP</td></tr><tr><td>X</td><td>Jan 9 17:02:48</td><td>WAN</td><td>10.240.176.13:67</td><td>55:68</td><td>UDP</td></tr><tr><td>X</td><td>Jan 9 17:02:48</td><td>WAN</td><td>178.37.102.45:4758</td><td>:51413</td><td>UDP</td></tr></tbody></table>													Act	Time	If	Source	Destination	Proto	X	Jan 9 17:02:49	WAN	68.80.155.72:28286	:51413	UDP	X	Jan 9 17:02:49	WAN	78.30.158.253:12608	:51413	UDP	X	Jan 9 17:02:49	WAN	217.16.128.36:44043	:20942	UDP	X	Jan 9 17:02:48	WAN	10.240.176.13:67	55:68	UDP	X	Jan 9 17:02:48	WAN	178.37.102.45:4758	:51413	UDP
Act	Time	If	Source	Destination	Proto																																											
X	Jan 9 17:02:49	WAN	68.80.155.72:28286	:51413	UDP																																											
X	Jan 9 17:02:49	WAN	78.30.158.253:12608	:51413	UDP																																											
X	Jan 9 17:02:49	WAN	217.16.128.36:44043	:20942	UDP																																											
X	Jan 9 17:02:48	WAN	10.240.176.13:67	55:68	UDP																																											
X	Jan 9 17:02:48	WAN	178.37.102.45:4758	:51413	UDP																																											

Exibição em resumo de log do Firewall

Essa é a tela de resumo de visualização de log do Firewall

Diagnostics: System logs: Firewall Log Summary

?



Veja também...

- Configurando um servidor de syslog externo
- Configurando um servidor de syslog externo

Configurando um servidor de syslog externo

Aqui vamos descrever como configurar o PfSense para usar um servidor de registro de log externo

Se preparando...

Para configurar o PfSense pra usar um servidor de registro de log externo, nós vamos precisar de um servidor separado para fazer o registro dos logs. Aqui vamos descrever como configurar um syslog em cada um dos principais sistemas operacionais.

Como fazê-lo...

1. Vá á **Status | System Logs**
2. Clique na aba **Settings**
3. marque a opção **Enable syslog'ing to remote syslog server**
4. Digite o IP do seu servidor externo
5. Marque os tipos de eventos que devem ser gerados no servidor externo

The screenshot shows the 'Status | System Logs' settings page. At the top, there is a checked checkbox labeled 'Enable syslog'ing to remote syslog server'. Below this, under 'Remote syslog servers', there is a list of three servers: 'Server 1' with IP '192.168.1.151', 'Server 2' (empty), and 'Server 3' (empty). A note below says 'IP addresses of remote syslog servers'. Underneath, there is a list of event types with checkboxes: 'system events', 'firewall events', 'DHCP service events', 'Portal Auth', 'PPTP VPN events', and 'Everything'. The 'Everything' checkbox is checked. At the bottom of the page is a 'Save' button and a note: 'Note: syslog sends UDP datagrams to port 514 on the specified remote syslog server. Be sure to set syslogd on the remote server to accept syslog messages from pfSense.'

6. Clique em **Save**
7. Clique em **Apply Changes**

Como ele funciona...

Uma vez configurado o PfSense enviará os logs dos eventos a um servidor externo, em vez de registrá-los localmente. Essa é uma ótima opção se você quiser salvar mais recursos de logs em uma maquina com capacidade de HD maior.

Executando um serviço de syslog em um Linux/Mac OS

Quase todas as distribuições Linux e MAC já incluem um serviço **syslogd**. Visite a pagina seguinte para mais informações <http://linux.die.net/man/8/syslogd>.

Executando um serviço de syslog em um Windows

Fazendo download e instalando um Servidor Kiwi Syslog para Windows em
<http://www.kiwisyslog.com>.

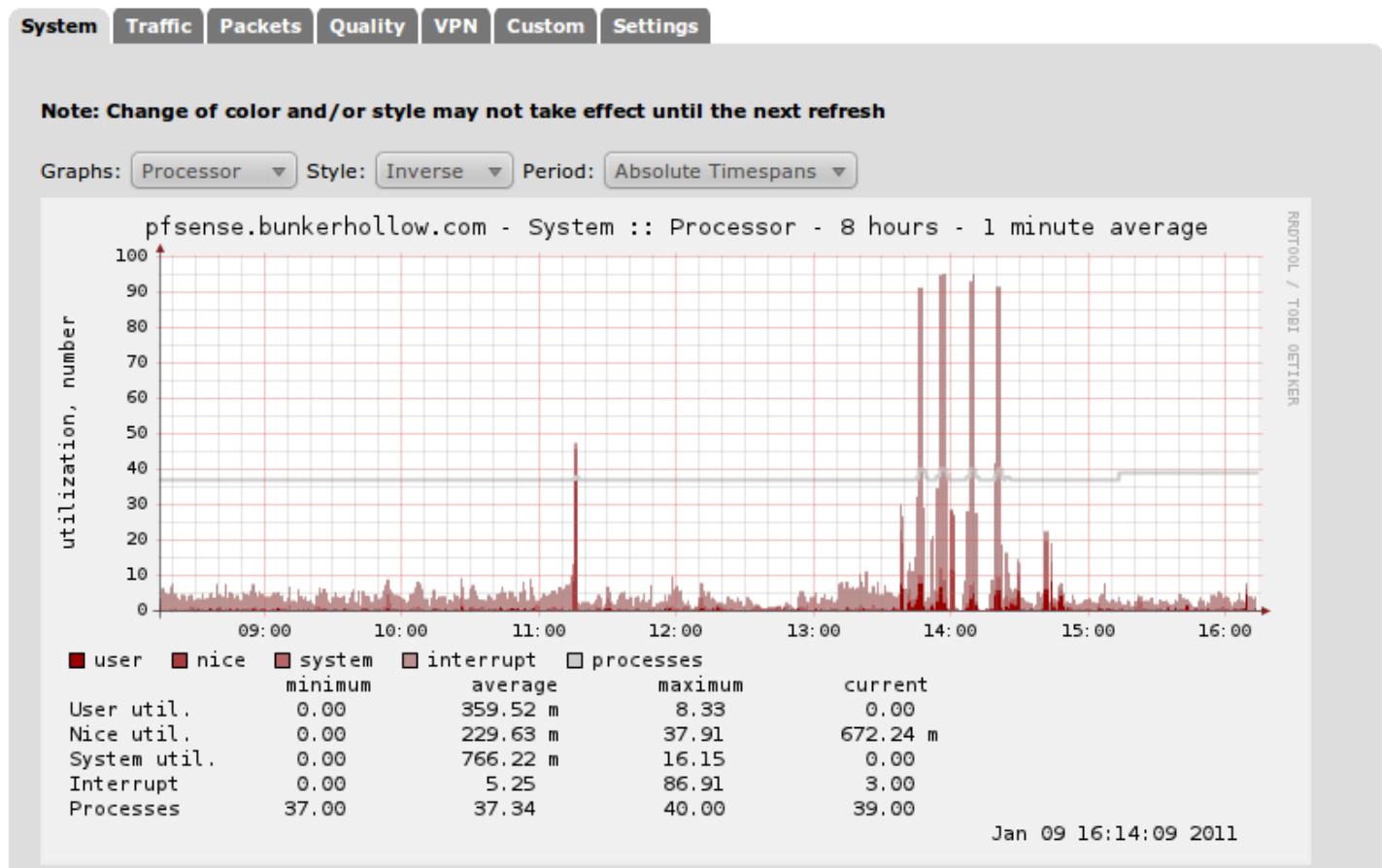
Visualizações de gráficos RRD

Aqui vamos descrever como exibir gráficos RRD no PfSense.

Como fazê-lo...

1. Vá á **Status | RRD Graphs**
2. Clique na aba **System**
3. Você pode selecionar o **Grafs, Style e Period** de acordo com o tipo de dados que você quer exibir

Status: RRD Graphs



Como ele funciona...

O PfSense registra os dados do sistema usando o conjunto de ferramentas open-source RRD para apresentar os dados graficamente na tela. Analisar os dados do sistema usando os gráficos RRD é uma ótima maneira de monitorar e solucionar problemas administrativos.

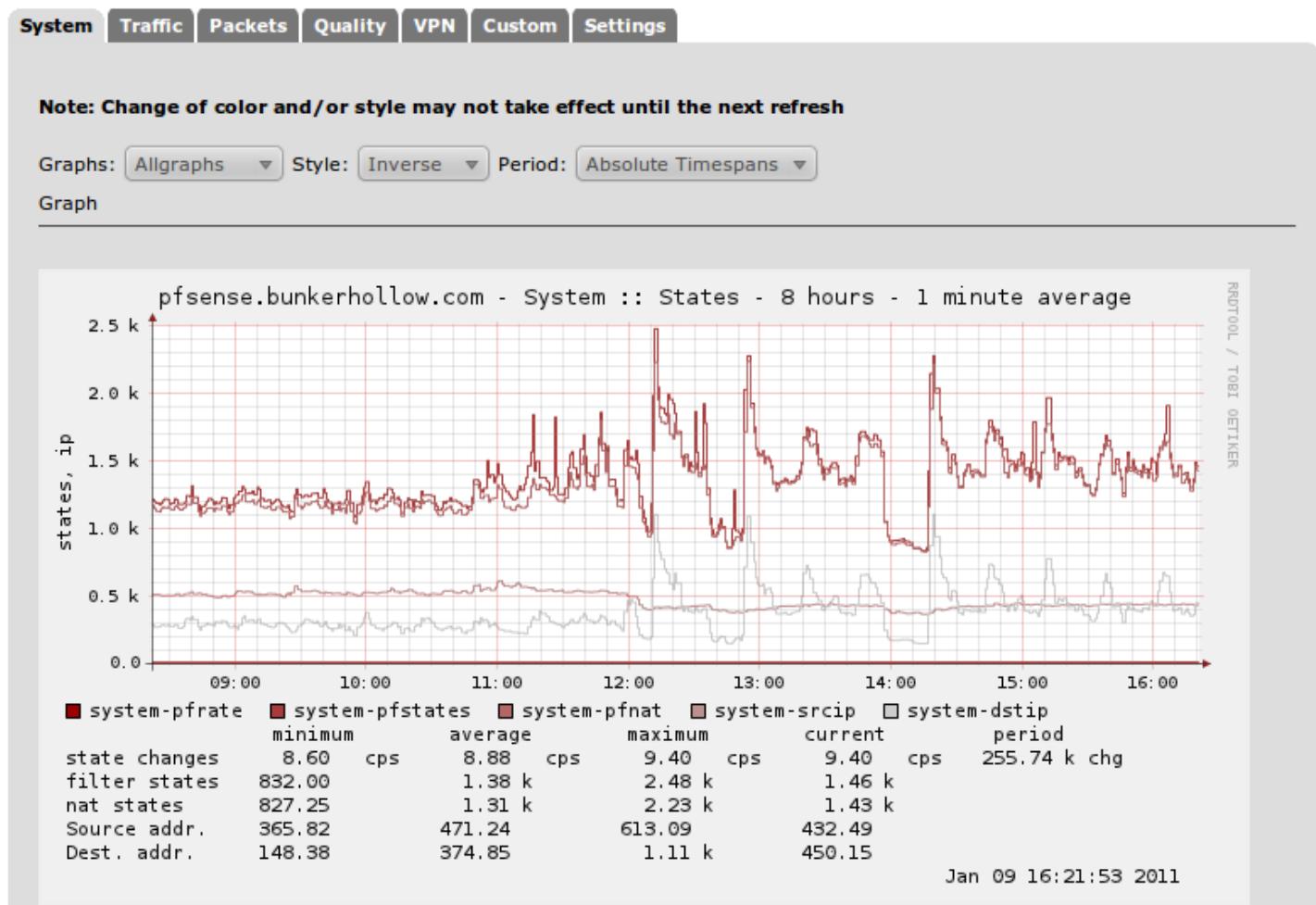
O PfSense pode analisar e exibir as seguinte informações no formato RRD

System

Na aba **System** exibe informações de hardware como:

- Throughput
- States
- Process
- Memory
- All

Status: RRD Graphs



Traffic

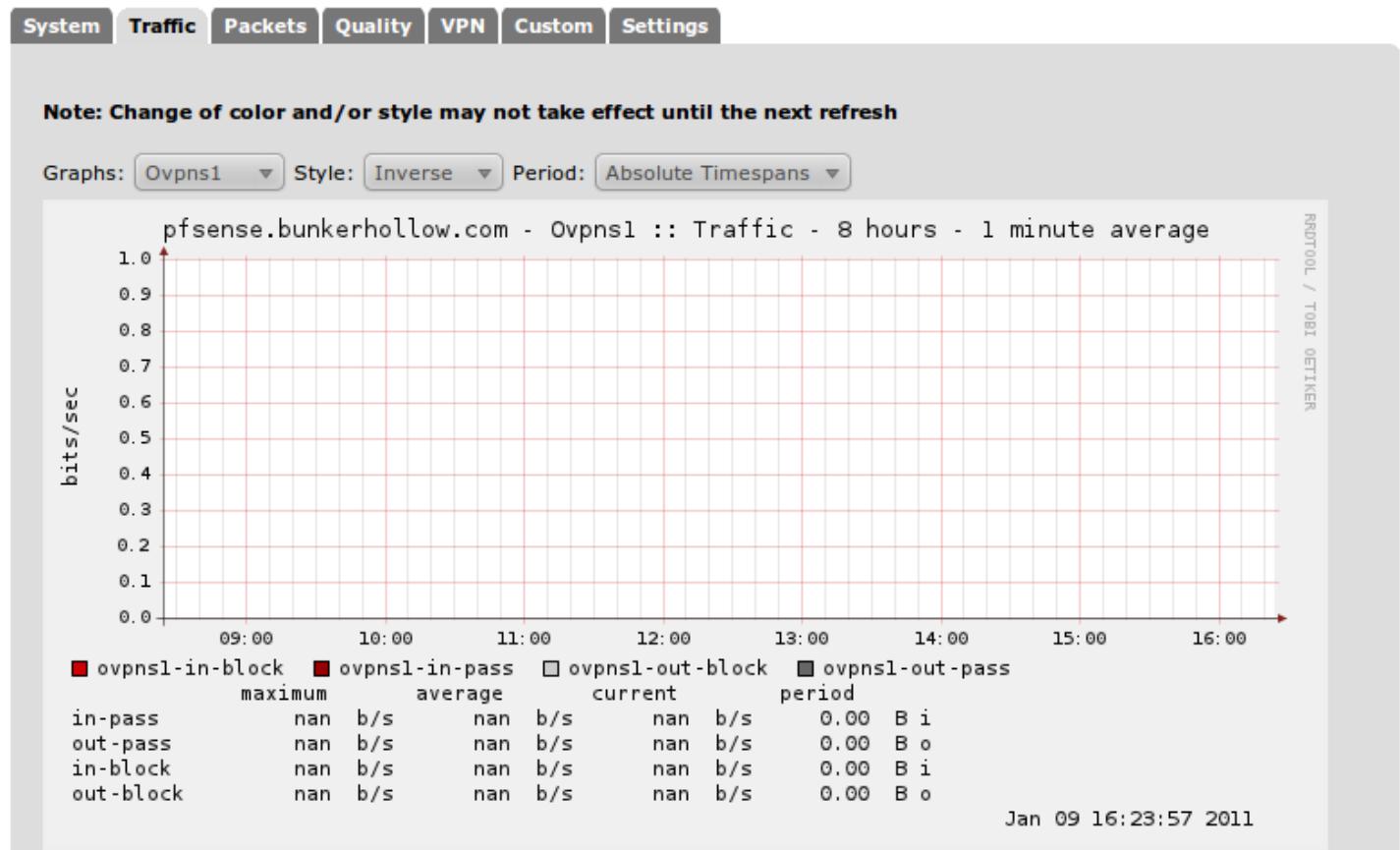
Na aba **Traffic** exibe informações sobre a rede de transferência para cada uma das interfaces do sistema.

- Outbound
- WAN
- LAN
- Optional Interface(s)
- OpenVPN
- IPSec

➤ All

Status: RRD Graphs

?



Packets

Na aba **Packets** exibe informações de pacotes de transferência para cada uma das interfaces

- Outbound
- WAN
- LAN
- Optional Interface(s)
- OpenVPN
- IPSec
- All

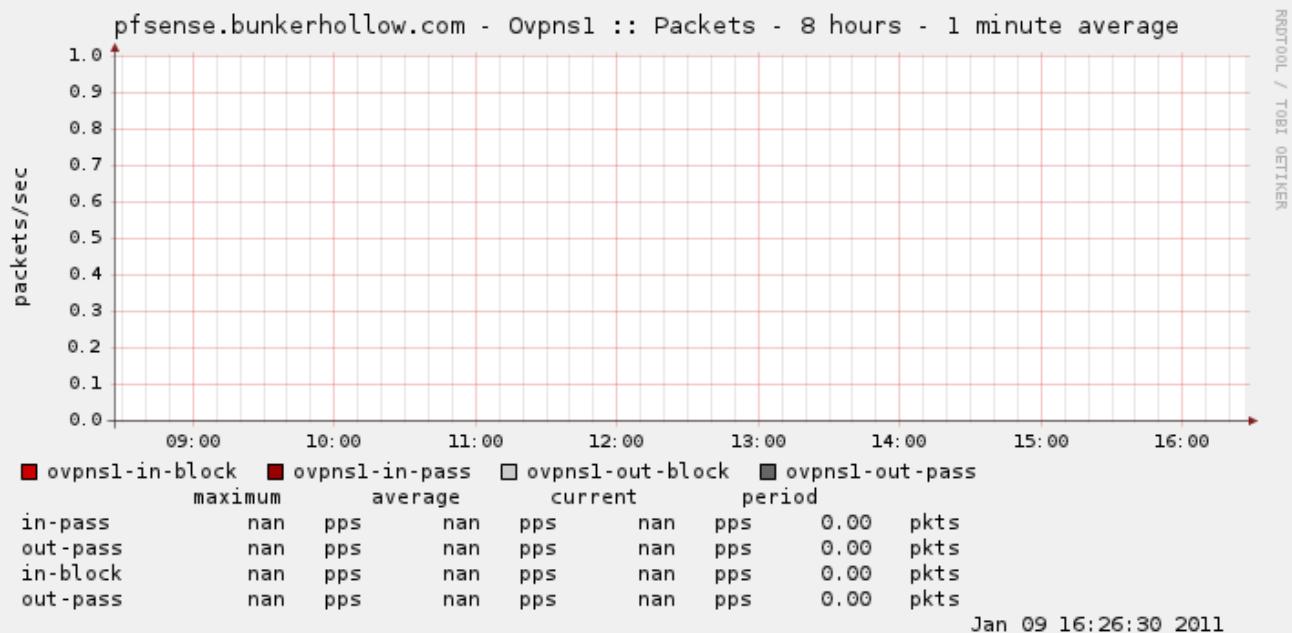
Status: RRD Graphs

?

System Traffic Packets Quality VPN Custom Settings

Note: Change of color and/or style may not take effect until the next refresh

Graphs: Ovpns1 Style: Inverse Period: Absolute Timespans



Quality

Na aba **Quality** reúne e exibe informações de perda de pacotes para cada uma das interfaces do sistema

- Outbound
- WAN
- Gateway(s)
- All

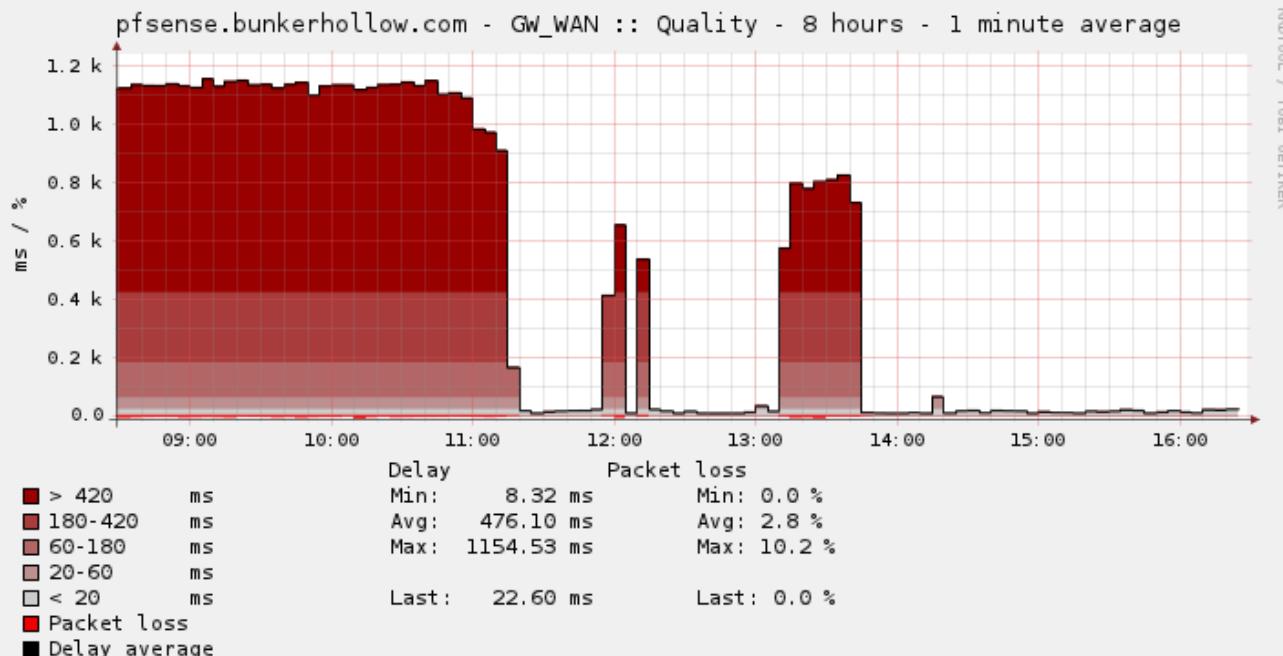
Status: RRD Graphs

?

System Traffic Packets Quality **Quality** VPN Custom Settings

Note: Change of color and/or style may not take effect until the next refresh

Graphs: GW_WAN Style: Inverse Period: Absolute Timespans



VPN

Na aba **VPN** vai exibir as informações de transferência VPN

- OpenVPN
- IPSec
- PPTP
- All

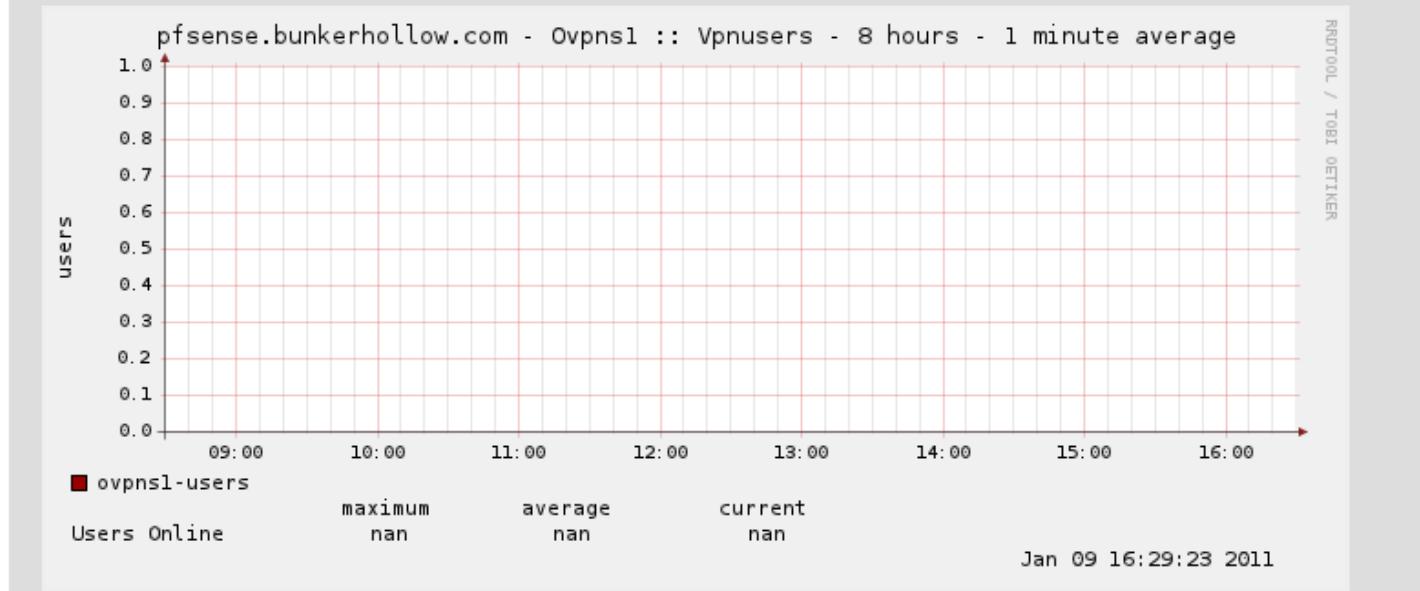
Status: RRD Graphs

?

System Traffic Packets Quality **VPN** Custom Settings

Note: Change of color and/or style may not take effect until the next refresh

Graphs: Ovpns1 Style: Inverse Period: Absolute Timespans



Personalizado

Escolha qualquer gráfico anterior para editar cada etapa

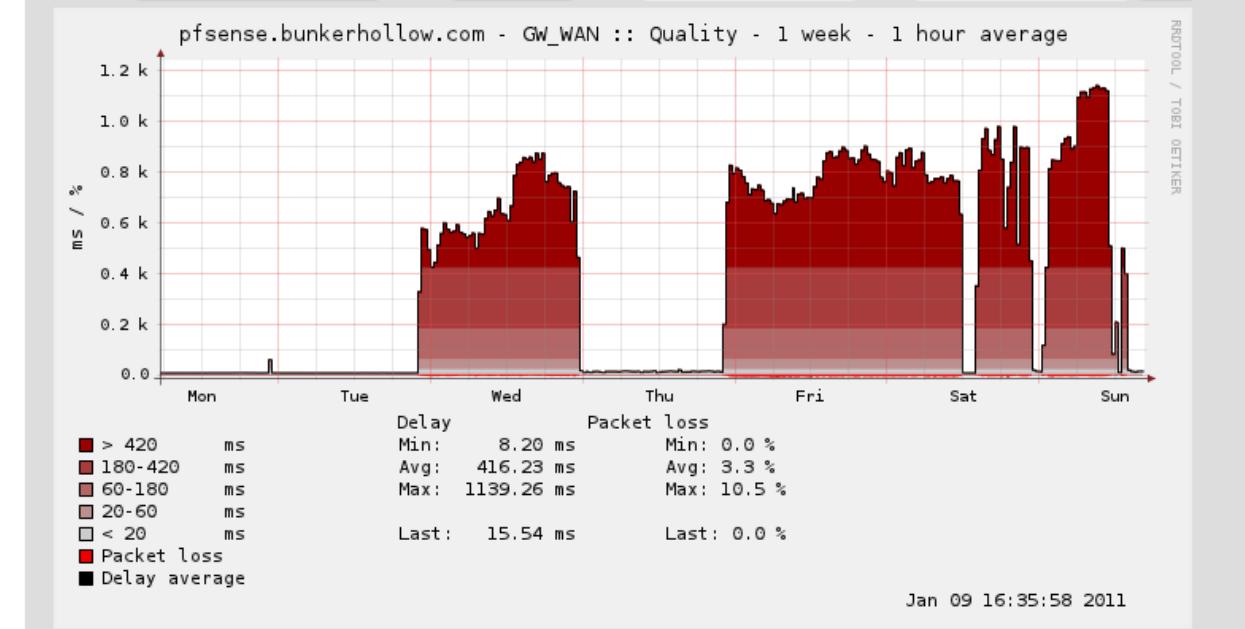
Status: RRD Graphs

?

System Traffic Packets Quality **VPN** Custom Settings

Note: Change of color and/or style may not take effect until the next refresh

Graphs: GW_WAN :: Quality Style: Inverse Start: 1294049972 End: 1294608958 Go



Visualizações de mapeamentos DHCP

Aqui vamos descrever como visualizar os mapeamentos DHCP do servidor

Como fazê-lo...

1. Vá á **Status | DHCP Leases**

Status: DHCP leases



IP address	MAC address	Hostname	Start	End	Online	Lease Type	
172.22.23.197	90:84:0d:9d:fc:57	Matts-iPhone	2011/01/09 20:56:00	2011/01/10 20:56:00	online	active	
172.22.23.199	00:1d:e0:a7:8e:c5	Thinkpad	2011/01/09 20:35:54	2011/01/09 22:35:54	offline	active	
172.22.23.192	00:26:08:ae:b3:3a	Alexs-iPhone	2011/01/09 20:24:25	2011/01/10 20:24:25	offline	active	
172.22.22.199	00:26:4a:18:81:a0		2011/01/09 11:12:07	2011/01/10 11:12:07	offline	active	
172.22.23.102	00:0e:08:db:08:0a	phone103	2011/01/09 20:23:45	2011/01/09 22:23:45	online	active	
172.22.22.200	00:1c:c0:51:a8:d8	tigas	n/a	n/a	online	static	
172.22.22.201	00:19:3c:3c:02:1e	raid	n/a	n/a	offline	static	
172.22.22.202	00:1e:37:8a:cc:43	t61p	n/a	n/a	online	static	

2. Por padrão só aparecem mapeamentos, ativos e estáticos, para ver os mapeamentos expirados, clique no botão **Show all configured leases**

Status: DHCP leases



IP address	MAC address	Hostname	Start	End	Online	Lease Type	
172.22.23.197	90:84:0d:9d:fc:57	Matts-iPhone	2011/01/09 20:56:00	2011/01/10 20:56:00	online	active	
172.22.23.199	00:1d:e0:a7:8e:c5	Thinkpad	2011/01/09 20:35:54	2011/01/09 22:35:54	offline	active	
172.22.23.192	00:26:08:ae:b3:3a	Alexs-iPhone	2011/01/09 20:24:25	2011/01/10 20:24:25	offline	active	
172.22.22.199	00:26:4a:18:81:a0		2011/01/09 11:12:07	2011/01/10 11:12:07	offline	active	
172.22.22.102	90:84:0d:9d:fc:57		2011/01/02 15:53:30	2011/01/02 16:53:11	offline	expired	
172.22.22.100	00:26:08:ae:b3:3a		2011/01/02 12:08:55	2011/01/02 16:48:18	offline	expired	

Como ele funciona...

Quando for configurado com um servidor DHCP, o PfSense libera IP para qualquer dispositivo que fizer a requisição. Essa pagina é a primeira pagina que tem que ser vista quando não se consegue aderir um IP.

Adicionando um mapeamento de DHCP estático

Se você ver um IP na lista de IPs e quer cadastrá-lo para sempre esse dispositivo pegar o mesmo IP, então temos que adicionar um mapeamento estático, para fazer isso tem que clicar no botão “+”.

Services: DHCP: Edit static mapping

S L ?

Static DHCP Mapping	
MAC address	<input type="text" value="90:84:0d:9d:fc:57"/> Copy my MAC address Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx
IP address	<input type="text"/> If no IP address is given, one will be dynamically allocated from the pool.
Hostname	<input type="text" value="Matts-iPhone"/> Name of the host, without domain part.
Description	<input type="text"/> You may enter a description here for your reference (not parsed).

[Save](#)

[Cancel](#)

Envio de Wake on LAN no mapeamento

Se vermos um dispositivo e queremos enviar um “pacote mágico”, podemos adicionar no mapeamento clicando no botão “w”.

Services: Wake on LAN: Edit

?

Edit WOL entry	
Interface	<input type="button" value="PUB"/> Choose which interface this host is connected to.
MAC address	<input type="text" value="90:84:0d:9d:fc:57"/> Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx
Description	<input type="text" value="Matts-iPhone"/> You may enter a description here for your reference (not parsed).

[Save](#)

[Cancel](#)

Gerenciando os serviços

Aqui vamos descrever como gerenciar os serviços em execução no PfSense.

1. Vá á **Status | Services**

Status: Services

?

Service	Description	Status	
dnsmasq	DNS Forwarder	Running	
ntpd	NTP clock sync	Running	
dhcpd	DHCP Service	Running	
miniupnpd	UPnP Service	Running	

2. Se quiser reiniciar um serviço clique no botão **Restart**

Status: Services

?



Service	Description	Status	
dnsmasq	DNS Forwarder	Running	
ntpd	NTP clock sync	Running	
dhcpd	DHCP Service	Running	
miniupnpd	UPnP Service	Running	

3. Se quiser parar o serviço clique no botão **Stop**

Status: Services

?



Service	Description	Status	
dnsmasq	DNS Forwarder	Running	
ntpd	NTP clock sync	Running	
dhcpd	DHCP Service	Running	
miniupnpd	UPnP Service	Stopped	

4. Se quiser startar um serviço clique no botão **Start**

Status: Services

?



miniupnpd has been started.

Close

Service	Description	Status	
dnsmasq	DNS Forwarder	Running	
ntpd	NTP clock sync	Running	
dhcpd	DHCP Service	Running	
miniupnpd	UPnP Service	Running	

Como ele funciona...

O PfSense gerencia os pacotes de serviços, podendo ser interrompidos e iniciados de forma independente, é útil quando um administrador quiser reiniciar um serviço ou derrubar todo o sistema.

Monitoramento de filtro de pacotes com PflInfo

Aqui vamos descrever como exibir informações de filtro de pacotes no PfSense

Como fazê-lo...

1. Vá á **Diagnostics | PflInfo**

Diagnostics: pfInfo

?

Status: Enabled for 7 days 07:02:29		Debug: Urgent
Hostid: 0xd54c9328		
Checksum: 0x09f3c370c92d212bc6f153a78f8c73f6		
Interface Stats for em2	IPv4	IPv6
Bytes In	45587928	0
Bytes Out	247865172	96
Packets In		
Passed	230792	0
Blocked	402	0
Packets Out		
Passed	598572	0
Blocked	0	1
State Table	Total	Rate
current entries	2770	
searches	467273767	741.5/s
inserts	3144108	5.0/s
removals	3141338	5.0/s
Source Tracking Table		
current entries	0	
searches	0	0.0/s
inserts	0	0.0/s
removals	0	0.0/s
Counters		
match	3966931	6.3/s

Como ele funciona...

Você encontrará as seguintes informações apresentadas sobre filtro de pacotes

- Estatísticas sobre as interfaces
- Tabela de estatísticas do estado
- Configurações de limites de velocidade
- Estado das regras
- Contadores de bytes
-

Monitoramento de tráfego com pfTop

Aqui vamos descrever como exibir o fluxo de tráfego em tempo real com o utilitário pfTop

Como fazê-lo...

Administradores de sistema podem usar o utilitário PfTop para monitorar o tráfego em tempo real da banda em uso. Os dados apresentados por esse utilitário podem ser apresentados por qualquer um dos seguintes critérios:

- Bytes
- Age
- Destination
- Destination Port
- Expiration
- None

- Peak
- Packets
- Rate
- Size
- Source Port
- Source

Veja também...

- Documentação sobre Monitoramento de banda

http://doc.pfsense.org/index.php/How_can_I_monitor_bandwidth_usage%3F#pftop

Monitoramento da atividade do sistema

Aqui vamos descrever como monitorar atividades do sistema PfSense

Como fazê-lo...

1. Vá á **Diagnostics | System Activity**

Diagnostics: System Activity ?

```

last pid: 6410;  load averages: 0.14, 0.27, 0.16  up 7+07:24:08   22:03:31
106 processes: 2 running, 80 sleeping, 24 waiting

Mem: 45M Active, 41M Inact, 68M Wired, 396K Cache, 110M Buf, 827M Free
Swap:

      PID USERNAME PRI NICE   SIZE    RES STATE      TIME    WCPU COMMAND
      10 root      171 ki31     OK     8K RUN    166.3H 92.97% idle
      11 root      -68      - OK    192K WAIT   178:51  0.98% {irq20: fxp0}
      11 root      -68      - OK    192K WAIT   151:35  0.98% {irq265: em3:rx 0}
  22730 root      48      0 54692K 15836K piperd  0:11  0.98% php
      11 root      -68      - OK    192K WAIT   12:19  0.00% {irq266: em3:tx 0}
      11 root      -32      - OK    192K WAIT   12:18  0.00% {swi4: clock}
      11 root      -64      - OK    192K WAIT   10:50  0.00% {irq15: atal}
      13 root      -16      - OK     8K -    10:13  0.00% yarrow
  31177 root      44      0 3316K 1300K select  3:33  0.00% apinger
 10765 root      76      20 3656K 1424K wait   3:22  0.00% sh
 19205 root      44      0 3316K 888K piperd  3:14  0.00% logger
 53022 nobody    44      0 5552K 2496K select  1:43  0.00% dnsmasq
 12723 root      76      0 54692K 16456K accept  1:15  0.00% php
 18890 root      44      0 11032K 8280K bpf   1:12  0.00% tcpdump
      0 root      -16      0  OK    112K sched   0:54  0.00% {swapper}
  52249 dhcpd    44      0 7776K 4068K select  0:52  0.00% dhcpcd
      2 root      -8      - OK     8K -    0:47  0.00% g_event
      7 root      -16      - OK     8K pftm   0:45  0.00% pfpurge

```

Como ele funciona...

Os administradores podem monitorar o sistema central do PfSense, incluindo os seguintes recursos:

- O ID do ultimo processo (PID)

- Carga média
- Uptime
- Estatísticas de Processador
- Estatísticas de Memória
- Estatísticas de uso do SWAP

B

Determinar os Requisitos de Hardware

Neste capítulo vamos bordar os seguintes tópicos:

- Determinando o cenário de implantação
- Determinando os requisitos de rendimento
- Determinando os requisitos das interfaces
- Escolher o tipo de instalação
- Melhor forma de uso

Introdução

Se o nosso cenário é uma rede doméstica de dois computadores ou um centro de dados corporativos com centenas de máquinas, é essencial sabermos primeiro determinar exatamente a função do nosso firewall.

A versatilidade do PfSense nós apresenta uma grande variedade de opções de configuração, o PfSense vai ser instalado em um novo computador, mas como vamos ver, o PfSense oferece inúmeras outras alternativas para atender as necessidades de qualquer ambiente de segurança.

Determinando o cenário de implantação

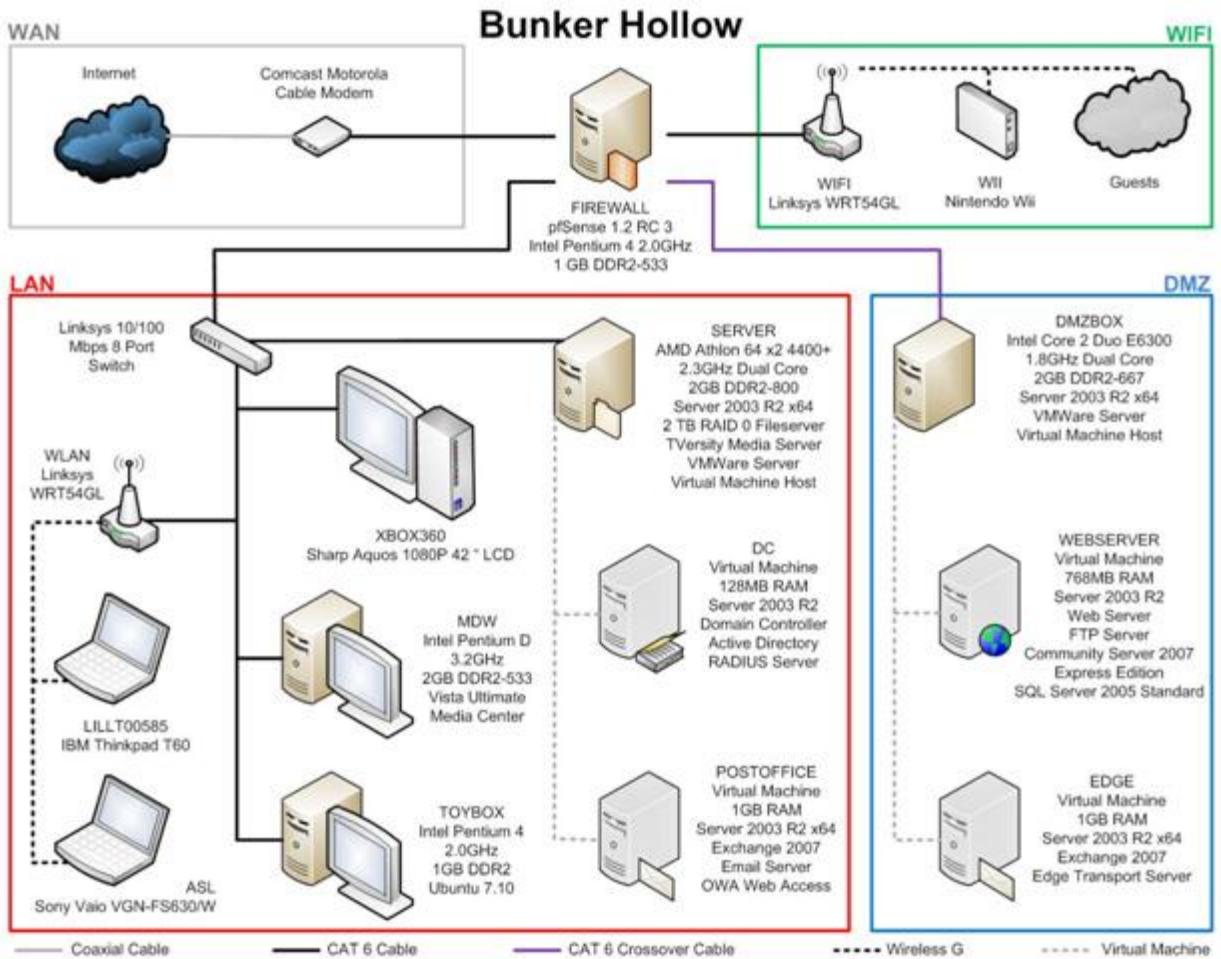
Aqui vamos descrever como determinar qual dos cenários de implantação será certo para nosso ambiente de rede.

Se preparando...

Aqui vamos descrever como entender o uso do diagrama para saber como o PfSense se encaixa em nosso ambiente. Como exemplo vamos usar o meu diagrama de rede que faço em casa. Esse diagrama é um bom exemplo típico de um escritório pequeno (tirando os consoles de vídeo game)

Como fazê-lo...

- Vamos analisar nosso diagrama de rede



- Neste cenário de um pequeno escritório, o firewall que temos no diagrama se encaixa perfeitamente. Esse é o mais comum de todas as implantações do PfSense.

Como ele funciona...

Um firewall captura todo o tráfego que flui em uma interface. Vamos definir regras de firewall baseado em como queremos que o tráfego fluia. Algumas regras comuns entre a maioria das redes são:

- **Permitir tudo da LAN para WAN:** Permite que os usuários tenham acesso externo, usando serviço de e-mails, e assim por diante.
- **Permitir alguns da LAN para WAN:** Permite a filtragem de saída de pacotes para limitar o tipo de tráfego autorizado a sair de uma rede restringindo os dados maliciosos.
- **Bloquear todos de WAN para LAN:** Não permite que dados externos entrem na nossa rede privada.
- **Permitir tráfego HTTP da LAN para DMZ:** Permite que usuários internos possam acessar o servidor web da nossa empresa
- **Permitir tráfego HTTP da WAN para DMZ:** Permite que usuários externos possam acessar o servidor web da nossa empresa

- **Bloquear todos da DMZ para LAN:** Nossa DMZ é insegura, já que estamos permitindo que os usuários externos possam acessar o servidor web. Então temos que bloquear todo o tráfego que tentar acessar a nossa LAN pela DMZ.

O PfSense também emprega muitas características de firewall avançadas, para acomodar as necessidades de redes mais complexas. O PfSense é capaz de:

- Superta dezenas de interfaces, se necessário.
- Pode lidar com varias conexões múltipla de internet, no caso de uma ligação de internet primaria falhar.
- Failover de proteção, no caso se o firewall principal falhar
- Balanceamento de carga, para otimizar o tráfego de rede.

Há mais...

O PfSense é altamente flexível e pode ser também configurado como qualquer um dos seguinte dispositivos. É importante notar que esses papéis são simplesmente serviços que vamos usar na nossa implantação de firewall, mas em ambientes maiores pode ter a necessidade de fazer mais de um servidor para melhorar o desempenho.

- **Roteador:** Este é a segunda implantação do PfSense mais comum. Um roteador determina o destino de um pacote e envia para o seu caminho, sem aplicar quaisquer regras de fierewall.
- **Aplicação VPN:** Um servidor VPN fornece conexões criptografadas de rede remota. O PfSense suporta todos os principais tipos de protocolos de rede virtual privada, como IPSec, PPTP, OpenVPN e L2TP.
- **Aplicação DHCP:** Um servidor DHCP atribui endereços de IP a clientes que solicitem.
- **Aplicação DNS:** Um servidor DNS associa o endereço ao nome de IP. É muito mais fácil lembrar www.google.com do que “173.194.33.104”
- **Aplicação VoIP:** é a telefonia digital, é possível fazer isso no PfSense usando o pacote FreeSWITCH.
- **Aplicação de SNIFFER:** Sniffers analisa os pacotes para o padrão. Isso é muitas vezes para detectar e impedir o tráfego que tenta explorar vulnerabilidades conhecidas. O PfSense utiliza o pacote mais amplamente implantado sniffer na existência, o Snort.
- **Wireless Access Point:** O PfSense pode ser implantado como um servidor access point de acesso wireless.

O PfSense pode ser configurado como muito mais outros dispositivos de servidor, sendo implantado como uma aplicação de propósito específico, só é limitado pelo numero de pacotes suportados pela plataforma.

Para mais informações, leia a documentação do PfSense online: Implementações comuns

http://www.pfsense.org/index.php?option=com_content&task=view&id=71&Itemid=81

Determinando os requisitos de rendimento

Aqui vamos explicar como determinar os requisitos de rendimento e, posteriormente, os requisitos de processamento e memória necessária em nosso ambiente.

Se preparando...

Vamos ter que preparar nossas necessidades, reunindo as seguintes informações:

- A velocidade de conexão com a internet
- A velocidade de hardware de rede. Ver se a rede vai ser capaz de transferir 10, 100 ou 1000 Mbps.
- Qual velocidade de conexão liberado para cada usuário

Como fazê-lo...

1. Vamos ver as diretrizes gerais de rendimento (disponível em <http://pfsense.com> em **Hardware | Seleção e dimensionamento**)

A taxa de transferência do Firewall	Poder de processamento	Hardware do servidor PCI-e
10-20 Mbps	266-MHz CPU	Não
21-50 Mbps	500-MHz CPU	Não
51-200 Mbps	1-GHz CPU	Não
201-500 Mbps	2-GHz CPU	Recomendado
501+ Mbps	3-GHz CPU	Recomendado

A tabela a seguir mostra os requisitos mínimos para determinados recursos opcionais:

Características	Recursos adicionais
VPN	Na transferência criptografada o CPU fica com 20% do seu rendimento a menos, se você tiver um processador com recursos baixos você vai precisar de uma placa só para esse serviço.
Captive Portal	Ambientes com um numero grande de usuários como mais que 100, você vai precisar de uma placa com processamento maior já que a taxa de transferência é maior.
Tabelas em larga escala	O tamanho padrão de entradas de tabela são 10.000, ocupando 10MB de RAM. Em grandes ambientes com centenas de milhares de entradas de tabela será necessária uma quantidade de memoria RAM maior.
Pacote Squid	É um pacote usado para guardar e gerenciar cache de web, que requer um uso intensivo do HD e uma grande quantidade de armazenamento. Não é recomendado em uso embutido, já que é usado um cartão compacto e não tem muito espaço.
Pacote SNORT	É um pacote de detecção de intrusão de sniffer requer no mínimo 512MB de RAM só para esse serviço.
Pacote NTop	É um pacote de ferramentas de tráfego de rede. Será necessário no mínimo 512MB de

2. Agora, vamos determinar nossas próprias exigências.

- Nossa empresa é de médio porte, tendo 100 usuários em media. Na nossa infraestrutura tem cabo CAT5 e um switch de 100Mbps. A maioria do nosso tráfego é em navegação web, e-mails e compartilhamento de arquivos pequenos. Nossa conexão de internet é de 100Mbps, a nossa maior preocupação é ser capaz de usar 100% do link.
- Queremos proporcionar um acesso VPN para acessarem de qualquer lugar, para não ter problemas na hora de conexão, para auxiliar nós usamos o Pacote Ntop para não ter problemas futuros e poder ter confiança em uma transferência VPN.
- Por último levando em consideração o dinheiro economizado por estar usando o PfSense que é um sistema de código aberto, vamos ter um computador adicional para servir como Failover.

3. Aqui vamos identificar nossas necessidades:

- Uma placa de rede de 1Gbps (incluindo cabos e switches)
- Rendimento da taxa de transferência eh de 100Mbps
- A taxa de transferência encriptada (VPN) de 20Mbps
- 1-GHz CPU, 1-GB RAM.
- A segunda maquina tem que ser idêntica para ser usada como Failover.

Como ele funciona...

A taxa de transferência é a quantidade de dados que podem ser processados em um determinado momento. Vamos ter uma conexão de 100Mbps de internet de fibra ótica, mas se nossa placa de rede só puder processar 20Mbps então essa vai ser nossa velocidade de internet.

A taxa de transferência do firewall é apenas um fator de tráfego que passa pelo firewall. O tráfego da internet passa por esse requisito (LAN <| WAN). No entanto entre duas máquinas da rede interna, a transferência entre essas duas máquinas não vai passar pelo firewall.

Há mais...

É importante lembrar que certos recursos de firewall tem seu próprio recurso de hardware. Por exemplo, as conexões VPN exigem um processamento adicional e o pacote de web Squid não é adequado para uma instalação embutida em disco compacto.

Lista de pacotes disponíveis

Infelizmente, a lista de pacotes disponíveis para o PfSense não é mantida online. Uma vez o PfSense instalado podemos ver os pacotes disponíveis em **System | Packages**.

Determinando os requisitos das interfaces

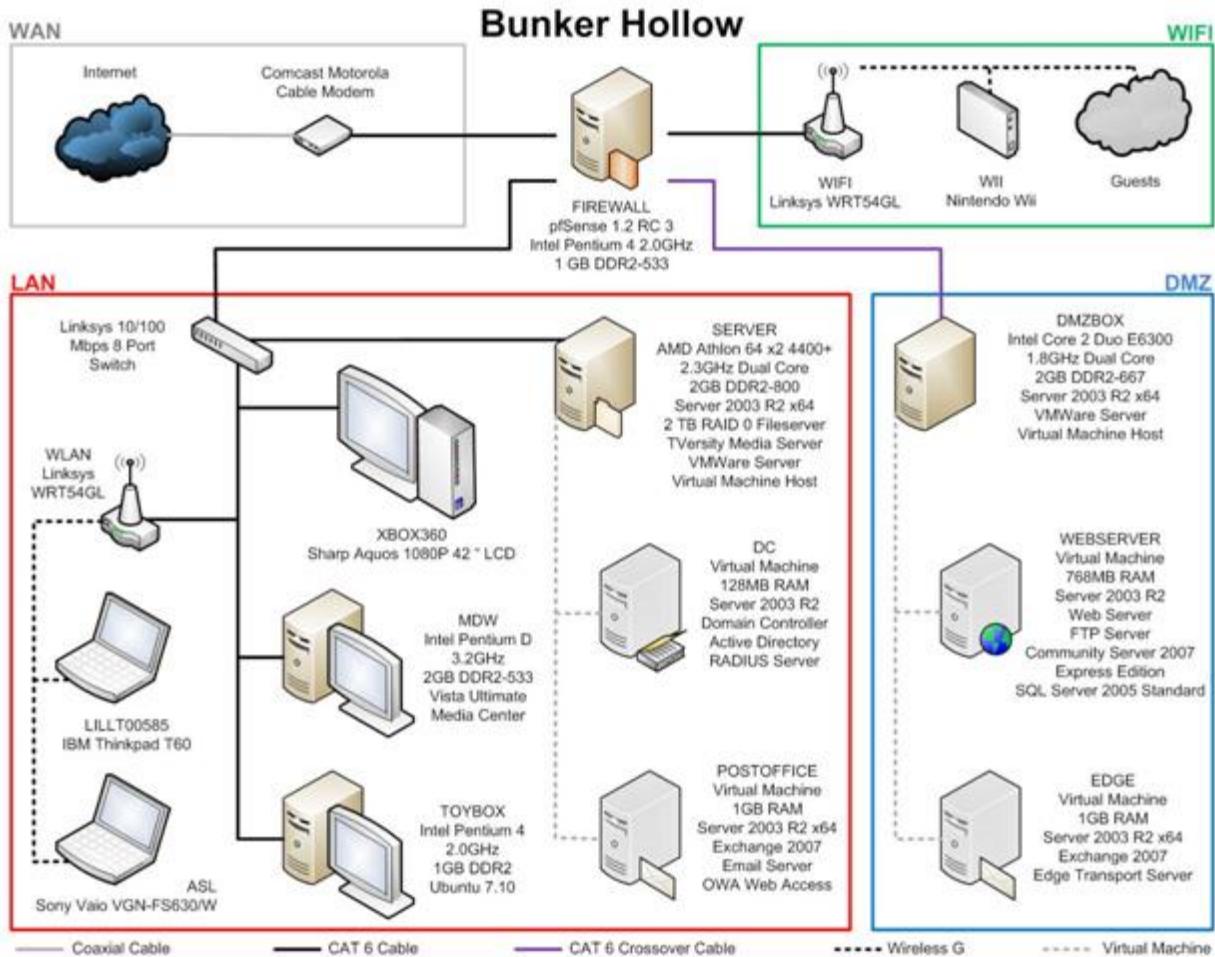
Aqui vamos descrever como ajudar a determinar as necessidades da nossa interface através da análise do nosso projeto de rede.

Se preparando...

Aqui vamos descrever uma análise do nosso diagrama de rede para entender como as interfaces da nossa rede vão funcionar. Como exemplo, vamos usar o diagrama de rede de casa, que é basicamente usado em um pequeno escritório.

Como fazê-lo...

1. Vamos analisar o nosso diagrama de rede:



2. Podemos ver que nosso ambiente é composto por 4 interfaces separadas:

- **WAN (Wide Area Network):** A internet
- **LAN (Local Area Network):** A rede interna primária
- **DMZ (Zona Desmilitarizada):** É a nossa rede interna que permite o acesso externo ao servidor web, servidores de e-mail, e qualquer outro dispositivo liga a essa interface.
- **WiFi (Para visitantes poderem acessar wireless):** Nós criamos essa rede para aceitar novos acessos de convidados. Eles podem se conectar com senha ou não e navegar na web.
Vamos considerar essa interface insegura já que qualquer pessoa vai poder se conectar, então vamos definir regras para quem se conectar nessa interface não possa se comunicar com outras interfaces.

É evidente que nosso firewall tem quatro placas de rede.

Em uma opção alternativa o diagrama a cima poderia ser feito com duas interfaces (WAN e LAN) e duas VLANs (DMZ e WiFi).

Como ele funciona...

O firewall requer uma placa de rede para cada interface separada. Isso garante uma separação física do tráfego de rede. Todo o tráfego entre as redes é forçado a passar pelo firewall, onde as nossas regras vão ser aplicadas e cumpridas. Por essa razão um firewall exige no mínimo duas placas de rede para funcionar corretamente, uma para o tráfego externo e outra para o tráfego interno, cada interface opcional vai exigir outra placa de rede que pode ser adicionada a qualquer momento.

Há mais...

Tipicamente, uma placa de rede terá uma única porta Ethernet. No entanto algumas placas de rede podem ter duas, quatro ou até mais portas em uma única placa de rede. No firewall do nosso cenário a cima pode funcionar tanto com quatro placas de rede com uma entrada Ethernet cada uma, ou uma placa de rede com quatro entradas Ethernet, nas duas alternativas funcionaria da mesma forma.

Placa de rede com uma entrada Ethernet	Placa de rede com quatro entradas Ethernet
	

PfSense 2.0: Os requisitos de numero de interface mínimo

Isso é novo na versão 2.0 do PfSense, pois agora é permitido a instalação do PfSense 2.0 em um computador com apenas uma placa de rede, que antes não era possível (era obrigado ter duas placas).

Escolher o tipo de instalação

Aqui vamos descrever como escolher entre a versão normal ou embutida do PfSense.

Se preparando...

Cada recurso padrão usado em uma plataforma de instalação pode ser usado em outra, mas certos pacotes não. O Squid por exemplo tem que ser instalado em uma instalação normal feita no próprio HD.

Como fazê-lo...

1. Vamos rever os pacotes que decidimos instalar:

Pacote NTop: É uma ferramenta de análise de tráfego. Ele requer um mínimo 512MB de RAM, mas não tem restrição quanto ao tipo de armazenamento.

2. Com base nessas informações vamos fazer a instalação do PfSense em uma plataforma imbutida

Como ele funciona...

A imagem padrão foi feita para ser instalado em um disco rígido. A versão embutida é feita para ser instalado em dispositivos como um pendrive por exemplo. Mas pendrive tem um número limitado de gravações durante sua vida útil, por isso que a versão embutida do PfSense é projetada para limitar o que ele escreve no disco. Cada plataforma tem suas vantagens e desvantagens distintas:

Plataforma	Prós	Contra
Padrão	Suporta todos os pacotes e funcionalidades. Grande quantidade de espaço de armazenamento.	Todo o HD deve ser exclusivo para o sistema (dual boot não é permitido). Requer um uso de energia maior.
Embutida	Tempos de resposta rápida. Os pendrives podem ser facilmente trocados, por outro pendrive de backup ou com o sistema já atualizado. Requer pouca energia. Silencioso	Pendrives têm um número limitado de gravações durante sua vida útil. Nem todos os pacotes são suportados nesse tipo de plataforma de instalação.

Há mais...

A forma de instalação do PfSense no HD é feita através do CD. Mas se você quiser apenas usar o PfSense sem precisar instalar você também pode com o mesmo CD, dando boot por ele. Você pode até salvar suas configurações em um pendrive.

Melhor forma de uso

Aqui vamos descrever como escolher a melhor configuração de hardware, baseado nas necessidades do nosso firewall.

Se preparando...

É mais fácil saber a melhor forma de uso do PfSense , se todos os pré-requisitos já foram obedecidos:

- Cenário de implantação
- Requisitos de taxa de transferência
- Requisitos de interfaces
- A plataforma de instalação

Como fazê-lo...

Avaliando os diferentes tipos de uso do PfSense:

1. **Uso pequeno:** energia restrita, silencioso, um pequeno rendimento de impressão.
2. **Área de trabalho:** o hardware é de um computador normal. Facilmente atualizável de uso padrão do PfSense.
3. **Servidor:** em ambientes maiores podem requerer um computador mais robusto do tipo Servidor.

Considerando a necessidade da exigência de um hardware especial. No nosso caso, precisamos de um rendimento moderado se não precisar usar pacotes que exigem hardware especial. Para ser usado em um baixo consumo de energia e em uma operação silenciosa para o nosso pequeno escritório então vamos usar uma forma de uso mais pequena.

Como ele funciona...

A escolha da forma de uso tem haver com o ambiente de uso do PfSense. Cada ambiente varia a forma de uso do PfSense. Graças a grande variedade de hardwares disponíveis no mercado hoje, qualquer implantação do PfSense pode ser possível.

Há mais...

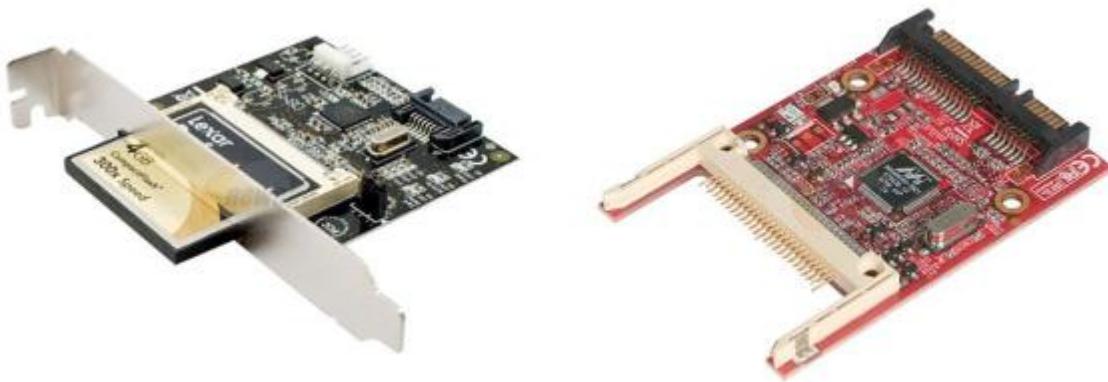
Não há nada que impeça do PfSense ser instalado em um notebook! O maior obstáculo sem dúvida seria não poder adicionar placas de rede, mas uma alternativa seria adicionar dispositivos USB com saída Ethernet.

Assim como todos os projetos de código aberto, terá primeiro que ver a compatibilidade do dispositivo antes de instalar o novo hardware.



Instalando o PfSense em uma plataforma embutida em um desktop/servidor/laptop

Algumas pessoas realmente tiram um maior proveito do sistema usando em um pendrive. Testar uma nova versão do PfSense ou então restaurar um backup, podendo somente trocar o cartão de memoria. Mas na maioria dos desktops não vem com um leitor de cartão, mas existem varias outros dispositivos semelhantes que podem ajudar:



Instando a versão padrão no laptop

De todos os tipos de cenários de instalações diferentes, instalar a versão padrão em um disco rígido do laptop é o desafio maior. Pois os aparelhos são pequenos, e as vezes não vem com leitor de cd, e as vezes não tem entrada de vídeo externo para poder ser visto melhor, e vai precisar de uma entrada serial ou USB.

Traduzido por **Christopher Persaud**

E-mail: christopherpersaud@gmail.com

MSN: christopher@uze.com.br