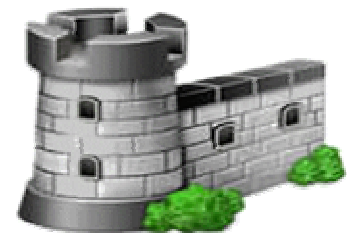


Managing IPTABLES Rules with Firewall Builder (FWBuilder)

Moisés Benigno
moises@moisebenigno.com
[beniGNU]



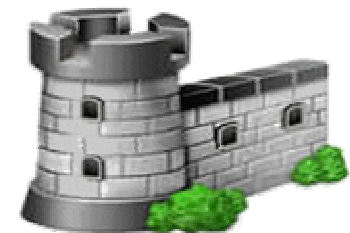
Dia 'D'ebian
REC/AGO2009



Speaker



“Analista de Suporte, Graduado em Sistemas de Informação, Pós-graduado em Gestão da Tecnologia da Informação e Comunicação pela FAFIRE, Mestrando em Ciências da Computação pela UFPE. Desde o ano de 1999, vem se dedicando ao Sistema Operacional GNU/Linux, implantando e implementando soluções em Infraestrutura, Segurança e Administração de Redes/Sistemas multiplataforma. Colaborador e participante ativo da comunidade regional de Software Livre. Atualmente, é supervisor de TIC e docente da Faculdade FAFIRE em Recife/PE.”



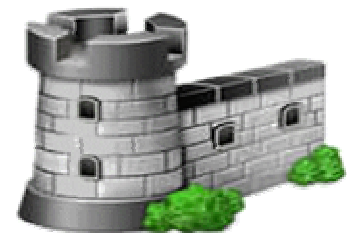
Schedule

- Motivation;
- Overview of Firewall Builder Features;
- Installing Firewall Builder;
- Configuration;
- Getting Started;
- Firewall Builder GUI;
- Power Templates;



Schedule (continue)

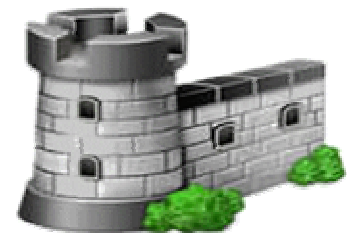
- Working with Objects;
- Service Object;
- Firewall Policies;
- Policies and Rules;
- Compiling and Installing Firewall Policies;
- File Structure .fwb and .fw;
- Startup Scripts;



Firewall – WFIT ??!!

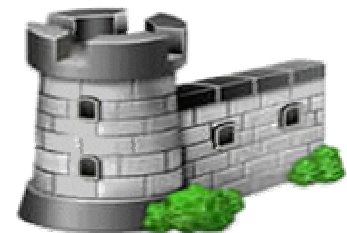
“A firewall is a part of a computer system or network that is designed to block unauthorized access while permitting authorized communications. It is a device or set of devices configured to permit, deny, encrypt, decrypt, or proxy all (in and out) computer traffic between different security domains based upon a set of rules and other criteria.”

Wikipedia



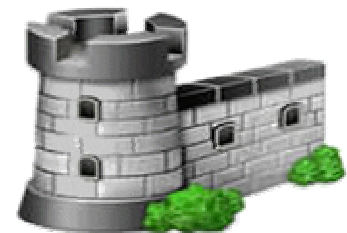
Type of Firewall

- *Packet Filter: Looks at each packet entering or leaving the network and accepts or rejects it based on user-defined rules – (**First Generation**)*
- *Application Gateway: Applies security mechanisms to specific applications, such as FTP and Telnet servers – (**Third Generation**)*



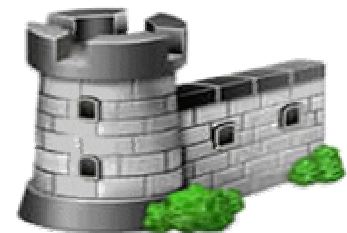
Type of Firewall

- *Circuit-Level Gateway: Applies security mechanisms when a TCP or UDP connection is established – (**Second Generation**)*
- *Proxy Server: Intercepts all messages entering and leaving the network. The proxy server effectively hides the true network addresses.*

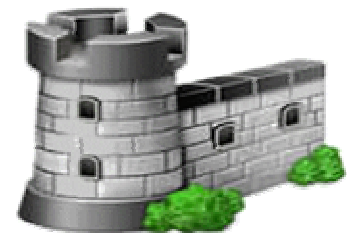
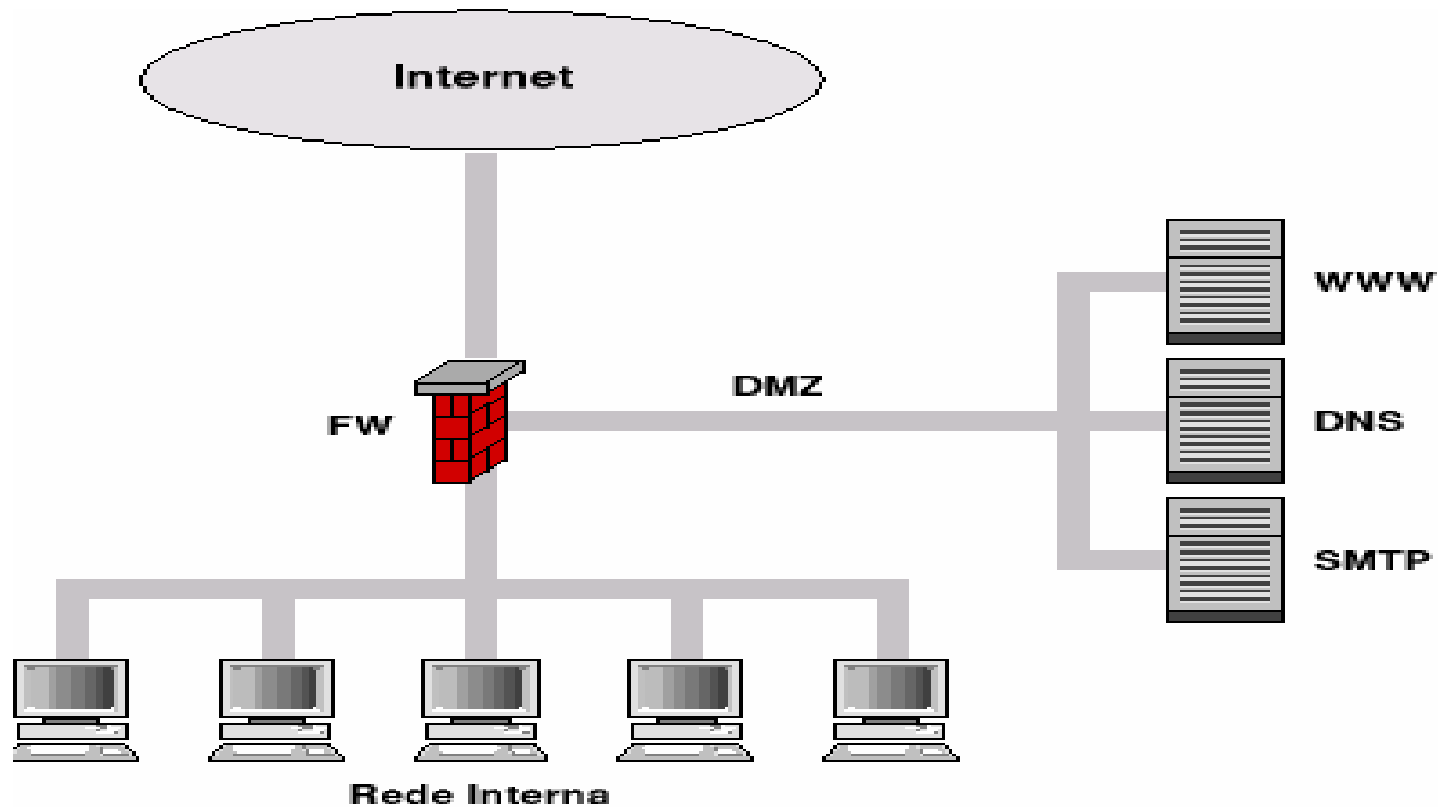


Type of Firewall

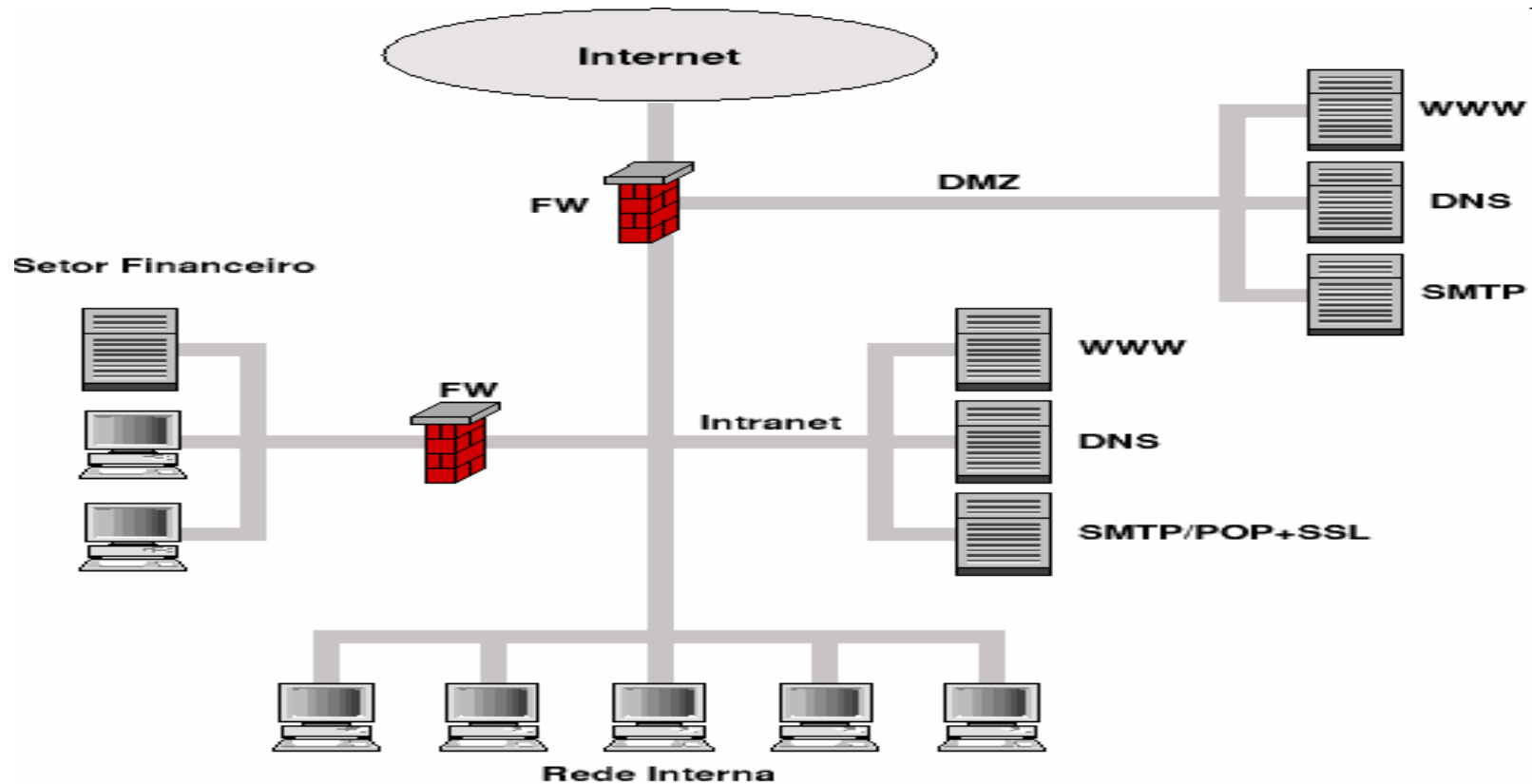
- *Middleboxs: Promove a deep packet inspection functionality of modern firewalls like Stateful Inspection and can be shared by Intrusion-Prevention Systems (IPS). (**Forth Generation**)*
- *Examples: FORTINET, Juniper, Checkpoint (FireWall-1)*



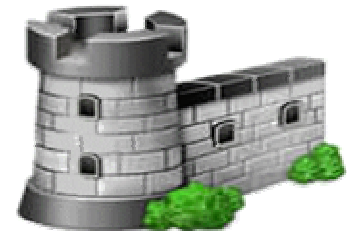
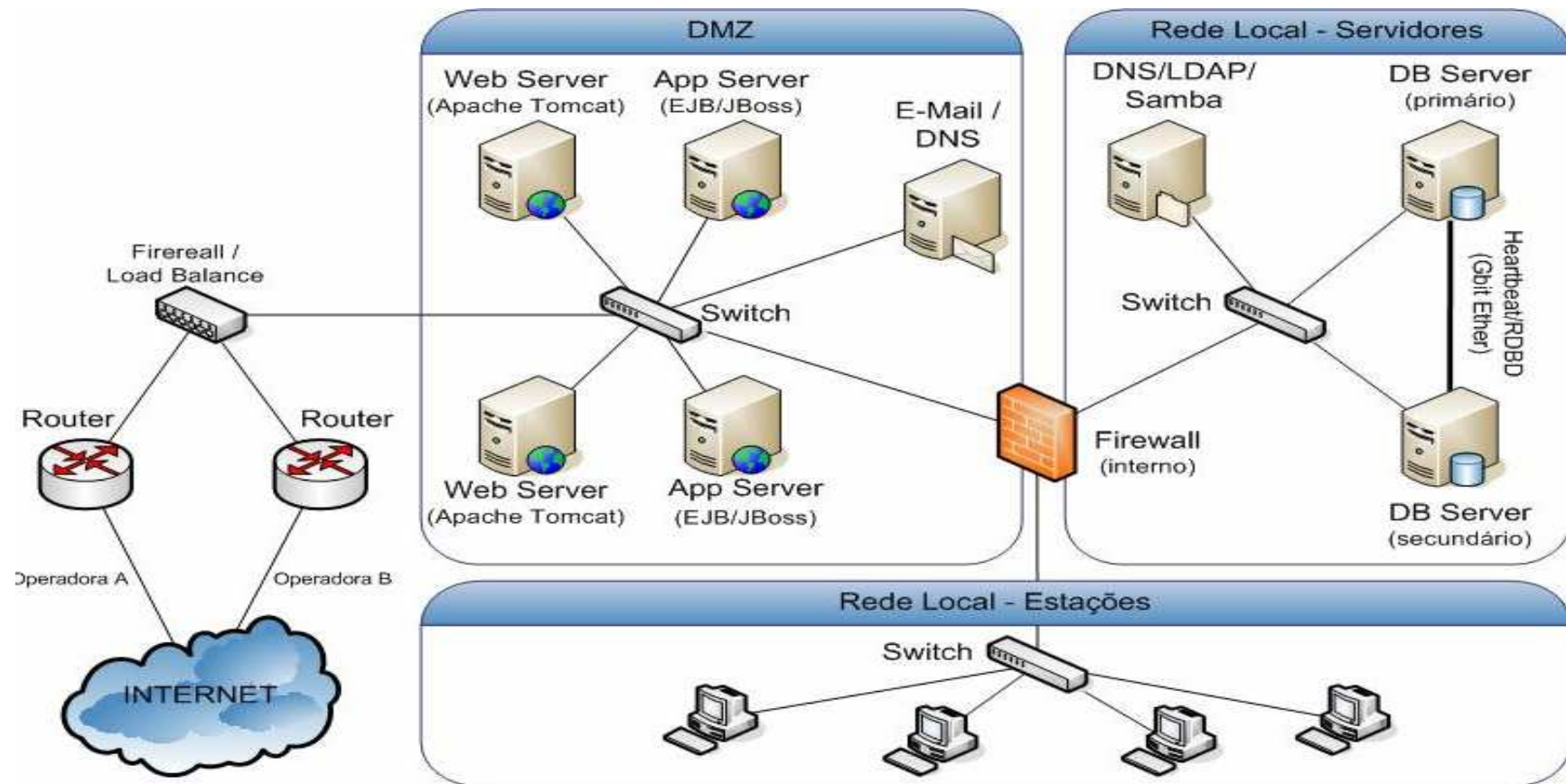
Topology [1]



Topology [2]

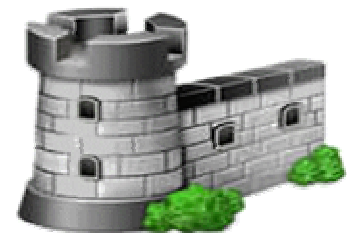


Topology [3]



FWBuilder – WFIT??!! [1]

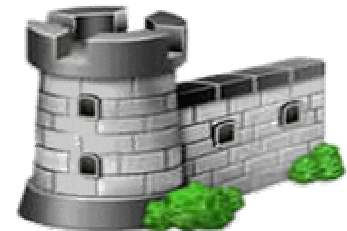
- *“Firewall Builder simplifies the firewall policy management for a number of firewall platforms, including Netfilter/iptables, ipfw, PF, Cisco PIX, and others. Firewall Builder provides a professional-grade GUI to these platforms, simplifying administration tasks. (...) Instead of thinking in terms of obscure commands and parameters, you simply create a set of objects describing your firewall, servers, and subnets, and then implement your firewall policy by dragging objects into policy rules.”*



FWBuilder – WFIT??!! [2]

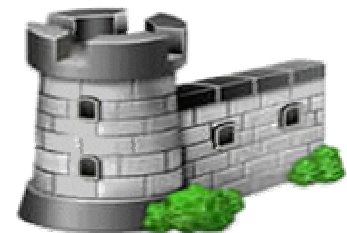
<i>Plataform</i>	<i>OS</i>
iptables	Linux (kernel 2.4.x / 2.6.x)
ipfilter	FreeBSD, OpenBSD, Solarias
ipfw	FreeBSD, MacOS X
pf	OpenBSD

<i>OS</i>	<i>Distributions and Versions</i>
Linux	Red hat, SuSE, Ubuntu, Gentoo
FreeBSD	5.3 and later
Mac OS X	10.2.3 and newer
M\$ Windows 2000, XP, Vista	All current



Before ...

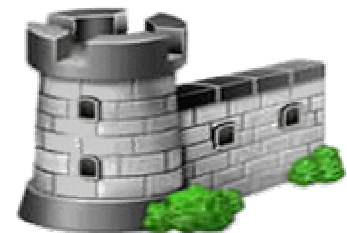
```
iptables -A FORWARD -i eth1 -j ACCEPT
iptables -A FORWARD -m state --state NEW -i eth1 -j ACCEPT
iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A FORWARD -m state --state NEW,INVALID -i eth0 -j DROP
iptables -A FORWARD -m limit --limit 60/minute --limit-burst 60
iptables -A INPUT -p tcp ! --syn -i $EXT -j ACCEPT
iptables -t mangle -A OUTPUT -p tcp --dport 22 -j TOS --set-tos Minimize-Delay
iptables -t mangle -A OUTPUT -p tcp --dport 23 -j TOS --set-tos Minimize-Delay
iptables -t mangle -A OUTPUT -p tcp --dport 110 -j TOS --set-tos Minimize-Delay
iptables -A INPUT -p udp -s 0/0 -i $EXT --dport 33435:33525 -j DROP
iptables -A INPUT -s 192.168.0.254 -p tcp --dport 22 -j ACCEPT
iptables -A INPUT -p tcp -m multiport --dport 21,22,25,53 -j ACCEPT
iptables -A FORWARD -p tcp --syn -m limit --limit 1/s -j ACCEPT
iptables -A FORWARD -p tcp --tcp-flags SYN,ACK,FIN,RST RST -m limit --limit 1/s
-j ACCEPT
iptables -A FORWARD -m unclean -j DROP
iptables -N syn-flood
iptables -A INPUT -i $INT -p tcp --syn -j syn-flood
iptables -A syn-flood -m limit --limit 1/s --limit-burst 4 -j RETURN
```



- Garota de programa de Odete ...
- Vendendo Herbalife ...



***Como ganhar
R\$ 500,00
em 25 minutos?***



Tchannraaaammmm ...

Firewall Builder: t.fwb

File Edit Object Rules Tools Help

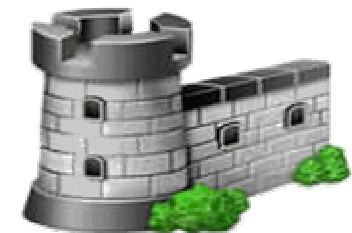
guardian

Firewalls: guardian

Policy NAT Routing

	Source	Destination	Service	Interface	Direction	Action	Time	Options	Comment
0	guardian net-192.168.1.0	Any	Any	vlan1		Red circle	Any		anti spoofing rule
1	Any	Any	Any	loopback		Green circle	Any		
2	net-192.168.1.0	guardian	TCP ssh DNS	All		Green circle	Any		SSH Access to firewall is permitted only from internal network Also firewall serves DNS for internal network
3	net-192.168.1.0	guardian	DHCP	All		Green circle	Any		DHCP requests are permitted from internal network
4	old-broadcast	broadcast							
5	guardian	net-192.168.1.0	DHCP	All		Green circle	Any		DHCP replies
6	Any	web_server	TCP http	All		Green circle	Any		
7	Any	guardian	Any	All		Red circle	Any		All other attempts to connect to the firewall are denied and logged
8	net-192.168.1.0	Any	Any	All		Green circle	Any		
9	Any	Any	Any	All		Red circle	Any		

Object Type: Firewall
Object Name: guardian
Platform: iptables
Version: any
Host OS: linksys
Modified: Wed Apr 2 20:09:37 2008
Compiled: -
Installed: -
Similar to fw 1, but the firewall is used as DHCP and DNS server for internal



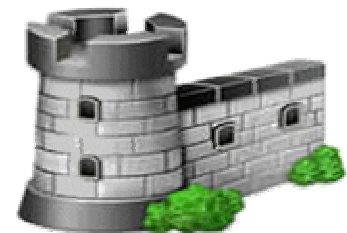
Packages Repository

- *Debian/Ubuntu*

```
deb http://www.fwbuilder.org/deb/stable/ intrepid contrib
```

To access Debian/Ubuntu repository of testing packages, add the following line to the file `/etc/apt/sources.list` (replace "intrepid" here with "hardy" or "jaunty" depending on your version):

```
deb http://www.fwbuilder.org/deb/testing/ intrepid contrib
```



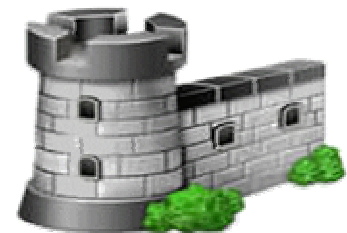
Packages Repository

- *Red Hat/Fedora*

To access repository of RPM packages, create file `/etc/yum.repos.d/fwbuilder.repo` with the following contents:

```
[fwbuilder]
name=Firewall Builder
failovermethod=priority
baseurl=http://www.fwbuilder.org/rpm/stable/fedora-$releasever-$basearch
enabled=1

[fwbuilder-testing]
name=Firewall Builder Test Builds
failovermethod=priority
baseurl=http://www.fwbuilder.org/rpm/testing/fedora-$releasever-$basearch
enabled=0
```



Packages Repository

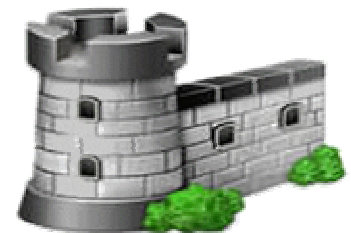
- *OpenSuse RPMs*

<http://download.opensuse.org/repositories/home:/worldcitizen/>



The time of truth ...

DEMO



References

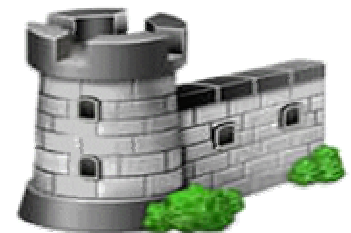
FWBuilder - FAQ

FWBuilder – HOW TO

Firewall Builder Cook Book

FWBuilder – Release Notes

Available: <http://www.fwbuilder.org>



ThankZzZ :)

<http://www.moisesbenigno.com>

moises@moisesbenigno.com

[MSN: ch_root@hotmail.com](mailto:ch_root@hotmail.com)



Managing IPTABLES Rules with Firewall Builder (FWBuilder)

Moisés Benigno
moises@moisebenigno.com
[beniGNU]



Dia 'D'ebian
REC/AGO2009

