



Plan-Net propose, installe et supporte l'utilisation de routers/firewalls basés Linux.

Ces firewalls fonctionnent sur une version LTS de Xubuntu, ce qui garanti les mises-à-jour (bug-fix et security updates) pendant une durée allant jusqu'à cinq années.

Ils proposent les fonctionnalités suivante:

- Firewalling complexe (iptables) avec interface d'administration centralisé, éventuellement distante FirewallBuilder.

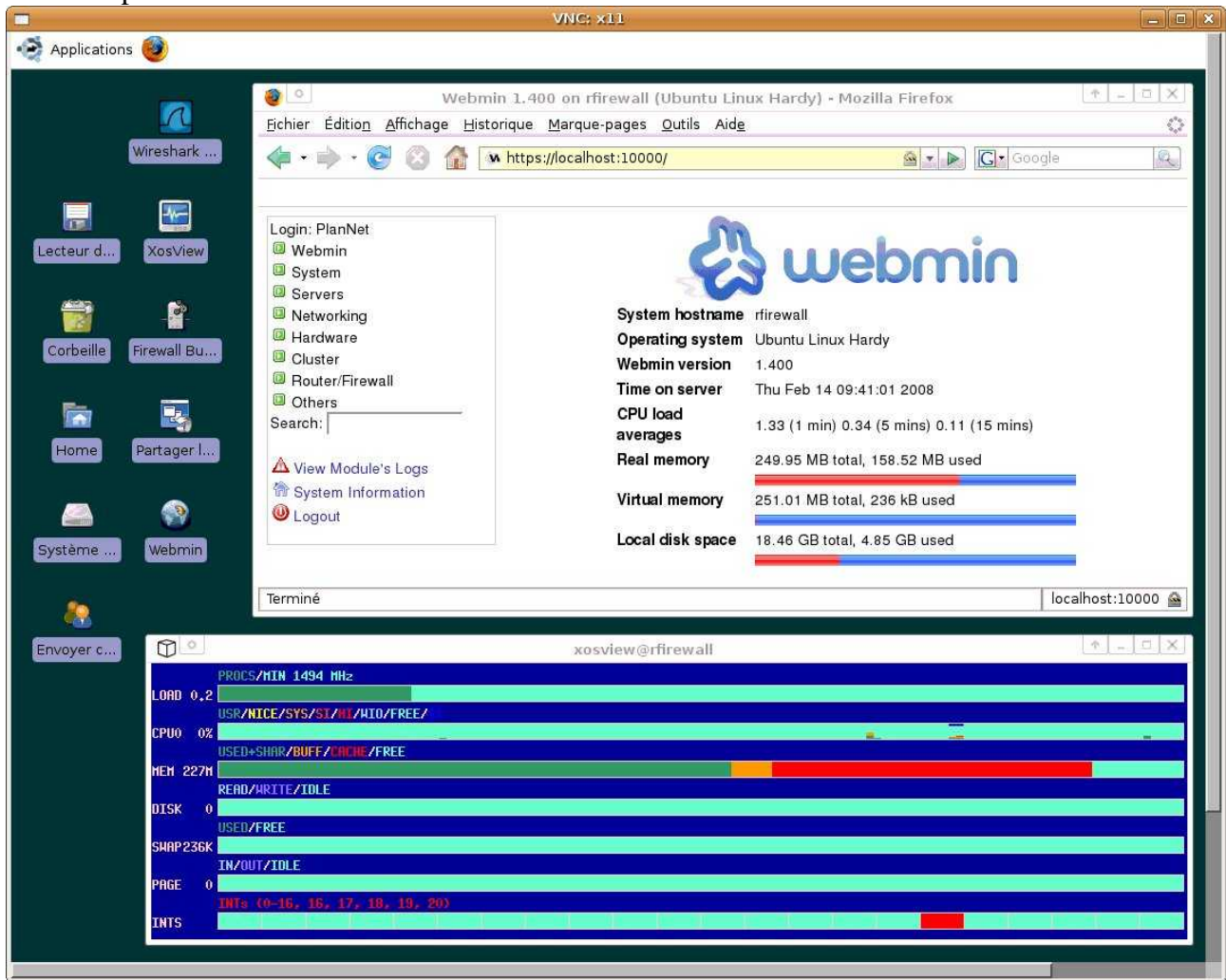
The screenshot shows the Firewall Builder interface for a configuration named 'test.fwb'. The main window displays a table of firewall rules with the following columns: Policy, Source, Destination, Service, Action, Time, Options, and Comment. The rules are as follows:

Policy	Source	Destination	Service	Action	Time	Options	Comment
0	net-192.168.1.0	test2	TCP ssh	Accept			
1	test2	internal server	DNS	Accept			
2	Any	test2	Any	Deny			
3	Any	Any	TCP auth	Reject			
4	Any	server on dmz	TCP smtp	Accept			
5	server on dmz	internal server	TCP smtp	Accept			
6	server on dmz	net-192.168.1.0	DNS, TCP smtp	Accept			
7	net-192.168.2.0	net-192.168.1.0	Any	Deny			
8	net-192.168.1.0	Any	Any	Accept			
9	Any	Any	Any	Deny			

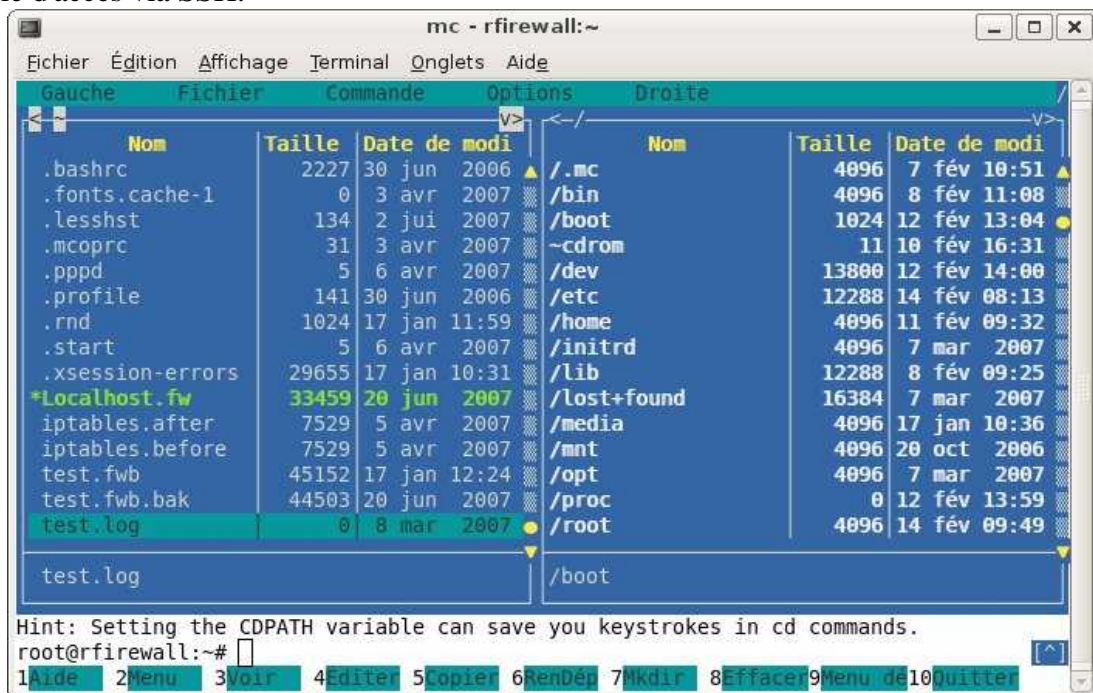
On the left, a tree view shows the 'User' library containing 'Firewalls' (test2, testfw), 'Objects', 'Services', and 'Time'. Below this, the 'Object Type: Firewall' details are shown for 'test2', including platform (iptables) and host OS (linux24). A descriptive comment is provided: 'This firewall has three interfaces. Eth0 faces outside and has a static routable address; eth1 faces inside; eth2 is connected to DMZ subnet. Policy includes basic rules to permit unrestricted outbound access and anti-spoofing rules. Access to the firewall is permitted only from internet'. On the right, the 'Firewall' configuration panel shows settings for 'test2', including platform (iptables), version (any), and host OS (Linux 2.4/2.6). An 'Apply Changes' button is located at the bottom right.

- Administration distante sécurisée via VNC, XDMCP, SSH, HTTPS, ...

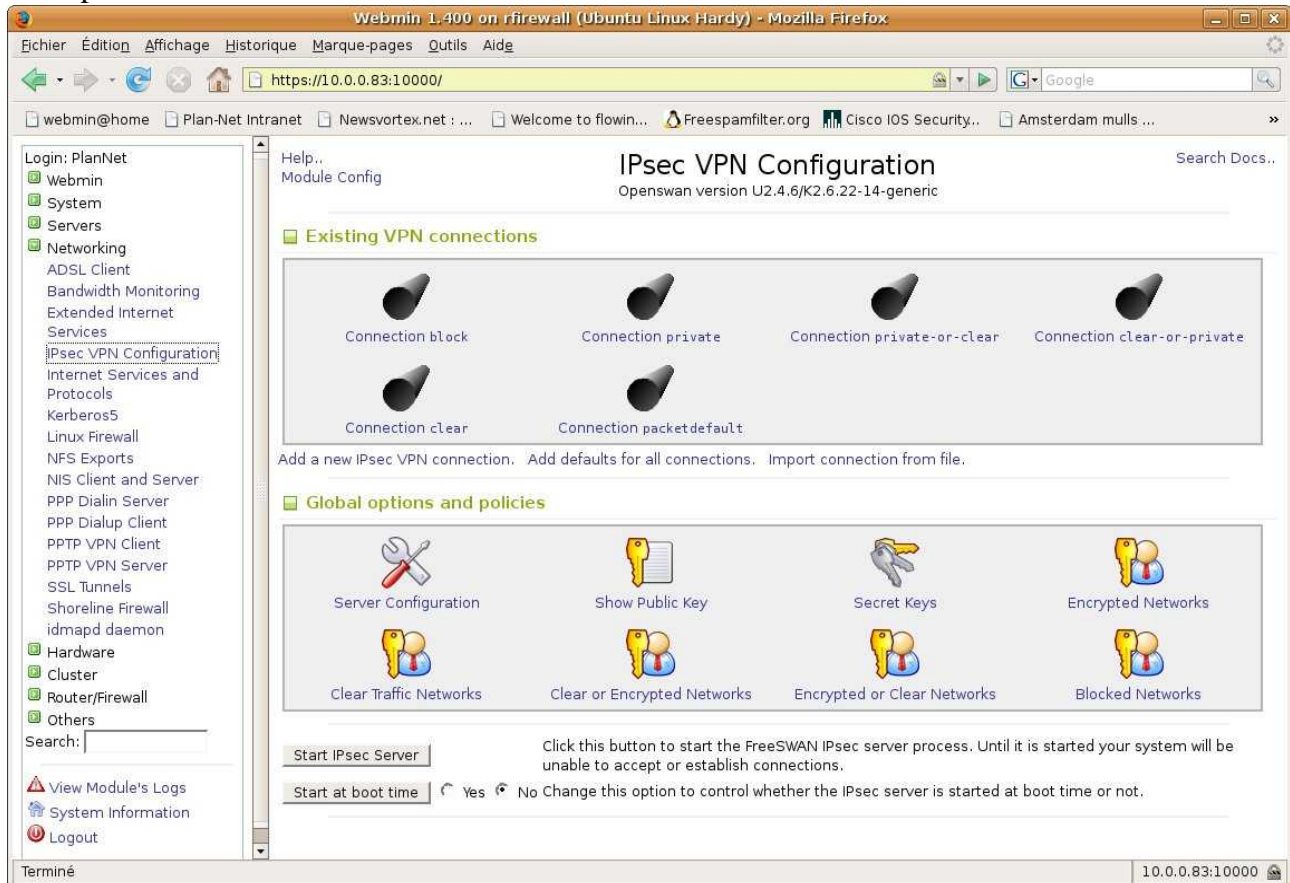
Exemple d'accès via VNC:



Exemple d'accès via SSH:



Exemple d'accès via HTTP/SSL:



Ils supportent divers types de tunnels (VPNs) dont:

1. OpenVPN: implémentation de tunnel OpenSource facile d'utilisation, disponible gratuitement pour MacOS, Windows, Linux, BSD, ... Fonctionne en mode client-serveur ou serveur-serveur. Se rétabli automatiquement même après de longues périodes d'indisponibilité de l'Internet. Peut fonctionner sur des adresses IP dynamiques, ...
2. IPSec: implémentation compatible avec d'autres stack IPSec (Cisco, ...)
3. Tunnels SSH, SSL, ...

Ils proposent des outils d'analyse du trafic réseau (WireShark, TcpDump, ...), de mesure des trafics (MRTG), de détection d'intrusions (SNORT), ...

Ils peuvent supporter des services optionnels, comme un serveur Web (Apache 2) en mode serveur ou reverse-proxy, des proxy-cache (Squid) avec ou sans contrôle d'accès, un serveur DNS, DHCP, ...

Les firewalls/routeurs Plan-Net sont totalement paramétrables, adaptables aux besoins de chacun. Ils offrent infiniment plus de fonctionnalités que leurs concurrents pour un prix négligeable, et indépendant de l'utilisation qui en est fait.

Pour tout renseignements, contactez Plan-Net Network Services s.a. au

+352-26.56.02.22