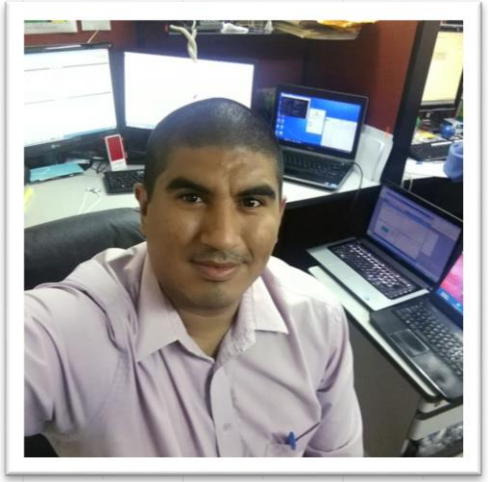
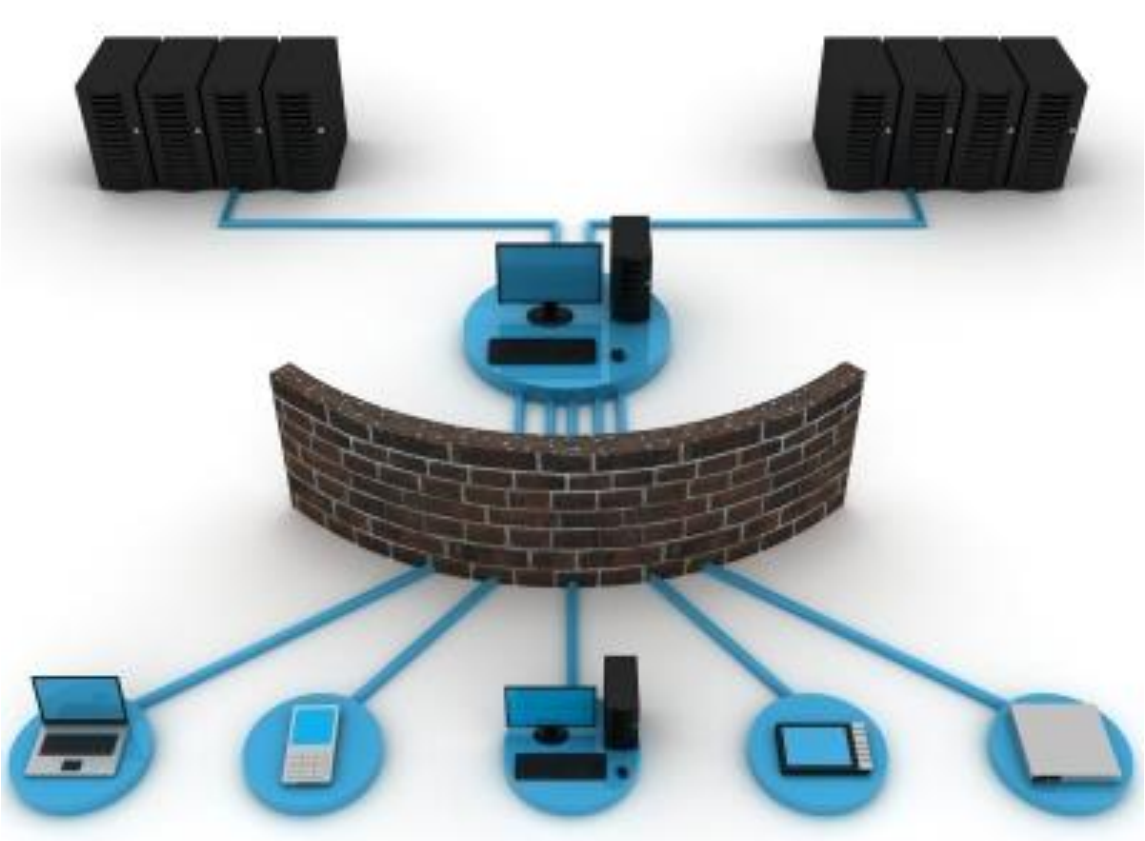
Seguridad Perimetral de Red para MIPYMES con Bajo Presupuesto

Iver Adolfo Vargas Villanueva

- Ingeniero en Sistemas de Información y Ciencias de la Computación
- Maestrías en Informática, Recursos Humanos y Energías Renovables
- Originario de Guastatoya, El Progreso
- Software, Bases de Datos, Infraestructura de Red, Ciberseguridad, Robótica, Inteligencia Artificial, etc
- Catedrático Universitario Titular en UMG
- Evaluador de Seminarios y Proyectos, así mismo conferencista en USAC y UGalileo.
- Miembro Organizador de las comunidades de Software Libre y Facebook Developer Circles
- Miembro Activo de las comunidades de Arduino, JavaUG, GDC, GDG y AWS.



Integración de elementos y sistemas, tanto electrónicos, lógicos como mecánicos, para la protección de perímetros físicos, detección de intrusos y otros.



Seguridad Perimetral de Red

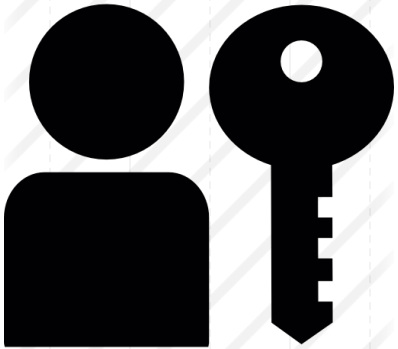
“Consiste en las políticas y prácticas adoptadas para prevenir y supervisar el acceso no autorizado, el uso indebido, la modificación o la denegación de una red informática y sus recursos accesibles.


Mi
PYME

Tamaño	Microempresa	Pequeña empresa	Mediana empresa
Trabajadores	1 – 10	11 – 80	81 -200
Ventas / salarios mínimos	<190	191 – 3,700	3,701 – 15,420
Ventas aproximadas en quetzales	< 480,764	De 480,765 a 9,364,788	De 9,364,789 a 39,017,843
Ventas aproximadas en dólares EUA a una tasa de Q.7.5	< 64,102	De 64,103 a 1,248,638	De 1,248,639 a 5,202,380


CONFIDENCIALIDAD
INTEGRIDAD
INFORMACIÓN
DISPONIBILIDAD

Elementos de Seguridad a Tomar en Cuenta



Autenticación

Políticas de Seguridad

Encriptación

Administración de Seguridad

“Ésta varía según las diversas situaciones. Una casa u oficina pequeña puede requerir solamente seguridad básica, mientras que las grandes empresas pueden requerir un software y hardware de alto mantenimiento y avanzado para evitar ataques maliciosos de piratería, spam u otros.

Tipos de Ataques

Pasivos

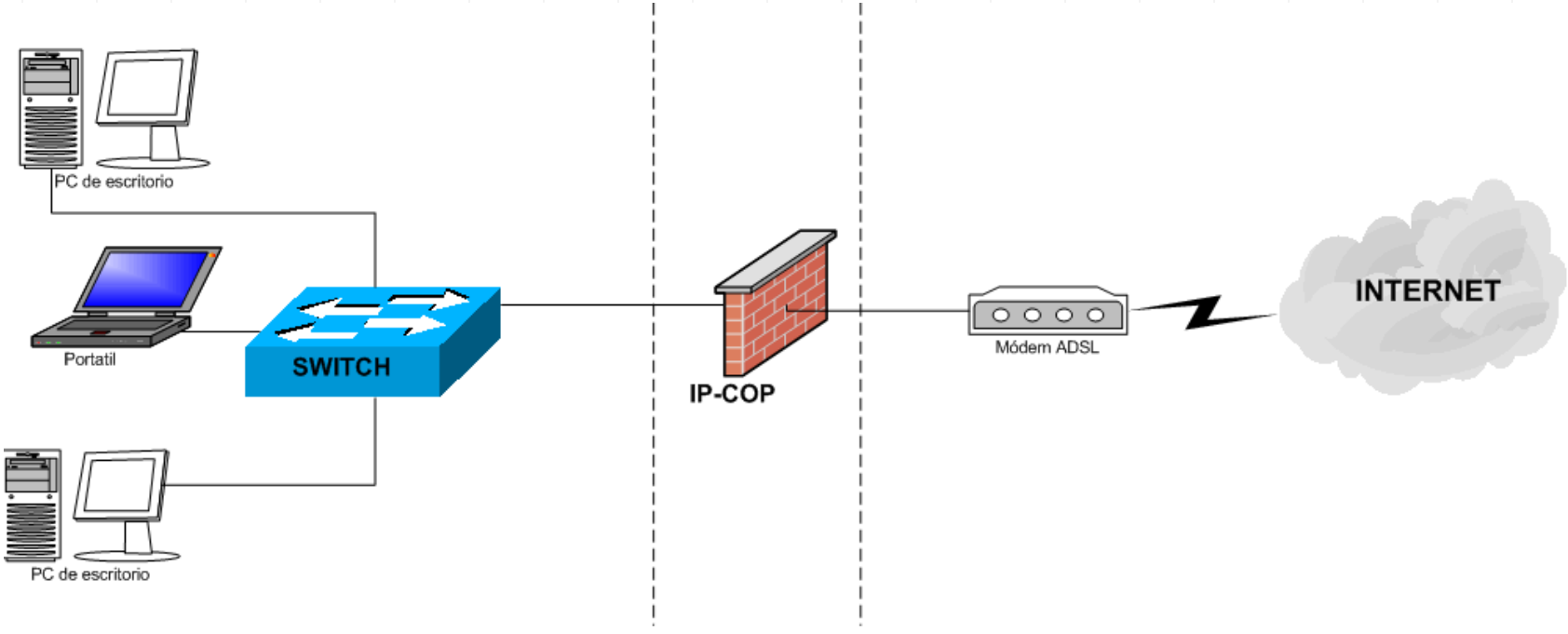
(Usuario Intercepta)

- Escuchas Telefónicas
- Escaneo de Puertos
- Escaneos Libres

Activos

(Espionaje por Códigos)

- DoS
- Middle in the Man
- SQL Injection
- Phishing

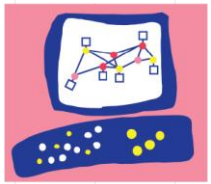

PC de escritorio
Portatil
SWITCH
PC de escritorio
IP-COP
Módem ADSL
INTERNET


FORTINET


paloalto
NETWORKS


WatchGuard


Barracuda
Your journey, secured.

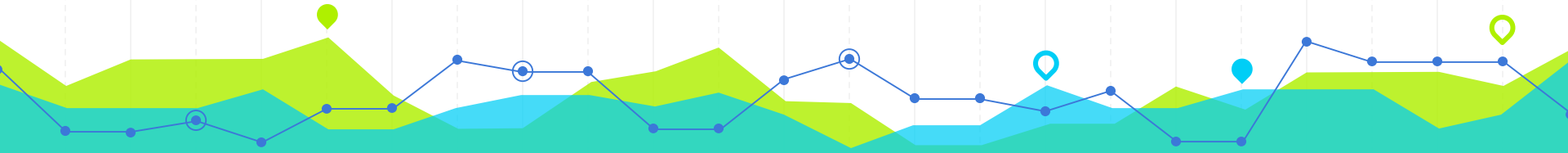



Check Point
SOFTWARE TECHNOLOGIES LTD.


websense

¿En que hay que invertir?

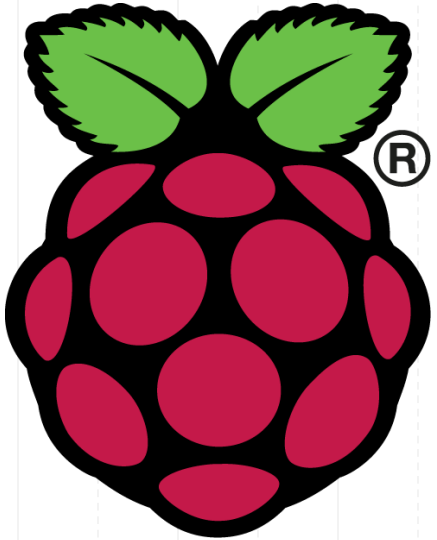
- Primer aparato
- Licenciamiento
- Soporte Técnico
- Capacitación
- Habilitación de otros módulos si fuera necesario



$ 150.00


IPFire


SanDisk
Ultra
32 GB
micro SD
HC I



IP Fire

“Distribución LINUX diseñada específicamente para hacer las funcionaes de un cortafuegos (firewall) y routing en una red local.

Una de las cualidades es que es un SO que utiliza pocos recursos, con tan solo 128MB de RAM podremos empezar a funcionar de manera eficiente.

Funcionalidades

- Servidor Proxy
- IDS – Sistema de Detección de Intrusos
- VPN a través de IPsec y OpenVPN
- Servidor DHCP
- Caché de nombres de dominio
- Servidor de Manejo de Hora
- Wake-on-Lan
- Servidor DNS y DDNS
- QoS
- Logs de todos los sucesos que ocurren en la red
- Funcionalidades adicionales a través de plug-ins para incorporar servicios de correo, Telefonía IP, DLNA, de Impresión, FTPs, etc.

https://www.ipfire.org

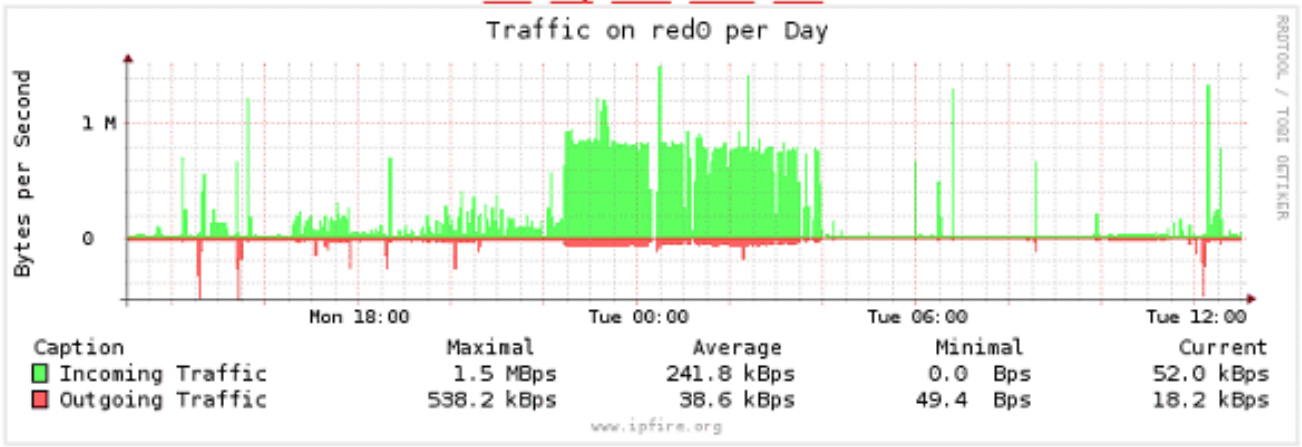
ipfire

network (external)

system | status | network | services | firewall | ipfire | logs

red0 graph

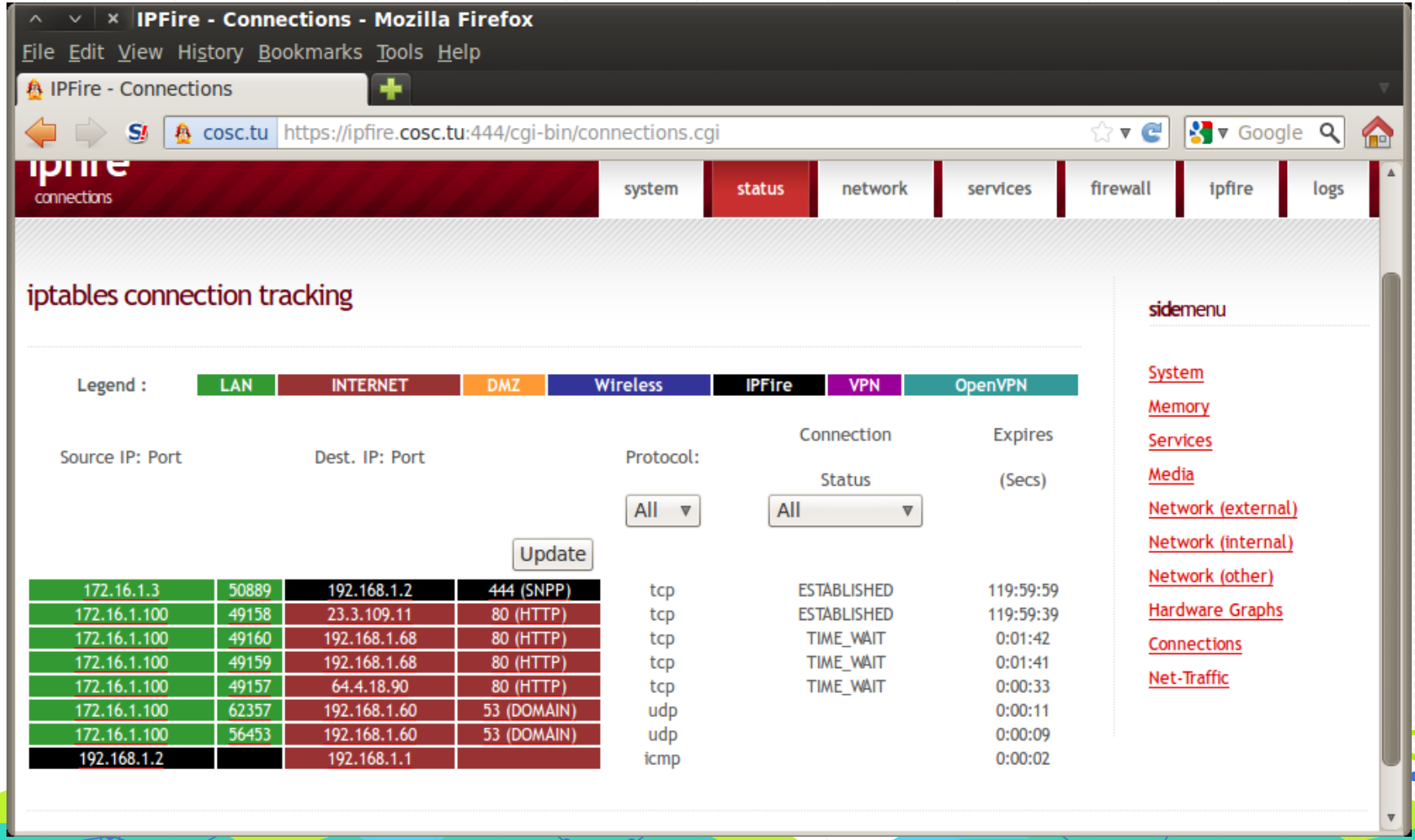
hour - Day - Week - Month - Year

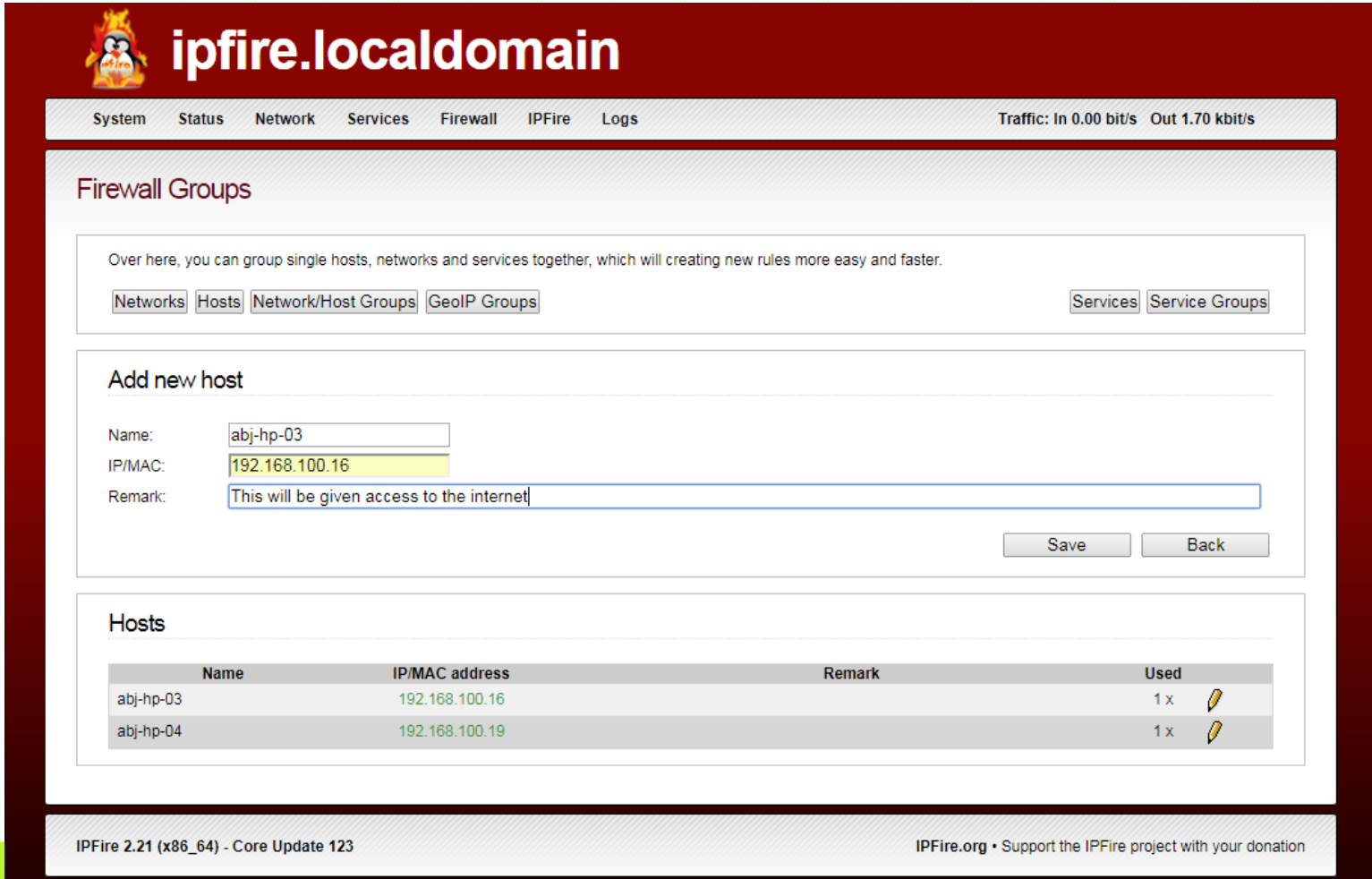


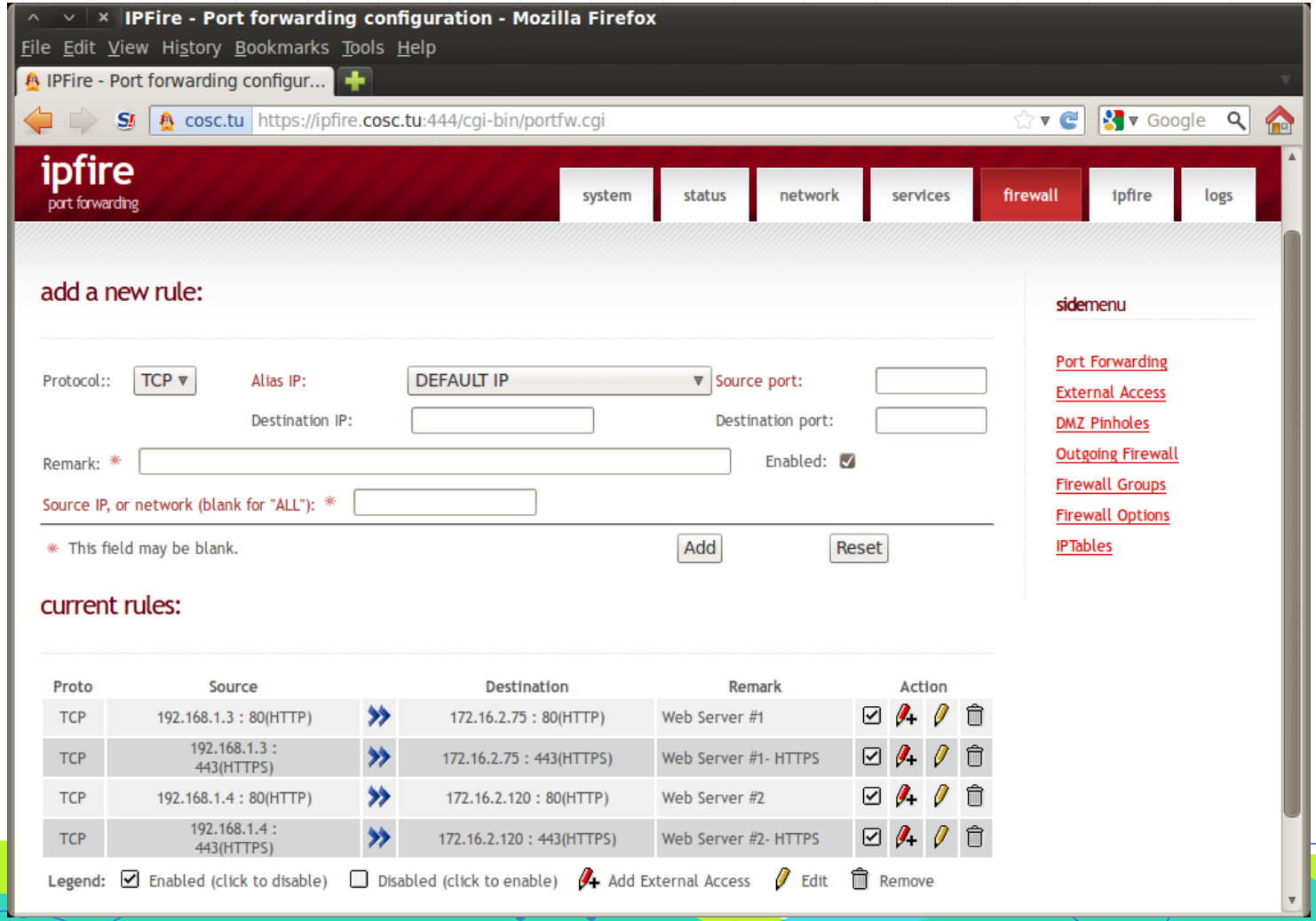
sidemenu

- System
- Memory
- Services
- Media
- Network (external)
- Network (internal)
- Network (other)
- Hardware Graphs
- Connections
- Net-Traffic


IPFire - Main page - Mozilla Firefox
File Edit View History Bookmarks Tools Help
IPFire - Main page
cosc.tu https://ipfire.cosc.tu:444/cgi-bin/index.cgi
Google
ipfire
home
system
status
network
services
firewall
ipfire
logs
ipfire
Reboot?
Refresh
Shutdown?
Network
IP
Status
INTERNET
192.168.1.2
Connected - (0d 1h 16m 48s)
Hostname:
ipfire.cosc.tu
Gateway:
192.168.1.1
DNS-Server:
192.168.1.60
192.168.1.61
LAN
172.16.1.2
Proxy off
DMZ
172.16.2.2
Online
• Please enable the fireinfo service.
sidemenu
Home
Dialup
SSH Access
Backup
GUI Settings
System information
Credits
status: connected - (0d 1h 16m 48s) uptime: 12:03:48 up 1:17, 1 user, load average: 0.05, 0.03, 0.00
bandwidth usage (external): incoming: 0 kb/s outgoing: 0 kb/s


IPFire - Connections - Mozilla Firefox
File Edit View History Bookmarks Tools Help
IPFire - Connections
cosc.tu https://ipfire.cosc.tu:444/cgi-bin/connections.cgi
Google
connections
system status network services firewall ipfire logs
iptables connection tracking
Legend : LAN INTERNET DMZ Wireless IPFire VPN OpenVPN
Source IP: Port
Dest. IP: Port
Protocol:
Connection Status
Expires (Secs)
All
All
Update
172.16.1.3 50889 192.168.1.2 444 (SNPP) tcp ESTABLISHED 119:59:59
172.16.1.100 49158 23.3.109.11 80 (HTTP) tcp ESTABLISHED 119:59:39
172.16.1.100 49160 192.168.1.68 80 (HTTP) tcp TIME_WAIT 0:01:42
172.16.1.100 49159 192.168.1.68 80 (HTTP) tcp TIME_WAIT 0:01:41
172.16.1.100 49157 64.4.18.90 80 (HTTP) tcp TIME_WAIT 0:00:33
172.16.1.100 62357 192.168.1.60 53 (DOMAIN) udp 0:00:11
172.16.1.100 56453 192.168.1.60 53 (DOMAIN) udp 0:00:09
192.168.1.2 192.168.1.1 icmp 0:00:02
sidemenu
System
Memory
Services
Media
Network (external)
Network (internal)
Network (other)
Hardware Graphs
Connections
Net-Traffic


ipfire.localdomain
System Status Network Services Firewall IPFire Logs
Traffic: In 0.00 bit/s Out 1.70 kbit/s
Firewall Groups
Over here, you can group single hosts, networks and services together, which will creating new rules more easy and faster.
Networks Hosts Network/Host Groups GeoIP Groups Services Service Groups
Add new host
Name: abj-hp-03
IP/MAC: 192.168.100.16
Remark: This will be given access to the internet
Save Back
Hosts
Name IP/MAC address Remark Used
abj-hp-03 192.168.100.16 1 x
abj-hp-04 192.168.100.19 1 x
IPFire 2.21 (x86_64) - Core Update 123
IPFire.org • Support the IPFire project with your donation


IPFire - Port forwarding configuration - Mozilla Firefox
File Edit View History Bookmarks Tools Help
IPFire - Port forwarding configur...
cosc.tu https://ipfire.cosc.tu:444/cgi-bin/portfw.cgi
Google
ipfire
port forwarding
system
status
network
services
firewall
ipfire
logs
add a new rule:
Protocol:: TCP
Alias IP: DEFAULT IP
Source port:
Destination IP:
Destination port:
Remark: *
Enabled:
Source IP, or network (blank for "ALL"): *
* This field may be blank.
Add
Reset
current rules:
Proto
Source
Destination
Remark
Action
TCP 192.168.1.3 : 80(HTTP) 172.16.2.75 : 80(HTTP) Web Server #1
TCP 192.168.1.3 : 443(HTTPS) 172.16.2.75 : 443(HTTPS) Web Server #1- HTTPS
TCP 192.168.1.4 : 80(HTTP) 172.16.2.120 : 80(HTTP) Web Server #2
TCP 192.168.1.4 : 443(HTTPS) 172.16.2.120 : 443(HTTPS) Web Server #2- HTTPS
Legend: Enabled (click to disable) Disabled (click to enable) Add External Access Edit Remove
sidemenu
Port Forwarding
External Access
DMZ Pinholes
Outgoing Firewall
Firewall Groups
Firewall Options
IPTables

¡¡¡Muchas Gracias!!!

@ing_ivargas84

ing.ivargas84@gmail.com

ingivargas84

www.vrinfosysgt.com