



Seguridad Perimetral de Red con Bajo Presupuesto

Como un pingüino se come una frambuesa

Ing. Iver Adolfo Vargas Villanueva



Seguridad Perimetral

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



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.







Elementos de Seguridad



Autenticación



**Aplicación
de
Políticas**

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 y spam.





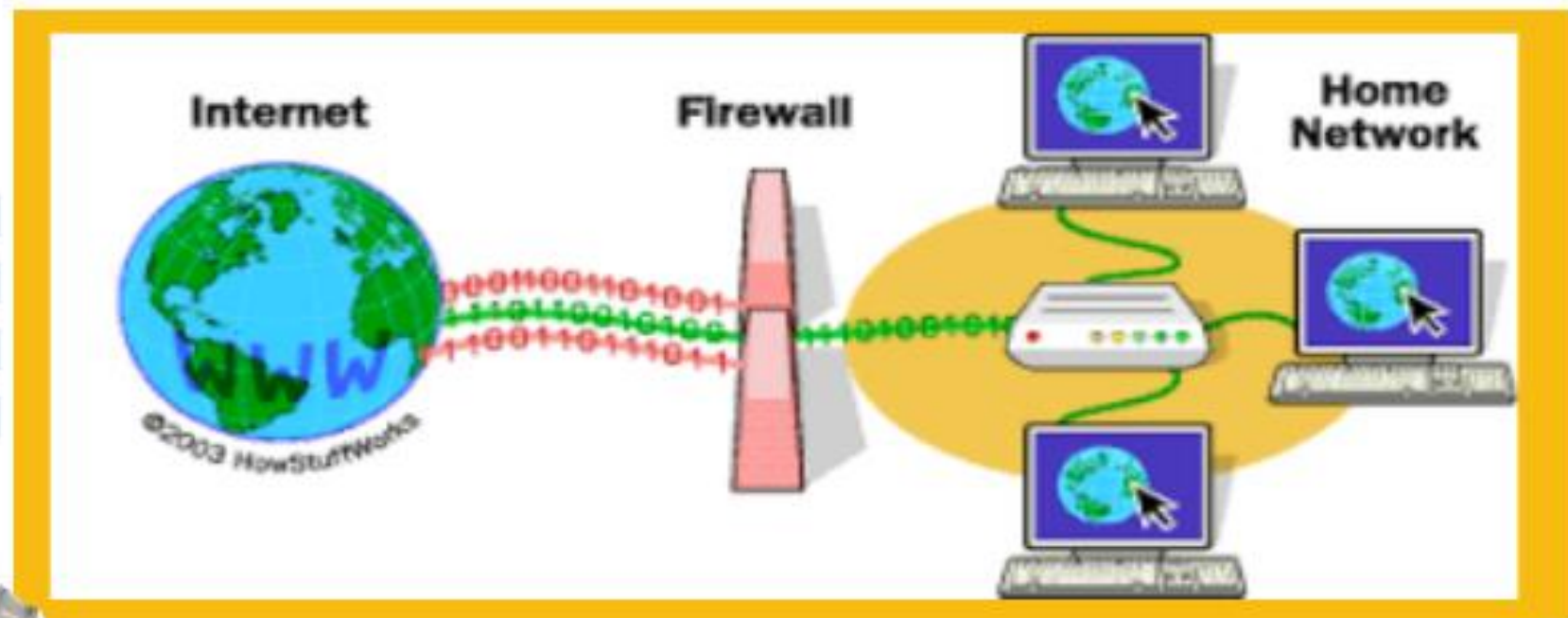
ATAQUES

Pasivos (usuario intercepta)

Escuchas Telefónicas
Escaneo de Puertos
Escaneos Libres

Activos (espionaje por códigos)

DoS
Middle in the Man
Inyección SQL
Phishing



FORTINET®



Check Point®
SOFTWARE TECHNOLOGIES LTD.



paloalto
NETWORKS®



websense®
ESSENTIAL INFORMATION PROTECTION™



Q.1,200.00



Raspberry Pi



IP Fire

IPFire es una distribución Linux diseñada específicamente para hacer las funciones de cortafuegos (firewall) y routing en una red local.

Una de las cualidades de IPFire es que es un sistema operativo que funciona con muy pocos recursos, con tan sólo 128MB de memoria RAM podremos empezar a funcionar con él, aunque si utilizamos todas las opciones y tenemos muchos equipos conectados, deberemos ampliar la capacidad de procesamiento y memoria del sistema.



FUNCIONALIDADES

- Servidor Proxy.
- Sistema de detección de intrusos en una red o equipo.
- VPN a través de IPsec y OpenVPN.
- Servidor DHCP.
- Caché de nombres de dominio.
- Servidor horario.
- Wake-on-Lan.
- Servidor DDNS.
- QoS.
- Completo Log de todos los sucesos que ocurren en el sistema.



IPFire permite la instalación de software adicional a través de plugins, algunas funcionalidades extra que podemos incorporarle es por ejemplo un servidor de archivos en red, servidor de impresión, Asterisk, TeamSpeak, servidor de correo, servidor de medios DLNA y otros plugins disponibles en la página web oficial.

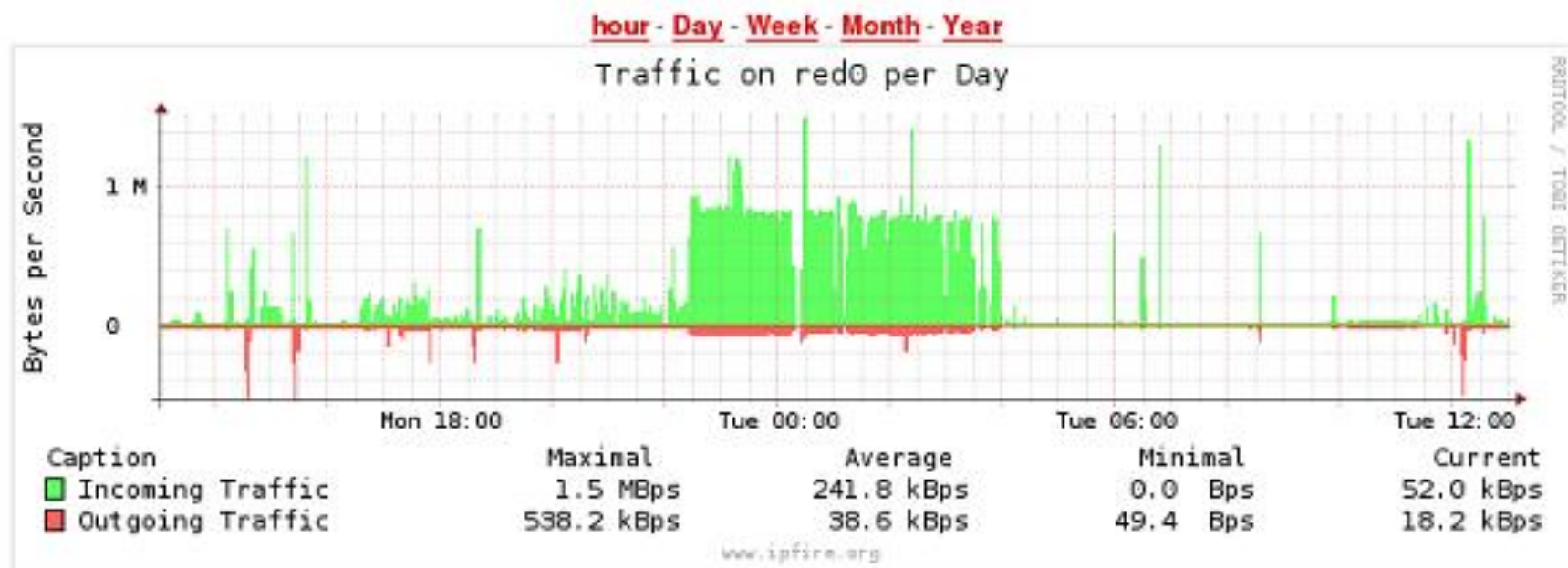
IPFire también es compatible con arquitecturas ARM, es decir, es compatible con Raspberry PI o equipos similares. IPFire se puede descargar desde su página web principal de forma totalmente gratuita.

<https://www.ipfire.org/>



Activar Windows

red0 graph



sidemenu

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

^ v x 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
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 - 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

sidemenu

Port Forwarding

External Access

DMZ Pinholes













Outgoing Firewall

Firewall Groups

Firewall Options

IPTables


current rules:


Proto	Source		Destination	Remark	Action
TCP	192.168.1.3 : 80(HTTP)	➡➡	172.16.2.75 : 80(HTTP)	Web Server #1	<input checked="" type="checkbox"/>   
TCP	192.168.1.3 : 443(HTTPS)	➡➡	172.16.2.75 : 443(HTTPS)	Web Server #1- HTTPS	<input checked="" type="checkbox"/>   
TCP	192.168.1.4 : 80(HTTP)	➡➡	172.16.2.120 : 80(HTTP)	Web Server #2	<input checked="" type="checkbox"/>   
TCP	192.168.1.4 : 443(HTTPS)	➡➡	172.16.2.120 : 443(HTTPS)	Web Server #2- HTTPS	<input checked="" type="checkbox"/>   


Legend:

☒ Enabled (click to disable)

☐ Disabled (click to enable)

 Add External Access

 Edit

 Remove



Ing. Iver Adolfo Vargas Villanueva
ivargas@vrinfosysgt.com
www.vrinfosysgt.com

¡¡Muchas Gracias!!

