Linux-IpFire hardening lan with suricata/IPS

whoami

01

Fabio Carletti aka Ryuw

Membro Clusit

Strategic IT consultant

Volontario nel progetto TOR

Criminologo IT Forense presso ANCRIM

Currently IT Security Specialist presso Onova SPA

I like unix ;-)

You can find me at Linkedin

02

Umberto Parma

Programmatore da 40 anni settore d'automazione industriale
Esperto in sicurezza nel settore OT
Fondatore della community italiana IPFire

Linux-IpFire hardening lan with suricata/IPS

IPFIRE-Security IT

La sicurezza del codice è un processo da inserire nella strategia security IT

- Il software scritto senza molte attenzioni nell'ambito della sicurezza sta influendo le fondamenta di infrastrutture informatiche
- Il mio sistema Operativo è sicuro..

IpFire

Statistiche (CLUSIT)...

- 73% dei dirigenti sono convinti della solidità delle pratiche di sicurezza
- 41% non sa quanti incidenti negli ultimi 24 mesi o non sa che tipo di incidenti sono avvenuti
- Audit e Controlli IT:verifica da parte di terzi
- Sicurezza IT: supervisione quotidiana dei sistemi

IpFire

Types of Cyber Attack

1. Viruses
2. Malware Attack
3. Phishing Attack
4. Password Attacks
5. Vishing Attacks
6. Man in the Middle Attacks
7. Dos/ DDoS
8. Brute Force Attack
9. Spyware & Keylogger
10. Cross Site Scripting
11. SQL Injection

IpFire

- Non è quasi mai possibile aggiungere la sicurezza ad un prodotto IT: 1)Acquisto HW...funzionalità di sicurezza non implementabili a posteriori 2)Procedure del Personale..difficile far cambiare le abitudini.
- Il firmware è il software che il router esegue e una versione obsoleta potrebbe contenere vulnerabilità di sicurezza note.
- Essere attenti alla sicurezza dei propri dati non significa solo diffidare dei tentativi di pishing e dei siti web pericolosi.
- Gli attaccanti possono facilmente entrare nelle reti approfittando di un firmware non aggiornato

IpFire

- Piuttosto che applicare la sicurezza alle applicazioni è più efficace progettare la sicurezza dall'inizio.
- The computer as a target
- The computer as a weapon
- Transmitting virus
- Malware (Malicious softWare)

Lessons learned

➲ Sicurezza, Qualità e Progetti

➲ Sicurezza Prima, Durante e Dopo

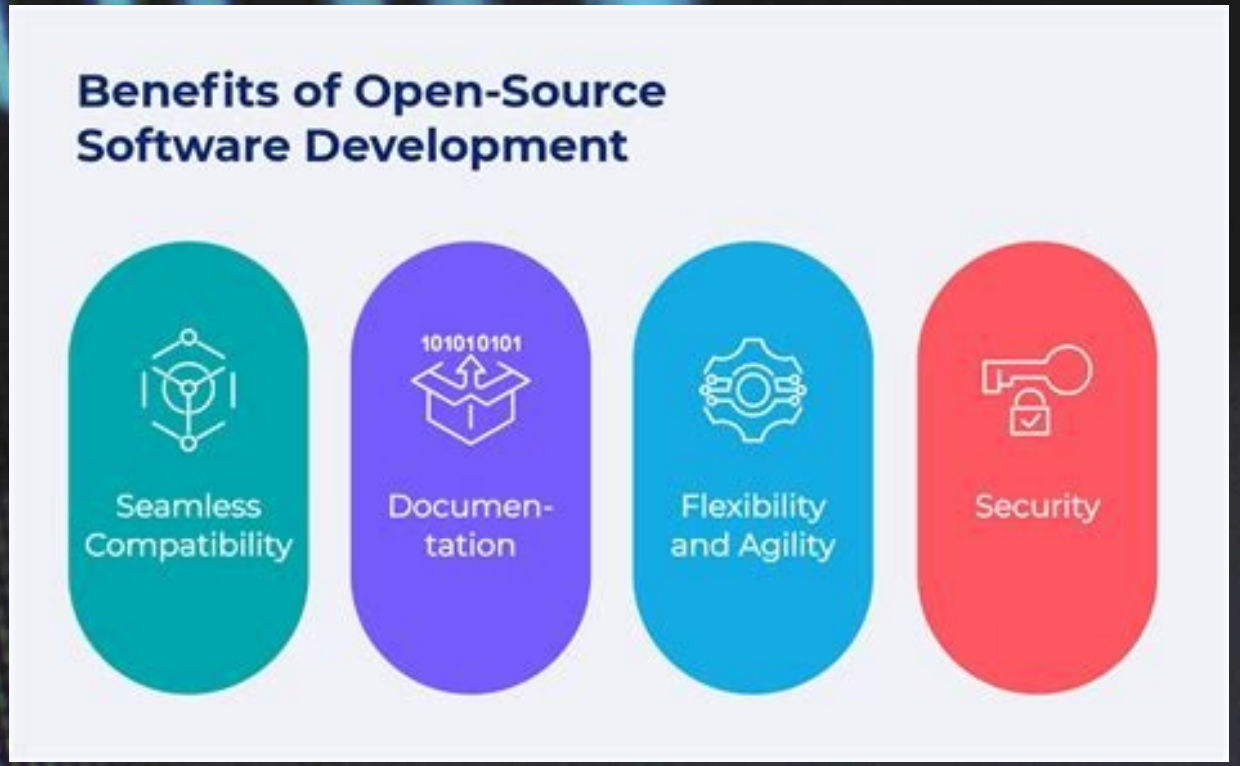
➲ Sicurezza Sempre Valutata da capo e su Tutto

----> il Progetto IPFIRE

GNU/linux IPFIRE

FIREWALL OPENSOURCE PROJECT

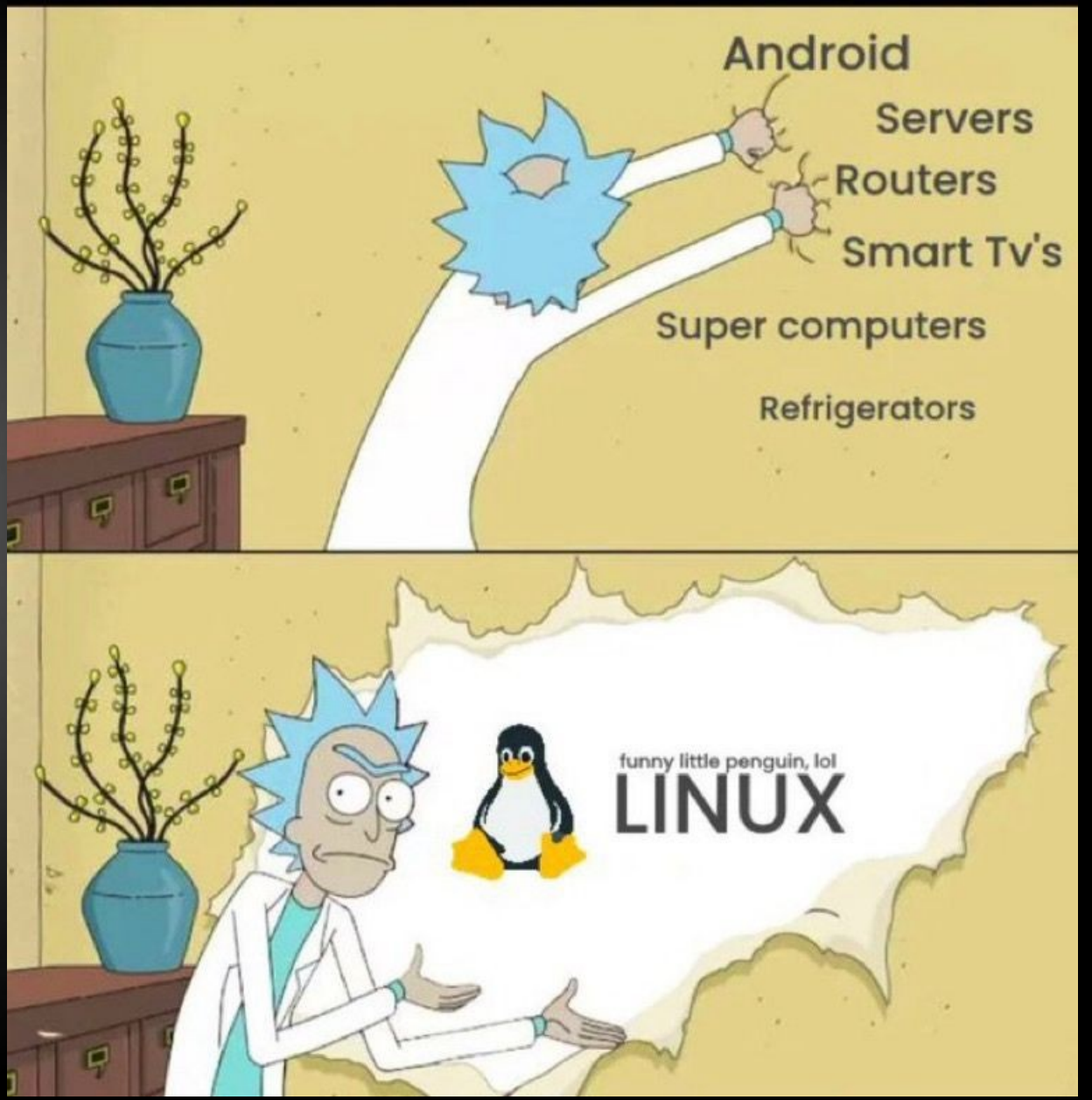
https://www.ipfire.org/



IpFire


PASSWORD


IPFIRE


Android
Servers
Routers
Smart Tv's
Super computers
Refrigerators
funny little penguin, lol
LINUX

GNU/Linux

- Gnu/Linux supporta un enorme quantità di Filesystem diversi. E' opensource il sorgente è visionabile. Una delle tipologie di IDS tipo snort/suricata è quella in cui vengono osservate le operazioni compiute sul sistema per rilevare i tentativi di eseguire operazioni non autorizzate.
- Progetto LIDS= Linux intrusion Detection System.
- Snort=è un applicativo GPL open source permette l'analisi dei pacchetti all'interno di una rete.
- Suricata=Suricata è un software open source ad alte prestazioni per l'analisi di rete e il rilevamento delle minacce, utilizzato dalla maggior parte delle organizzazioni pubbliche e private e integrato dai principali fornitori per proteggere le proprie risorse.

SNORT vs SURICATA

- SURICATA
- L'architettura multi-thread consente l'elaborazione efficiente di più attività contemporaneamente
- Migliori prestazioni in ambienti ad alto traffico
- Funzionalità avanzate di rilevamento e prevenzione delle intrusioni

- SNORT
- Architettura single-threaded
- Maggiore compatibilità con dispositivi, sistemi operativi e strumenti di terze parti grazie alla sua maggiore presenza sul mercato
- Migliori prestazioni in ambienti con risorse limitate

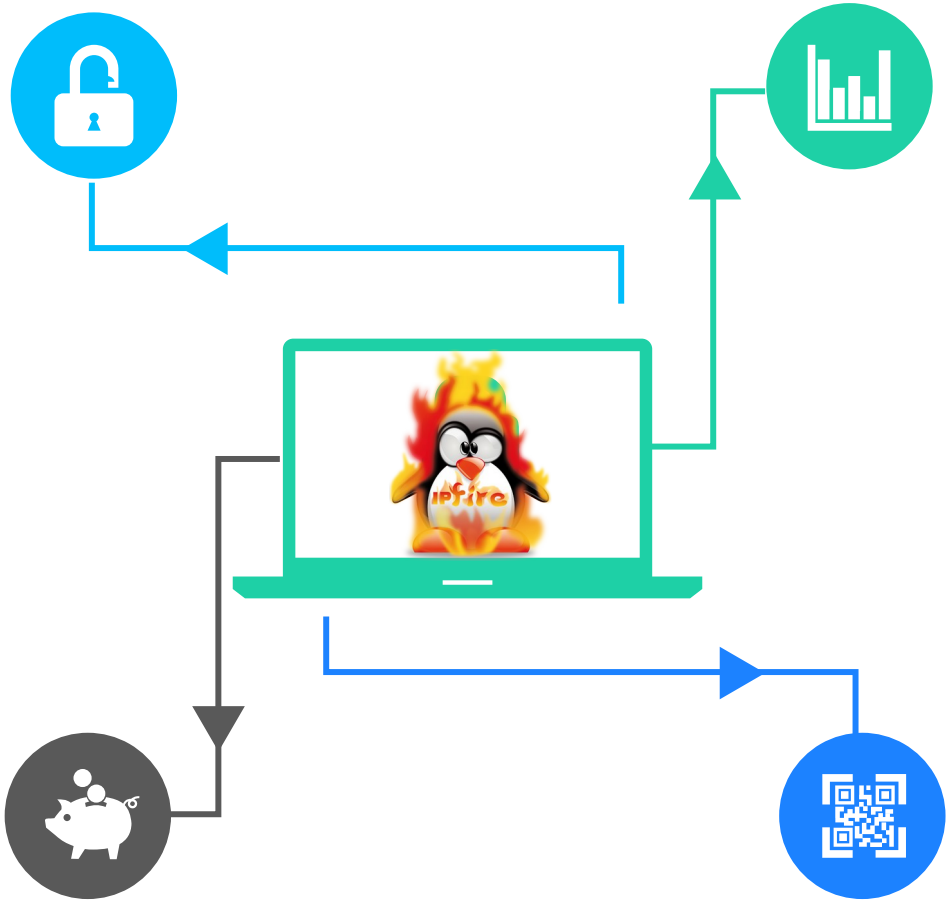
IpFire

IPFire è stato progettato tenendo conto sia della modularità che di un elevato livello di flessibilità. È possibile implementarne facilmente molte varianti, come un firewall, un server proxy o un gateway VPN. Il design modulare garantisce che funzioni esattamente come lo avete configurato e nulla più. Tutto è semplice da gestire e aggiornare tramite il gestore di pacchetti, rendendo la manutenzione non troppo complicata.

IPFIRE

Security by Design

Network segmentation is the key to a secure network. IPFire sets up a DMZ for your local infrastructure or a guest network for any visitors separating and protecting other parts of your network.



Industry-Leading Firewall Engine

Our stateful packet inspection firewall engine analyses traffic for the latest threats and performs deep packet inspection in real time. Due to our smart user interface, creating even complex setups is quick and straight-forward.

Supporting Global Standards

Commonly deployed in businesses and educational organisations of all sizes, IPFire interoperates perfectly with solutions from other vendors making it an ideal drop-in replacement.

Free As In Freedom

IPFire is free software. Our community develops and reviews all changes going into the code base and IPFire is regularly audited by independent third parties. Become a part of the community and help us to continue improving IPFire!

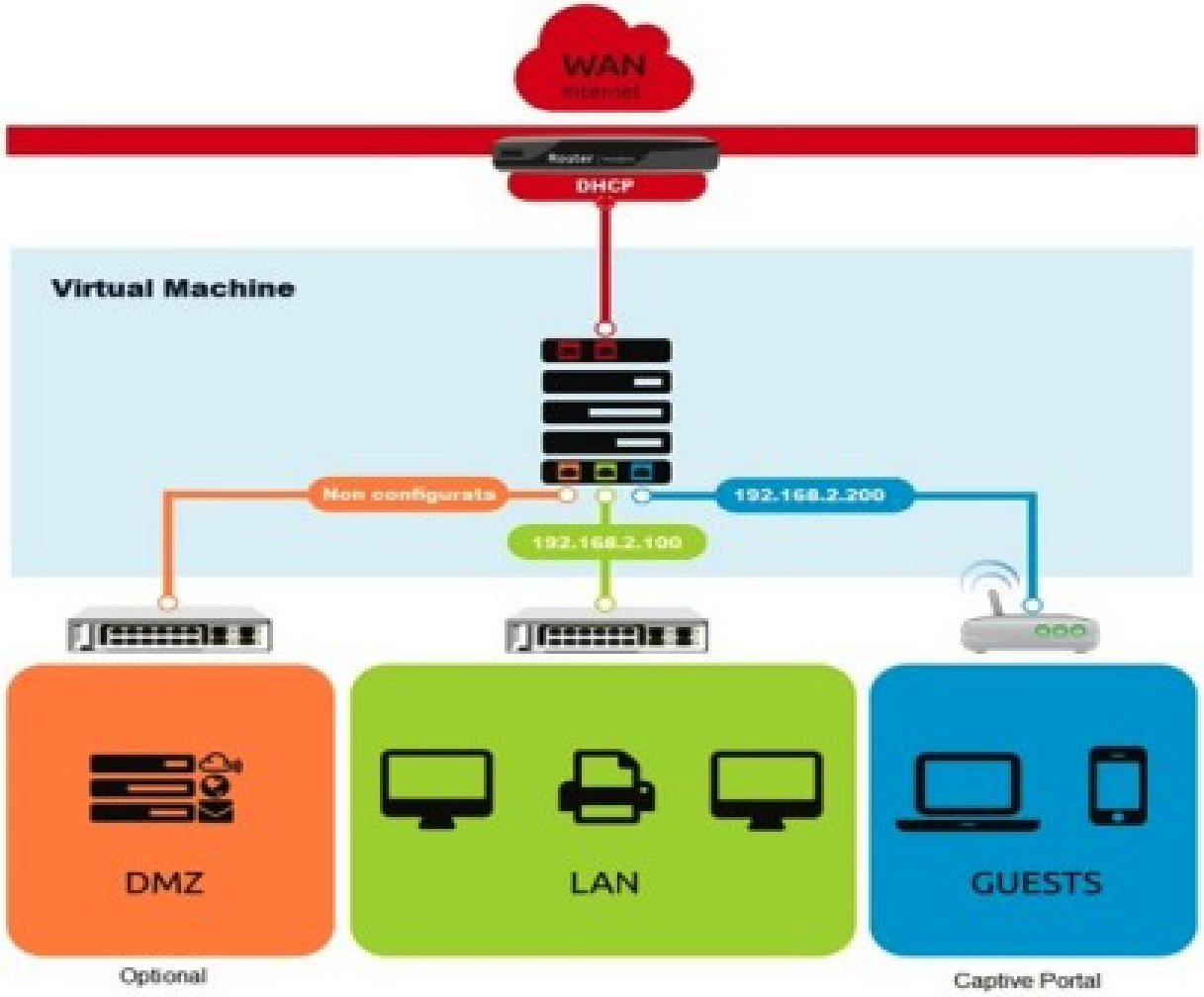
IPFIRE zone

RED-GREEN-Orange-BLUE

Red	**WAN**	**Rete esterna, collegato ad Internet (in genere una connessione all'ISP)**
Green	LAN	Rete privata / interna, collegamento a livello locale
Orange	DMZ	La zona demilitarizzata, una rete di server non protetti accessibili da internet
Blue	WLAN	Wireless Network, una rete separata per i client wireless e ospiti

IPFIRE zone

RED-WAN
GREEN-LAN
Orange-DMZ
BLUE-GUEST



IPFIRE zone

RED-WAN
GREEN-LAN
Orange-DMZ
BLUE-GUEST

Connessioni

Legenda : LAN | INTERNET | DMZ | Wireless | IPFire | VPN | WireGuard | OpenVPN | Multicast

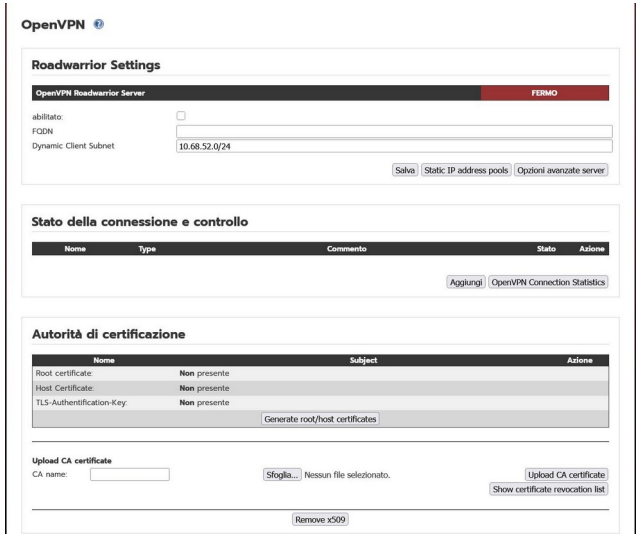
Search

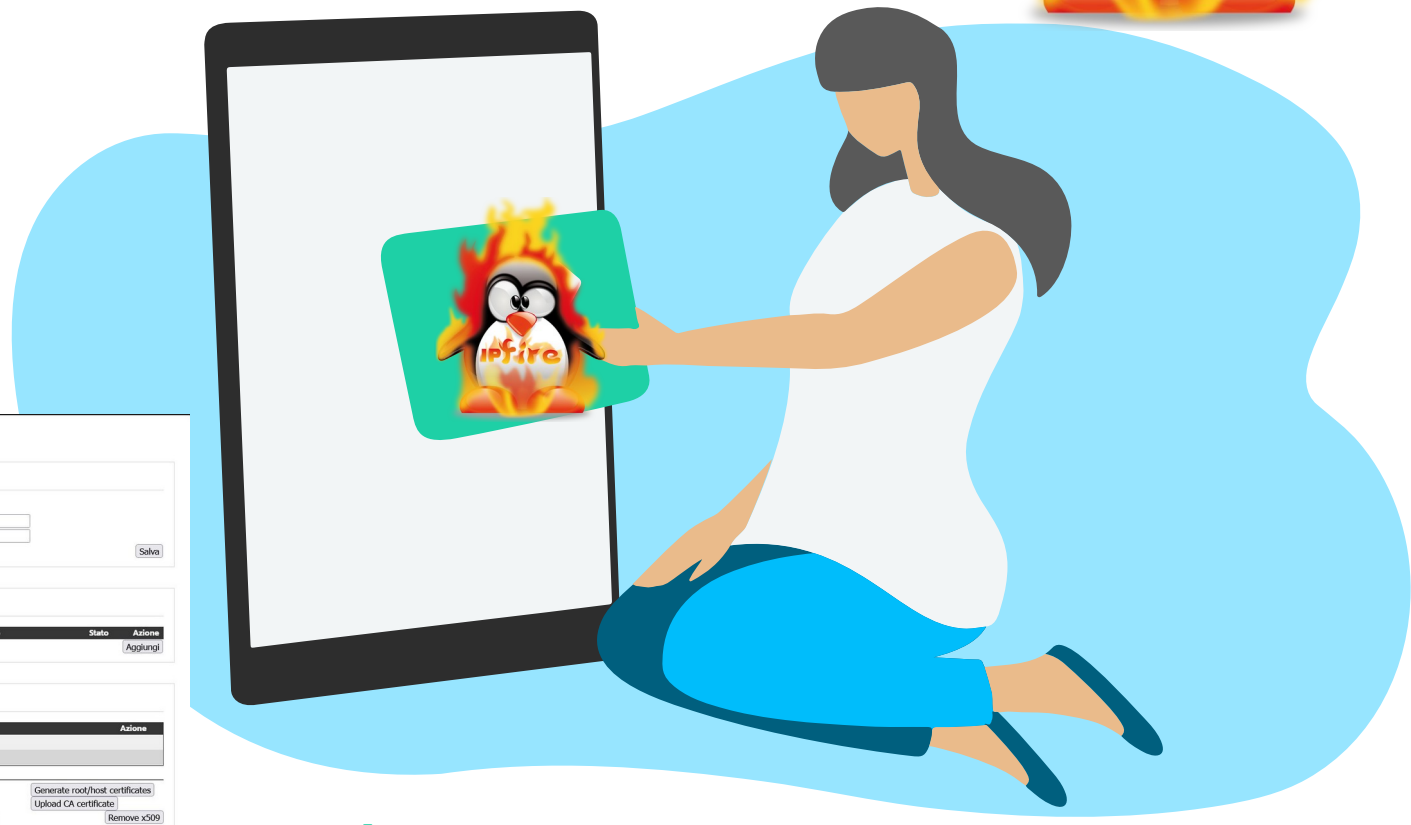
Indirizzo IP: Port: Protocollo Search

Protocollo	IP Sorgente: Porta		Ip Destinazione: Porta			Data Transfer		connessione Stato	Scade (O:M:S)
TCP	192.168.1.10	57368	194.76.116	443		> 1.84 KB	< 1.18 KB	ESTABLISHED	4d 23h 59m 59s
TCP	192.168.1.10	57362	194.76.116	443		> 1.78 KB	< 1.29 KB	ESTABLISHED	4d 23h 59m 59s
TCP	192.168.10.21 > 192.168.1.10	23206	216.58.21	443		> 5.61 KB	< 7.31 KB	ESTABLISHED	4d 23h 59m 59s
TCP	192.168.10.27	49670	192.168.10.1	800		> 14.48 KB	< 25.72 KB	ESTABLISHED	4d 23h 59m 59s
TCP	192.168.10.27 > 192.168.1.10	56573	149.154.167	443		> 745.66 KB	< 470.24 KB	ESTABLISHED	4d 23h 59m 59s
TCP	192.168.1.10	59010	52.123.200	443		> 15.69 KB	< 26.26 KB	ESTABLISHED	4d 23h 59m 59s
TCP	192.168.10.27 > 192.168.1.10	56562	149.154.167	443		> 748.33 KB	< 472.94 KB	ESTABLISHED	4d 23h 59m 59s
TCP	192.168.10.27 > 192.168.1.10	56568	149.154.167	443		> 747.51 KB	< 470.21 KB	ESTABLISHED	4d 23h 59m 59s
TCP	192.168.10.27 > 192.168.1.10	56575	149.154.167	443		> 1.19 MB	< 1.73 MB	ESTABLISHED	4d 23h 59m 59s
TCP	192.168.10.27	56938	192.168.10.1	800		> 996.00 B	< 788.00 B	ESTABLISHED	4d 23h 59m 58s
TCP	192.168.10.27	61843	192.168.10.1	800		> 335.06 KB	< 42.90 KB	ESTABLISHED	4d 23h 59m 58s
TCP	192.168.1.10	53526	34.107.221	80		> 1002.00 B	< 648.00 B	ESTABLISHED	4d 23h 59m 58s
TCP	192.168.10.27	58784	192.168.10.1	800		> 328.79 KB	< 382.14 KB	ESTABLISHED	4d 23h 59m 57s
TCP	192.168.10.14 > 192.168.1.10	45524	31.13.86.	443		> 2.76 KB	< 2.49 KB	ESTABLISHED	4d 23h 59m 57s
TCP	192.168.1.10	50542	149.154.16	443		> 3.86 KB	< 11.94 KB	ESTABLISHED	4d 23h 59m 56s
TCP	192.168.10.21 > 192.168.1.10	45156	3.160.212	443		> 3.10 MB	< 139.25 MB	ESTABLISHED	4d 23h 59m 56s
TCP	192.168.10.27	58819	192.168.10.1	800		> 548.22 KB	< 46.06 MB	ESTABLISHED	4d 23h 59m 55s

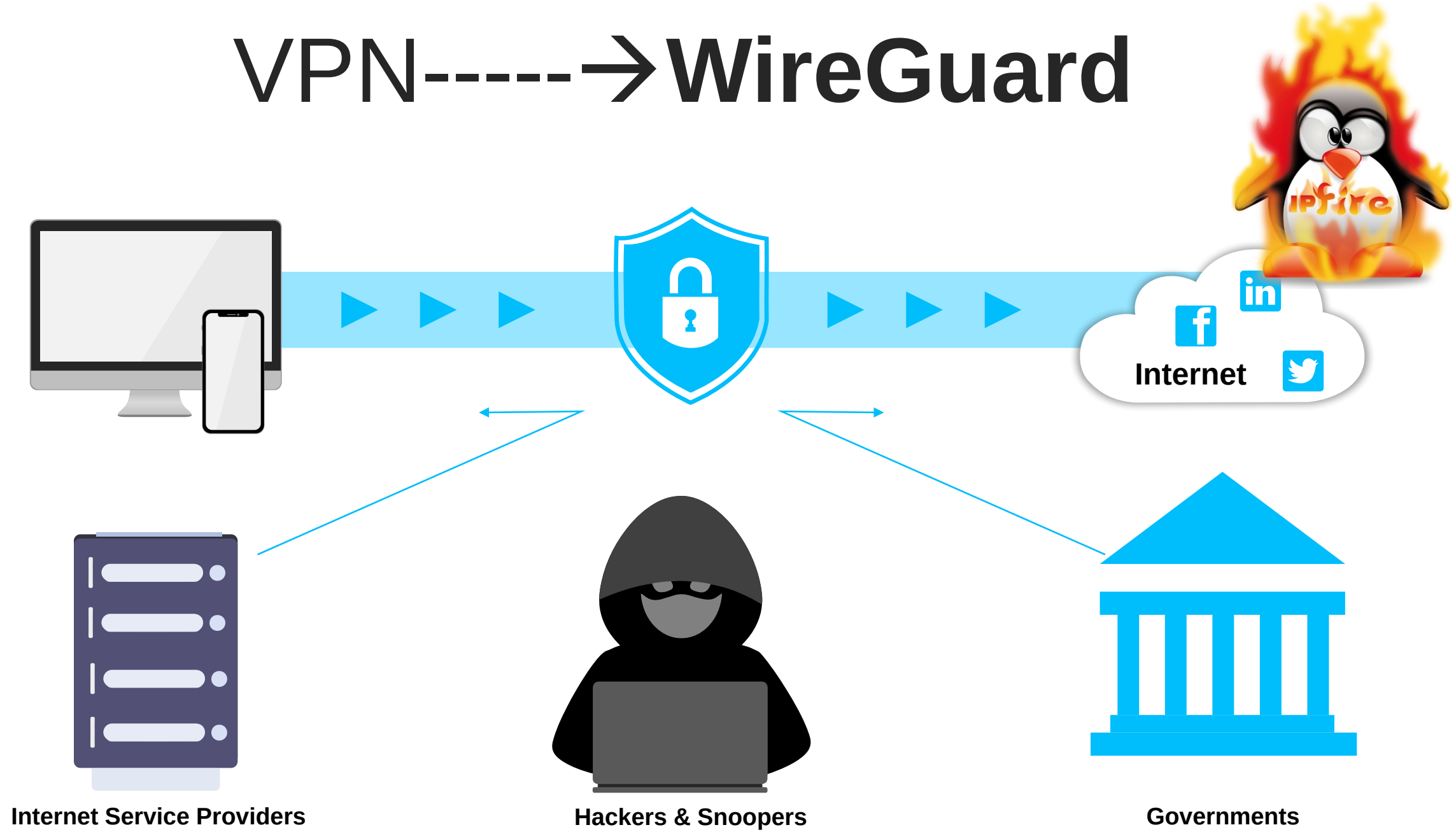
IPFIRE VPN

VPN OpenVPN e IPsec



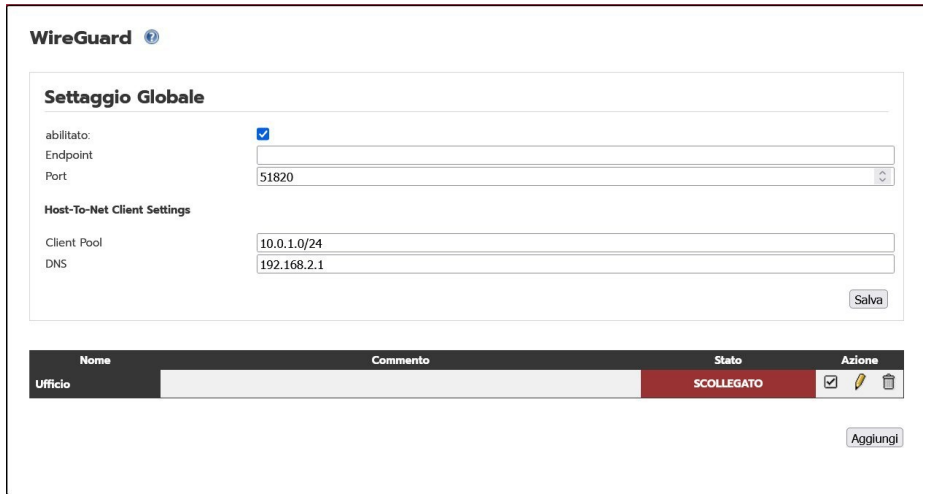


VPN----->**WireGuard**

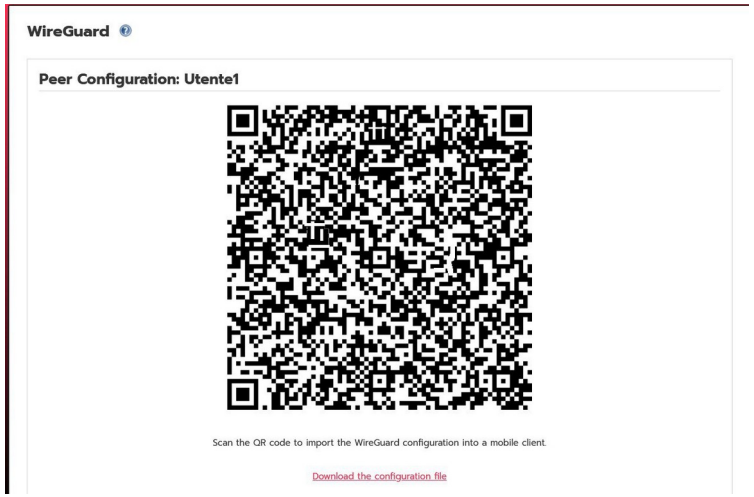


VPN----->WireGuard

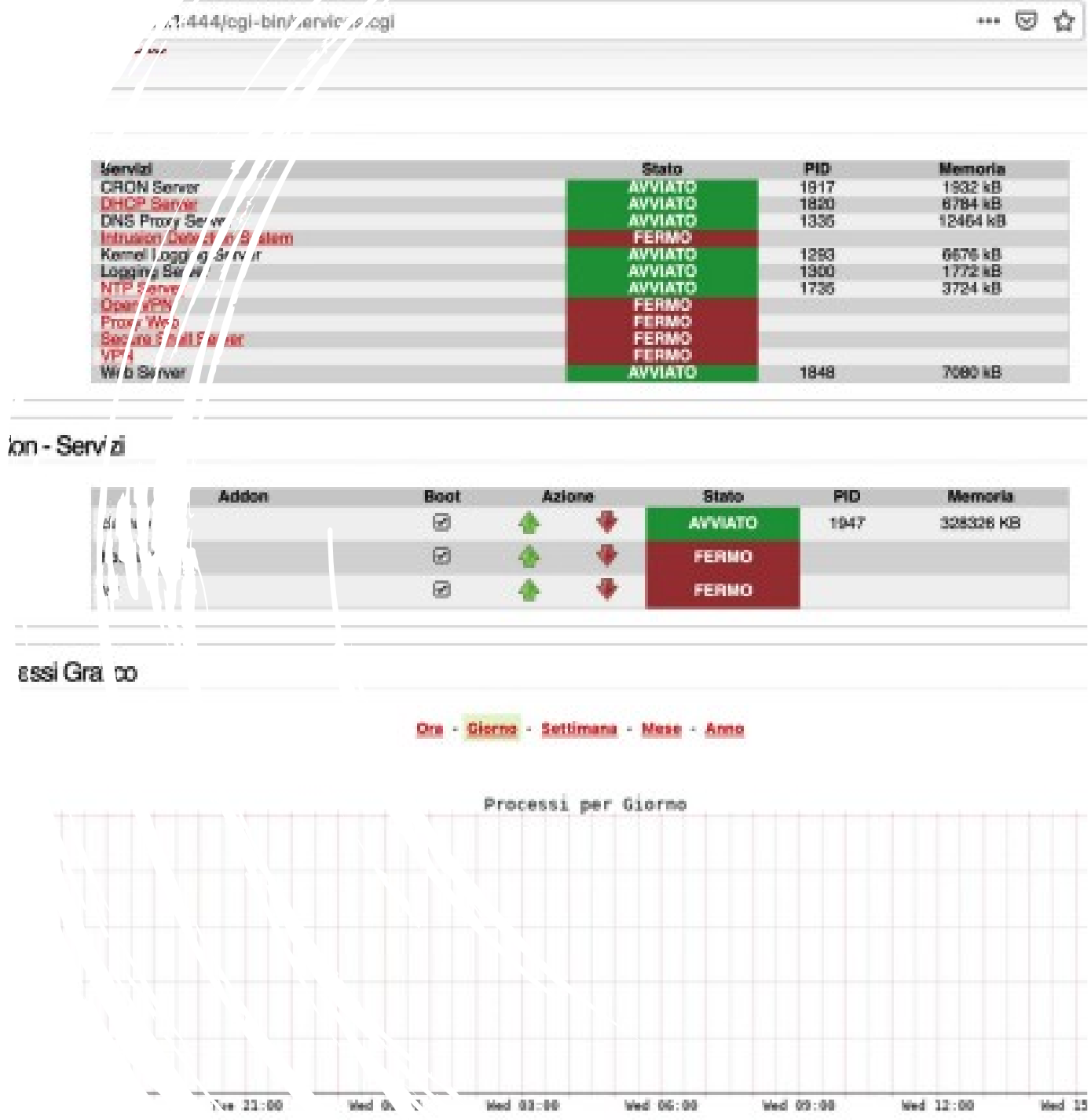
Semplicità nella configurazione server



Semplicità nella configurazione client



IPFIRE
services



“Nel vero OpenSource hai il diritto di controllare il tuo destino..Linus Torvalds”

IPFIRE
services

“Nel vero OpenSource hai il diritto di controllare il tuo destino..Linus Torvalds”

Informazioni e Stato

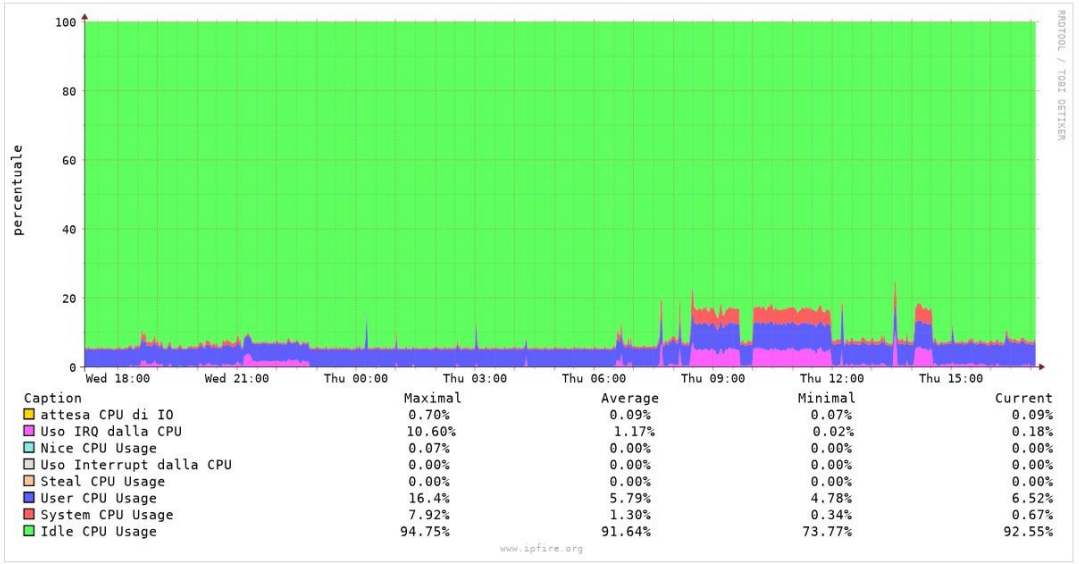
CRON Server	AVVIATO	1.98 MB RSS
DHCP Server	AVVIATO	6.38 MB RSS
DNS Proxy Server	AVVIATO	2.20 GB RSS
Intrusion Prevention System	AVVIATO	532.68 MB RSS
Kernel Logging Server	AVVIATO	12.99 MB RSS
Logging Server	AVVIATO	1.83 MB RSS
NTP Server	AVVIATO	3.44 MB RSS
OpenVPN Roadwarrior Server	FERMO	
Proxy Web	AVVIATO	81.96 MB RSS
Secure Shell Server	AVVIATO	2.33 MB RSS
VPN	FERMO	
Web Server	AVVIATO	28.07 MB RSS

Add-On - Servizi

Add-On Servizio	Boot	Azione	Stato	Memoria
arpwatch	☑		FERMO	
guardian	☑		AVVIATO	31.20 MB
hostapd	☑		AVVIATO	3.63 MB

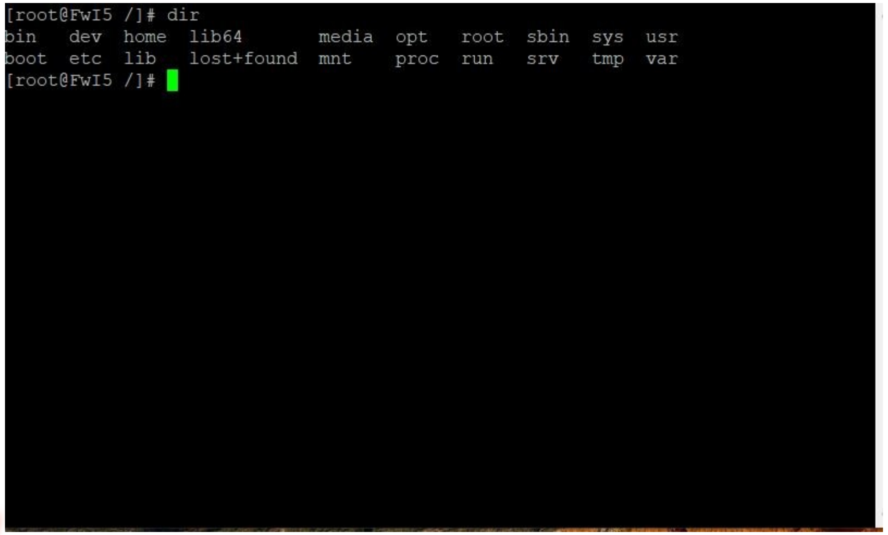
Informazioni e Stato

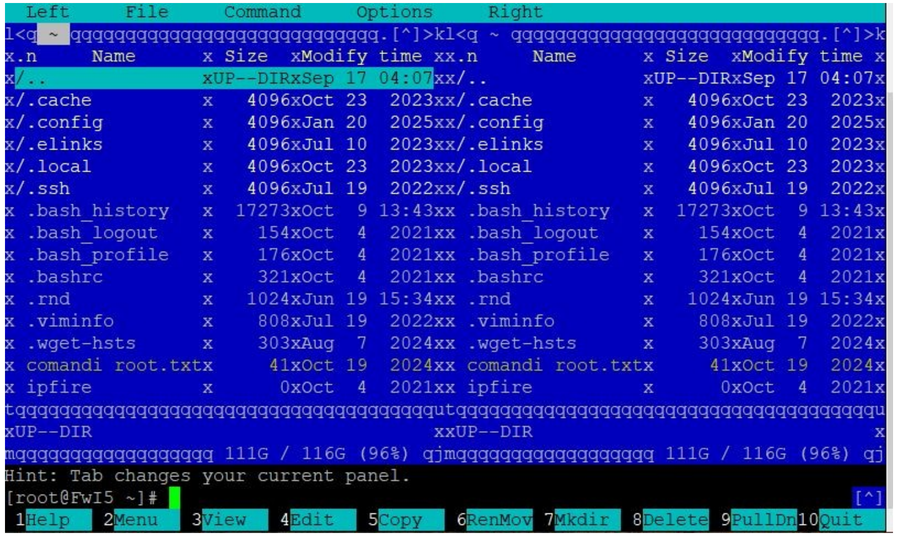
Processors

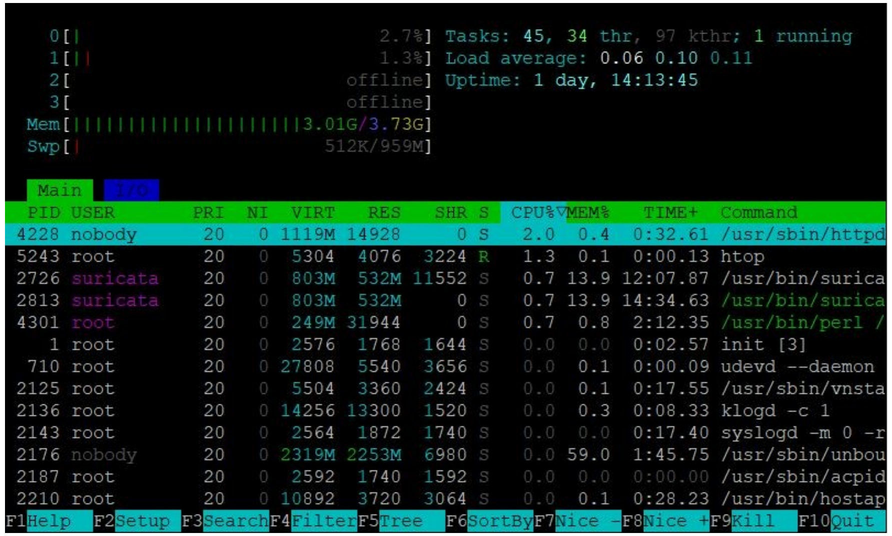


IPFIRE

Linux come cuore portante del sistema







IPFIRE community

https://www.ipfire.org/blog

You can simply impress your audience and add a unique zing and appeal to your Presentations.

https://www.ipfire.org/support

You can simply impress your audience and add a unique zing and appeal to your Presentations.

https://www.ipfireitalia.it/

You can simply impress your audience and add a unique zing and appeal to your Presentations.

https://community.ipfire.org/

You can simply impress your audience and add a unique zing and appeal to your Presentations. I hope and I believe that this Template will your Time, Money and Reputation.

Certificazioni

Merchandising

IPFIRE

LINKS:
-ipfire.org
-blog.ipfire.org
-community.ipfire.org
-facebook.com/IPFire.org
-youtube --→ ipfireproject
-linkedin.com/company/ipfire

Cyber Security

IPFire Italia: Comunità nata nel 2016 come supporto volontario e collaborativo Ci occupiamo di eseguire le traduzioni in italiano e di fornire supporto tecnico e sviluppo di alcune personalizzazioni

links IPFire Italia: -https://ipfireitalia.it
-https://www.facebook.com/IpfireItalia
-https://www.linkedin.com/groups/8909167/
https://t.me/IPFireItalia

THANK YOU

ANY QUESTION?