

IPFire The Open Source Firewall Distribution e-privacy 2016 Pisa Fabio Carletti aka Ryuw

IPFire.org



whoami

Consulente informatico IT

- Membro olografix,soldierx..ecc
- Titolare LEJOT Opensource technology
- Currently security IT specialist on lejot.info and RealService
- I like unix <;-)



e-privacy 2016

- https://www.google.com/intl/it_it/policies/privacy/
- Quando utilizzi i servizi di Google, ci affidi le tue informazioni. Le Norme sulla privacy ti consentono di capire meglio quali dati raccogliamo, perché li raccogliamo e come li utilizziamo. Sono informazioni molto importanti e ci auguriamo che le leggerai con attenzione.



e-privacy 2016

- Informazioni sui log
- Durante l'utilizzo da parte dell'utente dei nostri servizi o la visualizzazione di contenuti forniti da Google, raccogliamo e memorizziamo automaticamente alcune informazioni nei log del server. Queste informazioni comprendono:
 - Dati sulla modalità di utilizzo del nostro servizio, come le query di ricerca.
 - Informazioni sui log relativi alle telefonate, ad esempio numero di telefono, numero del chiamante, numeri di deviazione, ora e data delle chiamate, durata delle chiamate, informazioni sull'inoltro di SMS e tipi di chiamate.
 - Indirizzo di protocollo Internet.
 - Informazioni sulla attività del dispositivo quali arresti anomali, attività di sistema, impostazioni hardware, tipo di browser e lingua, data e ora delle richieste e degli URL di riferimento.
 - Cookie che potrebbero identificare in modo univoco il browser o l'account Google dell'utente.



e-privacy 2016

- Non forniamo informazioni personali a società, organizzazioni e persone che non fanno parte di Google, ad eccezione dei seguenti casi:
- Con il consenso dell'utente
- Forniamo dati personali a società, organizzazioni e persone che non fanno parte di Google con il consenso dell'utente. Chiediamo il consenso per l'attivazione della condivisione di dati personali sensibili.



e-privacy 2016

Privacy is not an absolute

Privacy = riservatezza

1 solitude

2 intimacy

3 anonymity

4 reserve



e-privacy 2016

Privacy on pc

Hostory file

Cookies

The internet and the web

Private network

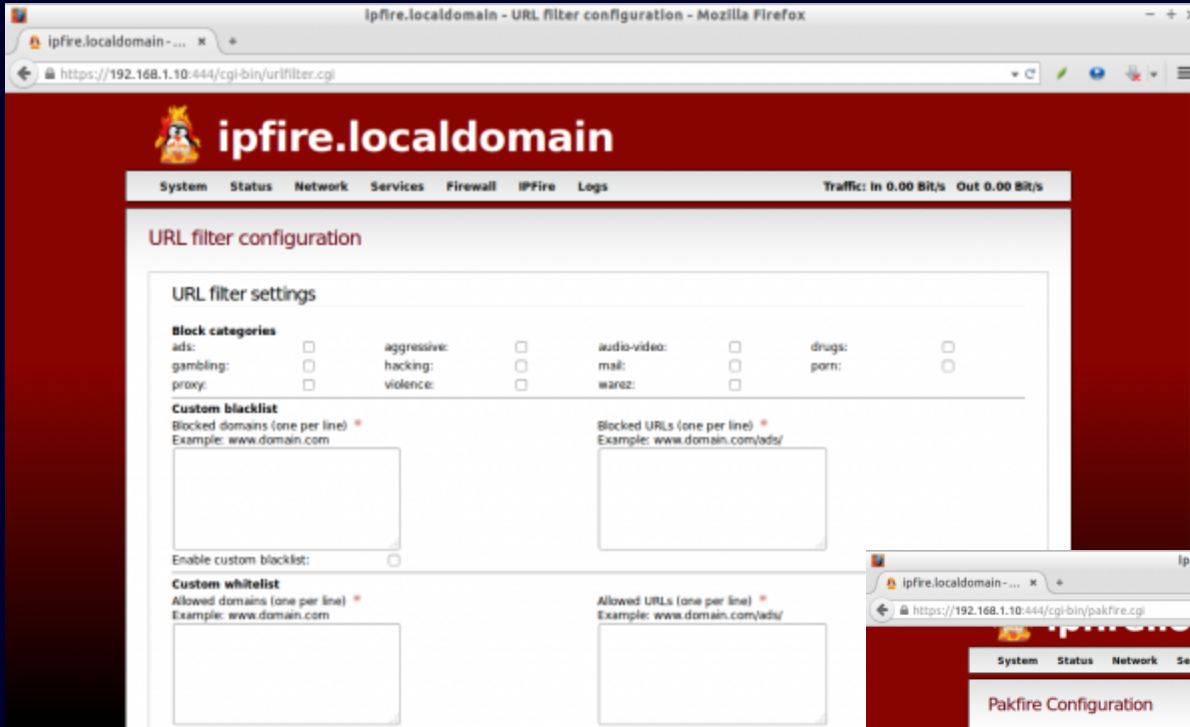


e-privacy 2016

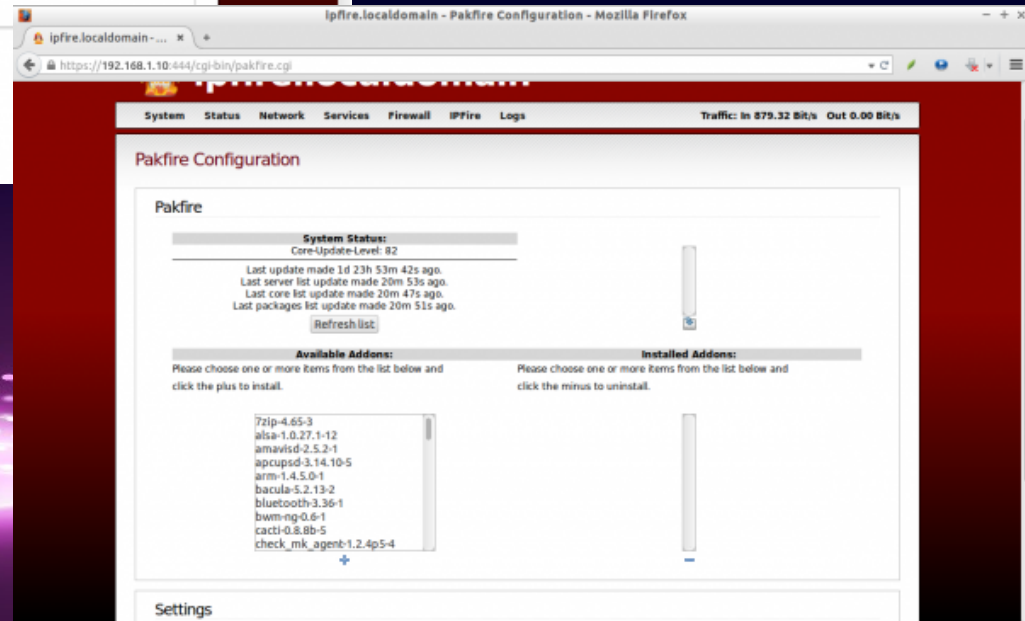
Firewall-Network Security- OpenSource-Easy to use



e-privacy 2016



The screenshot shows the IPFire web interface for URL filter configuration. The page title is "ipfire.localdomain - URL filter configuration - Mozilla Firefox". The URL in the address bar is "https://192.168.1.10:444/cgi-bin/urlfilter.cgi". The interface features a red header with the IPFire logo and the text "ipfire.localdomain". Below the header is a navigation menu with tabs for System, Status, Network, Services, Firewall, IPFire, and Logs. The main content area is titled "URL filter configuration" and contains "URL filter settings". Under "Block categories", there are checkboxes for ads, aggressive, audio-video, drugs, gambling, hacking, mail, porn, proxy, and violence. Below this are sections for "Custom blacklist" and "Custom whitelist", each with text input fields for blocked/allowed domains and URLs, and an "Enable custom blacklist" checkbox.



The screenshot shows the IPFire web interface for Pakfire Configuration. The page title is "ipfire.localdomain - Pakfire Configuration - Mozilla Firefox". The URL in the address bar is "https://192.168.1.10:444/cgi-bin/pakfire.cgi". The interface features a red header with the IPFire logo and the text "ipfire.localdomain". Below the header is a navigation menu with tabs for System, Status, Network, Services, Firewall, IPFire, and Logs. The main content area is titled "Pakfire Configuration" and contains "Pakfire" status information. The "System Status" section shows "Core-Update-Level: 82" and a list of update times for the last update, server list, core list, and packages list. Below this is a "Refresh list" button. The "Available Addons" section lists various addons like 7zip-4.65-3, aise-1.0.27.1-12, amavisd-2.5.2-1, apcupsd-3.14.10-5, arm-1.4.5.0-1, bacula-5.2.13-2, bluetooth-3.36-1, bwm-ng-0.6-1, cacti-0.8.8b-5, and check_mk_agent-1.2.4p5-4. The "Installed Addons" section is currently empty.



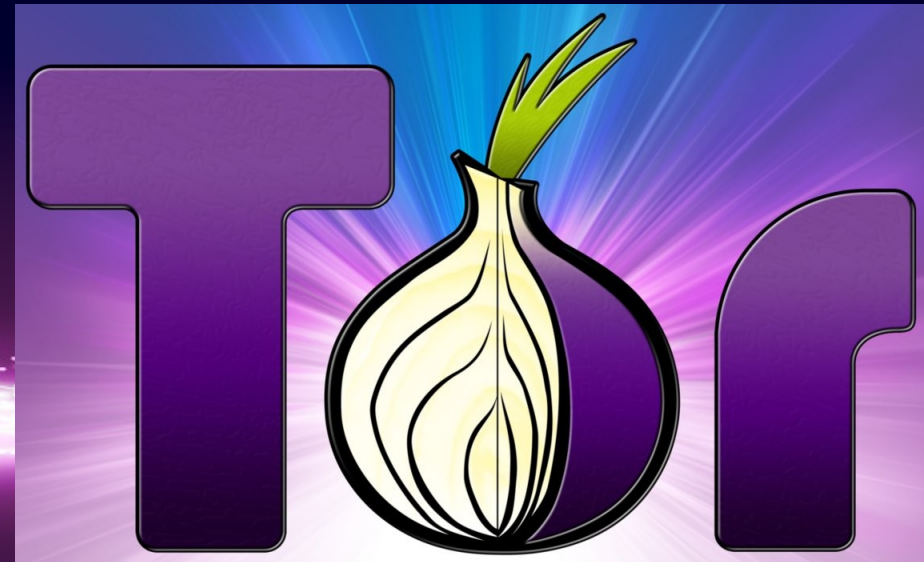
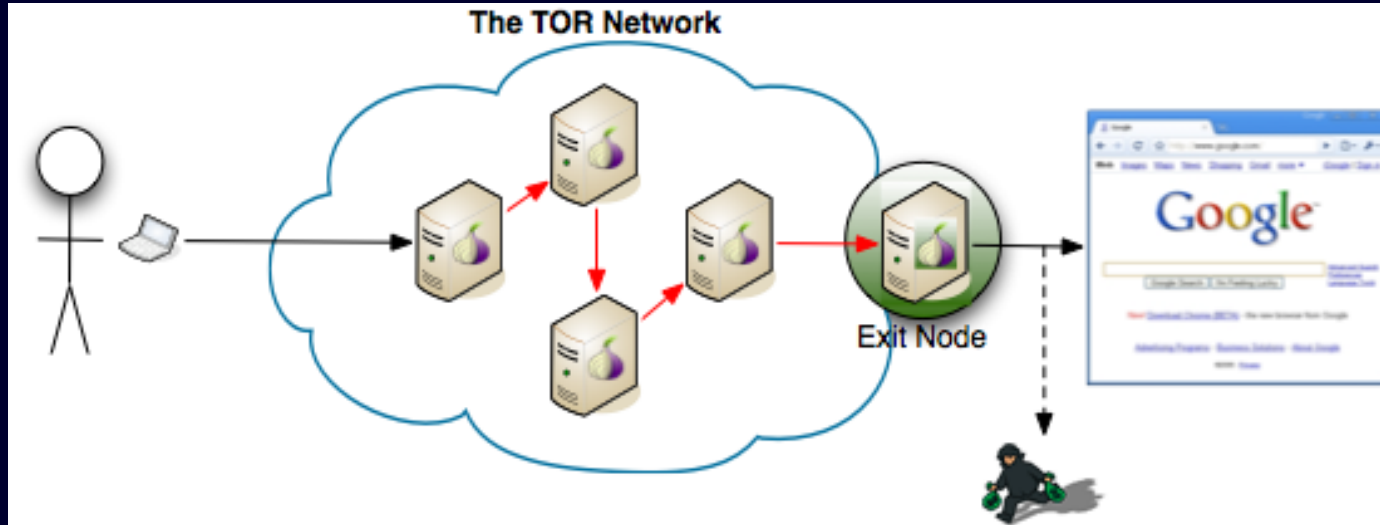
e-privacy 2016

services

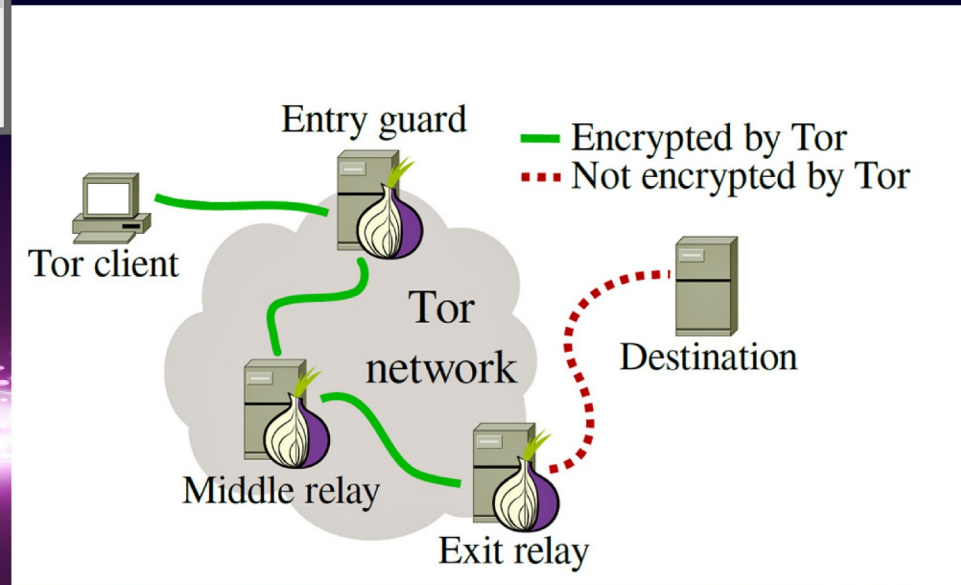
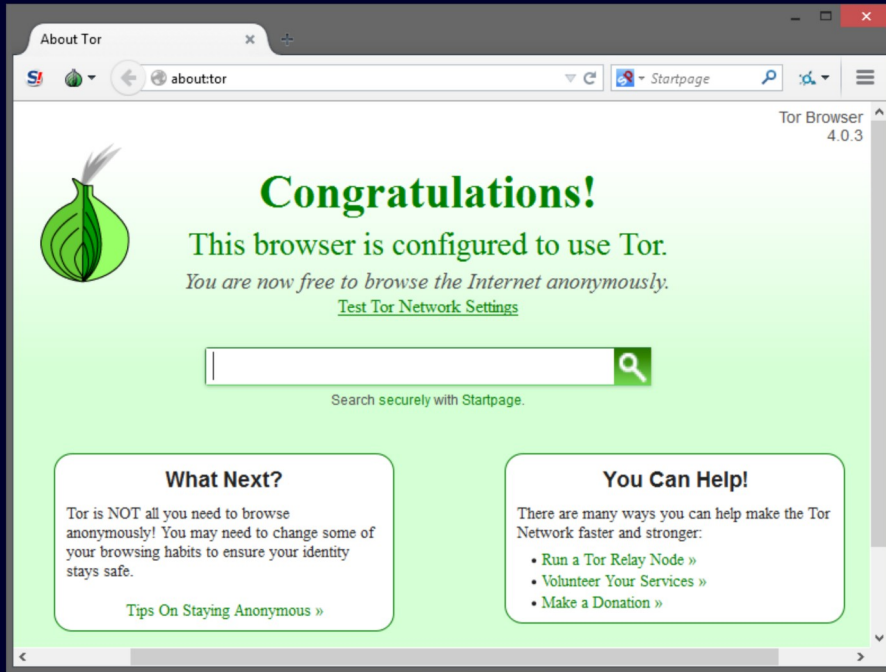
Services	Status	PID	Memory
CRON Server	RUNNING	3578	449 KB
<u>DHCP Server</u>	RUNNING	3211	886 KB
DNS Proxy Server	RUNNING	32336	419 KB
<u>Intrusion Detection System (GREEN)</u>	STOPPED		
<u>Intrusion Detection System (RED)</u>	STOPPED		
Kernel Logging Server	RUNNING	2152	546 KB
Logging Server	RUNNING	2159	396 KB
<u>NTP Server</u>	RUNNING	3122	914 KB
<u>OpenVPN</u>	RUNNING	710	944 KB
<u>Secure Shell Server</u>	RUNNING	3328	892 KB
<u>VPN</u>	RUNNING	884	707 KB
<u>Web Proxy</u>	RUNNING	454	3644 KB
Web Server	RUNNING	3515	4547 KB



e-privacy 2016



e-privacy 2016



e-privacy 2016

https://192.168.3.1:444/cgi-bin/tor.cgi

Tor Configuration

Tor

Tor Service	PID	AVVIATO	Memoria
Daemon	2570		5390 KB

Impostazioni Comuni

Enable Tor: SOCKS port: *

Enable Tor Relay:

Access Control

Allowed subnets (one per line):

```
192.168.3.0/255.255.0
```

Exit Nodes

Use only these exit nodes (one per line):

- Any country -

Tor Relay Configuration

Relay mode: Relay nickname:

Relay address: Relay port: *

Contact Info: Directory port: * 0 = disabled

Bandwidth Settings

Max. rate: Accounting limit (MB): *

Max. burst: Accounting period:



e-privacy 2016

https://192.168.3.1:444/cgi-bin/ids.cgi

Intrusion Detection System

Intrusion Detection System

GREEN Snort RED Snort Guardian

Snort rules update

Emergingthreats.net Community Rules

To utilize Sourcefire VRT Certified Rules, you need to register on www.snort.org.

Acknowledge the license, activate your account by visiting the url you got via mail. Then go to [Get an Oinkcode](#), press the "Generate code"-button and copy the 40 character Oinkcode into the field below.

Oinkcode:

Ruleset update from: Fri Jun 17 00:06:33 2016

Guardian Configuration

Interface

Timelimit

Logfile

Alertfile

Ignorefile

intrusion detection system rules

[emerging-activex.rules](#)
No description available
 [emerging-attack_response.rules](#)
No description available
 [emerging-botcc_portgrouped.rules](#)
No description available
 [emerging-botcc.rules](#)
No description available

[emerging-netbios.rules](#)
No description available
 [emerging-p2p.rules](#)
No description available
 [emerging-policy.rules](#)
No description available
 [emerging-pop3.rules](#)
No description available



e-privacy 2016

<http://wiki.ipfire.org/en/start>

- <http://planet.ipfire.org/>
- <https://grsecurity.net/>
- <https://www.snort.org/>
- <https://www.mozilla.org/en-US/privacy/firefox/>
- <https://www.torproject.org/>



e-privacy 2016



**Thanks for
your attention.**

Fabio Carletti aka Ryu

fabiocarlettiryuw@gmail.com

