# Introduzione a pfSense

Stefano David

Trento, 16 maggio 2017







## Outline

# Programma della serata

1. Introduzione a pfSense e cenni storici, qualche concetto di base, installazione.
2. Completare l'installazione: il *setup wizard*.
3. La *firewall state table*.
4. Traffico *ingress* ed *egress*, firewalling good e best practices.
5. Backup e archivio configurazioni.
6. Introduzione ed installazione di *packages* aggiuntivi.
7. Come monitorare pfSense.





# Qualche concetto introduttivo

- "Sicurezza informatica". Ma... perché fra virgolette? Lo scopriremo presto!
- Firewall: cosa erano e cosa sono diventati
- Networking: argomento vastissimo, vedremo solo qualche concetto base (non trattato).

# Cosa si intende per “Sicurezza informatica”?

## Una prima considerazione

Il livello ed il tipo di minacce per computer e reti locali è cambiato molto negli anni:

- Negli anni 1970/1980, un **Trojan** poteva distruggere il vostro Hard Disk, mentre un **worm** poteva diffondersi da un computer all’altro.
- Oggi abbiamo: Virus, Malware, Phishing, Ransomware, DDOS, botnet, code injection, . . .

→ Siamo passati da un tipo di minaccia prettamente distruttiva ad uno di tipo ri(s)cattatorio.

→ I “Firewall” non bastano più!





# Cosa è oggi la sicurezza informatica

La sicurezza informatica è diventata una vasta e multidisciplinare area che comprende varie branche:

- sviluppo di anti-{virus|Ransomware} etc.
- Pen(etration) testing
- (Ethical) Hacking
- Intrusion Prevention/Detection System
- Risk assessment, auditing
- Forensics
- . . .

# Firewall

**Un firewall è. . .**

. . . un componente di difesa perimetrale di una rete informatica, che può anche svolgere funzioni di collegamento tra due o più segmenti di rete, garantendo la protezione in termini di sicurezza informatica della rete stessa.

cfr. Wikipedia, http://www.tldp.org/LDP/nag2/x-087-2-firewall.introduction.html

**In altre parole:**

Un firewall è un dispositivo che analizza un flusso di dati e decide quale sarà il suo destino in base a regole ben definite.





# Le 4 generazioni di firewall

**Packet filter/stateless firewall** ogni pacchetto viene analizzato "a prescindere", senza tener conto di quelli precedenti - ~1970

**Stateful firewall** viene tenuta traccia della connessione cui un pacchetto appartiene. Un pacchetto viene scartato se non appartiene ad una connessione legittima - ~1990

**Application firewall** viene riconosciuta l'applicazione che genera il traffico e decidere se permettere o bloccare il traffico. Agisce a livello 7 ISO/OSI. ~ 1995

**Next Generation firewall** dispositivi che riuniscono le precedenti funzionalità ed altre per combattere (tutti) i possibili attacchi che una rete locale può ricevere. ~2005

cfr. vari white papers & articoli tecnici.

# Ma che significa **pfSense?**

Un po' di storia:

- 2004: fork di m0n0wall (embedded FreeBSD firewall) da parte di Chris Buechler e Scott Ullrich.
- Perché un fork? L'obiettivo è l'installazione su PC, impossibile per m0n0wall (RAM-loaded).
- 2006: versione 1.0 basata su FreeBSD 5.3
- Perché FreeBSD 5.3? Per sfruttare **pf**, ovvero Packet Filter, il software di firewalling usato da FreeBSD.
- 2017: versione 2.3.3 rilasciata il 20 Febbraio.





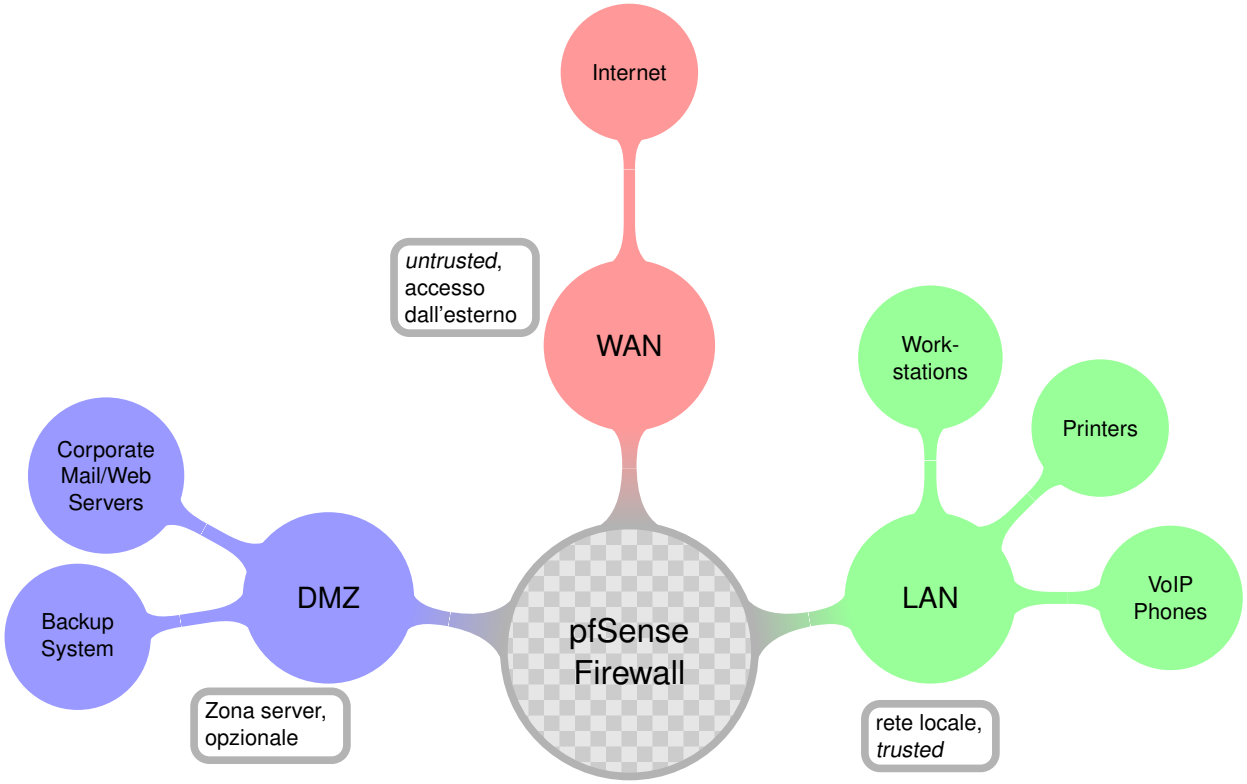
# Adesso ci dici cosa significa **pfSense**?!

- Esattamente quello che dice il nome!

  *pf**Sense** == "Making **sense** of **pf**"*

- Ovvero, permettere a chiunque di configurare ed usare un software per certi versi complesso come un firewall.
- Nel tempo anche pfSense si è evoluto, fino a diventare quello che è oggi: una distribuzione dedicata alla sicurezza di reti locali con tante altre peculiarità.

# Le tre zone








# Requisisti

## Requisiti minimi

- CPU 500 Mhz
- RAM 256 Mb
- 2 NIC

## Requisiti suggeriti

- CPU 1 Ghz 64bit (ove possibile)
- RAM 1 Gb
- 2 NIC

## Interfacce di rete

Intel Pro fino a 100/1000Mbs, altri vendor per > 1Gbs.

Maggiore traffico $\Longleftrightarrow$ CPU, RAM, NIC più potenti

# Principali funzionalità di pfSense

**Lista (incompleta) di funzionalità supportate da pfSense**

Stateful inspection • NAT - DNAT , 1:1, outbound, reflection/hairpin/loopback • supporto per VPN (OpenVPN e IPsec) • Alta affidabilità (CARP/pfsync) • Multi-WAN balancing/failover • Server Load Balancing • reporting& monitoring • Captive portal • DHCPD & DHCP relay • Traffing shaping • SNMP • DynDNS • Routing • bridging . . .





# Installazione

Adesso inizia il bello! Ma. . .

**. . . appena finita l'installazione...**

- Vediamo come si accede a pfSense e completiamo il *Setup wizard*.
- Configuriamo alcuni servizi di base come NTP, SSH, HTTPS, il backup.
- Facciamo una panoramica su importanti caratteristiche di pfSense, da tenere sempre a mente.
- Impariamo come **non** restare chiusi fuori.

# Accesso e Setup Wizard

## Come accedo a pfSense?

Vi sono tre modi di accedere a pfSense:

- **Web: http(s)://LAN IP/**
- Console (anche per installazioni fisiche e accesso remoto)
- SSH

## Setup Wizard

- È la prima cosa da fare una volta terminata l'installazione.
- Si configurano alcuni elementi base dell'installazione:
  a) *hostname* e *domain name*
  b) Server DNS
  c) NTP e fuso orario
  d) Uplink e IP LAN
  e) Password di **admin**





# Firewall, Concetti di Base

Terminologia:

| | |
|---|---|
| Rule | condizione da verificare per eseguire un'azione. |
| Ruleset | insieme di tutte le regole. |
| Ingress | si riferisce al traffico in ingresso e alle regole di firewall corrispondenti (*Ingress filtering*). |
| Egress | si riferisce al traffico in uscita e alle regole di firewall corrispondenti (*Egress filtering*). |
| FW Aliases | nome dato ad un insieme di host o network o porte. |

Le regole vengono processate in sequenza. → L'ordine è importante!

## Esempi di regole:

Il traffico Egress verso l'IP 123.45.67.89 va bloccato.
Il traffico Ingress sulla porta 25 va inviato all'IP 192.168.123.12.

# Stateful Firewalling

pfSense è uno *stateful firewall*.

**Caratteristiche di uno *stateful firewall*:**

- Viene tenuta traccia della connessione cui un pacchetto appartiene.
- Quando una connessione inizia, viene creata una voce nella *State Table*.
- Ogni replica a (o traffico collegato a) questa connessione viene automaticamente permessa (se la connessione è legittima).





# La *State Table*

- È l'elenco delle connessioni che passano dal firewall.
- Ogni voce contiene parecchie informazioni sulla connessione.
- Ogni voce occupa circa **1kb** di memoria RAM.

→ Bisogna saper preventivare il volume di traffico che attraverserà il firewall!

- **Nessuna** connessione permessa con *State Table* piena!

## Firewalling Best Practice

**La regola d'oro è:**

Bloccare **TUTTO** il traffico che non è esplicitamente permesso.

*"Ma anche il traffico in uscita? I miei utenti sono tutti fidati!"*

# Sì! Anche il traffico in uscita!

Il traffico in uscita può risultare più pericoloso di quello in entrata.
Esempio molto attuale: Ransomware (Cryptolocker & Co.)





## Regole Specifiche di pfSense

- **Anti-lockout** (System → Advanced) Permette il traffico dalle reti locali verso la GUI.
- **Anti-spoofing** Blocca il traffico da IP che non corrispondono all'interfaccia da cui provengono.
- **Private Networks** Il traffico Ingress da network privati viene bloccato (Setup wizard).
- **Bogon Networks** Traffico Ingress proveniente da network privati, riservati, o non assegnati viene bloccato (Setup wizard).
- **Deny rule** Tutto il traffico non permesso è bloccato.

Esempio: Traffico da em2 con IP sorgente 10.20.30.40, ma su em2 è definita 192.168.100.0/24. Lista mantenuta su `files.pfsense.org`.

# Aggiornare pfSense

Ci sono due modi per aggiornare:

- via WEB.
- via console, opzione **13**.





# Backups Diagnostics → Backup & Restore

- Si può scegliere cosa includere nel backup.
- Si può criptare il backup.
- Si può esportare la configurazione del backup.
- A pagamento opzione di *offsite backup* con salvataggio criptato sui server pfSense (pacchetto AutoConfigBackup)

# Packages System → Package Manager

- I **Packages** sono software aggiuntivi sviluppati dalla *Community*.
- Ogni pacchetto permette di integrare applicazioni non disponibili di default in pfSense.

**Alcuni esempi di *packages*:**

Squid • FreeRADIUS • snort e suricata ([N]IDS) • Zabbix e Nagios • AutoConfigBackup • varie networking utility: iftop, iperf, nmap.





# Come monitorare pfSense

Vi sono diversi modi per controllare e verificare il funzionamento di pfSense:

**Log files**

- Si trovano in Status { → System Logs / → System Packages
- Hanno lunghezza fissa.
- Possibilita di remote logging ← molto importante per il troubleshooting!
- Opzioni di configurazione in Status → System Log → Settings
- Consultabili da console (/var/log)

# Come monitorare pfSense

Vi sono diversi modi per controllare e verificare il funzionamento di pfSense:

- Log files

**Stato del sistema**

- La *landing page* è anche una pagina di stato con moltissime informazioni.
- Si può raggiungere da Status → Dashboard.
- le voci del menu Status mostrano lo stato di pfSense in tempo reale (refresh ogni pochi secondi).



Programma Introduzione pfSense Primi Passi Setup Wizard Firewalling Backup Packages Monitoraggio

# Come monitorare pfSense

Vi sono diversi modi per controllare e verificare il funzionamento di pfSense:

- Log files
- Stato del sistema

**Grafici RRD**

- Si trovano sotto Status → Monitoring.
- Mostrano in forma di grafico dati storici su traffico dati (LAN/WAN/VPN) e sistema (RAM/CPU etc).
- Ampiamente configurabili anche come intervallo di tempo.
- Opzioni per esportare i dati in formato CSV.