**FirewallD** یا Firewall Dynamic یک کنترلر **frontend** برای **iptables** است که اجرای رول‌ها در یک شبکه پایدار را بر عهده دارد. **FirewallD** دارای دستورات و محیط گرافیکی جهت کنترل و اجرای فرامین را دارا بوده و برای اکثر لینوکس ها قابل نصب می‌باشد و شما براحتی از مخازن لینوکس‌های مختلف می‌توانید آن را دانلود و نصب نمایید.

در مقایسه **مدیریت و کانفیگ FirewallD** و [**مدیریت و کانفیگ** **iptables**](https://azaronline.com/%D8%AA%D9%86%D8%B8%DB%8C%D9%85%D8%A7%D8%AA-%D9%81%D8%A7%DB%8C%D8%B1%D9%88%D8%A7%D9%84-%D8%B3%D9%86%D8%AA%D9%88%D8%B3/) دو تفاوت اساسی وجود دارد:

1. Firewalld از **Zones** و **Services** استفاده می کند و **iptables** از **Chain** و **Rules**.
2. برای کنترل رول‌ها و تغییرات در آنها **FirewallD** هیچ گونه قطعی یا **session Expire** دیده نمی شود.

**FirewallD در اصل یک نسخه داینامیک از iptables است که به کاربر قابلیت مدیریت بهتر نسبت iptables را می دهد. FirewallD به نوعی جایگزین iptables خواهد شد ولی همچنان دستورات iptables را اجرا می کند ، اما پیشنهاد شده از دستورات FirewallD برای پیکربندی آن استفاده گردد.**

معرفی فایروال FirewallD در CentOS

[**FirewallD**](http://www.firewalld.org/)به صورت پیش فرض در لینوکس **CentOS 7** نصب می باشد اما غیر فعال است.

شما می توانید با دستورات زیر آن را فعال سازید.

sudo systemctl start firewalld

sudo systemctl enable firewalld

برای غیر فعال کردن آن نیز از دستورات زیر استفاده می‌شود.

sudo systemctl stop firewalld

sudo systemctl disable firewalld

جهت چک کردن وضعیت **FirewallD** از دستور زیر استفاده کنید.

sudo firewalld-cmd --state

همچنین دستور زیر را می‌توان برای دریافت **وضعیت FirewallD** استفاده نمود.

sudo systemctl status firewalld

جهت ریلود کردن ( بارگذاری مجدد ) **تنظیمات FirewallD** از دستور زیر استفاده می گردد.

sudo firewalld-cmd --reload

تمام تنظیمات و پیکربندی **فایروال FirewallD** در فایل‌های **XML** در دایرکتوری **etc/lib/firewalld/**  و  **etc/firewalld/**  قرار دارد اما برای تنظیم آن نیازی نیست که فایل‌ها را ویرایش نمایید.

نکته : تقریبا برای تمام دستورات موارد زیر وجود دارد

* Add که باعث اضافه شدن آن مورد می شود مثلا
  + Firewall-cmd –add-source=10.10.10.0/24
  + Firewall-cmd –add-port=22/tcp
* Remove که باعث حذف آن مورد می شود
  + Firewall-cmd –remove-source=10.10.10.0/24
  + Firewall-cmd –remove-port=22/tcp
* List که وضعیت فعلی را نشان می دهد
  + Firewall-cmd –list-source
  + Firewall-cmd –list-port

نکته : موارد کلی که می تواند تحت add, remove, list قرار بگیرند به شرح زیر است

* Port
* Source
* Service
* Source-port
* Forward-port
* ipset=x add/remove/get-entry
* interface
* forward که به این روش فوروارد کردن ترافیک داخل یک زون مجاز می شود
  + البته در این روش ابتدا باید فواردینگ در کرنل را فعال کرد
  + echo "net.ipv4.ip\_forward=1" > /etc/sysctl.conf
  + to check : sysctl -p

نکته : می توان