IPFire

An Open Source Firewall Distribution

Mohammad Mortaji

Univercity Of Qom

Spring ۲۰۱۵

بسم اللّه الرّحمن الرّحیم

همانگونه که می دانید لینوکس یک سیستم عامل متن باز می باشد که دارای توزیع های فراوانی با کارکردهای تخصصی می باشد.
در این مقاله ما می خواهیم با یکی از این توزیع ها که در زمینه امنیت فعالیت می کند آشنا بشویم؛آی پی فایر(فایروال).
آی پی فایر یک توزیع لینوکس مبتنی بر دیواره آتش می باشد؛ امنیت را از سطح کاربران خانگی تا شرکت های بزرگ ارایه می دهد.
اگر توانستم مقالاتی هم در رابطه با آشنایی با توزیع
تیلز(بسیار امنیتی می باشد بدینصورت که شناسایی کسی که از این نوع توزیع استفاده می کند در اینترنت امکان چذیر نخواهد بود)
و
کالی(توزیعی مخصوص هکرها می باشد که می توان با این توزیع هر چیزی را هک کرد)
نیز خواهم نوشت.

بعضی از خواص این سیستم عامل:

امنیت

هدف اصلی این توزیع امنیت می باشد.مهم می باشد که یک مدیر شبکه در رابطه با محیط و امنیت در شبکه خود آشنا باشد.
در این توزیع می توان هر بخش شبکه را بطور سفارشی تنظیمات امنیتی آن را انجام داد.
بروزرسانی آن نیز بصورت امضاهای دیجیتالی , رمزگذاری شده اند وهمچنین می توان بطور خودکار از Pakfire بروزرسانی کرد.مدیریت بسته های Pakfire آسان هستند و به مدیریت شبکه احساسی می دهد که دارد از آخرین نرم افزارهای امنیتی استفاده می کند.

دیواره آتش

در حین نصب سیستم عامل قسمت های مختلف شبکه پیکربندی می شوند.این طرح امنیتی قسمت بندی شده بدین معنی می باشد که برای هر ماشین درون شبکه مکان مناسبی وجود دارد.این قسمت های تفکیک شده بسته به نیاز شما می توانند فعال و یا غیر فعال گردند.هر بخش نشان دهنده یک گروه از رایانه ها هستند که دارای یک سطح امنیتی می باشند.

سبز نشان دهنده منطقه امنی می باشد.این منطقه معمولا از یک شبکه کابلی تشکیل شده است.کاربران در منطقه سبز می توانند به تمامی بخش ها بدون محدودیت دسترسی داشته باشند.

قرمز نشانگر خطر و یا متصل شدن به اینترنت می باشد.در منطقه قرمز هیچ کسی اجازه عبور از دیوار آتشین را ندارد مگر اینکه مدیریت شبکه به آن اجازه دهد.

آبی قسمتی از شبکه محلی که بصورت بیسیم می باشند(بدین دلیل که رنگ آسمان نیز آبی می باشد)شبکه های بیسیم امکان بالقوه برای سوء استفاده را دارند . کاربران در این شبکه ها باید قبل از دسترسی به شبکه باید صریحا اجازه بگیرند.

نارنجی اشاره دارد به منطقه غیر نظامی .

هر سروری که در دسترس عموم است از شبکه جدا می شود تا امنیت کل شبکه را پایین نیاورد.

Pakfire[۱]

سیستم مدیریت بسته IpFire

از نقطه نظر فنی IpFireدارای حداقل سیستم دیواره آتشی قوی می باشد که همراه با سیستم عامل عرضه می شود که ان را PakFireمی نامند.وظیفه اصلی PakFire بروزرسانی سیستم تنها با یک کلیک است.نصب وصله های امنیتی و رفع اشکالات و ... همراه با این بسته بسیار آسان می باشد.دیگر وظیفه بسته نصب نرم افزارهای اضافی می باشد که امکانات جدیدی به سیستم عامل می افزاید.

-سرویس اشتراک گذاری فایل از قبیل Samba and vsftpd هست

-سرویس دهنده ارتباطات از ستاره استفاده می کند

بروزرسانی

پایه این توزیع لینوکس می باشد به همین دلیل هسته آن نیز متن باز می باشد ؛ پایه اش روی دیگر توزیعات نمی باشد همانند KNOPPIX که پایه آن روی دبیان می باشد.

بروزرسانی هسته هر چهار هفته یکبار انجام می شود.حتی در صورتیکه مسئله امنیتی اورژانسی اتفاق بیافتد شما می توانید در کمتر از یکروز سیستم را بروز رسانی کنید.تمامی بروزرسانی ها می توانند بوسیله بسته جامع سیستم بطور اتوماتیک انجام شوند همچنین کاربران نیز از طریق ایمیل اطلاع رسانی میشوند.

مودم[۲]

این نوع توزیع به عنوان دروازه ای برای ورود به شبکه جهانی از متدهای مشهور پشتیبانی می کند.

VDSL

VDSL کوتاه شده ی Very High Data Rate Digital Subscriber Line می باشد.در حال حاضر از ۵۰ مگابیت بر ثانیه در بالاترین و ۱۰ مگابیت بر ثانیه در پایین ترین نوع خودش ارائه می دهد.از این نوع اتصال می توان از تکنولوژی جدید IPTV نیز بهره برد.این نوع توضیع را می توان جایگزین کرد بجای یک سیستم کاملی که IPTV را به خانه تان می آورد.

ADSL/SDSL

از DSL معمولی نیز پشتیبانی میکند همچنین از نظر تکنیکی آنرا PPPoE یا PPPoA می نامند.در برخی از کشورها پروتکل PPTP بطور گسترده استفاده می شود و آن نیز توسط IPFIRE بطور کامل پشتیبانی می شود.

Ethernet

همچنین این نوع توزیع می تواند به اینترنت بوسیله اترنت متصل بشود و آی پی آدرس را توماتیک یا پیکربندی ایستا بدست آورد.

۳G/٤G

اتصالات بیسیم از قبیل ۳G, CDMA, HSDPA ,UMTS یا LTE توسط IPFIRE پشتیبانی می شود.

وب پراکسی[۳]

شامل یک وب پراکسی تمام عیار متن باز می باشد.توسط ISPs دانشگاه ها و مدارس و شرکت های بزرگ چون دارای تنوع و پایداری و توسعه می باشد استفاده می شود.حتی برای شبکه های خانگی کوچک نیز مفید می باشد.

بعلاوه فیلترینگ SPI بوسیله دیوار اتشین روی لایه TCP/IP و منتقل کننده هایی نظیر HTTP, HTTPS یاFTP بخوبی می تواند فیلتر انجام دهد.

---

۱ Pakfire The IPFire package management system

۲ Dialup

۳ Web proxy

شبکه خصوصی مجازی[٤]

این نوع توزیع همچنین دارای قابلیت VPN می باشد, VPN یک دروازه برای اتصال به شبکه محلی از راه دور بطور امن می باشد.
برای انعطاف پذیری بیشتر آی پی فایر از دو پروتکل IPsec وOpenVPN استفاده می کند

سیستم های تشخیص نفوذ[٥]

سیستم های تشخیص نفوذ IDS، یک تکه از نرم افزار طراحی شده برای تشخیص حملات علیه سیستم های کامپیوتری و شبکه ها است.

سیستم پیشگیری از نفوذ IPS علاوه بر سیستم تشخیص نفوذ نیز وجود دارد.سیستم پیشگیری از نفوذ می گیرد اطلاعات را از سیستم تشخیص نفوذ و بر این اساس واکنش نشان میدهد.

شبکه را آنالیز می کند و اگر کار غیر عادی اتفاق بیافتد آن را نشان میدهد .آی پی فایر امکان دستیابی به رابط های وب را نیز به شما می دهد.برای پیشگیری خودکار, آی پی فایر دارای یک افزونه به نام نگهبان می باشد که بصورت اختیاری می تواند نصب شود

رمز نویسی[٦]

رمزنویسی پایه خدمات متفاوتی به VPN و اتصال ایمن به اینترنت هست بنابراین آی پی فایر بر این موضوع تاکید دارد.

سخت افزار

پایه آی پی فایر آخرین ورژن هسته لینوکس می باشد و آخرین سخت افزارها را پشتیبانی می کند بطور مثال کارت شبکه ده گیگابایتی و کارت شبکه های متنوعی. توسعه دهندگان آی پی فایر بسیار علاقمند می باشند که این سیستم عامل بر روی تمامی سخت افزارها اجرا شود.

حداقل سیستم مورد نیاز برای اجرای آی پی فایر (Intel Pentium I (i٥٨٦, and ١٢٨MB RAM ٢GB hard drive space می باشد.

مجازی سازی[٧]

آی پی فایر می تواند برای استفاده ازسیستم عامل های دیگر شبیه سازی نیز کند.

KVM

مخفف Kernel-based Virtual Machine می باشد که توسط شرکت رد هت گسترش می یابد.

VMware

ماشین های مجازی متفاوتی همانند vSphere, ESXi and VMware workstation

Xen

آخرین شبیه ساز متن باز می باشد ولیکن به موفقیت KVM نمی رسد.

نقطه دسترسی بیسیم[٨]

آی پی فایر چندین گزینه برای ادغام کاربران بیسیم پیشنهاد می دهد.

اول اتصال به وسیله یک کارت شبکه است در این سناریو از MAC/IP برای محدود کردن دسترسی کاربران به شبکه پیشنهاد می دهد کاربران بطور پیش فرض دسترسی دارند به اینترنت ولیکن دسترسی به شبکه ندارند.

---

٤ VPN Virtual Private Networks

٥ Intrusion detection system

٦ Cryptography

٧ Virtualization

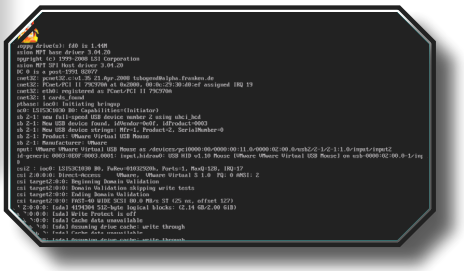
٨ Wireless Access Point

گزینه دوم نصب کردن یک کارت شبکه بیسیم می باشد.از رمزگذاری های WPA/WPA۲ و پهنای باند پنج گیگاهرتز(استاندارد ۸۰۲,۱۱a) پشتیبانی می کند.

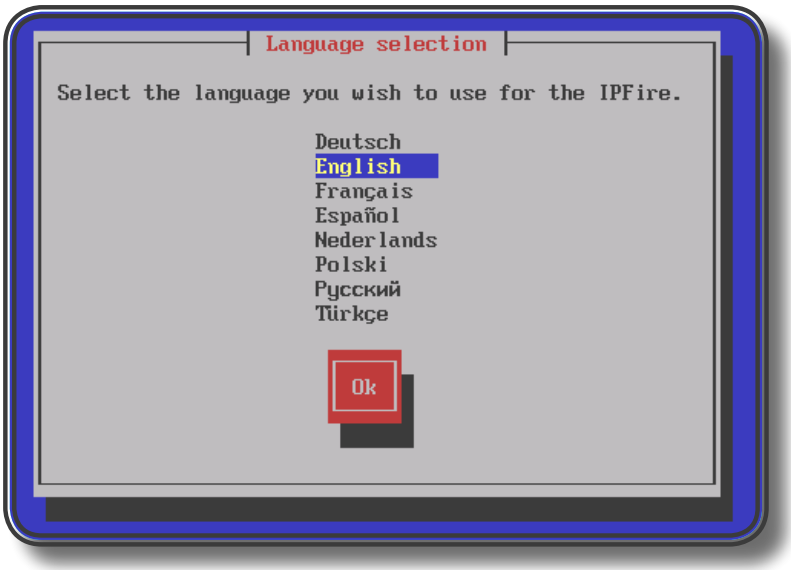
مراحل نصب سیستم عامل(بصورت مختصر و مفید)

صفحه اول نصب بدینگونه می باشد که می بینید ,حاوی خوش آمد گویی و معرفی توزیع و ورژن آن می باشد ؛پنج گزینه موجود می باشد که برای نصب کامل باید گزینه اول را انتخاب کرد.

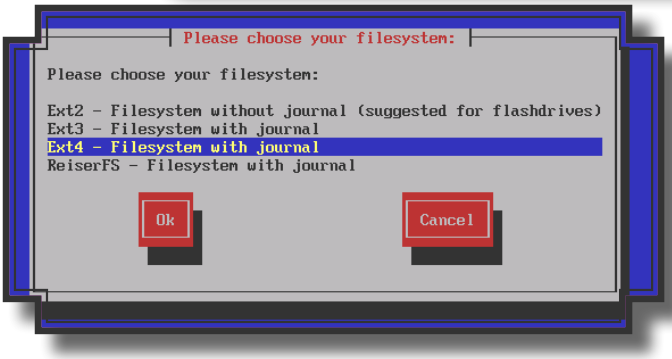
پس از انتخاب گزینه نصب(اول) صفحه مشکی زیر می آید تا سپس شما را به مرحله تنظیمات ببرد.



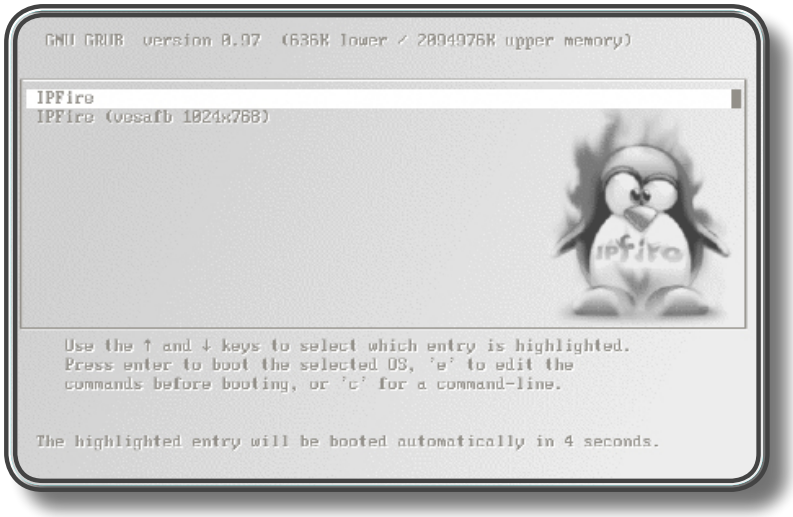
در تصویر روبرو زبان را انتخاب کرده.



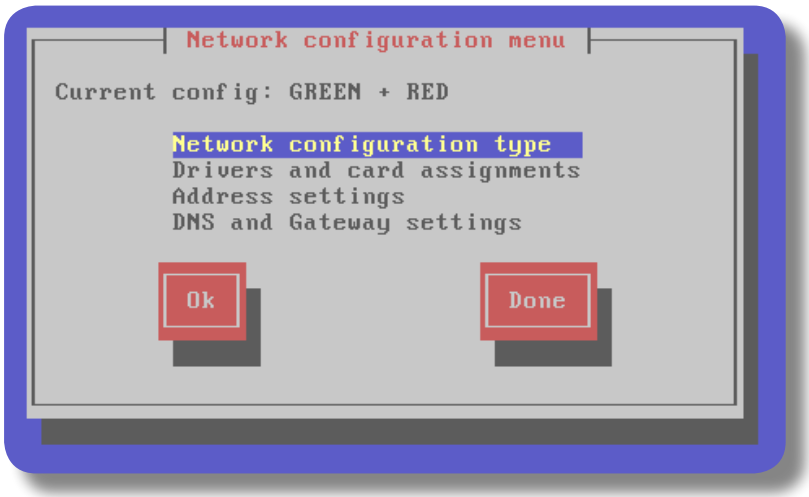
در اینجا نیز نوع فایل ها.



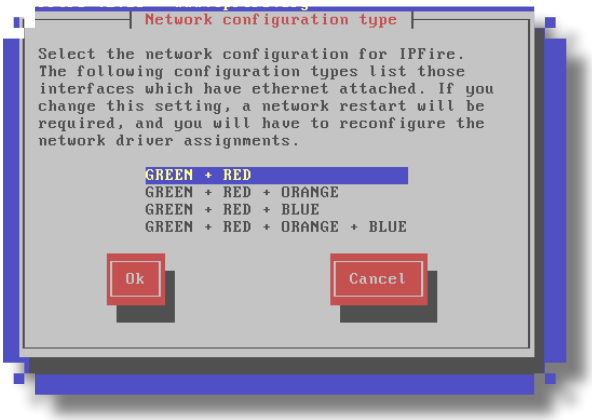
بعد از یکبار روشن و خاموش شدن صفحه زیر ظاهر می شود که خب یکی از دو انتخاب را انتخاب می کنیم.



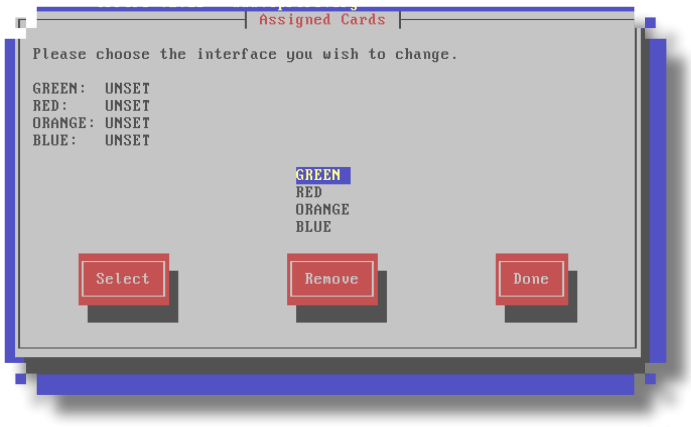
باید سیستم را تنظیم کنیم،چهار گزینه دارد که هر کدام نیز مراحلی دارند.

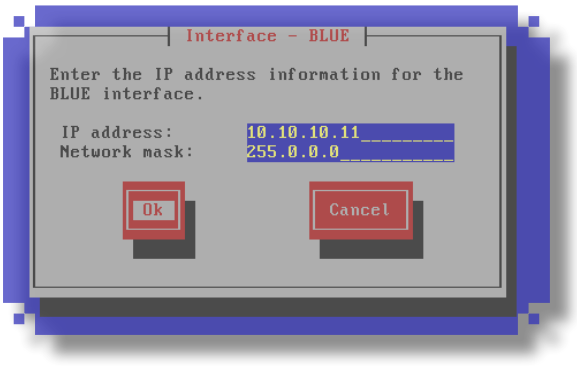


با انتخاب گزینه اول به صفحه زیر می رسیم که باید تعیین کنیم که سیستم را می خواهیم به چند قسمت تقسیم کنیم(توضیحات بیشتر)

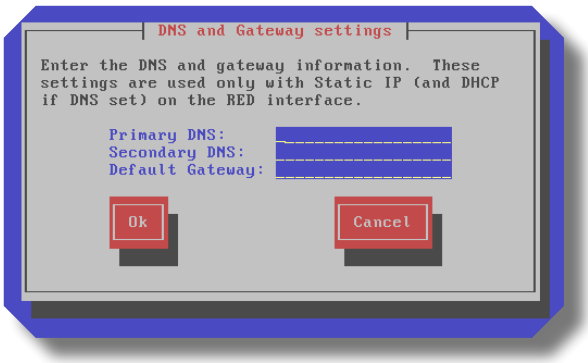


با توجه به اینکه سیستم ما به چند قسمت تقسیم شده است باید آی پی آدرس آنها را نیز تعیین کنیم.



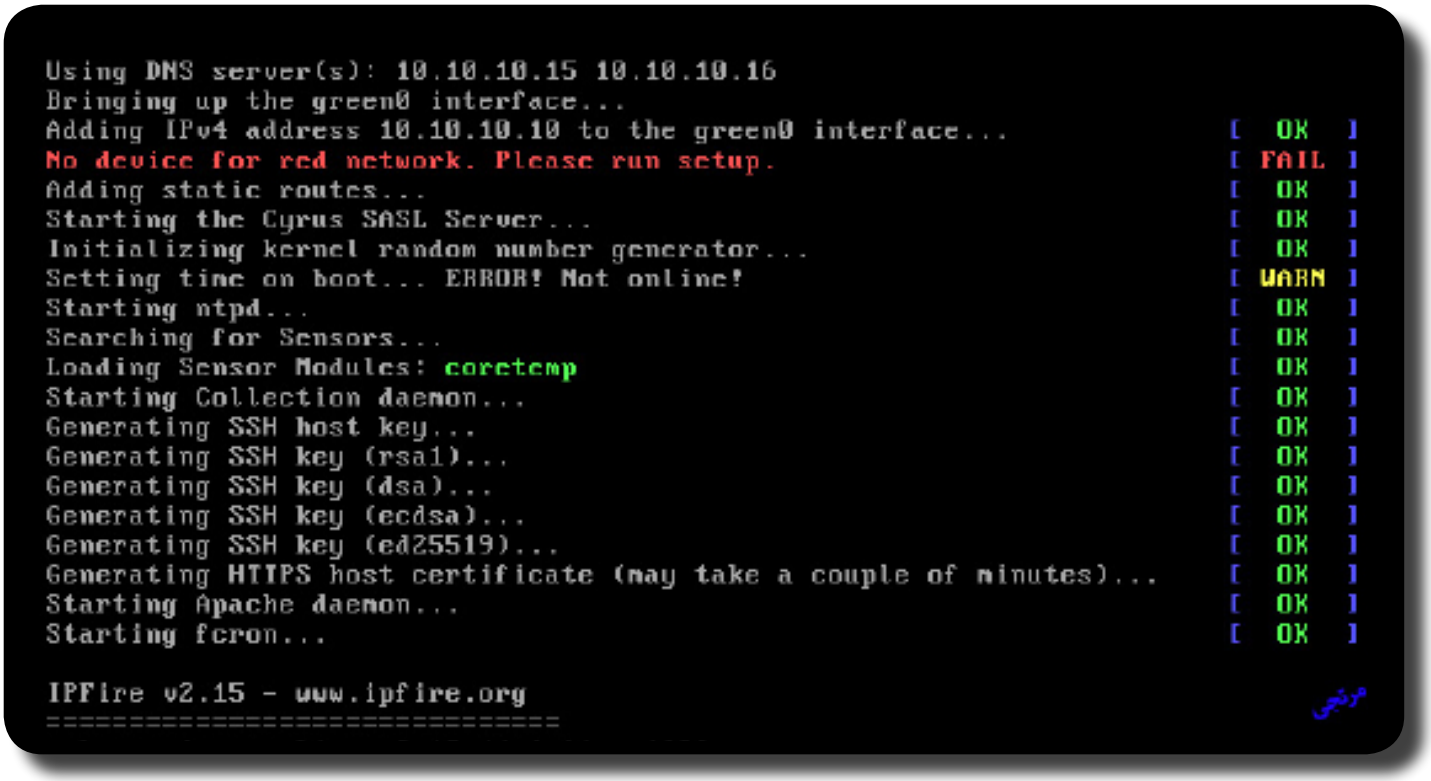


با انتخاب گزینه چهارم این صفحه خواهد آمد:



و تعیین بعضی تنظیمات دیگر از قبیل انتخاب نام و رمز عبور و ... کار پیکربندی به اتمام رسیده و پس از خاموش و روشن شدن ؛ سیستم آماده کار می باشد.

خب البته سیستم گرافیکی نمی باشد بلکه باید از فرمان متنی استفاده کرد.



محمّد مرتجی

iri1404mm@gmail.com