



آموزش مقدماتی

Pfsense

www.Mabedini.ir

نویسنده

محمد عابدینی

فهرست منابع

| | |
|----------|--|
| 3..... | فصل اول معرفی pfSense و نصب کردن آن |
| 30..... | بخش دوم آشنایی با منوی کنسول در Pfsense |
| 46..... | فصل سوم روش اتصال به رابط وب |
| 58..... | فصل چهارم شبکه در FreeBSD |
| 78..... | فصل پنجم منوی وضعیت در pfSense |
| 115..... | فصل ششم بخش کارت شبکه در رابط وب pfSense |
| 133..... | راه اندازی کردن ssh در pfSense |
| 150..... | راه اندازی کردن DNS در pfSense |
| 156..... | سرور زمان در Pfsense |
| 165..... | نصب کردن برنامه در FreeBSD |
| 166..... | کردن برنامه‌های مختلف در pfSense آشنا می‌شوید. |
| 171..... | نصب کردن برنامه‌های موجود در مخازن pfSense با استفاده از رابط وب |
| 178..... | نوشتن رول با استفاده از فایروال pfSense |



سلام به خوانندگان عزیز

محمد عابدینی هستم بنیانگذار وب سایت Mabedini.ir

من یک شعار در زندگی خودم دارم:

"هر چیز سخت قابلیت ساده شدن و آموزش دادن داره"

از این شعار در آموزش دیدن سیستم عامل FreeBSD استفاده کردم، با این سیستم عامل در سال 1381 در یکی از شبکه های اینترنتی در کرج آشنا شدم و در اون زمان برای من بسیار جذاب و کاربردی به نظر رسید ولی منابع آموزشی محدود داشت.

همیشه آرزو داشتم که منابع آموزشی کامل و به زبان ساده در باره این سیستم عامل ایجاد کنم و این ایده دلیل اصلی در راه اندازی کردن وب سایت Mabedini و تهیه کردن آموزشهایی در این مودر است.

با دوره های متنوع در خدمت شما هستم

راه ارتباطی با من mabedini@mabedini.ir

فصل اول معرفی pfSense و نصب کردن آن

سلام دوستان

تجربه اول من با دنیای BSD از یک فایروال شروع شد، این تجربه رو با شما به اشتراک می‌زارم برای بهتر شدن سطح دانش در این زمینه، من برای اولین بار در شبکه‌ای مشغول به کار شدم که قرار شد به‌عنوان مدیری شبکه داخلی و شیفت شب شروع به کار کنم من ویندوز خون‌ده بودم و به این سیستم‌عامل تعصب خاصی داشتم. مدیرم به من گفت که برای مدیریت کردن کاربران شبکه داخلی که بخش فروش و پشتیبانی و غیره بودن که در حدود 10 تا سیستم می‌شد ما نیاز به یک سروری داریم که از طریق اون سرور به اینترنت متصل به شن، من هم مثل همه مهندسين شبکه ماکروسافت سرویس nat و isa سرور رو پیشنهاد کردم. ازطوی کیفیت CD ویندوز رو درآوردم و شروع کردم به نصب ویندوز 2000 تا اینجای ماجرا همه‌چیز خوب بود تا اینکه برای به‌روزرسانی سیستم رو متصل کردم به شبکه اینترنت با استفاده از یک IP معتبر تا اینکه پیغام زیر من رو بیچاره کرد، این پیغام رو در شکل زیر مشاهده می‌کنید:

این پیغام یک ویروس جدید بود که سیستم‌عامل‌های ویندوزی رو هدف گرفته بود و به Sasser معروف بود و به‌محض اینکه سیستم شما به شبکه اینترنت متصل می‌شود سیستم شما رو بعد از 60 ثانیه خاموش می‌کرد. کلاً چند باری ویندوز رو نصب کردم تا خسته شدم و مدیرم وقتی این موضوع رو دید من رو صدا کرد و گفت با ویندوزت چیکار می‌کنی!!! من هم هیچی نگفتم، بعدش به هم گفت این کیس کنار پارت رو نگاه کن یک کیس معمولی بود که حتی در درست‌وحسابی هم نداشت، گفت یکی دیگ هم هست که اون گوشه است و کل شبکه رو مدیریت می‌کنه . این دستگاه‌ها بر روش سیستم‌عامل FreeBSD نصب‌شده بود با استفاده از فایروالی که روش کانفیک شده بود همه ترافیک شبکه رو مدیریت می‌کرد و ویروس هم بهش نفوذ نمی‌کرد. کلاً به این سیستم‌عامل علاقه‌مند شدم ولی هیچی در موردش نبود و فقط سایت خودش بود و یک سری آموزش داشت بنام hadBook که زیاد هم‌زبان من خوب نبود برای یاد گیریش. یاد رفت به گم که این سیستم‌عامل یک محیط سیاه‌وسفید داشت محیطی سیاه با نوشته‌های سفید و چند خط متن!!! بهش گفتم همین با این چیکار می‌شد کرد، خیلی ساده برگشت به من گفت به این بخش میان خط فرمان و می‌شد بله‌اش به دنیا حکومت کرد دنیا منظورش اینترنت بود، گفت اله اینترنت برای شما محیط گرافیکی و چند تا کلیک هست اینجا محیط فقط سیاه‌وسفید و خط فرمان حکومت می‌که. گفت تو با این سیستم‌عامل حرف می‌زنی، براش تایپ می‌کنی و جوابش رو بهت شون میده، خلاصه برای من محیط جذابی شد ولی خب سخت بود برای کسی که با چند کلیک یک سرویس راه‌اندازی می‌کردی و

خلاصه رفتم سراغ آموزش سیستم عامل FreeBSD اول سایتش رو پیدا کردم به دنبال آموزش فارسی بودم که هیچی که نبود آموزش با زبان اصلیش هم به زبان فاخری نوشته شده بود و باید برای پیدا کردن معنی یک کلمه کل خط رو کلمه به کلمه ترجمه می کردی تا بهش برسی، این بخشش برای من بسیار سخت بود و من به سخت تونستن این سیستم عامل رو دانلود کنم و نصب کنم اخه اینترنت ها در سال 1381 زیاد پر سرعت نبود.

بعد از طی کردن این دوره که بسیار هم سخت بود با خودم فکر کردم که چرا دیگرانی که دوست دارن با این سیستم عامل کار کنن باید سختی بکشن این شد به فکر ترجمه فصل به فصل کتاب اصلی سایت FreeBSD افتادم که البته باید به گم دوره من سایت و شبکه اجتماعی و این چیزا نبود و برای انتشار کتابم رفتم سراغ انتشاراتی که البته به دلیل گرون بودن هیچ وقت این کار رو نکردم چون من جون بودم و پولی نداشتم که هزینه کنم. اما الان اوضاع من فرق می کنه من در سه سایت مختلف هر بار از اول شروع کردم به نوشتن مطلب فارسی در این زمینه و بار اخرش هم در سایت خودم به نام Mabedini این کار رو کردم. من جدید کارم رو ترک کردم و قصد دارم که صد در صد توان خودم رو بزارم روی این موضوع و مطلب.

می خواستم که این کتاب رو در مورد سیستم عامل FreeBSD ولی گفتم برای جذاب شدن کتاب تمرکز رو بزارم روی فایروالهای تحت FreeBSD که یکی از محصولاتی که تحت FreeBSD با رابط وب و فایروال معروف PF کار می کنن رو بهتون معرفی کنم، این محصول چیزی نیست جز فایروال Pfsense که به صورت رایگان در دسترس شما دوستان هست و من هم دوره آموزش تصویری این فایروال رو در سایت ITpro.ir برای شما دوستان عزیز قرار دادم. این کتاب تلاش می شد که تکمیلی باشه بر آموزشهای این دوره تصویری که علاوه بر پوشش بخش اول این دوره تصویری بحثهایی که در اون دوره تهیه نشده رو برای شما در قالب این کتاب بیان می کنم. با امید به خدای مهربون نگارش این کتاب رو شروع می کنم.

Pfsense چیست؟

به عنوان شروع در قدم اول قصد داریم به این سوال پاسخ بدم که Pfsense چیست و چه قابلیت‌هایی دارد، در یک خط همیشه اینطور Pfsense رو تعریف کرد که یک نرم افزار رایگان و یک توزیع انتخابی شده و تغییر یافته ای از سیستم عامل FreeBSD است که دو ویژگی اصلی دارد علاوه بر اینکه یک فایروال است نقش یک روتر را هم می تواند داشته باشد و از طریق یک رابط وب قابل مدیریت است. این برنامه علاوه بر اینکه یک فایروال قوی و قدرتمند است به شما این امکان را می دهد که به آن برنامه های دیگری را هم در قالب برنامه های متن باز اضافه کنید و از طریق همان رابط وب برنامه های جانبی که به تناسب نیاز شما وجود دارد را مدیریت کنید، از جمله این برنامه ها می توان به squid ، snort و حتی Zabbix اشاره کرد که در نصب پیش فرض آن وجود ندارد ولی شما می توانید هر کدام را بسته به نیاز خود نصب و راه اندازی و استفاده کنید، این برنامه فقط از طریق مخازن خود سایت pfsense در دسترس است و در آموزشهای این بخش هم به شما یاد می دم که به چه صورتی برنامه های خارج از این مخازن را هم نصب کنید برنامه هایی که در FreeBSD وجود دارد در pfsense هم قابل نصب و راه اندازی است، به عنوان آخرین کاری که در pfsense نصب کردن برنامه zabbix server است که حتی با یک رابط گرافیکی بر روی یک وب سرور جداگانه و بر روی پورت دیگری راه اندازی کرده ام، به دلیل پیکربندی خوب php در pfsense سرعت رابط وب Zabbix بسیار بالاست. برای دریافت آموزش در این بخش شما به فصل نصب کرد برنامه ها در pfsense مراجعه کنید.

اولین بار pfsense در سال 2004 توسط دو فرد اصلی به نام های Chris Buechler و Scott Ullrich و گروه بزرگی از توسعه دهندگان ارائه شده است، طرح اصلی این فایروال از پروژه m0n0wall گرفته شده است که این پروژه یک فایروال embedded شده ای است که در حجم کم ارائه شده ولی مشکل اصلی آن این بود که بر روی RAM بارگذاری می شود و نمی تواند هیچ قابلیت به آن اضافه کنید چون بر روی هارد دیسک نصب و راه اندازی نمیشد، این ایراد در فایروال pfsense رفع شده و شما باید آنرا بر روی هارد دیسک خود نصب کنید و از طریق هارد سیستم را راه اندازی کنید و می توانید به آن قابلیت اضافه کنید. در ورژن جدید از این فایروال قابلیت نصب بر روی zfs هم به آن اضافه شده است که شما می توانید از قابلیت های این فایل سیستم قوی هم در فایروال pfsense خود استفاده کنید.

حال دلیل انتخاب این نام را در آدرس زیر بیان شده است که مختصری از آنرا برای شما بیان می کنم

<https://www.netgate.com/blog/so-what-does-pfsense-stand-formean-anyway.html>

این پروژه در روزهای اول خودش هیچ اسمی نداشته و فقط از قابلیت jail در FreeBSD استفاده می شود و از طریق CVS به عنوان سیستمی برای توسعه آن استفاده می کنند. در ابتدا دو نفر به نام های Scott و Chris Buechler در این پروژه مشغول به کار و فعالیت بودن و برای ثبت کردن یک نام دامنه با مشکل مواجه بودند، به دلیل اینکه در این فایروال از PF به عنوان بخش اصلی استفاده می شود و از بخش اول این اسم و نام sense به معنای حس در ادامه این نام استفاده کردند که یک حس جدیدی از pf را برای شما ایجاد می کند. پس به این دلیل بود که این نام برای این برنامه انتخاب و اعلام شد، در حال حاضر Chris Buechler از این پروژه در سال 2016 جدا شده است.

هر برنامه متن بازی در قالب یک مجوز ارایه می شود که به نگاه آن به دنیای متن باز اشاره دارد. لایسنس های مختلف و متفاوتی وجود دارد به نام های BSD GNU Apache و که هر کدام به در انیترنترنت قوانین اهداف و شرایط خودشون رو بیان کرده اند. مجوزی که Pfsense از آن استفاده می کند مجوز Apache در ورژن 2 است که در نه بند ارایه شده است؛ برای دسترسی به مجوز های apache به آدرس زیر مراجعه کنید:

<http://www.apache.org/licenses>

بخش اولیه مجوز pfsense به صورت زیر بیان شده است:

A permissive license whose main conditions require preservation of copyright and license notices. Contributors provide an express grant of patent rights. Licensed works, modifications, and larger works may be distributed under different terms and without source code.

یک مجوز قابل قبول که شرایط اصلی آن حفظ اطلاعات کپی رایت و مجوز است. همکاران ارائه یک حق اظهارنامه حق ثبت اختراع. کارهای مجاز، اصلاحات و کارهای بزرگتر ممکن است تحت شرایط مختلف و بدون کد منبع توزیع شود.

در این مجوز پروژه pfsense این اجازه را دارد که کد منبع را ارایه نکند. دسترسی ها و محدودیت های این مجوز را در جدول زیر مشاهده می کنید:

| | |
|------------|------------|
| محدودیت ها | دسترسی های |
|------------|------------|

| | | | |
|--|--|---|---|
| Trademark use Liability Warranty | استفاده از علامت تجاری مسئولیت ضمانتنامه | Commercial use Modification Distribution Patent use Private use | استفاده تجاری تغییر توزیع استفاده از اختراع استفاده خصوصی |
|--|--|---|---|

راههای ارتباطی با پروژه اصلی pfSense :

وب سایت اصلی این پروژه به نام pfsense.org معروف است. که در بخش معرفی این سایت شما می توانید راه های ارتباطی را مشاهده کنید، در ادامه خلاصه این اطلاعات را مشاهده می کنید:

| | |
|--|------------------------|
| sales@netgate.com | بخش فروش و خدمات مشتری |
| support@netgate.com | بخش پشتیبانی و خدمات |
| coreteam@pfsense.org | بخش پروژه pfSense |

در جدول بالا شما با آدرس سایتی به نام [netgate](http://netgate.com) را مشاهده می کنید که بخش آموزش و پشتیبانی پروژه Pfsense را دارد. این شرکت شعاری دارد به شرح زیر:

ما بر روی ارائه ارتباط امن شبکه با کارایی بالا برای همه متمرکز شده ایم.

در این سایت شما با پرداخت 99 دلار در سال می توانید از خدمات حرفه ای در زمینه آموزش و پشتیبانی از pfSense با استفاده از فیلم های آموزشی دقیق و کتاب اصلی این پروژه استفاده کنید. این خدمات به نام خدمات طلایی عضویت pfSense معروف است.

قابلیت فایروال pfSense را می توان در دسته بندی های زیر بیان کنید:

قابلیت Firewall

- فیلتر کردن منبع و مقصد IP، پروتکل IP، منبع و مقصد پورت برای ترافیک TCP و UDP
- محدود کردن اتصالات همزمان بر اساس یک rule
- نرم افزار pfSense با استفاده از pf، یکی از ابزارهای رمزنگاری پیشرفته سیستم عامل / شبکه به شما اجازه می دهد تا توسط سیستم عامل شروع به اتصال به فیلتر کنید. آیا می خواهید سیستم های FreeBSD و Linux را به اینترنت متصل کنید، اما دستگاه های ویندوز را مسدود کنید؟ نرم افزار pfSense قابلیت تفکیک رولهای فایروال را بر اساس سیستم عامل را هم دارد که این قابلیت در سیستم عامل های مبتنی بر BSD پیدا سازی می شود.
- قابلیت گرفتن log و یا غیرفعال کردن log بروی هر رول.
- قابلیت های پیشرفته در routing که به شما این اجازه را می دهد که هم زمان چندین gateway داشته باشید.
- دارا بودن قابلیت alias در آدرسها پورت ها و غیره که نوشتن رولها را خلاصه و ساده تر می کند و شما می توانید چندین رول را در یک خط بنویسید.
- فعال کردن فایروال در لایه دوم به صورت Transparent و مدیریت کردن ترافیک در بین کارت های شبکه ای که این قابلیت بروی آنها فعال شده است.
- قابلیت Packet normalization
- غیرفعال کردن قابلیت فیلتر کردن ترافیک در استفاده از قابلیت routing

قابلیت (NAT) Network Address Translation

- قابلیت Port forwards بروی چندین آدرس ip
- قابلیت NAT 1:1 برای آدرس های IP جداگانه برای یک sub net.
- قابلیت Outbound NAT در تنظیمات پیش فرض NAT همه ترافیک ها به سمت یک آدرس IP ارسال می شود ولی در این روش بجای استفاده از آدرس IP از نام کارت شبکه wan استفاده می شود در حالت multiple WAN.
- قابلیت NAT Reflection که اجازه دسترسی سرویس های پشت فایروال را از طریق آدرس valid فایروال در دسترس است.

قابلیت Multi-WAN

- قابلیت چند شبکه WAN امکان استفاده از اتصالات اینترنتی متعددی را فراهم می کند، با توازن بار و / یا خرابی، برای افزایش دسترسی به اینترنت و توزیع استفاده از پهنای باند.

قابلیت Server Load Balancing

- قابلیت Server Load Balancing برای توزیع بار بین چند سرور استفاده می شود. این معمولا با سرورهای وب، سرورهای پست الکترونیکی و دیگر سرورها استفاده می شود. سرورهایی که قادر به پاسخگویی به درخواست های پینگ یا اتصالات پورت TCP نیستند نمی توانند از این سرویس استفاده کنند.

قابلیت Virtual Private Network (VPN)

- نرم افزار pfsense از سه برنامه برای اتصال استفاده می کنند VPN، IPsec و OpenVPN.

قابلیت Reporting and Monitoring

- در این بخش pfsense از RRD Graphs استفاده می کند تا بتواند اطلاعات زیر را در قالب وب برای شما نمایش دهد:
 - استفاده از پردازنده
 - مجموع خروجی
 - وضعیت فایروال
 - سرعت ارسال هر بسته بر روی هر کارت شبکه
 - زمان پاسخگویی Ping در شبکه wan
 - نمایش وضعیت صف در کارتهای شبکه ای که قابلیت Traffic shaper در آنها فعال است.

قابلیت Dynamic DNS

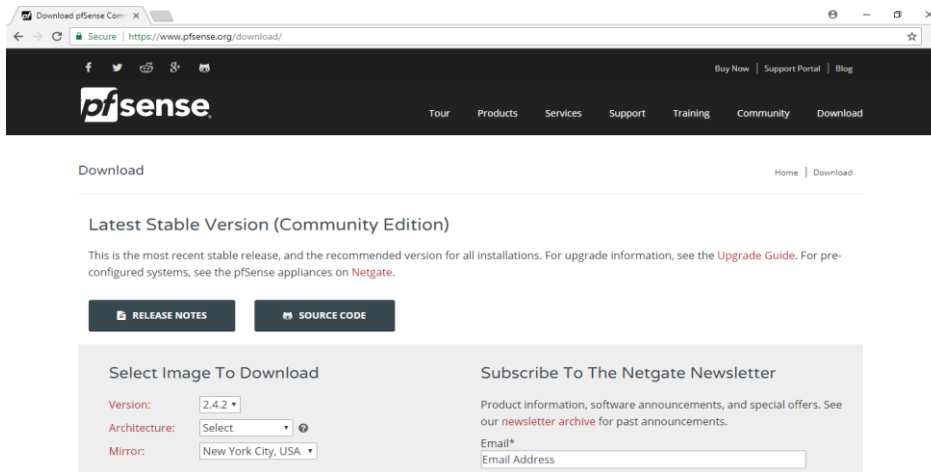
- این قابلیت در pfSense به شما این امکان را می دهد که نام آدرسهای IP که به صورت خودکار توسط DHCP ارائه می شود را در سرور DNS ثبت کند که این امر باعث ارائه کردن ارتباط مبتنی بر نام به جای آدرس ip در شبکه هایی که آدرسهای ip آنهاست را می دهد.

قابلیت Captive Portal

این قابلیت به فایروال pfSense این امکان را اضافه می کند که قبل از ارائه کردن دسترسی به شبکه اینترنت با انتقال داده صفحه وب درخواست از سمت کلاینت به سمت یک صفحه خاص و انجام دادن authentication اجازه دسترسی را به شبکه دیگر که در بیشتر موارد Internet است را می دهد، در این سرویس شما می توانید صفحه خاص خود را داشته باشید و تعداد login کردن کاربران را مدیریت کنید. این سرویس برای شبکه های بی سیم که به صورت رایگان در اختیار مشترکین مهاجر قرار داده می شوند بسیار مفید و کاربردی است.

قابلیت DHCP Server

- یکی از سرویسهای مهم در شبکه های بزرگ و کوچک مدیریت کردن آدرسهای IP است که از طریق سرور DHCP قابل اجرا است که در pfSense هم این قابلیت به صورت حرفه ای با امکانات خوب ارائه می شود.
- سایت اصلی این پروژه www.pfsense.org و شما در این سایت می تونید همه اطلاعات لازم و فایل های مورد نیاز برای نصب کردن و روشهای استفاده از pfSense برای شما بیان شده برای دانلود کردن شما باید به صفحه ای به ادرس زیر مراجعه کنید:
- <https://www.pfsense.org/download>
- این سایت در زمانی که مشغول نوشتن این کتاب هستم به صورت زیر است :



- در این سایت بخش وجود دارد برای انتخاب کردن ورژن و نوع Archive که شما برای نصب کردن به آن نیاز دارید و در بخش بعدی هم باید نزدیکترین سرور را برای دانلود کردن انتخاب کنید در حال حاضر شما می توانید دو ورژن 2.3 و 2.4 را دانلود کنید و از دو حالت usb و iso می توانید برای راه اندازی سیستم خود برای نصب انتخاب کنید، اگر سیستم شما از طریق USB راه اندازی می شود می توانید image این حالت را دانلود کرده و بر روی فلش با استفاده از برنامه win32disk این کار رو براحتی انجام دهید.
- خوب برای نصب کردن شما باید به حداقل سخت افزاری که نیاز دارید توجه کنید و به میزان ترافیکی که قراره از این سیستم رد و بدل بشه بستگی داره ولی خود pfsense در حالت پایه ای به مقادیر زیر نیاز دارید.
- سیستم شما باید حداقل دو کارت شبکه داشته باشه و توجه به این نکته الزامیست که یک کارت شبکه باید به شبکه داخلی شما متصل باشه و کارت شبکه هم باید به شبکه ای متصل باشه که به شبکه دیگه که شبکه قابل اعتمادی نیست مثل اینترنت متصل است.
- خوب بسته به سناریو و میزان ترافیک شبکه خودتون نوع سخت افزار سیستم خودتون رو انتخاب کنید و مراحل نصب رو شروع کنید شما می تونید در نرم افزارهایی مثل Virtualbox هم فایروال خودتون رو نصب کنید که باید به این نکته توجه کنید که نوع سیستم عامل خودتون رو FreeBSD انتخاب کنید.

2.3 نصب کردن Pfsense ورژن

در این بخش با یک نصب ساده و سریع فایروال pfsense آشنا می‌شوید که به صورت کامل تصویری توضیح داده شده است، قبل از نصب به بخش قبلی که در مورد دانلود کردن و سخت‌افزار موردنیاز توضیح داده شده است یک سری بزنید تا با این موارد آشنا شوید، در این بخش فرض بر آن است که شما pfsense را دانلود کرده و سیستم شما سخت‌افزار موردنیاز را دارد و حداقل دو کارت شبکه را دارد. در این بخش شما باید سیستم خود را راه‌اندازی کنید که در بخش اول با تصویری به صورت شکل زیر مواجه می‌شوید:

```
Looking for config.xml on done.
Generating a MFS /home partition... done.
Disabling APM on /dev/ad3
(pass1:ata1:0:1:0): SETFEATURES. ACB: ef 85 00 00 00 40 00 00 00 00 00
(pass1:ata1:0:1:0): CAM status: ATA Status Error
(pass1:ata1:0:1:0): ATA status: 41 (DRDY ERR), error: 04 (ABRT )
(pass1:ata1:0:1:0): RES: 41 04 00 00 00 00 00 00 00 00 00
Failed to configure APM: No such file or directory

Welcome to pfSense 2.3.5-RELEASE on the 'cdrom' platform...

Mounting unionfs directories...done.
Creating symlinks.....ELF ldconfig path: /lib /usr/lib /usr/lib/compat /usr/local/lib /usr/local/lib/ipsec /usr/local/lib/per15/5.24/mach/CORE
a.out ldconfig path: /usr/lib/aout /usr/lib/compat/aout
done.
```

در زیر نشان‌واره‌ی pfsense برای شما ورژنی که در حال نصب کردن آن هستید را نمایش می‌دهد و به شما می‌گوید که از طریق CD-ROM در حال بارگذاری هست. بعد از راه‌اندازی شدن این بخش شما با پیغام خوش‌آمد گویی که در شکل زیر نمایش داده شده است مواجه می‌شوید در این بخش شما می‌توانید روش راه‌اندازی شدن سیستم را انتخاب کنید، این منو را در زمانی که نصب هم انجام شده است برای شما نمایش داده می‌شود، دو بخش در این منو پرکاربردتر است بخش multi User که راه‌اندازی سیستم را به صورت کامل بارگذاری می‌کند و بخش single user mode که این بخش دقیقه بعد از راه‌اندازی هسته و قبل از راه‌اندازی شدن init است و برای وارد شدن به آن شما نیاز به انتخاب کردن یک Shell دارید که بتوانید در این بخش شما یک سری اموری که ریکاوری کننده است را انجام دهید

این امور مثل تغییر دادن رمز عبور و غیراست که بیشتر مباحث برای مدیریت کردن سیستم عامل FreeBSD است و در Pfsense برای شما کاربردی ندارد.

در این قسمت بیان شده چند کلمه کاربردی بیان شده است که در زیر با آن آشنا می شوید، هسته و کرنل:

این بخش مدیریت کردن کامل سیستم عامل را انجام می دهد و مدیریت کل سیستم عامل را بر عهده دارد مثل اختصاص دادن فضای Ram به برنامه ها و مدیریت کردن کاربران و پردازش ها و غیره، این بخش به تناسب پشتیبانی کردن از سخت افزارها و نرم افزارهای می تواند دارای حجم متفاوتی باشد، در آموزش هایی که در سایت من قرار دارد روش کامپایل کردن هسته و بارگذاری ماژول ها در هسته به صورت کامل بیان شده است.

پردازش `init`:

این پردازش یکی از پردازش های اصلی و مهم در راه اندازی سیستم عامل FreeBSD است که در بعد از راه اندازی هسته راه اندازی می شود و در سیستم عامل های لینوکسی کل مراحل نصب را انجام می دهد ولی در FreeBSD این پردازش فقط به صورت سنبلیک وجود دارد. عدد پردازشی این برنامه 1 است که دقیقه بعد از عدد 0 که خود هسته است راه اندازی می شود. بعد از راه اندازی این پردازش شما می توانید وارد بخش `single user mode` شوید، بعد از راه اندازی این بخش پردازش `init` سایر مراحل راه اندازی به برنامه `rc` داده می شود که بخش راه اندازی کردن سرویسهاست که با رنگ خاکستری پیغام های خود را نمایش می دهد.

حالت `Multi User`:

این حالت بعد از اتمام کار پردازش `rc` شروع می شود که در حقیقت پایان بخش `RC` و شروع بخش ورود کاربران است، در این بخش شما با استفاده از کاربران متعبر می توانید به سیستم وارد شوید که البته مرحله ورود به `pfsense` با سیستم عامل FreeBSD متفاوت است و در `pfsense` یک منوی کنسول برای کاربر نمایش داده می شود که در بخشهای بعدی به صورت کامل با آن آشنا خواهید شد.



بعد از انتخاب کردن حالت **multi User** پیغام های نمایش داده شده اول در دو رنگ است رنگ اولی سفید است که در این بخش هسته در حال چک کردن سخت افزار های سیستم شما است و هر دستگاهی را که شناسایی می کند برای شما با اطلاعات بیشتر نمایش می دهد، این بخش را شما در مراحل راه اندازی می توانید با فرمان **dmesg** مشاهده کنید. در شکل زیر شما این پیغام ها را مشاهده می کنید:


```

iwi_ibss: If you agree with the license, set legal.intel_iwi.license_ack=1 in /b
oot/loader.conf.
module_register_init: MOD_LOAD (iwi_ibss_fw, 0xc0846a10, 0) error 1
iwi_monitor: You need to read the LICENSE file in /usr/share/doc/legal/intel_iwi
/.
iwi_monitor: If you agree with the license, set legal.intel_iwi.license_ack=1 in
/boot/loader.conf.
module_register_init: MOD_LOAD (iwi_monitor_fw, 0xc0846ac0, 0) error 1
netmap: loaded module
kbd1 at kbdmux0
cryptosoft0: <software crypto> on motherboard
padlock0: No ACE support.
acpi0: <INTEL 440BX> on motherboard
acpi0: Power Button (fixed)
hpet0: <High Precision Event Timer> iomem 0xfed00000-0xfed003ff on acpi0
Timecounter "HPET" frequency 14318180 Hz quality 950
cpu0: <ACPI CPU> on acpi0
attimer0: <AT timer> port 0x40-0x43 irq 0 on acpi0
Timecounter "i8254" frequency 1193182 Hz quality 0
Event timer "i8254" frequency 1193182 Hz quality 100
atrtc0: <AT realtime clock> port 0x70-0x71 irq 8 on acpi0
Event timer "RTC" frequency 32768 Hz quality 0
Timecounter "ACPI-fast" frequency 3579545 Hz quality 900
acpi_timer0: <24-bit timer at 3.579545MHz> port 0x1000-0x100b on acpi0

```

بخش هسته بعد از اتمام به صورت حالت زیر پیغام های خاکستری به صورت زیر برای شما نمایش داده می شود، این پیغام ها در زمان راه اندازی و در زمان نصب متفاوت است، شروع این بخش را در شکل زیر مشاهده می کنید که 3 خط آخر پیغام های است که توسط RC ایجاد می شود:

```

ada0: 33.300MB/s transfers (UDMA2, cd0 at ata1 bus 0 scbus1 target 0 lun 0
cd0: <NECUMWar UMWare IDE CDR10 1.00> Removable CD-ROM SCSI device
cd0: Serial Number 1000000000000000001
cd0: 33.300MB/s transfers (UDMA2, ATAPI 12bytes, PIO 65534bytes)
cd0: 585MB (299587 2048 byte sectors)
cd0: quirks=0x40<RETRY_BUSY>
PIO 32768bytes)
ada0: 20480MB (41943040 512 byte sectors)
ada0: Previously was known as ad3
ugen0.2: <UMWare> at usb0
uhid0: <UMWare> on usb0
Timecounter "TSC" frequency 1599951000 Hz quality 1000
uhid1: <UMWare> on usb0
Root mount waiting for: usb1 usb0
Root mount waiting for: usb1 usb0
ugen0.3: <vendor 0x0e0f> at usb0
uhub2: <UMWare Virtual USB Hub> on usb0
uhub1: 6 ports with 6 removable, self powered
Root mount waiting for: usb0
uhub2: 7 ports with 7 removable, self powered
Trying to mount root from cd9660:/dev/iso9660/PFSENSE [ro]...
Configuring crash dumps...
Generating MFS /var partition
Generating MFS /etc partition

```

بعد از اتمام این بخش پیغامی به صورت شکل زیر برای شما نمایش داده می شود که در بخش شما می توانید حالت نصب یا ریکاوری را انتخاب کنید، این منو به صورت خودکار عمل کرده و شما را وارد بخش نصب می کند که البته این بخش بعد از هفت ثانیه بارگذاری می شود،

```
done.
Launching the init system..... done.
Initializing..... done.
Starting device manager (devd)...done.

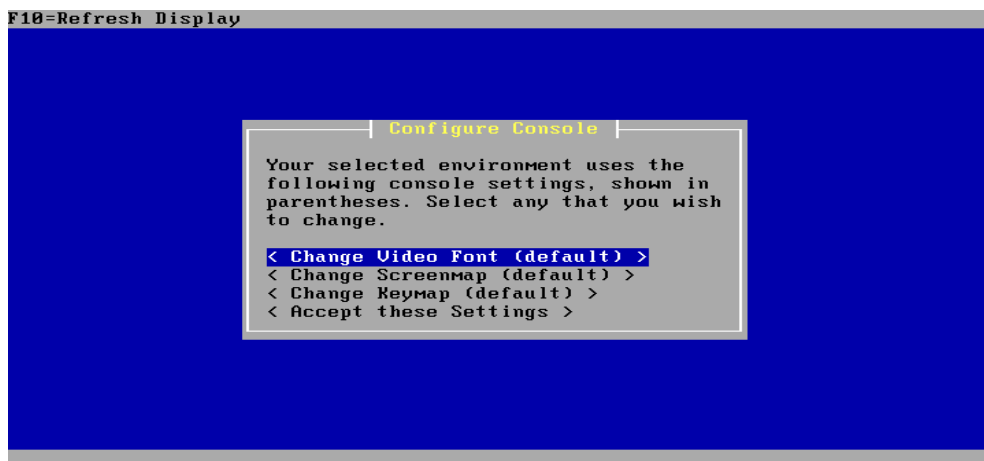
[ Press R to enter recovery mode or ]
[ press I to launch the installer ]

(R)ecovery mode can assist by rescuing config.xml
from a broken hard disk installation, etc.

(I)nstaller will be invoked

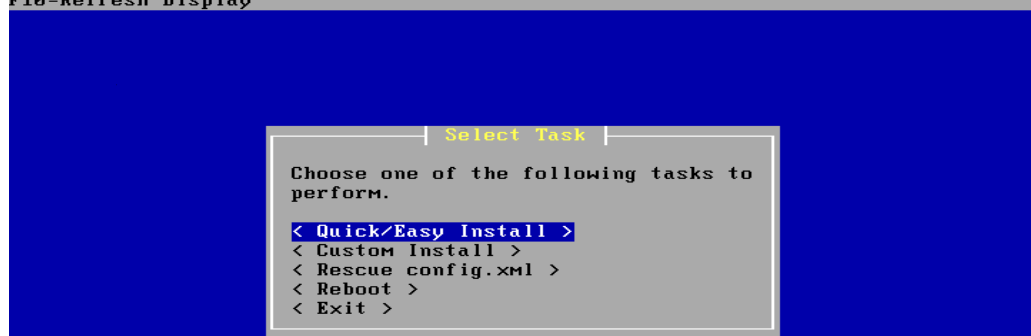
Timeout before auto boot continues (seconds): 7
```

بعد از اتمام هفت ثانیه و طی کردن مراحل بوت شما وارد محیط نصبی می شوید که این بخش را شما در شکل زیر مشاهده می کنید:



در منوی اولیه این بخش شما می توانید فونت، وضعیت نمایش و وضعیت صفحه کلید که در حقیقت چیدمان صفحه کلید است را تغییر دهید که این تنظیمات پیش فرض این بخش برای سیستم هایی که به صفحه نمایش متصل هستند مناسب بوده و شما با رفتن بر روی گزینه آخر با استفاده از کلید جهت پایین و زدن **Enter** شما وارد بخش بعدی نصب می شوید که در شکل زیر مشاهده می کنید:

F10=Refresh Display



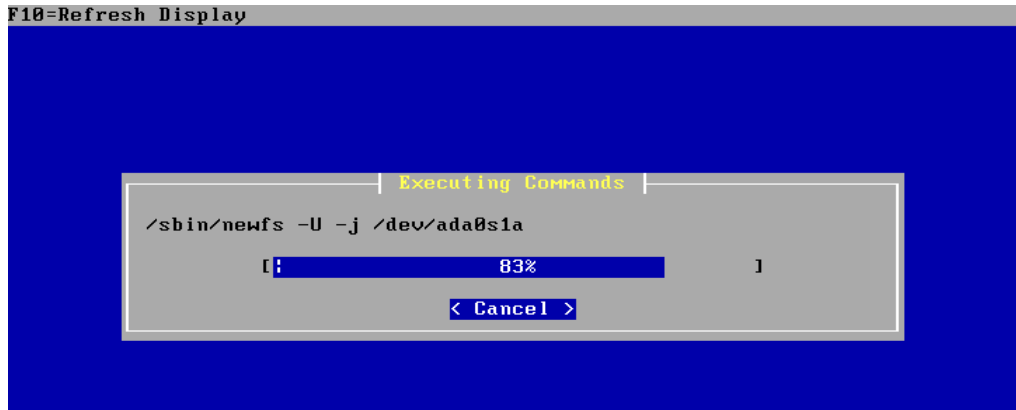
در این بخش شما با حالت نصب را انتخاب می کنید نصب سریع و آسان نصبی است که از شما چندان سوال نمی شود و به راحتی pfsnes برای شما نصب می شود در این مرحله از این گزینه برای نصب استفاده کنید نصب انتخابی برای زمانی است که شما در نصب کردن به مهارت رسیده باشید، در مورد فایل xml هم که شما از طریق آن می توانید تنظیمات سیستم خود را بازگردانی کنید در بخش backup گیری توضیح داده خواهد شد. بعد از انتخاب کردن گزینه اول مراحل نصب شروع خواهد شد و شما با منو هایی به صورت زیر مواجه می شوید:

F10=Refresh Display

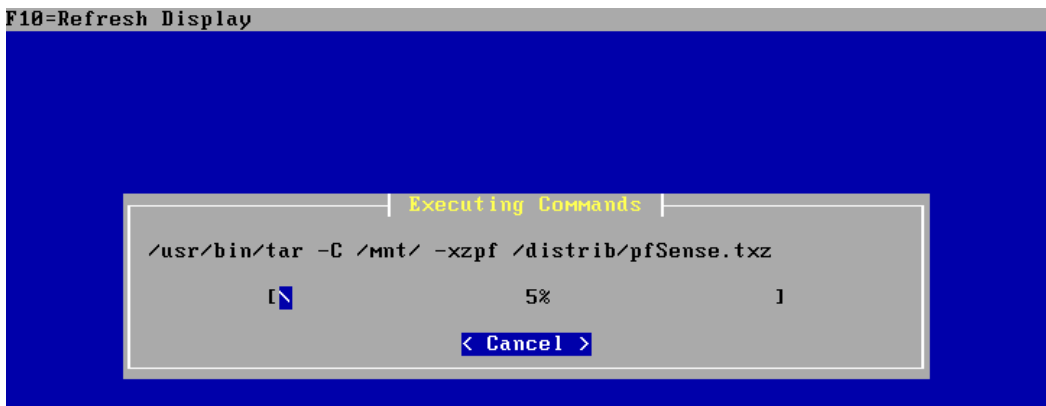


این منو به شما پیغامی را نمایش میدهد که دریافت تایید نصب است و به شما اعلان می کند که شما در مرحله قبل نوع نصب Easy را انتخاب کرده اید و همه اطلاعاتی که بر روی هارد دیسک شما وجود دارد پاک می شود، اگر هم دوست دارید کنترل بیشتری بر روی مراحل نصب داشته باشید حالت Custom را انتخاب کنید. این پیغام حکم پیام

آخر را دارد و بعد از OK کردن آن مراحل نصب با پارتیشن بندی دیسک شما شروع می شود و همه اطلاعات دیسک شما پاک خواهد شد، نصب هم به صورت منو هایی به شما بصورت زیر نمایش داده می شود:



در شکل بالا برنامه نصب با استفاده از `newfs` در حال ایجاد کردن پارتیشن های لازم برای نصب کردن است که علاوه بر ایجاد کردن پارتیشن ها را هم برای استفاده `format` می کند.



بعد از اتمام مرحله قبل که پارتیشن بندی بود در این مرحله برنامه نصبی به صورت خودکار شروع به نصب کردن می کند این بخش به تناسب سرعت سیستم شما قابل تغییر خواهد بود.

F10=Refresh Display

Install Kernel

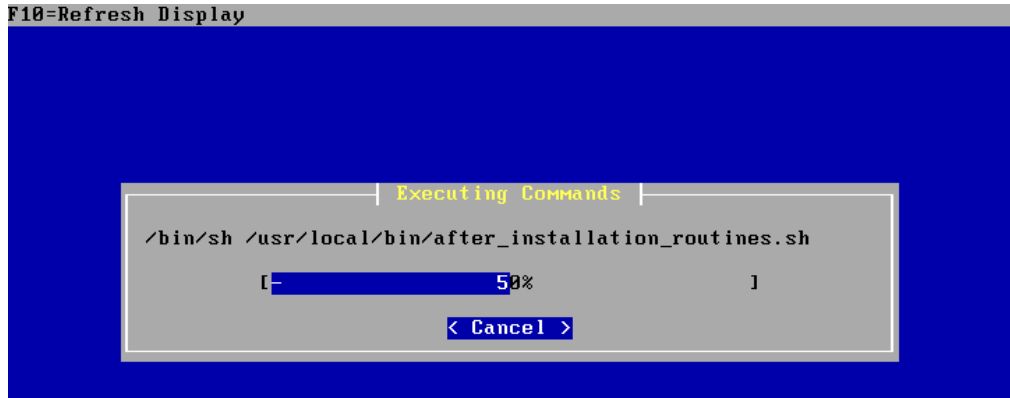
You may now wish to install a custom Kernel configuration.

< Standard Kernel >

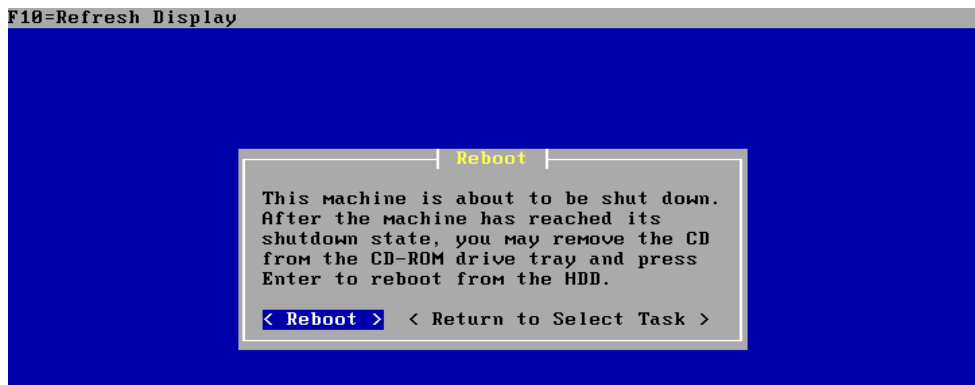
< Embedded kernel (no VGA console, keyboard) >

بعد از اتمام مرحله قبلی در این بخش از شما در مورد نوع هسته سوال پرسیده می شود که دو حالت برای شما نمایش داده می شود شما می توانید یکی از آنها را انتخاب کنید. حالت Standard که در این روش برای سیستم هایی است که از صفحه نمایش، کارت گرافیک و صفحه کلید و غیر استفاده می کنند، در مقابل این نوع از سیستم ها، سیستم هایی وجود دارد که به Embedded معروف هستند که هیچ یک از سخت افزارهای بیان شده را دارا نیستند و شما می توانید فقط از طریق رابط شبکه و وب با آنها ارتباط برقرار کنید که بحث ما در این کتاب نیست ولی شما می توانید به راحتی pfSense را بر روی این نوع از سخت افزارها نصب کنید و با استفاده از آدرس ip پیش فرض 192.168.1.1 به آن متصل شوید. (در بخش ارتباط با رابط وب با روش اتصال به رابط وب آشنا می شوید).

بعد از انتخاب کردن هسته استاندارد مرحله نصب به صورت زیر ادامه پیدا می کند:



در این مرحله هم هسته و pfSense به صورت کامل بر روی سیستم شما نصب می شود و بعد از اتمام آن برای شما پیغام زیر نمایش داده می شود:



بعد از اتمام نصب شما باید سیستم خود را Restart کنید و بخش دوم مرحله نصب را که شامل انتخاب کردن کارتهای شبکه برای شبکه های اینترنت و داخلی است را انتخاب و تنظیم کنید، در این مرحله به شما توصیه می شود که CD را از درایو خود خارج کنید و سیستم را از طریق هارد دیسک راه اندازی کنید.

```

pfSense is now rebooting

After the reboot is complete, open a web browser and
enter https://192.168.1.1 (or the LAN IP Address) in the
location bar.

You might need to acknowledge the HTTPS certificate if
your browser reports it as untrusted. This is normal
as a self-signed certificate is used by default.

*DEFAULT Username*: admin
*DEFAULT Password*: pfsense

Rebooting in 5 seconds. CTRL-C to abort.
Rebooting in 4 seconds. CTRL-C to abort.
Rebooting in 3 seconds. CTRL-C to abort.

```

در شکل بالا مشاهده می کنید که سیستم شما در حال Restart شدن است. در این پیغام برای شما توضیح داده شده است که برای ورود به بخش رابط وب از چه آدرس IP استفاده کنید که همان 192.168.1.1 است که باید از طریق شبکه Lan به pfsense متصل شوید و اگر هم مشکل Certificate دارید آنرا را نادیده بگیرید و برای متصل شدن از نام کاربری admin و رمز عبور pfsense استفاده کنید که در بخش مربوطه برای شما کامل توضیح خواهم داد، بعد از راه اندازی شدن مجدد سیستم شما با loader سیستم عامل FreeBSD که به صورت شکل زیر است مواجه می شوید:

```

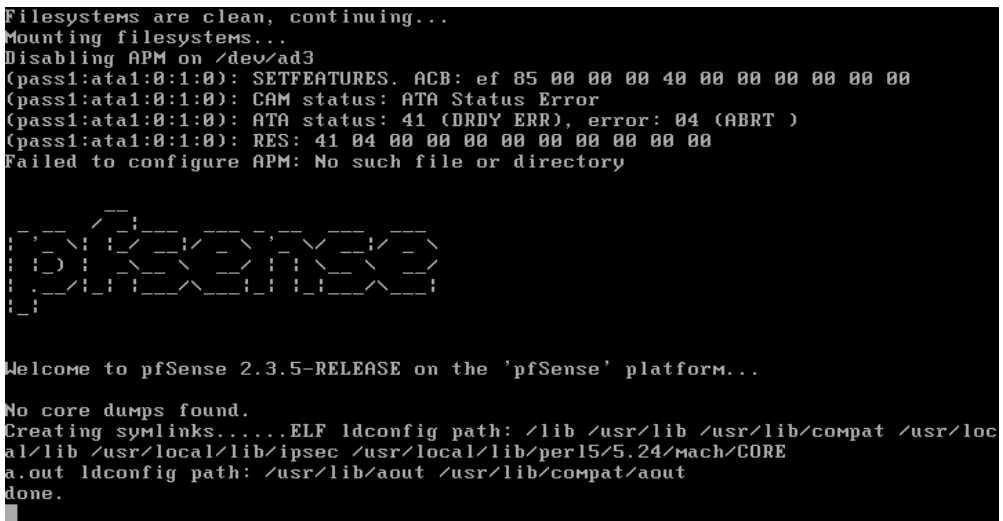
F1 pfSense
F6 PXE
Boot: F1

```

این بخش به صورت خودکار باعث راه اندازی شدن pfsense شما می شود که البته یک مدت زمانی برای مثال 15 ثانیه زمان خواهد برد و شما می توانید با استفاده از کلید F1 روی صفحه کلید سرعت راه اندازی را بیشتر کنید که البته به آن نیازی ندارید این بخش یک loader قدیمی در FreeBSD است که برای انتخاب کردن حالت های boot سیستم عامل هایی که کنار FreeBSD بر روی سیستم شما نصب شده است استفاده می شود و شما در این بخش هم می توانید راه اندازی PXE را هم انتخاب کنید که برای راه اندازی از طریق شبکه استفاده می شود. بعد از بخش شما وارد بخش راه اندازی قبل از هسته و انتخاب کردن نوع single و یا multi user می شوید که در صورتی که انتخابی انجام ندهید و یا Enter کنید وارد حالت راه اندازی کامل یا همان multi User می شوید.



بعد از این بخش شما پیغام های هسته را مشاهده می کنید به صورت نمایش داده شده و مراحل نصب به صورت شکل زیر ادامه پیدا میکند تا شما وارد بخش تنظیمات کارت شبکه ها را مشاهده کنید:



در شکل زیر شما کارت شبکه های سیستم خود را که هسته آنها را تشخیص داده شده است را با رنگ سفید مشاهده می کنید که وضعیت هر دو آنها UP است (در بخش شبکه به صورت کامل با فرمان های این بخش آشنا می شوید).


```

Creating symlinks.....ELF ldconfig path: /lib /usr/lib /usr/lib/compat /usr/local/lib /usr/local/lib/ipsec /usr/local/lib/perl5/5.24/mach/CORE
a.out ldconfig path: /usr/lib/aout /usr/lib/compat/aout
done.
External config loader 1.0 is now starting... ada0s1 ada0s1a.0 is now starting..
. ada0s1b.0 is now starting...
Launching the init system..... done.
Initializing..... done.
Starting device manager (devd)...done.
Loading configuration.....done.

Default interfaces not found -- Running interface assignment option.
le0: link state changed to UP
le1: link state changed to UP

Valid interfaces are:

le0      00:0c:29:b1:74:4f (down) AMD PCnet-PCI
le1      00:0c:29:b1:74:59 (down) AMD PCnet-PCI

Do VLANs need to be set up first?
If VLANs will not be used, or only for optional interfaces, it is typical to
say no here and use the webConfigurator to configure VLANs later, if required.

Should VLANs be set up now [y;n]? █

```

خب از شما در این بخش از شما درخواست می شود که VLAN را پیکربندی کنید که البته نیازی هم به انجام این عمل در این بخش نیست و در فصلی این بخش برای شما کامل توضیح داده خواهد شد، در پیام پایانی این بخش شما می توانید از دو مقدار V به معنی بله و n به معنی خیر استفاده کنید، این دو حالت با خطی افقی از هم جدا شده است و به شما می گوید که فقط یکی از این دو حالت را می توانید انتخاب کنید، به دلیل که این بخش ما قصد پیکربندی vlan را نداریم از گزینه n و بعد Enter استفاده کنید تا وارد بخش بعدی که در شکل زیر مشاهده می کنید شوید:

```

le0      00:0c:29:b1:74:4f (down) AMD PCnet-PCI
le1      00:0c:29:b1:74:59 (down) AMD PCnet-PCI

Do VLANs need to be set up first?
If VLANs will not be used, or only for optional interfaces, it is typical to
say no here and use the webConfigurator to configure VLANs later, if required.

Should VLANs be set up now [y;n]? n

If the names of the interfaces are not known, auto-detection can
be used instead. To use auto-detection, please disconnect all
interfaces before pressing 'a' to begin the process.

Enter the WAN interface name or 'a' for auto-detection
(le0 le1 or a): █

```

در مرحله بعد شما باید کارت های شبکه ای را که به سیستم خود متصل کردید و در شبکه های خاصی وجود دارد را انتخاب کنید، هدف اصلی از استفاده از pfSense در قدم اول قرار گرفتن آن بین شبکه wan و lan است، پس در قدم اول شما باید کارت شبکه ای که به شبکه wan شما متصل است و به اینترنت دسترسی دارد را انتخاب کنید که اولین کارت شبکه شماست، در این بخش شما باید نام کارت شبکه را که مشاهده می کنید را وارد کنید و یا از کلمه a که حالت خودکار است را انتخاب کنید تا به صورت خودکار این عمل انجام شود.

نکته:

برای انتخاب کردن کارت شبکه درست شما می توانید از آدرس mac هر کارت شبکه که به صورت خاص و منحصر بفرد است استفاده کنید و در قسمت نمایش کارتهای شبکه که به صورت سفید رنگ برای شما نمایش داده شده است آدرس mac هر کارت شبکه برای شما نمایش داده شده است و به شما این توان را می دهد که کارت شبکه خود را در این بخش به درستی انتخاب کنید.

بعد از این بخش شما باید کارت شبکه ای که به شبکه Lan متصل است را به صورت حالت قبلی انتخاب کنید که در شکل زیر آنرا مشاهده میکنید:

```
Default interfaces not found -- Running interface assignment option.
le0: link state changed to UP
le1: link state changed to UP

Valid interfaces are:

le0    00:0c:29:b1:74:4f (down) AMD PCnet-PCI
le1    00:0c:29:b1:74:59 (down) AMD PCnet-PCI

Do VLANs need to be set up first?
If VLANs will not be used, or only for optional interfaces, it is typical to
say no here and use the webConfigurator to configure VLANs later, if required.

Should VLANs be set up now [y;n]? n

If the names of the interfaces are not known, auto-detection can
be used instead. To use auto-detection, please disconnect all
interfaces before pressing 'a' to begin the process.

Enter the WAN interface name or 'a' for auto-detection
(le0 le1 or a): le0

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(le1 a or nothing if finished):
```

در این مرحله هم شما می توانید کارت lan خود را انتخاب کنید و یا اگر مقدار آنرا وارد نکنید به منزله پایان این بخش تلقی می شود و مرحله انتخاب کارتهای شبکه به پایان می رسد.

```
Default interfaces not found -- Running interface assignment option.
le0: link state changed to UP
le1: link state changed to UP

Valid interfaces are:

le0    00:0c:29:b1:74:4f (down) AMD PCnet-PCI
le1    00:0c:29:b1:74:59 (down) AMD PCnet-PCI

Do VLANs need to be set up first?
If VLANs will not be used, or only for optional interfaces, it is typical to
say no here and use the webConfigurator to configure VLANs later, if required.

Should VLANs be set up now [y;n]? n

If the names of the interfaces are not known, auto-detection can
be used instead. To use auto-detection, please disconnect all
interfaces before pressing 'a' to begin the process.

Enter the WAN interface name or 'a' for auto-detection
(le0 le1 or a): le0

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(le1 a or nothing if finished):
```

حال بعد از انتخاب کردن کارت شبکه wan حال باید کارت شبکه lan را انتخاب کنید که بتوانید از طریق شبکه lan به pfSense دسترسی داشته باشید. البته این بخش هم از طریق منوی کنوسل باز هم در دسترس است.

```
Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(le1 a or nothing if finished): le1

Enter the Optional 1 interface name or 'a' for auto-detection
(a or nothing if finished):

The interfaces will be assigned as follows:

WAN  -> le0
LAN  -> le1

Do you want to proceed [y;n]?
```

در منوی آخر زمانی که کارت های شبکه را مشخص کرده اید و یا Finish را استفاده کنید به شما وضعیت کارت های شبکه شما نمایش داده می شود که اگر این تنظیمات را قبول دارید Y را وارد کنید و دیگر بخش نصب و تنظیمات به پایان رسیده است و حال در شکل زیر مشاهده می کنید که سرویسها راه اندازی می شود

```

Do you want to proceed [y/n]? y

Writing configuration...done.
Updating configuration.....done.
Checking config backups consistency...done.
Setting up extended sysctls...done.
Setting timezone...done.
Configuring loopback interface...done.
Starting syslog...done.
Starting Secure Shell Services...done.
Setting up polling defaults...done.
Setting up interfaces microcode...done.
Configuring loopback interface...done.
Creating wireless clone interfaces...done.
Configuring LAGG interfaces...done.
Configuring VLAN interfaces...done.
Configuring QinQ interfaces...done.
Configuring WAN interface...done.
Configuring LAN interface...done.
Configuring CARP settings...done.
Syncing OpenVPN settings...done.
Configuring firewall.....done.
Starting PFLOG...done.
Setting up gateway monitors...done.
Starting DNS Resolver...

```

در مرحله بعد پایانی pfSense شما به صورت کامل راه اندازی شده است و شما وارد منوی کنسول می شوید به صورت زیر:

```

Starting CRON... done.
pfSense (pfSense) 2.3.5-RELEASE i386 Mon Oct 30 11:08:09 CDT 2017
Bootup complete

FreeBSD/i386 (pfSense.localdomain) (ttyv0)

pfSense - Netgate Device ID: 66973cbe59c6f3fea0b5

*** Welcome to pfSense 2.3.5-RELEASE (i386 full-install) on pfSense ***

WAN (wan)      -> le0          -> v4/DHCP4: 192.168.174.129/24
LAN (lan)      -> le1          -> v4: 192.168.1.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults   13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                15) Restore recent configuration
7) Ping host                  16) Restart PHP-FPM
8) Shell

Enter an option:

```

این بخش در آموزش های بعدی به صورت کامل مورد بررسی قرار خواهد گرفت، در این مرحله نصب به پایان رسیده است و حال سیستم شما آماده پیکربندی و استفاده است.

نکته:

به صورت پیش فرض فایروال بر روی کارت شبکه WAN شما فعال است و اگر همه شبکه wan شما از آدرسهای invalid استفاده کنید از طریق شبکه Wan به pfSense دسترسی نخواهید داشت و حتما باید از طریق یک سیستم در شبکه Lan از طریق رابط وب به pfSense وارد شوید.

نکته:

برای غیرفعال کردن موقت فایروال باید از منوی کنسول وارد بخش Shell شوید که در منوی کنسول باید عدد 8 را در مقابل Enter an Option: وارد کنید و بعد Enter کنید تا وارد محیط Shell شوید به صورت شکل زیر:

```
FreeBSD/i386 (pfSense.localdomain) (ttyv0)
pfSense - Netgate Device ID: 66973cbe59c6f3fea0b5
*** Welcome to pfSense 2.3.5-RELEASE (i386 full-install) on pfSense ***
WAN (wan)      -> le0          -> v4/DHCP4: 192.168.174.129/24
LAN (lan)      -> le1          -> v4: 192.168.1.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                    16) Restart PHP-FPM
8) Shell

Enter an option: 8
[2.3.5-RELEASE][root@pfSense.localdomain]/root: |
```

در این بخش شما برای غیرفعال کردن فایروال باید از فرمان pfctl استفاده کنید ، این فرمان برای مدیریت کردن فایروال pf استفاده می شود که دارای سوئیچ های مختلفی دارد که دو سوئیچ معروف دارد به نام d و e ، برای غیر فعال کردن این فایروال از فرمان زیر استفاده کنید:

```
#pfctl -d
```

برای فعال کردن هم از فرمان زیر استفاده کنید:

```
#pfctl -e
```

به اختصار سوئیچ d برای disable و سوئیچ e برای enable کردن استفاده می شود. در شکل زیر خروجی این فرمان نمایش داده شده است:

```
*** Welcome to pfSense 2.3.5-RELEASE (i386 full-install) on pfSense ***

WAN (wan)      -> le0          -> v4/DHCP4: 192.168.174.129/24
LAN (lan)      -> le1          -> v4: 192.168.1.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces         10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system            14) Enable Secure Shell (sshd)
6) Halt system              15) Restore recent configuration
7) Ping host                16) Restart PHP-FPM
8) Shell

Enter an option: 8

[2.3.5-RELEASE][root@pfSense.localdomain]/root: pfctl -d
pf disabled
[2.3.5-RELEASE][root@pfSense.localdomain]/root: pfctl -d
pfctl: pf not enabled
[2.3.5-RELEASE][root@pfSense.localdomain]/root: pfctl -e
pf enabled
[2.3.5-RELEASE][root@pfSense.localdomain]/root: |
```

برای خارج شدن از این بخش فرمان exit را اجرا کنید و بعد از اجرای آن وارد منوی کنسول می شوید.

بخش دوم آشنایی با منوی کنسول در Pfsense

آشنایی با منوی کنسول در Pfsense

این بخش شامل دو بخش عمده می باشد بخش بالای آن آدرس های ip کارت های شبکه شما را نمایش می دهد که به شما برای اتصال به رابط وب کمک می کند و بخش پایین شامل 16 منوی مختلف است با استفاده از عدد آن در بخش پایین صفحه و زدن Enter وارد آن بخش می شوید. در این بخش شما به صورت مختصر با این 16 بخش آشنا می شوید که برخی برای نمایش گزارشات، دسترسی به Shell، تنظیم کردن آدرس IP و راه اندازی کردن مجدد سرویسها و تغییر دادن رمز عبور رابط وب استفاده می شود که در ادامه با آنها آشنا می شوید. شکل زیر یک منوی کنسول را برای شما نمایش داده می شود که ورژن نصبی و آدرسهای IP را به شما نمایش می دهد.

```

Enter an option:

FreeBSD/i386 (pfSense.localdomain) (ttyv0)
pfSense - Netgate Device ID: 66973cbe59c6f3fea0b5
*** Welcome to pfSense 2.3.5-RELEASE (i386 full-install) on pfSense ***

WAN (wan)      -> le0          -> v4/DHCP4: 192.168.174.129/24
LAN (lan)      -> le1          -> v4: 192.168.1.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces         10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system             14) Enable Secure Shell (sshd)
6) Halt system               15) Restore recent configuration
7) Ping host                  16) Restart PHP-FPM
8) Shell

Enter an option:

```

عدد 0 یا منوی Logout:

این بخش در زمانی که شما از طریق ssh به سرور pfsense شما متصل می شود کار می کند، شما می توانید از راه دور با استفاده از پروتکل ssh به pfsense متصل شوید و از این منوی کنسول هم استفاده کنید، در بخشی شما با روش راه اندازی ssh در pfsense به صورت کامل آشنا خواهید شد و روش استفاده از کلید به جای رمزعبور را آموزش خواهید دید، این منوی برای خارج شدن از ssh استفاده می شود.

عدد 1 یا منوی انتخاب کردن کارت های شبکه:

در این بخش شما می توانید کارتهای شبکه خود را انتخاب کنید این بخش در زمان نصب و بعد از reboot شدن سیستم و قبل از وارد شدن به سیستم این بخش توضیح داده شده است و شما می توانید به بخش نصب مراجعه کنید و با سوالات این منو بیشتر آشنا شوید. در شکل زیر بخش اولیه شروع این منو را مشاهده میکنید:

```

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: 1

Valid interfaces are:

le0      00:0c:29:b1:74:4f   (up) AMD PCnet-PCI
le1      00:0c:29:b1:74:59   (up) AMD PCnet-PCI

Do ULANs need to be set up first?
If ULANs will not be used, or only for optional interfaces, it is typical to
say no here and use the webConfigurator to configure ULANs later, if required.

Should ULANs be set up now [y;n]?

```

در بخش اول کارتهای شبکه با آدرسهای mac را برای شما نمایش میدهد ، در ادامه با تنظیم کردن Vlan شروع می شود و ادامه این بخش مثل سوالات بخش زمان نصب شما می توانید کارتهای شبکه Lan و Wan را انتخاب کنید برای خروج از این بخش از کلید های هم زمان Ctl+C استفاده کنید.

عدد 2 با منوی set interface IP address:

در این بخش بعد از انتخاب کردن کارتهای شبکه خود می توانید آدرسهای IP آنها را نیز تنظیم کنید، بعد از انتخاب کردن این منو شما با بخش زیر برای شما نمایش داده می شود:

```

*** Welcome to pfSense 2.3.5-RELEASE (i386 full-install) on pfSense ***

WAN (wan)      -> le0          -> v4/DHCP4: 192.168.174.129/24
LAN (lan)      -> le1          -> v4: 192.168.1.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults   13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                15) Restore recent configuration
7) Ping host                  16) Restart PHP-FPM
8) Shell

Enter an option: 2

Available interfaces:

1 - WAN (le0 - dhcp, dhcp6)
2 - LAN (le1 - static)

Enter the number of the interface you wish to configure: █

```

در ابتدا امر کارتهای شبکه و تنظیمات آدرس IP برای شما نمایش داده می شود، برای مثال در این سیستم شما دو کارت شبکه دارید که قسمت wan از طریق dhcp آدرس ip دریافت می کند و قسمت lan هم به صورت دستی آدرس ip دریافت کرده است و ما در ادامه قصد داریم که این آدرس IP را تغییر دهیم، امکان استفاده از DHCP به صورت پیش فرض بر روی کارت شبکه lan وجود ندارد مگر شما از آدرس ip آنرا پاک کنید و از طریق خط فرمان DHCPD را بر روی آن فعال کنید ، قابلیت دریافت خودکار ip برای کارت شبکه lan از طریق فایروال مسدود شده است که در بخش فایروال روش غیرفعال کردن این بخش را برای شما توضیح می دهیم، در شکل زیر شما مراحل کامل تغییر آدرس ip کار شبکه lan از مشاهده می کنید:

```

1 - WAN (le0 - dhcp, dhcp6)
2 - LAN (le1)

Enter the number of the interface you wish to configure: 2

Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.10.1

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0    = 8

Enter the new LAN IPv4 subnet bit count (1 to 31):
> 24

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Enter the new LAN IPv6 address. Press <ENTER> for none:
>

Do you want to enable the DHCP server on LAN? (y/n) n

```

در قدم اول کارت شبکه دوم را انتخاب می کنیم ، در بخش بعدی شما در مقابل علامت > باید آدرس ip جدید را وارد کنید که البته اگر چیزی وارد کنید به صورت خودکار از طریق DHCP تنظیمات را دریافت می کند که در شبکه lan قابل پیاده سازی نیست، در مقابل سوال بعدی شما باید Subnet Mask را وارد کنید که اعداد استاندارد این بخش را برای شما بیان کردن است، برای مثال عدد 24 معادل 255.255.255.0 است. در شبکه wan شما باید آدرس gateway را هم وارد کنید که در شبکه Lan شما به آن نیاز ندارید. در صورت تمایل هم می توانید آدرس ورژن 6 را هم در این بخش وارد کنید.

اگر کارت شبکه شما wan باشد در این بخش این امکان وجود دارد که DHCP را هم انتخاب کنید و در غیر این صورت گزینه n را وارد کنید تا وارد بخش بعدی به صورت شکل زیر شوید:

```

255.0.0.0      = 8

Enter the new LAN IPv4 subnet bit count (1 to 31):
> 24

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Enter the new LAN IPv6 address. Press <ENTER> for none:
>

Do you want to enable the DHCP server on LAN? (y/n) n

Please wait while the changes are saved to LAN...
Reloading filter...
Reloading routing configuration...
DHCPD...

The IPv4 LAN address has been set to 192.168.10.1/24
You can now access the webConfigurator by opening the following URL in your web
browser:

      http://192.168.10.1/

Press <ENTER> to continue.

```

در ادامه بارگذاری مجدد تنظیمات فایروال و مسیریابی و غیره تنظیمات شبکه شما نمایش داده شده و روش دسترسی به pfSense را هم با آدرس ip جدید برای شما نمایش می دهد. کلید enter را فشار دهید تا به منوی اصلی کنسول بازگردید و این بار آدرس ip جدید برای شما در بالای صفحه نمایش داده می شود.

عدد 3 یا منوی Reset Web Configurator password:

در این بخش شما می توانید رمز عبور رابط وب را به رمز پیش فرض تغییر دهید. بعد از وارد شدن به این بخش در پیغامی ذکر می شود که رمز پیش فرض برای کاربر Admin که کاربر اصلی برای پیکربندی از طریق وب است pfSense است ، حال اگر شما قصد که رمز کاربر Admin را به رمز پیش فرض تغییر دهید تغییر به سوال پرسیده شده y را پاسخ دهید تا رمز برای شما به صورت خودکار به pfSense تغییر پیدا کند، این مراحل را شما در شکل زیر مشاهده می کنید:

```
Enter an option: 3

The webConfigurator admin password and privileges will be reset to the default (
which is "pfsense").
Do you want to proceed [y!n]? y

The password for the webConfigurator has been reset and
the default username has been set to "admin".

Remember to set the password to something else than
the default as soon as you have logged into the webConfigurator.
Press ENTER to continue.
```

بعد از زدن enter مجدد شما به صفحه اصلی کنسول برخواهید گشت و رمز به مقدار پیش فرض تغییر پیدا کرده است.

عدد 4 یا منوی Reset factor Default :

در این بخش شما می توانید در صورتی نیاز داشته باشید تنظیمات فایروال خود را به حالت اولیه و پیش فرض تغییر دهید، این منو باعث می شود که همه تنظیماتی که شما انجام داده اید پاک شده و به حالت اولیه باز گردد در استفاده از این بخش دقت فرمایید.

عدد 5 یا منوی Reboot System :

برای راه اندازی کردن مجدد سیستم خود شما می توانید از این بخش استفاده کنید، بعد از انتخاب کردن این منو برای شما پیغام زیر نمایش داده می شود:

```
Enter an option: 5

pfSense will reboot. This may take a few minutes, depending on your hardware.
Do you want to proceed [y!n]?
```

بعد از پاسخ y دادن به سوال سیستم شما راه اندازی مجدد خواهد شد.

عدد 6 یا منوی halt system:

در برخی از موارد شما نیاز به خاموش کردن سیستم خود را دارید، برای این کار شما از طریق منوی شماره 6 می توانید این کار را انجام دهید و از انتخاب کردن این بخش و پاسخ ۷ به سوال سیستم شما به صورت خودکار خاموش خواهد شد.

عدد 7 منوی Ping host:

یکی از ابزارهای تست کردن شبکه فرمان ping است که در این منو شما ب راحتی می توانید از آن برای چک کردن روشن بودن و در دسترس بودن هر آدرس ip استفاده کنید به صورت نمایش داده شده در شکل زیر شما می توانید این کار را انجام دهید:

```

Enter an option: 7

Enter a host name or IP address: yahoo.com

PING yahoo.com (98.137.246.7): 56 data bytes
64 bytes from 98.137.246.7: icmp_seq=0 ttl=128 time=345.082 ms
64 bytes from 98.137.246.7: icmp_seq=1 ttl=128 time=328.631 ms
64 bytes from 98.137.246.7: icmp_seq=2 ttl=128 time=404.844 ms

--- yahoo.com ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 328.631/359.519/404.844/32.746 ms

Press ENTER to continue.
    
```

شما در این بخش هم می توانید از آدرس ip استفاده کنید هم از نام سایتها در شکل بالا سایت yahoo.com را ping کرده و تعداد 4 بسته برای آن ارسال شده و جواب درخواست ping برای شما نمایش داده شده است و بعد از enter کردن شما دوباره به منوی اصلی باز می گردید.

عدد 8 یا منوی Shell:

این بخش منوی پرکاربردی است و شما از طریق آن می توانید با استفاده از خط فرمان کارهای مدیریتی و سایر اعمال را انجام دهید کاربرد این بخش به صورت مورد در هر زمانی که شما نیاز به استفاده از خط فرمان و فرمانهای داشته باشید بیان می شود.

عدد 9 منوی pftop:

همانطوری که می دانید و از نام pfsense مشخص است این برنامه از فایروال pf استفاده می کند ، اگر هم شما از top در خط فرمان برای نمایش وضعیت پردازشهای سیستم استفاده کرده باشید با خروجی آن آشنا هستید ، در FreeBSD برنامه جداگانه برای مشاهده وضعیت pf در قالب top وجود دارد که شما از این منو می توانید به صورت لحظه ای وضعیت فایروال pf خود را مشاهده کنید که در شکل زیر نمایش داده شده است:

```
pfTop: Up State 1-1/1, View: default, Order: none, Cache: 10000 19:08:56
2
R  D SRC          DEST          STATE  AGE   EXP  PRTS  BYTES
icmp 0 192.168.174.129:22237 192.168.174.2:22237 0:0   4474  9 17294 472K
```

برای خارج شدن از این برنامه از کلید q استفاده کنید تا به منوی کنسول برگردید.

عدد 10 منوی filter log:

برای مشاهده کردن وضعیت log فایروال خود از این زیر منوی استفاده کنید، خروجی این فرمان را شما در شکل زیر مشاهده می کنید که در بخشی جداگانه در مورد log یا همان گزارشات با شما صحبت خواهیم کرد. برای خارج شده از این بخش از کلید های ctrl+c استفاده کنید:

```
Apr 1 19:03:59 pfSense filterlog: 5,16777216,,1000000103,le1,match,block,in,4,0
x0,,128,2649,0,none,17,udp,78,192.168.40.1,192.168.40.255,137,137,58
Apr 1 19:04:00 pfSense filterlog: 5,16777216,,1000000103,le1,match,block,in,4,0
x0,,128,2650,0,none,17,udp,78,192.168.40.1,192.168.40.255,137,137,58
Apr 1 19:04:01 pfSense filterlog: 5,16777216,,1000000103,le1,match,block,in,4,0
x0,,128,2651,0,none,17,udp,78,192.168.40.1,192.168.40.255,137,137,58
Apr 1 19:04:04 pfSense filterlog: 62,16777216,,12000,le0,match,block,in,4,0x0,,
128,14426,0,none,17,udp,78,192.168.174.1,192.168.174.255,137,137,58
Apr 1 19:04:05 pfSense filterlog: 62,16777216,,12000,le0,match,block,in,4,0x0,,
128,14427,0,none,17,udp,78,192.168.174.1,192.168.174.255,137,137,58
Apr 1 19:04:06 pfSense filterlog: 62,16777216,,12000,le0,match,block,in,4,0x0,,
128,14429,0,none,17,udp,78,192.168.174.1,192.168.174.255,137,137,58
Apr 1 19:11:28 pfSense filterlog: 5,16777216,,1000000103,le1,match,block,in,4,0
x0,,128,2653,0,none,17,udp,78,192.168.40.1,192.168.40.255,137,137,58
Apr 1 19:11:29 pfSense filterlog: 5,16777216,,1000000103,le1,match,block,in,4,0
x0,,128,2654,0,none,17,udp,78,192.168.40.1,192.168.40.255,137,137,58
Apr 1 19:11:30 pfSense filterlog: 5,16777216,,1000000103,le1,match,block,in,4,0
x0,,128,2655,0,none,17,udp,78,192.168.40.1,192.168.40.255,137,137,58
Apr 1 19:11:33 pfSense filterlog: 62,16777216,,12000,le0,match,block,in,4,0x0,,
128,14473,0,none,17,udp,78,192.168.174.1,192.168.174.255,137,137,58
Apr 1 19:11:34 pfSense filterlog: 62,16777216,,12000,le0,match,block,in,4,0x0,,
128,14474,0,none,17,udp,78,192.168.174.1,192.168.174.255,137,137,58
Apr 1 19:11:34 pfSense filterlog: 62,16777216,,12000,le0,match,block,in,4,0x0,,
128,14476,0,none,17,udp,78,192.168.174.1,192.168.174.255,137,137,58
```

عدد 11 منوی Restart WebConfigurator:

در برخی از موارد شما نیاز دارید که رابط وب را دوباره راه انداز کنید با استفاده از این کنسول می توانید این کار را انجام دهید.

عدد 12 منوی php-shell pfsense-tools:

این بخش یک منوی توسعه دهنده برای برنامه pfsense است که شما با استفاده از این بخش هم می توانید Development را با استفاده از این منو انجام دهد و تغییراتی در ساختار pfsense ایجاد کنید در شکل زیر منوی ورودی و فرمان های اجرای در این بخش را مشاهده می کنید:


```
2) Set interface(s) IP address      11) Restart webConfigurator
3) Reset webConfigurator password   12) PHP shell + pfSense tools
4) Reset to factory defaults        13) Update from console
5) Reboot system                    14) Enable Secure Shell (sshd)
6) Halt system                      15) Restore recent configuration
7) Ping host                        16) Restart PHP-FPM
8) Shell

Enter an option: 12

Starting the pfSense developer shell...

Welcome to the pfSense developer shell

Type "help" to show common usage scenarios.

Available playback commands:
  changepassword disablecarp disablecarpmaint disabledhcpd disablereferercheck
  enableallowallwan enablecarp enablecarpmaint enablesshd externalconfiglocator
  gatewaystatus generateguicert gitsync installpkg listpkg panchordrill pftabledr
  ill removepkgconfig removeshaper resetwebgui restartdhcpd restartipsec svc uninst
  allpkg

pfSense shell: █
```

بعد از اجرا کردن Help شما روش استفاده از این بخش را مشاهده می کنید. علاوه بر تغییراتی که شما می توانید در php فایروال اعمال کنید از فرمان playback هم می توانید برای اعمال تغییراتی که در شکل بالا مشاهده می کنید استفاده کنید، برای مثال برای فعال کردن سرویس ssh باید از فرمان playback به صورت زیر استفاده کنید:

```

Enter an option: 12
Starting the pfSense developer shell...
Welcome to the pfSense developer shell
Type "help" to show common usage scenarios.

Available playback commands:
  changepassword disablecarp disablecarpmaint disabledhcpd disablereferercheck
  enableallowallwan enablecarp enablecarpmaint enablesshd externalconfiglocator
  gatewaystatus generateguicert gitsync installpkg listpkg panchordrill pftabledr
  ill removepkgconfig removeshaper resetwebgui restartdhcpd restartipsec svc unins
  tallpkg

pfSense shell: playback
Could not locate playback file.
pfSense shell: playback enablesshd

Playback of file enablesshd started.

Starting enablesshd.....
Enabling SSHD, please wait...

pfSense shell:

```

به صورت پیش فرض شما از طریق آدرس ip کارت شبکه Wan به رابط وب در pfSense دسترسی ندارید در این بخش شما با استفاده از فرمان playback می توانید به صورت زیر این کار را انجام دهید:

```

Enter an option: 12
Starting the pfSense developer shell...
Welcome to the pfSense developer shell
Type "help" to show common usage scenarios.

Available playback commands:
  changepassword disablecarp disablecarpmaint disabledhcpd disablereferercheck
  enableallowallwan enablecarp enablecarpmaint enablesshd externalconfiglocator
  gatewaystatus generateguicert gitsync installpkg listpkg panchordrill pftabledr
  ill removepkgconfig removeshaper resetwebgui restartdhcpd restartipsec svc unins
  tallpkg

pfSense shell: playback enableallowallwan

Playback of file enableallowallwan started.

Adding allow all rule...
Turning off block private networks (if on)...
Turning off block bogon networks (if on)...
Reloading the filter configuration...

pfSense shell:

```

بعد از اجرا شدن این فرمان به صورت کامل شما می توانید از طریق آدرس ip کارت شبکه Wan هم به رابط وب pfSense متصل شوید، برای خارج شدن از این بخش شما کافیست که فرمان exit را اجرا کنید تا دوباره به منوی کنسول بازگردید.

عدد 13 منوی Update From console

برای بروز رسانی کردن برنامه های نصب شده بر روی pfSense شما می توانید از این بخش استفاده کنید که بعد از وارد شدن به این بخش به صورت خودکار سیستم بسته ها بروز رسانی می شود این بخش را در شکل زیر مشاهده می کنید:

```
Enter an option: 13
>>> Updating repositories metadata...
Updating pfSense-core repository catalogue...
pfSense-core repository is up to date.
Updating pfSense repository catalogue...
pfSense repository is up to date.
All repositories are up to date.
>>> Unlocking package pfSense-kernel-pfSense... done.
```

بعد از بروز رسانی در این بخش شما با لیستی از بسته های که باید بروز شود را مشاهده می کنید،

```

php56-gettext: 5.6.31 -> 5.6.32 [pfSense]
php56-filter: 5.6.31 -> 5.6.32 [pfSense]
php56-dom: 5.6.31 -> 5.6.32 [pfSense]
php56-curl: 5.6.31 -> 5.6.32 [pfSense]
php56-ctype: 5.6.31 -> 5.6.32 [pfSense]
php56-bz2: 5.6.31 -> 5.6.32 [pfSense]
php56-bcmath: 5.6.31 -> 5.6.32 [pfSense]
php56: 5.6.31 -> 5.6.32 [pfSense]
pfSense-rc: 2.3.5 -> 2.3.5_1 [pfSense-core]
pfSense-kernel-pfSense: 2.3.5 -> 2.3.5_1 [pfSense-core]
pfSense-default-config: 2.3.5 -> 2.3.5_1 [pfSense-core]
pfSense-base: 2.3.5 -> 2.3.5_1 [pfSense-core]
pfSense-Status_Monitoring: 1.6.2 -> 1.6.5 [pfSense]
pfSense: 2.3.5 -> 2.3.5_1 [pfSense]
ntp: 4.2.8p10_2 -> 4.2.8p11 [pfSense]
libxml2: 2.9.4 -> 2.9.7 [pfSense]
curl: 7.56.1 -> 7.57.0 [pfSense]

Number of packages to be upgraded: 42

44 MiB to be downloaded.

*** WARNING ***
Reboot will be required!!
Proceed with upgrade? (y/N)

```

در انتها میزان حجم بسته های دانلود شده را به شما نمایش می دهد، در زمان انجام بروز رسانی سیستم خود را خاموش و یا reboot نکنید. در صورتی که شما به این بخش پاسخ y دهید بروز رسانی شروع خواهد شد.

عدد 14 منوی disable sshd:

یکی از راه های ارتباطی با pfSense استفاده از ssh است ، این سرویس را به صورت کامل در بخش راه اندازی سرویس ها توضیح داده می شود، با استفاده از منو در کنسول می توانید آنرا غیرفعال کنید.

عدد 15 منوی Restore resent configuration:

در برخی از موارد شما تغییراتی اعمال میکنید که باعث ایجاد خرابی می شود در این زیر منو می توانید آخرین تغییر را بازنگرید کنید. این زیر منو را در لیست زیر مشاهده می کنید:

```
Enter an option: 15
```

```
Restore Backup from Configuration History
```

```
1) List Backups
2) Restore Backup
Q) Quit
```

```
Please select an option to continue: █
```

در منوی شماره 1 شما می توانید لیستی از backups را مشاهده کنید که در حقیقت آخرین وضعیت رولهای و سایر تغییراتی است که شما در فایروال خود ایجاد را نمایش می دهد که در شکل زیر آنرا مشاهده می کنید:

```
05. 4/4/18 06:33:20      v15.8  (system)
    pfSsh.php added allow all wan rule

04. 4/4/18 06:35:46      v15.8  (system)
    pfSsh.php added allow all wan rule

03. 4/4/18 06:57:11      v15.8  admin@192.168.174.1
    /services_captiveportal.php made unknown change

02. 4/4/18 07:00:59      v15.8  admin@192.168.1.10
    /services_captiveportal.php made unknown change

01. 4/4/18 07:02:15      v15.8  admin@192.168.1.10
    /services_captiveportal.php made unknown change
```

```
Restore Backup from Configuration History
```

```
1) List Backups
2) Restore Backup
Q) Quit
```

```
Please select an option to continue: █
```

برای بازگردانی از منوی 2 استفاده کنید که بعد از وارد شدن به این بخش شما باید عددی را که نیاز دارید به آن تنظیمات برگشت داده شود را وارد کنید، این زیر منو را در شکل زیر مشاهده می کنید:

```
Enter an option: 15

Restore Backup from Configuration History

1) List Backups
2) Restore Backup
Q) Quit

Please select an option to continue: 2
Which configuration would you like to restore?
1-30 : █
```

برای خارج شدن از این بخش شما باید از گزینه Q استفاده کنید.

عدد 16 منوی Restart PHP-FPM:

فایروال pfSense برای رابط وب خود از زبان برنامه نویسی php و ساختار php-fpm استفاده می کند، در برخی موارد سرویس php-fpm دارای کندی می شود و برای راه اندازی مجدد آن می توانید از این زیر منو استفاده کنید.

خلاصه بخش:

قبل از وارد شدن به رابط وب و دسترسی از این طریق برنامه pfSense برای شما منوی را در نظر گرفته اند که شما می توانید از طریق آن بسیار از کارهای ساده و حیاتی و یا حتی تجات دهنده را انجام دهید. در این فصل شم با 16 زیر منوی اصلی کنسول آشنا می شوید.

فصل سوم روش اتصال به رابط وب

روش اتصال به رابط وب

یکی از مزیت های فایروال pfSense بخش راب وبی است که برای این فایروال در نظر گرفته شده است و کارکرد آنرا ساده کرده و در عین حال شما می توانید با استفاده از آن همه کارهای مورد نظر خود را انجام داده و هر برنامه کاربردی قابل نصب در pfSense هم برای خودش یک بخش در رابط وب بعد از نصب ایجاد می کند و مدیریت کردن این فایروال قدرتمند را برای شما ساده می کند.

برای اتصال به این رابط وبی شما می توانید از هر مرورگر وب استفاده کنید و برای اتصال به آن باید به این نکته توجه کنید که این بخش در تنظیمات اولیه فقط از طریق شبکه Lan و آدرس ip 192.168.1.1 که آدرس پیش فرض و قابل تغییر است در دسترس است شما به سیستم برای این کار نیاز دارید که در این شبکه حضور داشته باشد.

در زمان نصب فایروال pfSense برای شما کاربر Admin را با رمز pfSense ایجاد می کند و شما در مرحله اول وارد شدن به وب از آن باید استفاده کنید، این رمز قابل بازگردانی است که در بخش کار با منوی کنسول روش بازگردانی آنرا بیان کرده ام.

شما به دو روش کلی می توانید به رابط وب وصل شوید، روش اول داشتن یک سیستم در شبکه lan با رنج آدرس ip خاص 192.168.1.0 که سیستم شما باید مرورگر وب داشته باشد.

روش دوم هم غیرفعال کردن عدم دسترسی به وب از طریق آدرس ip کارت شبکه wan که این کار به صورت پیش فرض و عمومی پیشنهاد نمی شود و فقط در شرایط خاص این کار را انجام دهید. با این روش در ادامه آشنا می شوید.

روش اتصال از طریق شبکه Wan به pfSense :

برای این کار شما نیاز به دسترسی سخت افزاری به فایروال خود دارید و باید به منوی کنسول دسترسی داشته باشید. از این منو باید گزینه 12 را انتخاب کنید تا وارد منوی pfSenseShell شوید این بخش را در شکل زیر مشاهده می کنید:


```
Enter an option: 12
Starting the pfSense developer shell...
Welcome to the pfSense developer shell
Type "help" to show common usage scenarios.

Available playback commands:
  changepassword disablecarp disablecarpmaint disabledhcpd disablereferercheck
  enableallowallwan enablecarp enablecarpmaint enablesshd externalconfiglocator
  gatewaystatus generateguicert gitsync installpkg listpkg pfanchordrill pftabledrill
  removepkgconfig removeshaper resetwebgui restartdhcpd restartipsec svc uninstal
  lallpkg
pfSense shell: █
```

در بخش فرمان زیر را وارد کنید:

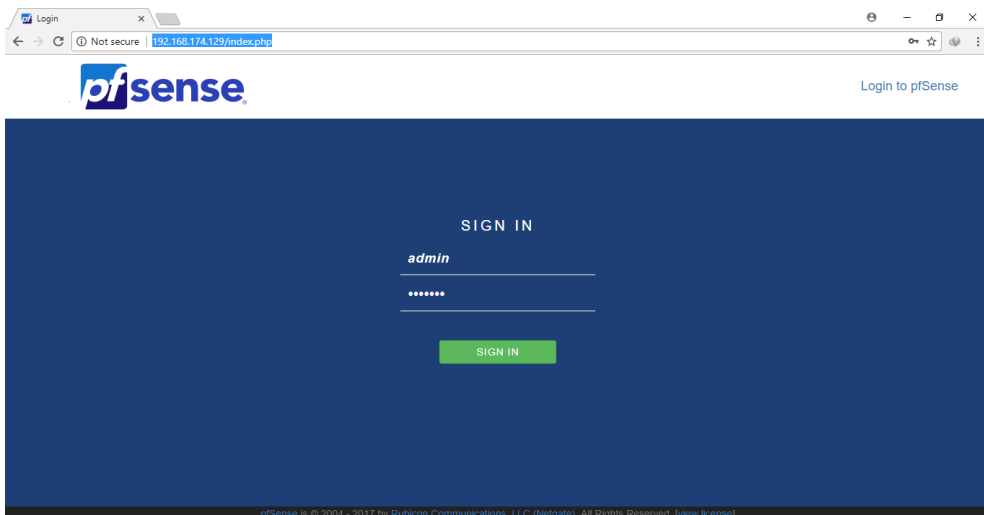
```
pfSense shell: playback enableallowallwan
```

بعد از اجر این فرمان خروجی به صورت شکل زیر را مشاهده می کنید:

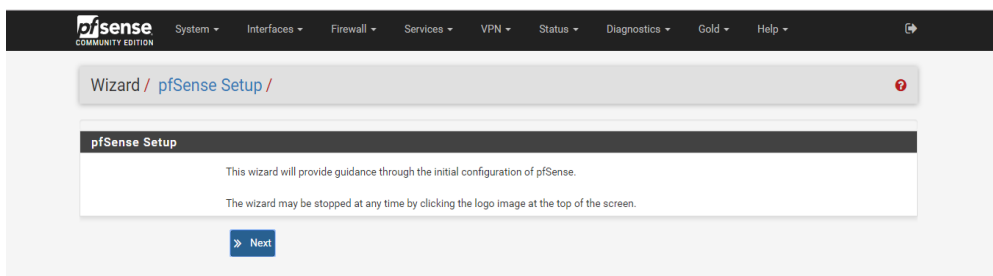
```
installpkg
pfSense shell: playback enableallowallwan
Playback of file enableallowallwan started.

Adding allow all rule...
Turning off block private networks (if on)...
Turning off block bogon networks (if on)...
Reloading the filter configuration...
pfSense shell: █
```

همانطوری که مشاهده می کنید در خروجی این فرمان دو مورد اصلی که باعث عدم دسترسی از طریق شبکه های محلی می شود را غیرفعال کردن است ، حال شما از طریق آدرس کارت شبکه WAN به Pfsense متصل شوید تا صفحه ای به صورت زیر برای شما باز شود که صفحه اصلی وارد شدن به سیستم است:

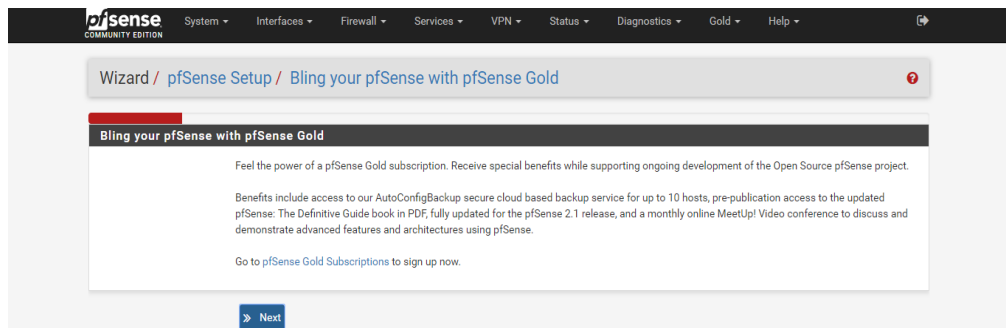


برای وارد شدن باید در بخش نام کاربری **Admin** و در بخش رمزعبور رمزپیش فرض که **pfSense** است را وارد کنید. اگر رمز را تغییر داده اید برای تغییر دادن به حالت پیش فرض به منوی کنسول مراجعه کنید، بعد از ورود به سیستم شما با پیغام زیر که یک **wizard** اولیه است مواجه می شوید که در شکل زیر انرا مشاهده می کنید:

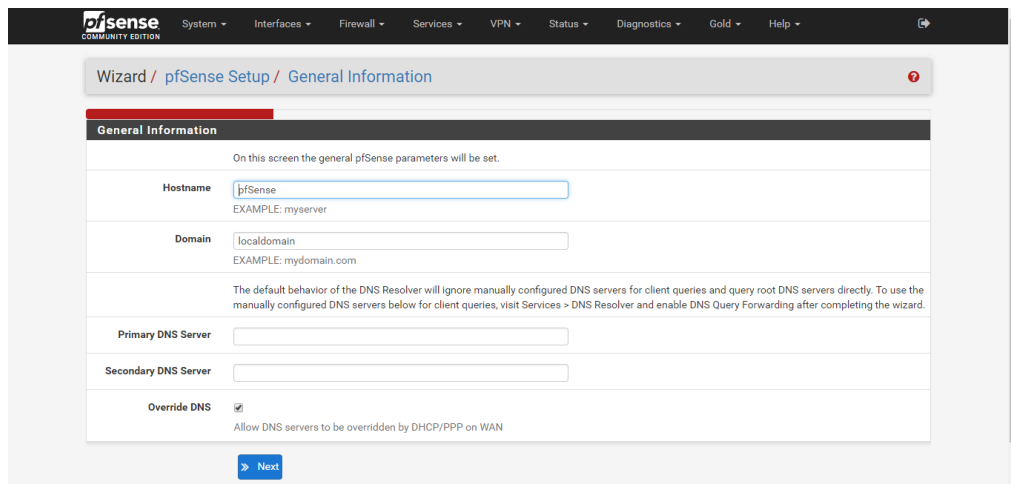


شما با استفاده از این **Wizard** می توانید یک سری تنظیمات اولیه را انجام دهید که در بخشهای بعدی هم به تناسب هر بخش می توانید این تنظیمات را انجام دهید، برای خارج شدن از این بخش هم می توانید بر روی آیکن **pfSense** کلیک کنید.

منوی wizard در راه اندازی اولیه رابط وب:

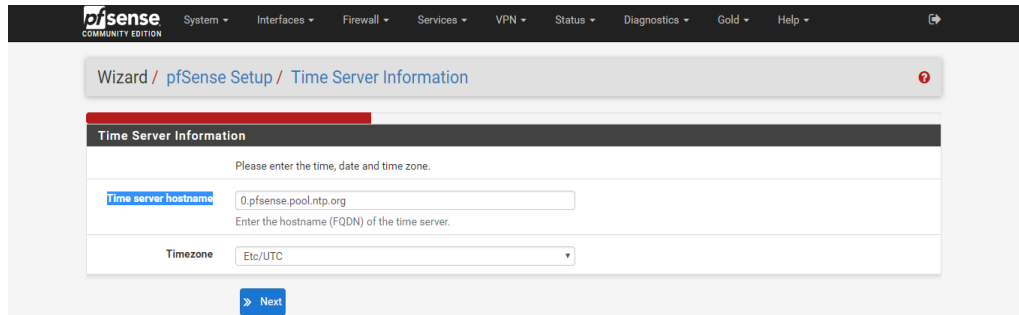


در قدم اول خاصیت‌های استفاده از pfSense Gold را که سیستم حق اشتراکی در استفاده از pfSense است را برای شما معرفی می‌کند. بعد از next کردن این بخش شما می‌توانید تنظیمات hostname و سرورهای DNS را انجام دهید که این بخش در شکل زیر نمایش داده شده است:



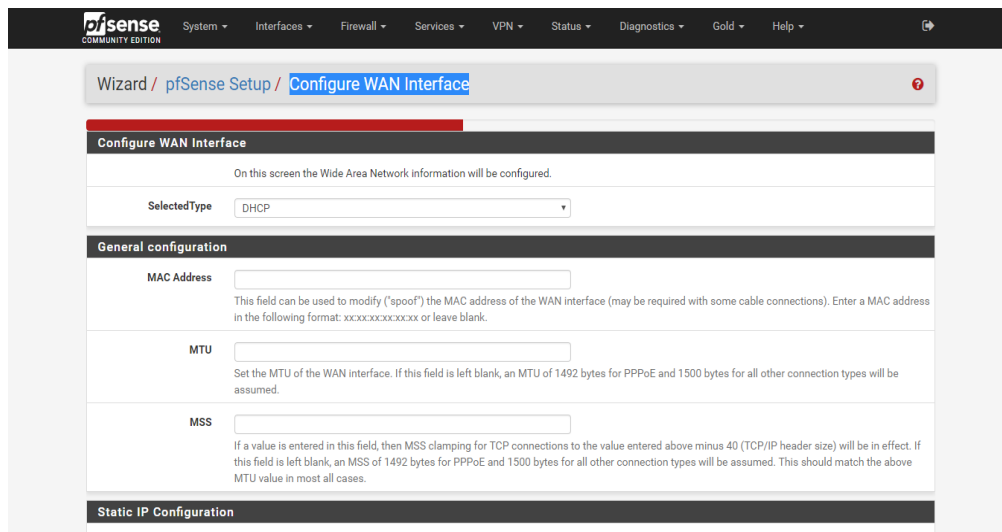
اگر قصد دارید که سرورهای DNS شما از طریق DHCP که در شبکه Wan شما وجود دارد تنظیم شود گزینه Override DNS را انتخاب کنید. در بخش بعدی تنظیمات Time Server که در شکل زیر مشاهده می‌کند منطقه جغرافیای خود را انتخاب کنید و در بخش Time server hostname هیچ تغییری اعمال نکنید که در بخش راه

اندازی NTP به صورت کامل در مورد راه اندازی سرور زمان و سرورهای زمان موجود در اینترنت صحبت خواهیم کرد. این بخش را شما در شکل زیر مشاهده می کنید:



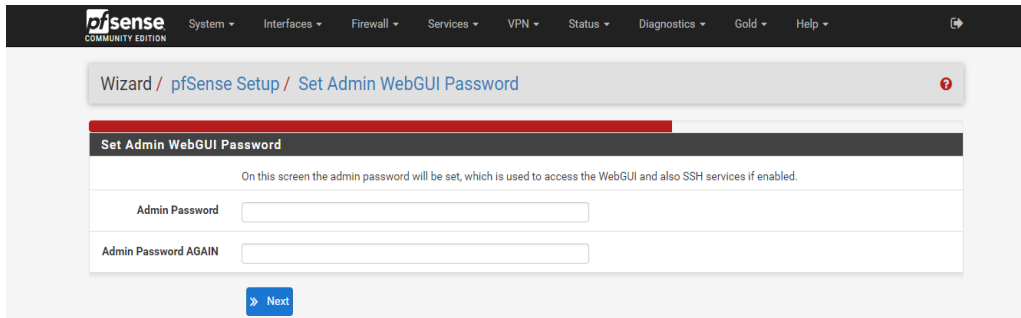
The screenshot shows the 'Time Server Information' configuration page in the pfSense wizard. The page title is 'Wizard / pfSense Setup / Time Server Information'. Below the title, there is a section 'Time Server Information' with the instruction 'Please enter the time, date and time zone.' There are two input fields: 'Time server hostname' with the value '0.pfsense.pool.ntp.org' and 'Timezone' with the value 'Etc/UTC'. A 'Next' button is located at the bottom of the form.

در بخش بعدی شما کارت شبکه wan را که به pfSense متصل کرده اید را پیکربندی کنید **Configure WAN Interface** این بخش در قسمت تنظیمات کارت شبکه به صورت کامل مورد بررسی قرار خواهد گرفت ، به این دلیل که اکثر شبکه های wan از آدرسهای ip پویا استفاده می کنند از سرور DHCP که وظیفه اختصاص آدرس IP را دارد استفاده می کنند، به همین دلیل به صورت پیش فرض در بخش IP گزینه DHCP فعال است. این قسمت را شما در شکل زیر مشاهده می کنید:

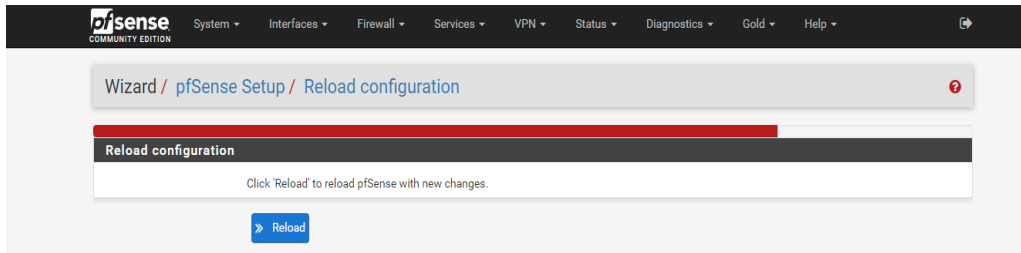


The screenshot shows the 'Configure WAN Interface' configuration page in the pfSense wizard. The page title is 'Wizard / pfSense Setup / Configure WAN Interface'. Below the title, there is a section 'Configure WAN Interface' with the instruction 'On this screen the Wide Area Network information will be configured.' There is a 'SelectedType' dropdown menu with 'DHCP' selected. Below this is a section 'General configuration' with three input fields: 'MAC Address', 'MTU', and 'MSS'. Each field has a descriptive text below it. At the bottom, there is a section 'Static IP Configuration' which is currently empty.

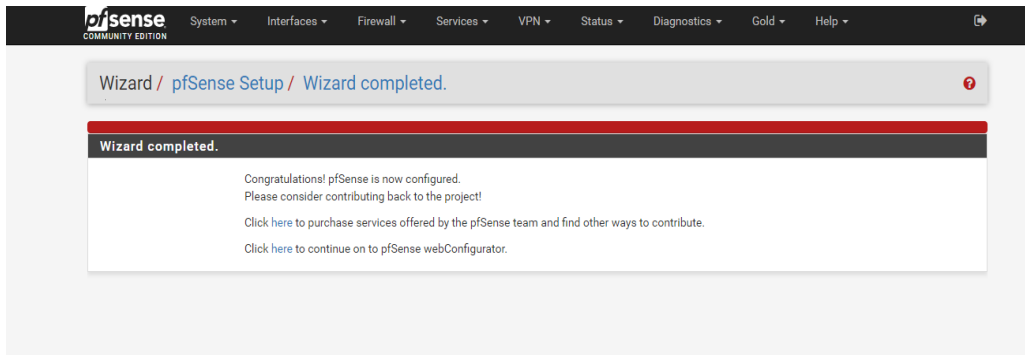
قسمت بعدی Admin WebGUI Password است که شما از طریق این منوی می توانید رمزعبور کاربر admin را تغییر دهید این رمز را باید دوبار پیشتر سر هم وارد کنید و توجه داشته باشید که برای مدیریت کردن از طریق همین رابط وب و ssh از آن استفاده کنید، این بخش را در شکل زیر مشاهده می کنید:



حال اگر در بخش های این Wizard شما تغییراتی اعمال کرده باشید نیاز به راه اندازی مجدد سیستم وجود دارد که شما می توانید از این بخش Reload configuration را انجام دهید که در شکل زیر این بخش را مشاهده می کنید:



بعد از انتخاب کردن Reload شما وارد صفحه بعدی می شوید که در حقیقت بخش (Wizard completed) پایانی است. این بخش را در شکل زیر مشاهده می کنید و برای وارد شده به محیط پیکربندی وب بروی [Click here to continue on to pfSense webConfigurator](#) کلیک کنید تا به صفحه اصلی پیکربندی وب وارد شوید.



آشنایی با بخش Dashboard:

بعد از وارد شدن به سیستم شما با بخشی به نام Dashboard آشنا می شوید که در شکل زیر آنرا مشاهده می کنید که منوی پیش فرضی است که هر زمانی که به سیستم وارد می شوید برای شما باز می شود از آن بخش از زیر منوی موجود در بخش status در دسترس است:

The screenshot shows the pfSense dashboard with the following sections:

- System Information:**
 - Name: pfSense.localdomain
 - System: pfSense, Netgate Device ID: 66973cbe59c6f3fea0b5
 - BIOS: Vendor: Phoenix Technologies LTD, Version: 6.00, Release Date: 05/19/2017
 - Version: 2.3.5-RELEASE-p1 (i386), built on Wed Dec 13 07:43:29 CST 2017, FreeBSD 10.3-RELEASE-p26. Note: The system is on the latest version.
 - Platform: pfSense
 - CPU Type: Intel(R) Celeron(R) CPU N3060 @ 1.60GHz
 - Uptime: 00 Hour 37 Minutes 46 Seconds
 - Current date/time: Thu Apr 5 11:21:15 IRDT 2018
 - DNS server(s): 127.0.0.1, 192.168.174.2
 - Last config change: Thu Apr 5 11:06:50 IRDT 2018
- Netgate Services And Support:** Retrieving support information.
- Interfaces:** WAN (autoselect) with IP 192.168.174.129.
- Resource Usage:**
 - State table size: 0% (5/47000)
 - MBUF Usage: 3% (270/10036)
 - Load average: 0.30, 0.33, 0.29
 - CPU usage: 11%
 - Memory usage: 17% of 479 MIB
 - SWAP usage: 0% of 1023 MIB
 - Disk usage (/): 4% of 18GiB - ufs
 - Disk usage (/var/run): 3% of 3.4MiB - ufs in RAM

این بخش قابل تغییر است و شما می توانید به تناسب نیاز خود بخشهای نمایش داده شده را تغییر دهید و هر قسمتی که برای شما مفید است را قرار دهید. برای مثال شما برنامه ای ایجاد میکنید که برای نمایش وضعیتش می توانید در صفحه Dashboard بخش نمایش وضعیتش را وارد کنید تا در زمان وارد شدن به رابط وب آنرا به سرعت مشاهده کنید. بخش بزرگ در این قسمت بخش system Informations است که اطلاعات جالبی را برای شما نمایش میدهد. این بخش را در شکل زیر مشاهده می کنید:

| System Information | |
|-------------------------|---|
| Name | pfSense.localdomain |
| System | pfSense Netgate Device ID: 66973cbe59c6f3fea0b5 |
| BIOS | Vendor: Phoenix Technologies LTD Version: 6.00 Release Date: 05/19/2017 |
| Version | 2.3.5-RELEASE-p1 (i386) built on Wed Dec 13 07:43:29 CST 2017 FreeBSD 10.3-RELEASE-p26 The system is on the latest version. Version information updated at 2018-04-05 10:45 |
| Platform | pfSense |
| CPU Type | Intel(R) Celeron(R) CPU N3060 @ 1.60GHz |
| Uptime | 00 Hour 42 Minutes 50 Seconds |
| Current date/time | Thu Apr 5 11:26:19 IRDT 2018 |
| DNS server(s) | <ul style="list-style-type: none"> 127.0.0.1 192.168.174.2 |
| Last config change | Thu Apr 5 11:06:50 IRDT 2018 |
| State table size | 0% (3/47000) Show states |
| MBUF Usage | 3% (270/10036) |
| Load average | 0.41, 0.41, 0.33 |
| CPU usage | 22% |
| Memory usage | 16% of 479 MiB |
| SWAP usage | 0% of 1023 MiB |
| Disk usage (/) | 4% of 18GiB - ufs |
| Disk usage (/var/run) | 3% of 3.4MiB - ufs in RAM |

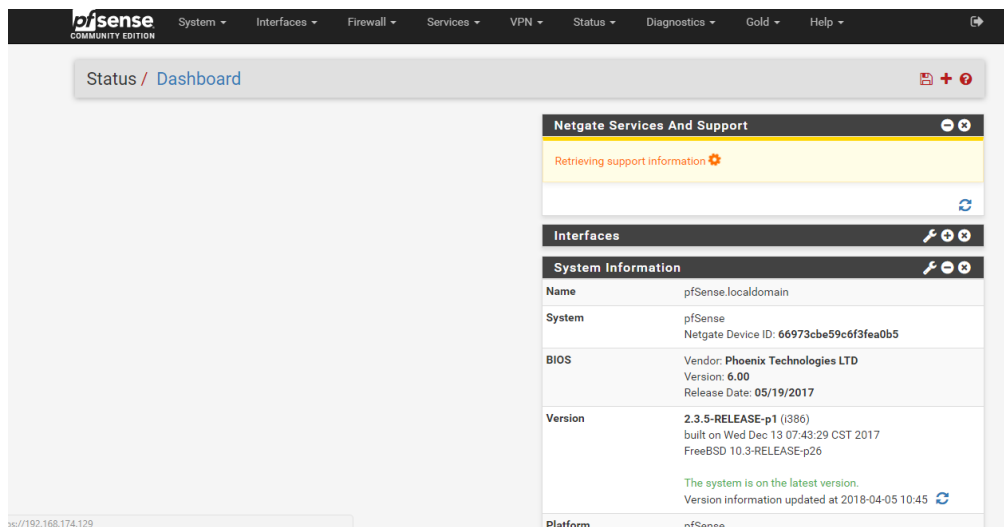
در قسمت اول `hostname` فایروال شما را نمایش می دهد، این بخش را در زمان استفاده از `wizard` می توانید تغییر دهید (روشهای دیگری هم برای تغییر این بخش وجود دارد) در بخش بعدی `ID` که برای ثبت در سایت `netgate` به آن نیاز دارید را برای شما نمایش میدهد. بخش های دیگر هم نوع `CPU`، مدت زمان راه اندازی شدن سیستم، منطقه جغرافیای، ورژن و غیر را نمایش میدهد که در این میان یک بخش مهمی به نام `Last config change` وجود دارد که آخرین زمان تغییر در پیکربندی را برای شما نمایش می دهد و به شما کمک می کند که تغییرات را پیگیری کنید.

در زیر بخشهای این قسمت شما به صورت پویا و در لحظه می توانید بار وارد شده به CPU و RAM سیستم را مشاهده کنید و میزان فضای مصرف شده از هارد را هم برای شما نمایش میدهد که این بخش به تناسب تغییراتی که در سیستم اعمال می شود تغییر می کند.

در بالای هر منوی شکلی به صورت زیر وجود دارد :



شما با استفاده از این آیکن ها می توانید بخش نمایش داده شده را کلا از dashboard حذف کنید و یا آنرا minimize کرده و یا تغییراتی در آن اعمال کنید. شما با دکمه darck کردن می توانید محل منوی های نمایش داده شده در این بخش را تغییر دهید برای مثال در شکل زیر بخش کارتهای شبکه minimize شده و بخش system information در زیر بخش شبکه قرار داده شده است:



برای اضافه کردن بخش های جدید و ثبت کردن تغییرات شما می توانید از آیکونهای موجود در بالا سمت چپ این بخش که به صورت شکل زیر هستند استفاده کنید:

Status / Dashboard



بعد از کلیک کردن بروری + شما منوی به صورت شکل زیر مشاهده می کنید:

Available Widgets -

| | | | |
|--|--|--|---|
| <ul style="list-style-type: none"> + Captive Portal Status + Gateways + IPsec + Picture + Thermal Sensors | <ul style="list-style-type: none"> + CARP Status + GEOM Mirror Status + Load Balancer Status + Rss + Traffic Graphs | <ul style="list-style-type: none"> + Dynamic DNS Status + Installed Packages + NTP Status + S.M.A.R.T. Status + Wake-on-Lan | <ul style="list-style-type: none"> + Firewall Logs + Interface Statistics + OpenVPN + Services Status |
|--|--|--|---|

شما از این بخش می توانید بخشهای قابل نمایش در قسمت داشبورد را مشاهده کنید و در صورت نیاز می توانید از علامت + آنها برای اضافه کردن آنها استفاده کنید، برای مثال در این بخش قسمت CARP به منوی داشبورد اضافه شده است به صورت شکل زیر:

CARP Status - x

| CARP Interface | IP Address | Status |
|---|------------|--------|
| No CARP Interfaces Defined. Click here to configure CARP. | | |

که شما به راحتی می توانید آنرا در هم مکانی که نیاز دارید قرار دهید و بعد حالت مورد نظر خود را Save کنید با استفاده از آیکون های بالای صفحه.

فصل چهارم شبکه در FreeBSD

هشدار!!

قبل از شروع به کار با فایروال pfSense شما نیاز دارید که با خط فرمان و مختصری سیستم عامل FreeBSD آشنا باشید. همه چیز رابط وب نیست.

فصلی که در پیش رو داریم دو بخش کاملا جدا از هم رو داره که در حقیقت همه مطالب به دنبال یک هدفه اون هم فرمان ها و بخشهایی که به شما وضعیت pfSense رو نمایش میده ولی در دنیای کاملا متفاوت، در بخش اول که یک مقداری سخت تر هست بخش فرمان های مورد نیاز است که برای اون دسته از دوستانی که از دنیای کلیک کردن استفاده می کنند و در این بخش فعالیت دارن یک مقداری سخت تر خواهد بود و پیشنهاد می کنم بیشتر این بخش رو بخونن و برای اون دسته از دوستان که با سیستم عامل های متن باز و خط فرمان کار کردند این بخش مطلب جدید نداره غیر از چند فرمان مهمی که در pfSense اجرا میشه. در بخش بعدی از این فصل هم شما با بخش شبکه در FreeBSD آشنا می شوید، در بخش پایانی هم با دو منوی پرکاربرد در رابط وب که از ان برای نمایش وضعیت استفاده می شود آشنا می شوید.

خط فرمان چیست؟

شاید در بسیاری از مقالات و سایتها در مورد خط فرمان تعاریف شنیده باشید من قصد دارم در این بخش برای یک تعریف ساده ازش داشته باشم، اول شکل زیر رو مشاهده کنید:

```

File Edit Tab Help
$ dsdinfo
00001 01110100000011111 001000 OS: FreeBSD amd64
00011011001111000000110001001011001 Hostname: foo
0011001111011011010011111001110100 Kernel: 11.1-RELEASE-p4
0 0000010110011010111001100110011111 Uptime: 2:35
10010010011001101100110010000111000 Process: ssh
10101000010000100000111000001 00111 RAM: 1059M / 3959M
001101001000110001010011000010001101 CPU: Intel(R) Celeron(R) CPU G1610 @ 2.60GHz
1101110000101110011001001000111011011001 Shell: sh
115 0001001011110110111101100000000111
1101000111011001001001110000100100111
10 0001111001000110011100101011011001
001110010000011001110000011010010
00100000100010101011111111111
01101110010011000010101110
00011001110110011000
0011100000

$ screenfetch
          bobo@foo
          OS: FreeBSD
          Kernel: amd64 FreeBSD 11.1-RELEASE-p4
          Uptime: 2h 36m
          Packages: 344
          Shell: sh
          Resolution: 1600x900
          WM: Not Found
          CPU: Intel Celeron G1610 @ 2.60GHz
          GPU: Xeon E3-1200 v2/3rd Gen Core processor Graphics Controller
          RAM: 1106630MiB / 419430MiB
  
```

این شکل در حقیقت یک مقداری زیبا تر از اون چیزیه که شما برای بار اولی که خط فرمان رو باز می کنید آشنا می شوید. خط فرمان در حقیقت محلی است که شما می تونید از طریق آن با سیستم عامل خودتون صحبت کنید ، بهش دستور بدین و اون هم بعد از انجام کار خروجی رو به شما نمایش بده که در حقیقت جواب درخواست شما رو بهتون بر میگرددونه، با این خط فرمان شما می تونید به دنیای شبکه و اینترنت حکومت کنید و با زیر ساخت ها بخشهای مهم زیرین شبکه و سیستم عامل آشنا بشید. شاید در برخورد اول محیط بی روح و سیاه و سفیدی باشه ولی وقتی شما کار با این بخش رو یاد بگیرید ارزش لذت خواهید برد، حتی می تونید با استفاده از برنامه lynx صفحات وب رو بدون عکس باز کنی، یا فایل به فایل صوتی هم گوش کنید،(البته این بخش برای مدیران شبکه حرفه ای زیاد مهم نیست)

خط فرمان اولیه که در همه سیستم عامل های متن باز وجود دارند sh است که زیاد هم برای کار کردن جذاب نیست ولی خب همه جا هست، در حال حاضر خط فرمانی از دل sh ایجاد شده به نام bash که امکانات خوبی رو به شما می ده که البته اگر با sh کار کرده باشید به این قابلیت های جدید به عنوان امکانات نگاه می کنید.

هر خط فرمانی که بخش اعلانی داره که از طریق اون می تونید با استفاده از صفحه کلید فرمانهایی رو وارد کنید و خروجی رو مشاهده کنید اگر این بخش با # شروع بشه شما دسترسی کامل به همه بخشهای سیستم عامل دارید و

در حقیقت شما کاربر root هست اگر هم با \$ شروع بشه کاربر شما معمولی و فقط یک سری فرمان ها رو می تونید را اجرا کنید. خب بعد از یک تعریف از کاربر root اولین فرمان رو اجرا می کنیم.

کاربر Root:

در سیستم عامل های متن باز و همچنین FreeBSD یک کاربر همه کاره وجود داره که می تونه هر کاری در سیستم عامل شما انجام بده و مرز همه محدودیتهای اعمال شده رو رد می کنه (به همین دلیل است که گوشی های هوشمند اندروید رو به اصطلاح root میکنند تا بنونن برنامه های خاصی رو که در حالت معمولی بهشون دسترسی نصب نمی ده رو نصب کنن) این کاربر در زمان نصب ایجاد شده و فقط شما می تونید رمزعبور براش تعریف کنید که در تعریف کردن رمزعبور دقت کنید. در FreeBSD راه های مختلفی برای محدود کردن کاربران وجود داره که هیچ کدام از این محدودیتهای بر روی این کاربر اعمال نمی شود.

فرمانهای نمایش وضعیت در خط فرمان pfSense:

بعد از وارد شدن به خط فرمان اولین فرمانی که شما باید برای دریافت کردن نام سیستم عامل ازش استفاده کنید فرمان `uname` است که از سیستم عامل درخواست دارید که نام خودش رو معرفی کنه، هر فرمانی با سوئیچ های مختلفی اجرا می شود که این سوئیچ ها رفتار پیش فرض اون فرمان رو تغییر می دهد، برای دریافت همه اطلاعات سیستم عاملی که بهش وصل هستید از سوئیچ `a` استفاده کنید و این نکته رو در نظر داشته باشید که همه سوئیچ ها با - شروع میشه پس برای اجر این فرمان مثل شکل زیر اقدام کنید:

```
[S'3'2-BEFEVZE][root@pfsense: jcs9jqom9iu]\root: █
er\pfsense-32\fw\op\pni\qel\pfsense-32\fw\l6eB2D-2lc\2h2\pfsense 138e
2333(BEFEVZ'S-3): MOW Dsc TT 88:T2:S8 C2L S0T3 root@ce53-138e-pni\qel:~pni\q
l6eB2D pfsense:jcs9jqom9iu T8'3-BEFEVZE-h5e l6eB2D T8'3-BEFEVZE-h5e #T 88e1e4q
[S'3'2-BEFEVZE][root@pfsense: jcs9jqom9iu]\root: n9aM6 -g
l6eB2D
[S'3'2-BEFEVZE][root@pfsense: jcs9jqom9iu]\root: n9aM6
```

خط فرمان در pfSense متفاوت است ولی از ساختار Bash پیروی می کند، خب در فرمان اول فقط از `uname` استفاده شده و خروجی ساده ای برای شما نمایش داده شده است ، در فرمان دوم از سوئیچ `a` به معنی `all` استفاده شده است که همه اطاعات را به شما نمایش میدهد.

فرمان بعدی که خروجی بسیار مفیدی در اختیار شما قرار میدهد فرمان `iostat` است این فرمان برای نمایش وضعیت `i/o` دستگاهایی که به سیستم شما متصل است استفاده می شود و به صورت پیش فرض 5 دستگاه اول سیستم شما را نمایش می دهد مگر اینکه شما دستگاه خاصی را در نظر داشته باشید، طول خروجی این فرمان هم به صورت پیش فرض 80 ستون است. در شکل زیر خروجی این فرمان را مشاهده می کنید:

```
[2.3.5-RELEASE][root@pfSense.localdomain]/root: iostat
  tty      md0      ada0      cd0      cpu
tin tout KB/t tps MB/s KB/t tps MB/s KB/t tps MB/s us ni sy in id
0 2 0.00 0 0.00 26.33 2 0.05 0.00 0 0.00 2 0 3 0 94
[2.3.5-RELEASE][root@pfSense.localdomain]/root: iostat -c 5
  tty      md0      ada0      cd0      cpu
tin tout KB/t tps MB/s KB/t tps MB/s KB/t tps MB/s us ni sy in id
0 2 0.00 0 0.00 26.33 2 0.05 0.00 0 0.00 2 0 3 0 94
0 234 0.00 0 0.00 0.50 1 0.00 0.00 0 0.00 0 2 12 1 86
0 78 0.00 0 0.00 0.00 0 0.00 0.00 0 0.00 0 4 13 0 83
0 78 0.00 0 0.00 0.00 0 0.00 0.00 0 0.00 0 0 0 0 100
0 79 0.00 0 0.00 0.00 0 0.00 0.00 0 0.00 0 0 0 0 100
[2.3.5-RELEASE][root@pfSense.localdomain]/root: █
```

در خروجی فرمان اول شما فقط یک خط از خروجی این فرمان را مشاهده میکنید که چند دستگاه همی که به سیستم شما متصل است را وضعیت `IO` را برای شما نمایش می دهد، برای اینکه بتوانید تعداد این نمایش ها را بیشتر از یک خروجی کنید از سوئیچ `C` و بعد تعداد مورد نظر خود استفاده کنید که در فرمان بعدی با استفاده از عدد 5 درخواست نمایش 5 خروجی را کرده و خط فرمان هم بعد از اتمام این 5 خروجی دوباره به خط فرمان برگشت داده شده اید.

برای نمایش فقط `io` مربوط به دیسکها از سوئیچ `d` به صورت زیر استفاده کنید:

```
[2.3.5-RELEASE][root@pfSense.localdomain]/root: iostat -d
      md0      ada0      cd0      pass0
KB/t tps MB/s KB/t tps MB/s KB/t tps MB/s KB/t tps MB/s
0.00 0 0.00 26.49 2 0.04 0.00 0 0.00 0.00 0 0.00
[2.3.5-RELEASE][root@pfSense.localdomain]/root: █
```

همانطوری که مشاهده می کنید دو بخش `cpu` و `tty` در نمایش فرمان بالا حذف شده است. برای نمایش هرچه بهتر وضعیت دیسک ها در حالت گسترده از سوئیچ `X` استفاده کنید، در صورتی که تعداد دیسک های سیستم شما زیاد

باشد و همه در خروجی فرمان قرار نگیرند بهترین گزینه استفاده کرده از این مدل خروجی است که هر دیسک در یک خط افقی قرار می گیرد، نمایش این خروجی را در شکل زیر مشاهده می کنید:

```
[2.3.5-RELEASE][root@pfSense.localdomain]/root: iostat -x
extended device statistics
device      r/s      w/s      kr/s     kw/s  qlen  svc_t  %b
md0         0.0      0.1      0.0      0.0    0     0.3    0
ada0        0.4      1.3      8.9     35.7    0    15.8    1
cd0         0.0      0.0      0.0      0.0    0     0.1    0
pass0       0.0      0.0      0.0      0.0    0     0.0    0
pass1       0.0      0.0      0.0      0.0    0     1.4    0
[2.3.5-RELEASE][root@pfSense.localdomain]/root: █
```

یکی دیگر از فرمان های نمایش وضعیت سیستم شما که خود شامل چندین زیر فرمان و بخش مفید است فرمان `sysstat` است که در این بخش شما با بخشی از این فرمان در `pfSense` آشنا می شوید. این فرمان از تکنولوژی `ncurses` برای طبقه بندی کردن صفحه نمایش استفاده می کند، در بخش بالایی این خروجی `load` سیستم به صورت `bar` برای شما نمایش داده می شود و در بخش پایینی این فرمان شما می توانید اطلاعات انتخابی مورد نظر خودتون را برای نمایش انتخاب کنید. یک خروجی ساده از این فرمان را در شکل زیر مشاهده می کنید:

```

Load Average  /0 /1 /2 /3 /4 /5 /6 /7 /8 /9 /10
               /0% /10 /20 /30 /40 /50 /60 /70 /80 /90 /100
root          idle XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

```


برای وارد شدن به بخش اطلاعاتی که این فرمان می تواند برای شما نمایش دهد کافیتست که از علامت : استفاده کنید و بعد کلمه help را وارد کنید و به محض اجرا help با استفاده از کلید Enter در قسمت پایینی این فرمان خطی به صورت زیر برای شما نمایش داده می شود:

```
ping swap iostat vmstat netstat icmp ip icmp6 ip6 sctp tcp ifstat
```

در این بخش شما با وارد کردن هر یک از این کلمات می توانید وضعیت مورد نظر از سیستم خود را مشاهده کنید برای مثال برای نمایش وضعیت ip کافیتست که از این بخش دوباره : را وارد کنید و کلمه ip را نوشته و enter کنید تا خروجی به صورت زیر برای شما تغییر کند:

```

Load Average      /0 /1 /2 /3 /4 /5 /6 /7 /8 /9 /10
                  ;;

      IP Input
      1 total packets received
      0 - with bad checksums
      0 - too short for header
      0 - too short for data
      0 - with invalid hlen
      0 - with invalid length
      0 - with invalid version
      0 - jumbograms
      0 total fragments received
      0 - fragments dropped
      0 - fragments timed out
      0 - packets reassembled ok
      0 packets forwarded
      0 - unreachable dests
      0 - redirects generated
      0 option errors
      0 unwanted multicasts
      1 delivered to upper layer

      IP Output
      1 total packets sent
      1 - generated locally
      0 - output drops
      0 output fragments generated
      0 - fragmentation failed
      0 destinations unreachable
      0 packets output via raw IP

      UDP Statistics
      0 total input packets
      0 - too short for header
      0 - invalid checksum
      0 - no checksum
      0 - invalid length
      0 - no socket for dest port
      0 - no socket for broadcast
      0 - socket buffer full
      0 total output packets

Showing ip, refresh every 5 seconds.
```

در این خروجی شما وضعیت بسته های ip وارد شده و خارج شده از سیستم را مشاهده می کنید که هر 5 ثانیه یکبار به صورت پویا تغییر می کند.

در زمانی که سیستم شما دچار کندی در پردازش می شود یکی از بهتر فرمان های که می تواند در این بخش به شما کمک کند برای نمایش وضعیت پردازش های سیستم شما تا بتوانید سرویسی که بیشتر پردازش را از سیستم شما را دریافت می کند را مشخص کنید فرمان `top` است، خروجی این فرمان را در شکل زیر مشاهده می کنید:

```
last pid: 6288; load averages: 0.05, 0.09, 0.10 up 0+01:59:51 14:07:01
34 processes: 1 running, 33 sleeping
CPU: 0.0% user, 0.0% nice, 0.4% system, 0.8% interrupt, 98.8% idle
Mem: 25M Active, 58M Inact, 48M Wired, 42M Buf, 348M Free
Swap: 1024M Total, 1024M Free
```

| PID | USERNAME | THR | PRI | NICE | SIZE | RES | STATE | TIME | WCPU | COMMAND |
|-------|----------|-----|-----|------|--------|--------|--------|------|-------|----------------|
| 303 | root | 1 | 52 | 0 | 61636K | 32064K | accept | 0:26 | 0.00% | php-fpm |
| 300 | root | 1 | 52 | 0 | 61636K | 31556K | accept | 0:24 | 0.00% | php-fpm |
| 301 | root | 1 | 20 | 0 | 61504K | 31164K | accept | 0:24 | 0.00% | php-fpm |
| 8891 | root | 1 | 20 | 0 | 23952K | 6100K | kqread | 0:05 | 0.00% | nginx |
| 34824 | root | 5 | 20 | 0 | 10632K | 1056K | accept | 0:02 | 0.00% | dpinger |
| 6787 | root | 1 | 20 | 0 | 13060K | 13092K | select | 0:01 | 0.00% | ntpd |
| 55632 | root | 1 | 20 | 0 | 10020K | 3056K | pause | 0:01 | 0.00% | tcsh |
| 12944 | root | 1 | 20 | 0 | 10236K | 1896K | hpf | 0:01 | 0.00% | filterlog |
| 47275 | root | 1 | 20 | 0 | 10148K | 1896K | select | 0:01 | 0.00% | syslogd |
| 299 | root | 1 | 20 | 0 | 57408K | 22224K | kqread | 0:01 | 0.00% | php-fpm |
| 45587 | root | 1 | 52 | 20 | 10460K | 2116K | wait | 0:00 | 0.00% | sh |
| 41525 | unbound | 1 | 52 | 0 | 23512K | 9864K | kqread | 0:00 | 0.00% | unbound |
| 31632 | _dhcp | 1 | 20 | 0 | 10184K | 2004K | select | 0:00 | 0.00% | dhclient |
| 339 | root | 1 | 40 | 20 | 12036K | 3604K | kqread | 0:00 | 0.00% | check_reload_s |
| 21822 | root | 1 | 52 | 0 | 10184K | 1888K | select | 0:00 | 0.00% | dhclient |
| 28123 | root | 1 | 20 | 0 | 10108K | 1888K | nanslp | 0:00 | 0.00% | cron |
| 6288 | root | 1 | 20 | 0 | 11260K | 2412K | RUN | 0:00 | 0.00% | top |
| 25210 | root | 1 | 52 | 0 | 10460K | 2108K | wait | 0:00 | 0.00% | sh |

این فرمان اطلاعات مختلفی را از چند فرمان برای شما گرفته و نمایش میدهد در خط اولیه وضعیت روشن بودن سیستم را برای شما نمایش می دهد که شما می توانید از خروجی فرمان `uptime` آنرا مشاهده کنید، در خط بعدی در مورد تعداد پردازش هایی که بر روی سیستم شما راه اندازی شده و در حال فعالیت خواب هستند رو مشاهده می کنید، میزان مصرف CPU رم و پارتیشن Swap را از بخش های دیگر مشاهده می کنید (این بخش برای شما اطلاعات مفیدی را مشاهده می کنید و اگر سیستم شما دچار کمبود منابع باشد می توانید از این بخش گزارش آنرا مشاهده کنید) قسمت پایینی این برنامه لیست پردازش ها به صورت پویا و با میزان فضای استفاده هر کدام را مشاهده می کنید. برای خارج شده از این فرمان از کلید `q` استفاده کنید.

یکی از فرمان های مفید برای مشاهده مدت زمانی که چه کاربرانی و در چه مدت زمانی به سیستم شما متصل بوده اند مورد استفاده قرار می گیرند فرمان `last` است که خروجی این فرمان به صورت زیر است:

```
[2.3.5-RELEASE][root@pfSense.localdomain]/root: last
root      ttyv0      Thu Apr  5 11:16  still logged in
root      ttyv0      Wed Apr  4 12:39 - 11:16 (22:37)
root      ttyv0      Wed Apr  4 12:37 - 12:37 (00:00)
root      ttyv0      Wed Apr  4 12:29 - 12:37 (00:07)
root      ttyv0      Wed Apr  4 12:15 - 12:29 (00:13)
root      ttyv0      Wed Apr  4 12:09 - 12:15 (00:06)
root      ttyv0      Wed Apr  4 11:50 - 12:09 (00:19)
root      ttyv0      Wed Apr  4 11:43 - 11:50 (00:07)
root      ttyv0      Wed Apr  4 11:09 - 11:40 (00:31)
root      ttyv0      Wed Apr  4 11:02 - 11:09 (00:06)
root      ttyv0      Wed Apr  4 11:02 - 11:02 (00:00)
root      ttyv0      Wed Apr  4 10:57 - 11:02 (00:04)
root      ttyv0      Wed Apr  4 10:35 - 10:57 (00:22)
root      ttyv0      Tue Apr  3 17:28 - 10:35 (17:06)
root      ttyv0      Tue Apr  3 17:03 - 17:28 (00:25)
root      ttyv0      Tue Apr  3 16:57 - 17:03 (00:05)
root      ttyv0      Sun Apr  1 23:52 - 16:55 (1+17:02)
root      ttyv0      Sun Apr  1 23:41 - 23:50 (00:08)
root      ttyv0      Sun Apr  1 22:38 - 23:41 (01:03)
root      ttyv0      Sun Apr  1 22:30 - 22:38 (00:07)
root      ttyv0      Mon Apr  2 02:55 - 22:30 (19:35)

utx.log begins Sun Apr  1 22:30:30 +0430 2018
[2.3.5-RELEASE][root@pfSense.localdomain]/root: █
```

برای نمایش وضعیتی کاربرانی که در حال حاضر به سیستم شما وارد شده ان و آخرین فرمان اجرایی آنها چه بوده است از فرمان `w` استفاده کنید که به صورت زیر خروجی آنرا هم مشاهده می کنید:

```
[2.3.5-RELEASE][root@pfSense.localdomain]/root: w
 2:39PM up 2:32, 1 user, load averages: 0.27, 0.15, 0.12
USER      TTY      FROM          LOGIN@      IDLE WHAT
root      v0      -             Thu11AM     -    w
[2.3.5-RELEASE][root@pfSense.localdomain]/root: █
```

برای نمایش وضعیت سخت افزارهای نصب شده بر روی سرور شما و یا آخرین تغییرات سخت افزاری سیستم خود از فرمان `dmesg` استفاده کنید این فرمان در حقیقت پیغام هایی که هسته در زمان راه اندازی را برای شما نمایش میدهد را نمایش داده و شما بعد از راه اندازی سیستم می توانید به این پیغام ها بعد از راه اندازی کامل با استفاده از این فرمان دسترسی داشته باشید، خروجی این فرمان را شما در شکل زیر مشاهده میکنید که البته خروجی آن طولانی بوده است و شما باید از `more` یا `less` برای طبقه بندی در نمایش آن استفاده کنید:

```

Root mount waiting for: usb1 usb0
ugen0.2: <UMware> at usb0
uhid0: <UMware> on usb0
uhid1: <UMware> on usb0
Root mount waiting for: usb1 usb0
uhub0: 6 ports with 6 removable, self powered
ugen0.3: <vendor 0x0e0f> at usb0
uhub2: <UMware Virtual USB Hub> on usb0
Root mount waiting for: usb0
uhub2: 7 ports with 7 removable, self powered
Trying to mount root from ufs:/dev/ufs/5ac15aa1141b6a11 [rw]...
le0: link state changed to UP
le1: link state changed to UP
pflog0: promiscuous mode enabled
arpresolve: can't allocate llinfo for 192.168.174.2 on le0
arpresolve: can't allocate llinfo for 192.168.174.2 on le0
arpresolve: can't allocate llinfo for 192.168.174.2 on le0
arpresolve: can't allocate llinfo for 192.168.174.2 on le0
arpresolve: can't allocate llinfo for 192.168.174.2 on le0
arpresolve: can't allocate llinfo for 192.168.174.2 on le0
arpresolve: can't allocate llinfo for 192.168.174.2 on le0
arpresolve: can't allocate llinfo for 192.168.174.2 on le0
arpresolve: can't allocate llinfo for 192.168.174.2 on le0
arpresolve: can't allocate llinfo for 192.168.174.2 on le0
[2.3.5-RELEASE][root@pfSense.localdomain]/root:

```

هر قابلیت‌ای که شما قصد فعال کردن آنرا در pfSense را دارید مثل traffic shaping باید در هسته بارگزاری شود برای نمایش هسته در pfSense از فرمان kldstat استفاده می‌شود که خروجی این فرمان را در شکل زیر مشاهده می‌کنید:

```

[2.3.5-RELEASE][root@pfSense.localdomain]/root: kldstat
Id Refs Address      Size      Name
  1    3 0xc0400000 1eb61e4  kernel
  2    1 0xc5fa8000 20000    ipfw.ko
[2.3.5-RELEASE][root@pfSense.localdomain]/root:

```

همانطوری که مشاهده می‌کنید وضعیت اصلی هسته را مشاهده می‌کنید و ماژول ipfw که در هسته هم بارگزار شده است را مشاهده می‌کنید.

Reboot

در برخی از موارد شما نیاز دارید که سیستم خود را راه اندازی مجدد کنید برای انجام این کار از خط فرمان کافیست که فرمان `reboot` را اجرا کنید تا بعد از بسته شدن پردازشهای فعال بروی سیستم شما دوباره سیستم شما راه اندازی مجدد شود.

Halt

برای خاموش کردن سیستم سیستم خود برای انجام دادن پاره ای از تغییرات سخت افزاری شما می توانید از فرمان `halt` استفاده کنید که برای انجام شدن کامل خاموشی سیستم از سوئیچ `p` به معنی `power off` استفاده کنید.

در این بخش شما با فرمان های ابتدای دریافت اطلاعات آشنا شده اید در بخش بعدی شما با فرمان های شبکه ای در FreeBSD آشنا می شوید.

مفاهیم شبکه در FreeBSD:

سلام دوستان عزیز، شاید برای شما تعجب برانگیز باشد که چرا در این کتاب در مورد شبکه در FreeBSD صحبت می کنم، در طول مدتی که دوره `pfsense` رو برای دوستان به صورت آنلاین برگزار کردم یک مشکل جالبی برای دوستان علاقمند مشاهده کردم به دلیل خاص بودن فایروال `pfsense` به سمت این فایروال جذب شدند و خط یک رابط وب خوب هم برای انجام دادن کارها در این فایروال قدرتمند وجود داره که نیازی به دانش فرمانهای قابل اجرا در این سیستم رو کم می کنه، ولی در زمان بروز مشکلات خاص و در کل در همه موارد این فرمان های موجود در سیستم عامل FreeBSD است که سرعت عمل شما رو در انجام کارها بالا می بره و شما به عنوان یک مدیر شبکه می تونید به سرعت کار مورد نظر رو انجام بدید، برای مثال نمایش سوکتهای باز سیستم شما می تونه اطلاعات مفیدی در اختیار شما قرار بده درسته که در بخش گرافیکی وب `pfsense` این موضوع هم دیده شده و در ادامه همین فصل با اون آشنا میشید ولی فرض کنید که در مشکلی قرار گرفته اید که دسترسی به رابط وب ندارید و باید با خط فرمان با فایروال خودتون و از راه دور مشکل رو حل کنید، در نتیجه داشتن دانش کافی در مورد فرمان های کاربردی در بخش شبکه یکی از نیازهایی است که شما باید داشته باشید. در ادامه شما با فرمانهای مهم و کاربردی در تنظیمات شبکه

در FreeBSD که سیستم عاملی است که pfSense از آن استفاده می کند آشنا می شوید. خوب بدون تلف کردن وقت شما میریم سراغ دسته بندی این بخش که در ادامه مشاهده می کنید:

- فرمان های دریافت اطلاعات شبکه ای
- ifconfig
- تنظیمات DNS و DHCP
- راه اندازی کردن مجدد تنظیمات شبکه

فرمان های دریافت اطلاعات شبکه ای

فرمان Hostname

هر سیستم که در شبکه قرار دارد به یک نام نیاز دارد این نام را شما در زمان راه اندازی اولیه pfSense وارد کرده اید که البته از طریق رابط وب قابل تغییر است برای نمایش این نام در خط فرمان این فرمان را به صورت زیر وارد کنید:

```
[2.3.5-RELEASE][root@pfSense.localdomain]/root: hostname  
pfSense.localdomain  
[2.3.5-RELEASE][root@pfSense.localdomain]/root: █
```

نکته:

فایل اصلی پیکربندی pfSense

فایروال pfSense بیشتر تنظیمات را از یک فایل xml به نام config.xml دریافت میکند که در زیر شاخه /cf/conf قرار دارد، این فایل دارای بخش های مختلف پیکربندی است که در هر بخش در مورد آن توضیح داده خواهد شد. این بخش در فایل اصلی پیکربندی pfSense وجود دارد که با استفاده از فرمان زیر می توانید آنرا مشاهده کنید:

```
[2.3.5-RELEASE][root@pfSense.localdomain]/cf/conf: cat config.xml | grep hostname
<hostname>pfSense</hostname>
[2.3.5-RELEASE][root@pfSense.localdomain]/cf/conf: █
```

فرمان ping

یکی از اولین فرمان های در شبکه برای تست کردن در دسترس بودن یک سیستم مورد استفاده قرار می گیرد فرمان ping است که در بخش منوی console هم با آن آشنا شده اید. این فرمان را شما می توانید در خط فرمان نیز اجرا کنید و تفاوت خروجی این فرمان با فرمان موجود در ویندوز این است که در ویندوز فقط 4 بسته ارسال می شود ولی در یونیکس تعداد بسته ها محدود نیست و تا زمانی که شما از کلید Ctrl+C استفاده کنید بسته ها ارسال شده و گزارش آن برای شما نمایش داده می شود، در مقابل این فرمان هم می توانید از نام استفاده کنید و هم آدرس ip که در صورتی که از نام استفاده کنید با استفاده از DNS این نام به آدرس ip تغییر پیدا کرده و در نهایت آدرس ip است که ping می شود در زیر خروجی این فرمان را مشاهده می کنید:

```
[2.3.5-RELEASE][root@pfSense.localdomain]/cf/conf: ping yahoo.com
PING yahoo.com (98.137.246.7): 56 data bytes
64 bytes from 98.137.246.7: icmp_seq=0 ttl=128 time=307.446 ms
64 bytes from 98.137.246.7: icmp_seq=1 ttl=128 time=309.618 ms
64 bytes from 98.137.246.7: icmp_seq=2 ttl=128 time=287.745 ms
^C
--- yahoo.com ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 287.745/301.603/309.618/9.839 ms
[2.3.5-RELEASE][root@pfSense.localdomain]/cf/conf: █
```

اگر از نام استفاده کنید و به صورت شکل بالا خروجی را مشاهده کنید به این معنی است که DNS سرورهای شما هم بدرستی پیکربندی شده است .

فرمان arp

یکی از بسته های که در شبکه محلی برای برقرار ارتباط مورد استفاده قرار می گیرد بسته های arp است که شما از طریق این بسته ها می توانید آدرس های فعال در شبکه و mac آدرسهای آنها را پیدا کنید، خروجی این فرمان با استفاده از سوئیچ a را در زیر مشاهده می کنید:

```
[2.3.5-RELEASE][root@pfSense.localdomain]/cf/conf: arp
usage: arp [-n] [-i interface] hostname
       arp [-n] [-i interface] -a
       arp -d hostname [pub]
       arp -d [-i interface] -a
       arp -s hostname ether_addr [temp] [reject | blackhole] [pub [only]]
       arp -S hostname ether_addr [temp] [reject | blackhole] [pub [only]]
       arp -f filename
[2.3.5-RELEASE][root@pfSense.localdomain]/cf/conf: arp -a
? (192.168.174.2) at 00:50:56:e5:ad:d4 on le0 expires in 1191 seconds [ethernet]
? (192.168.174.129) at 00:0c:29:b1:74:4f on le0 permanent [ethernet]
? (192.168.174.254) at 00:50:56:f1:49:d4 on le0 expires in 212 seconds [ethernet]
]
```

فرمان Sockstat

هر سروری را که شما بر روی سیستم خود فعال می کنید برای برقراری ارتباط با شبکه از یک پورت استفاده می کند و هر ارتباطی که شما برقرار می کنید با هر سروری از طریق یک پورت برقرار می شود، فقط در سیستم عامل FreeBSD فرمانی به نام sockstat وجود دارد که وضعیت سوکت های که در حقیقت همان پورت های سیستم شما را نمایش می دهد، در این بخش برای نمایش فقط پورت هایی که سرور های شما در حال سرویس دهی هستند در ورژن 4 آدرس ip از سوئیچ 14 استفاده کنید که در شکل زیر خروجی این فرمان را مشاهده می کنید:


```
[2.3.5-RELEASE][root@pfSense.localdomain]/root: sockstat -l4
USER      COMMAND  PID  FD PROTO  LOCAL ADDRESS    FOREIGN ADDRESS
unbound   unbound  41525 6  udp4   *:53             *:
unbound   unbound  41525 7  tcp4   *:53             *:
unbound   unbound  41525 8  tcp4   127.0.0.1:953    *:
root      nginx    8899 6  tcp4   *:443            *:
root      nginx    8899 8  tcp4   *:80             *:
root      nginx    8891 6  tcp4   *:443            *:
root      nginx    8891 8  tcp4   *:80             *:
root      nginx    8590 6  tcp4   *:443            *:
root      nginx    8590 8  tcp4   *:80             *:
root      ntpd     6787 21 udp4   *:123            *:
root      ntpd     6787 23 udp4   192.168.174.129:123 *:
root      ntpd     6787 25 udp4   127.0.0.1:123    *:
root      syslogd  47275 8  udp4   *:514            *:
root      php-fpm  303 5  udp4   *:               *:
root      php-fpm  301 5  udp4   *:               *:
root      php-fpm  300 5  udp4   *:               *:
root      php-fpm  299 5  udp4   *:               *:
[2.3.5-RELEASE][root@pfSense.localdomain]/root: █
```

فرمان pftop

در بخش قبلی شما با فرمان top آشنا شده اید که بصورت پویا وضعیت پردازش ها شما را نمایش میدهد برای فایروال pf که پایه pfsense هست هم برنامه ای به این صورت ایجاد شده که وضعیت ارتباطاتی که از طریق pf شما در تبادل است را در یک لیست برای شما به صورت پویا نمایش می دهد که در شکل زیر یک خروجی از این فرمان را مشاهده می کنید:

```
pfTop: Up State 1-2/2, View: default, Order: none, Cache: 10000 15:36:46
P
R  D SRC          DEST          STATE  AGE  EXP  PKTS BYTES
icmp 0 192.168.174.129:34824 192.168.174.2:34824 0:0 6664 9 25876 707K
udp 0 192.168.174.129:123 194.225.50.25:123 2:1 4 27 2 152
```

برای خارج شدن از این برنامه از q استفاده کنید.

فرمان traceroute

برای چک کردن مسیر بین فایروال شما و شبکه های دیگر از فرمان traceroute استفاده کنید که باید بعد از این فرمان آدرس ip که شما قصد دارید تا آن شبکه مسیر چک شود را وارد کنید، این بخش هم می تواند آدرس ip باشد و هم نام یک سایت. خروجی این بخش را در شکل زیر مشاهده میکنید:

فرمان ifconfig

فرمان ifconfig دارای قابلیت های بسیاری است که در این بخش برای شما بیان خواهیم کرد این فرمان علاوه بر نمایش وضعیت کارتهای شبکه برای تنظیم کردن آدرس ip مورد استفاده قرار می گیرد و در برخی از موارد برای فعال کردن و غیر فعال کردن قابلیتی در کارت شبکه مورد استفاده قرار میگیرد. این فرمان در FreeBSD تنظیمات را از فایل معروف rc.conf میگیرد که در pfSense از تنظیمات را از فایل اصلی پیکربندی دریافت می کند در قدم اول برای نمایش همه کارتهای شبکه ای که بر روی سیستم شما است باید از این فرمان به صورت زیر استفاده کنید:

```
[2.3.5-RELEASE][root@pfSense.localdomain]/root: ifconfig -l  
le0 le1 pflog0 pfsync0 enc0 lo0  
[2.3.5-RELEASE][root@pfSense.localdomain]/root: █
```

حال که در این بخش کارتهای شبکه موجود بر روی فایروال خود را مشاهده کرده اید در مرحله بعد می کنید وضعیت هر کدام را با ذکر نام در مقابل فرمان ifconfig مشاهده کنید، خروجی این فرمان به صورت زیر است:

```
[2.3.5-RELEASE][root@pfSense.localdomain]/root: ifconfig le0
le0: flags=8843<UP, BROADCAST, RUNNING, SIMPLEX, MULTICAST> metric 0 mtu 1500
options=8<VLAN_MTU>
ether 00:0c:29:b1:74:4f
hwaddr 00:0c:29:b1:74:4f
inet6 fe80::20c:29ff:feb1:744f%le0 prefixlen 64 scopeid 0x1
inet 192.168.174.129 netmask 0xfffff00 broadcast 192.168.174.255
nd6 options=23<PERFORMNUD, ACCEPT_RTADV, AUTO_LINKLOCAL>
media: Ethernet autoselect
status: active
[2.3.5-RELEASE][root@pfSense.localdomain]/root: █
```

در خروجی این فرمان در بخش inet شما آدرس ipv4 کارت شبکه را مشاهده می کنید. در بخش status هم وضعیت کارت شبکه که فعال است برای شما نمایش داده می شود. برای فعال کردن و غیر فعال کردن یک کارت شبکه هم شما می توانید از فرمان ifconfig نام کارت شبکه و down و یا up استفاده کنید که در شکل زیر مشاهده می کنید که بعد از غیر فعال شدن شبکه دیگر در خروجی ifconfig وضعیت وجود ندارد:

```
[2.3.5-RELEASE][root@pfSense.localdomain]/root: ifconfig le0
le0: flags=8843<UP, BROADCAST, RUNNING, SIMPLEX, MULTICAST> metric 0 mtu 1500
options=8<VLAN_MTU>
ether 00:0c:29:b1:74:4f
hwaddr 00:0c:29:b1:74:4f
inet6 fe80::20c:29ff:feb1:744f%le0 prefixlen 64 scopeid 0x1
inet 192.168.174.129 netmask 0xfffff00 broadcast 192.168.174.255
nd6 options=23<PERFORMNUD, ACCEPT_RTADV, AUTO_LINKLOCAL>
media: Ethernet autoselect
status: active
[2.3.5-RELEASE][root@pfSense.localdomain]/root: ifconfig le0 down
[2.3.5-RELEASE][root@pfSense.localdomain]/root: ifconfig le0
le0: flags=8802<BROADCAST, SIMPLEX, MULTICAST> metric 0 mtu 1500
options=8<VLAN_MTU>
ether 00:0c:29:b1:74:4f
hwaddr 00:0c:29:b1:74:4f
inet6 fe80::20c:29ff:feb1:744f%le0 prefixlen 64 tentative scopeid 0x1
inet 192.168.174.129 netmask 0xfffff00 broadcast 192.168.174.255
nd6 options=23<PERFORMNUD, ACCEPT_RTADV, AUTO_LINKLOCAL>
media: Ethernet autoselect
[2.3.5-RELEASE][root@pfSense.localdomain]/root: █
```

برای تغییر دادن آدرس ip کفایت که بعد فرمان و نام کارت شبکه آدرس جدید را وارد کنید و به این نکته توجه کنید که subnet mask را هم باید وارد کنید این بخش در شکل زیر نمایش داده شده است و خروجی را هم برای شما بعد از تغییر آدرس نمایش داده شده است:

```
nd6 options=23<PERFORMNUD,ACCEPT_RTADV,AUTO_LINKLOCAL>
media: Ethernet autoselect
status: active
[2.3.5-RELEASE][root@pfSense.localdomain]/root: ifconfig le0 down
[2.3.5-RELEASE][root@pfSense.localdomain]/root: ifconfig le0
le0: flags=8802<BROADCAST,SIMPLEX,MULTICAST> metric 0 mtu 1500
options=8<VLAN_MTU>
ether 00:0c:29:b1:74:4f
hwaddr 00:0c:29:b1:74:4f
inet6 fe80::20c:29ff:feb1:744f%le0 prefixlen 64 tentative scopeid 0x1
inet 192.168.174.129 netmask 0xfffff00 broadcast 192.168.174.255
nd6 options=23<PERFORMNUD,ACCEPT_RTADV,AUTO_LINKLOCAL>
media: Ethernet autoselect
[2.3.5-RELEASE][root@pfSense.localdomain]/root: ifconfig le0 192.168.100.1/24
[2.3.5-RELEASE][root@pfSense.localdomain]/root: ifconfig le0
le0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
options=8<VLAN_MTU>
ether 00:0c:29:b1:74:4f
hwaddr 00:0c:29:b1:74:4f
inet6 fe80::20c:29ff:feb1:744f%le0 prefixlen 64 scopeid 0x1
inet 192.168.100.1 netmask 0xfffff00 broadcast 192.168.100.255
nd6 options=23<PERFORMNUD,ACCEPT_RTADV,AUTO_LINKLOCAL>
media: Ethernet autoselect
status: active
[2.3.5-RELEASE][root@pfSense.localdomain]/root: |
```

تنظیمات DNS و DHCP

در FreeBSD فایلی وجود دارد به نام resolv.conf که در زیر شاخه etc قرار دارد و محل ذخیره سازی آدرسهای DNS است، این فایل را شما می توانید با ویرایشگر ee تغییر دهید. این تنظیمات در زمان راه اندازی اولیه وب تنظیم شده است و برای تغییر به آدرسهای DNS مورد نظر خود هم می توانید از بخش وب این کار را انجام دهید که دائمی است و هم می توانید از طریق این فایل تغییرات را اعمال کنید که به صورت لحظه ای است و با restart شدن سیستم به حالت اولیه باز می گردد، در شکل زیر محتوای این فایل را مشاهده می کنید:

```
[2.3.5-RELEASE][root@pfSense.localdomain]/root: cat /etc/resolv.conf
nameserver 127.0.0.1
search localdomain
nameserver 192.168.174.2
[2.3.5-RELEASE][root@pfSense.localdomain]/root: █
```

کافیست که بعد از بخش nameserver با یک فاصله آدرس سرور خود را وارد کنید. برای چک کردن وضعیت DNS سرورهای سیستم خود که به درخواست های شما پاسخ می دهند از فرمان nslookup استفاده کنید که برای این کار باید فرمان را در خط فرمان اجرا کنید تا شما به این بخش به صورت تصویر در شکل وارد شوید:

```
[2.3.5-RELEASE][root@pfSense.localdomain]/root: nslookup
> mabedini.com
Server:          192.168.174.2
Address:         192.168.174.2#53

Non-authoritative answer:
Name:   mabedini.com
Address: 89.39.208.119
> █
```

همانطوری که در شکل بالا مشاهده می کنید با استفاده از این فرمان شما وضعیت DNS سرور سیستم خود را مورد ارزیابی قرار داده اید.

راه اندازی کردن مجدد تنظیمات شبکه

سیستم عامل FreeBSD از سیستم rc برای راه اندازی کردن سرویس ها استفاده می کند برای راه اندازی کردن مجدد تنظیمات شبکه هم از این سیستم استفاده می شود، سیستم rc از فرمان هایی استفاده می کند که در فایل هایی به نام rc.d استفاده می کند که در زیر شاخه /etc/rc.d/ قرار گرفته اند شما در این بخش می توانید هر سرویسی را که نیاز دارید در FreeBSD راه اندازی از این طریق راه اندازی کنید، برای راه مجدد کردن تنظیمات شبکه هم از فرمان زیر استفاده کنید

#/etc/rc.d/netif restart

خب در این فرمان نکاتی هست که بهتون می‌گم. هر فرمان rc.d دارای یک سری زیر شاخه و زیر فرمان است که در فرمان با از بخش Restart این فرمان استفاده کردیم، زمانی که شما این فرمان را بدون زیر فرمان خاصی اجرا کنید شما با خروجی help این فرمان و تمام زیر فرمانی‌های موجود در این بخش آشنا می‌شوید که در شکل زیر خروجی این فرمان را مشاهده می‌کنید:

```
[2.3.5-RELEASE][root@pfSense.localdomain]/root: /etc/rc.d/netif
Usage: /etc/rc.d/netif [fast|force|one|quiet](start|stop|restart|rcvar|enabled|c
loneup|clonedown|clear|vnetup|vnetdown)
[2.3.5-RELEASE][root@pfSense.localdomain]/root: █
```

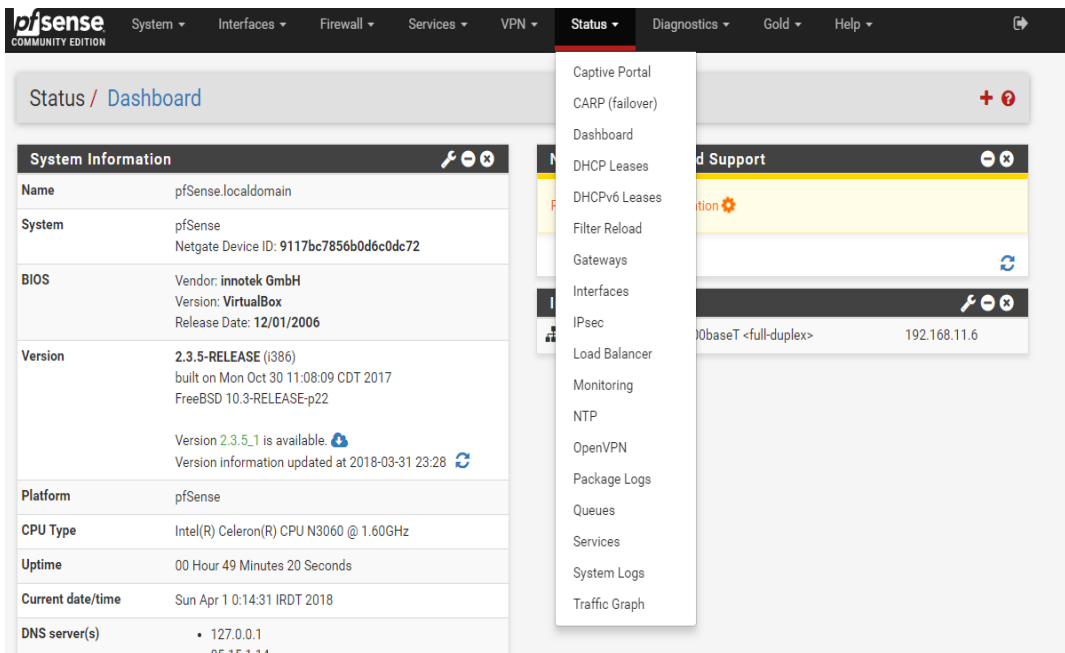
کار با فرمان dhclient

در سیستم عامل FreeBSD برای استفاده از dhcp در بخش کلاینتی از این فرمان استفاده می‌شود که باعث می‌شود تنظیمات کارت شبکه شما از طریق DHCP استفاده اعمال می‌شود، برای استفاده از این فرمان کافیست که نام کارت شبکه خود را بعد فرمان وارد کنید تا در صورت وجود به DHCP server این تنظیمات اعمال می‌شود.

فصل پنجم منوی وضعیت در pfsense

فصل پنجم منوی وضعیت در pfsense

در فایروال pfsense منوی به نام Status یا وضعیت وجود دارد که دارای زیر منوی های است که برای شما وضعیت سرویسها، وضعیت کل سیستم شما و شبکه شما را نمایش میدهد در این بخش ما قصد داریم که شما را با بخشهای این زیر منو به صورت مختصر و مفید آشنا کرده تا در سایر بخش های این کتاب شما به راحتی بتوانید از سیستم وضعیت برای استفاده درست و صحیح از pfsense استفاده کنید، در شکل زیر این منو را مشاهده می کنید.



The screenshot shows the pfSense web interface. At the top, there is a navigation bar with the following items: System, Interfaces, Firewall, Services, VPN, Status (highlighted), Diagnostics, Gold, and Help. Below the navigation bar, the main content area is titled "Status / Dashboard". On the left, there is a "System Information" section with a table of system details. On the right, there is a "Status" dropdown menu that is open, showing a list of system status options. The "System Information" table contains the following data:

| System Information | |
|--------------------|---|
| Name | pfSense.localdomain |
| System | pfSense Netgate Device ID: 9117bc7856b0d6c0dc72 |
| BIOS | Vendor: innotek GmbH Version: VirtualBox Release Date: 12/01/2006 |
| Version | 2.3.5-RELEASE (i386) built on Mon Oct 30 11:08:09 CDT 2017 FreeBSD 10.3-RELEASE-p22 Version 2.3.5.1 is available. Version information updated at 2018-03-31 23:28 |
| Platform | pfSense |
| CPU Type | Intel(R) Celeron(R) CPU N3060 @ 1.60GHz |
| Uptime | 00 Hour 49 Minutes 20 Seconds |
| Current date/time | Sun Apr 1 0:14:31 IRDT 2018 |
| DNS server(s) | <ul style="list-style-type: none"> 127.0.0.1 85.15.1.14 |

The "Status" dropdown menu lists the following options: Captive Portal, CARP (failover), Dashboard, DHCP Leases, DHCPv6 Leases, Filter Reload, Gateways, Interfaces, IPsec, Load Balancer, Monitoring, NTP, OpenVPN, Package Logs, Queues, Services, System Logs, and Traffic Graph.

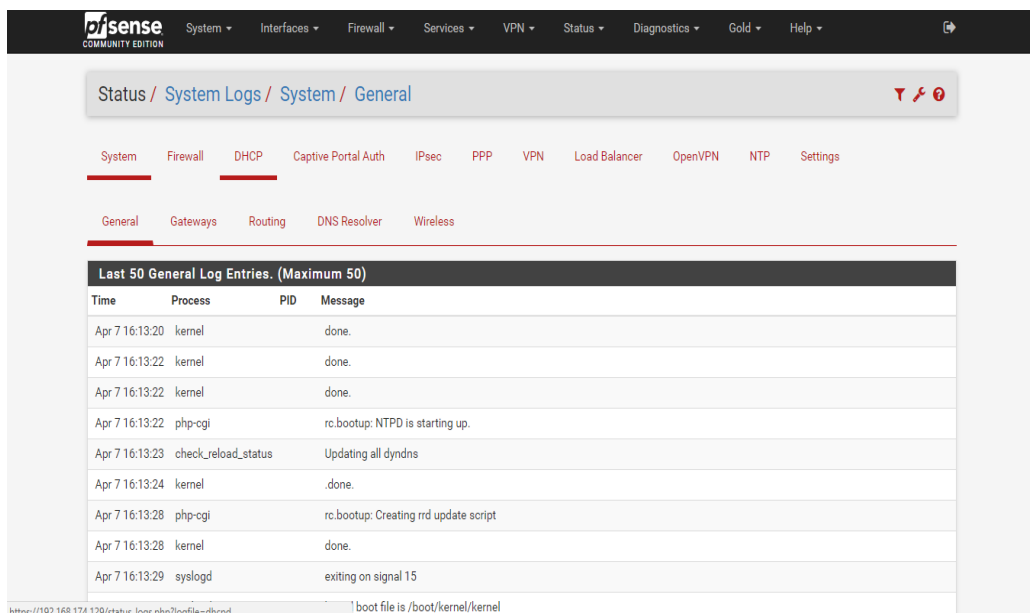
این منو را در شکل بالا مشاهده میکنید که هر سرویسی هم که شما به فایروال خود اضافه کرده باشید از طریق منوی می توانید وضعیت آنرا مشاهده کنید در حالت کلی هم شما می توانید بخشهای اصلی را هم با استفاده از این منو باز کنید.

یکی از منوی معروف در این بخش dashboard است که به محض ورود شما به سیستم برای شما باز می شود و در بخش های قبلی در زمان آموزش رابط وب با این بخش به طور کامل آشنا شده اید.

در زمان آموزش هر سرویس شما با منوی مخصوص status آن بیشتر آشنا می شوید، اما در این زیر منوی چند بخش مهم و عمومی وجود دارد که در ادامه با آنها آشنا می شوید.

زیر منوی system Log

هر برنامه، سرویس، سروری که در pfSense وجود دارد برای نمایش وضعیت خود از سیستم syslog استفاده می کند بعد از وارد شدن به این زیر منو شما با صفحه ای به صورت زیر مواجه می شوید:

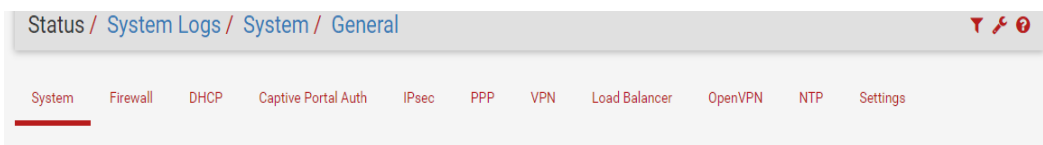


The screenshot shows the pfSense web interface. The top navigation bar includes: pfSense COMMUNITY EDITION, System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, Gold, and Help. The breadcrumb trail is: Status / System Logs / System / General. Below this, there are tabs for System, Firewall, DHCP, Captive Portal Auth, IPsec, PPP, VPN, Load Balancer, OpenVPN, NTP, and Settings. Under the System tab, there are sub-tabs for General, Gateways, Routing, DNS Resolver, and Wireless. The main content area displays "Last 50 General Log Entries. (Maximum 50)" with a table:

| Time | Process | PID | Message |
|----------------|---------------------|-----|---------------------------------------|
| Apr 7 16:13:20 | kernel | | done. |
| Apr 7 16:13:22 | kernel | | done. |
| Apr 7 16:13:22 | kernel | | done. |
| Apr 7 16:13:22 | php-cgi | | rc.bootup: NTPD is starting up. |
| Apr 7 16:13:23 | check_reload_status | | Updating all dyndns |
| Apr 7 16:13:24 | kernel | | .done. |
| Apr 7 16:13:28 | php-cgi | | rc.bootup: Creating rrd update script |
| Apr 7 16:13:28 | kernel | | done. |
| Apr 7 16:13:29 | syslogd | | exiting on signal 15 |

At the bottom of the log table, there is a URL: `https://192.168.174.129/status_logs.php?logfile=rfhrnd` and a file path: `| boot file is /boot/kernel/kernel`.

در خط بالایی از این منو شما حق انتخاب در بین حالت‌های مختلف زیر را دارید:



This screenshot shows the same pfSense web interface as above, but with the "System" tab selected and underlined. The breadcrumb trail remains: Status / System Logs / System / General. The sub-tabs under System are: General, Gateways, Routing, DNS Resolver, and Wireless.

هر کدام از این منو ها خود دارای زیر منوهای خاص و مخصوص خود هستند برای مثال منوی system دارای زیر منوی زیر است:

General

Gateways

Routing

DNS Resolver

Wireless

در این زیر منوها بخش **General** شما وضعیت لاگ کل سیستم خود را مشاهده می کنید که می توانید ردیف نمایش هر کدام را تغییر دهید، در شکل زیر یک مثال از این بخش را مشاهده می کنید:

| General | Gateways | Routing | DNS Resolver | Wireless |
|--|---------------------|---------|--|----------|
| Last 50 General Log Entries. (Maximum 50) | | | | |
| Time | Process | PID | Message | |
| Apr 9 11:55:35 | php-fpm | 301 | /rc.newwanip: ROUTING: setting default route to 192.168.174.2 | |
| Apr 9 11:55:35 | php-fpm | 301 | /rc.newwanip: rc.newwanip: on (IP address: 192.168.174.129) (interface: WAN[wan]) (real interface: le0). | |
| Apr 9 11:55:35 | php-fpm | 301 | /rc.newwanip: rc.newwanip: Info: starting on le0. | |
| Apr 9 11:55:34 | check_reload_status | | rc.newwanip starting le0 | |
| Apr 9 11:55:34 | kernel | | arpresolve: can't allocate llinfo for 192.168.174.2 on le0 | |
| Apr 9 11:55:32 | kernel | | arpresolve: can't allocate llinfo for 192.168.174.2 on le0 | |
| Apr 9 11:55:31 | kernel | | arpresolve: can't allocate llinfo for 192.168.174.2 on le0 | |
| Apr 9 11:55:31 | kernel | | arpresolve: can't allocate llinfo for 192.168.174.2 on le0 | |

برای مثال در شکل بالا در خط اول زمان ایجاد لاگ مربوطه، پردازشی که آنرا ایجاد کرده، عدد پردازش و در خط آخر پیغام ایجاد شده توسط پردازش را مشاهده می کنید. با کلید کردن در هر بخشی شما می توانید ردیف هر کدام را تغییر دهید.

بخش بعدی و مهم در این بخش **firewall** است که شامل زیر منوی های نمایش داده شده در شکل زیر است:

| Status / System Logs / Firewall / Normal View | | | | | | | | | | |
|---|--------------|--------------|---------------------|-------|-----|-----|---------------|---------|-----|----------|
| System | Firewall | DHCP | Captive Portal Auth | IPsec | PPP | VPN | Load Balancer | OpenVPN | NTP | Settings |
| Normal View | Dynamic View | Summary View | | | | | | | | |
| Last 50 Firewall Log Entries. (Maximum 50) | | | | | | | | | | |

در بخش اول حالت نمایش معمولی است که گزارش کل سیستم فایروال را مشاهده می کنید که این بخش در شکل زیر نمایش داده شده است:

Normal View Dynamic View Summary View

Last 50 Firewall Log Entries. (Maximum 50)

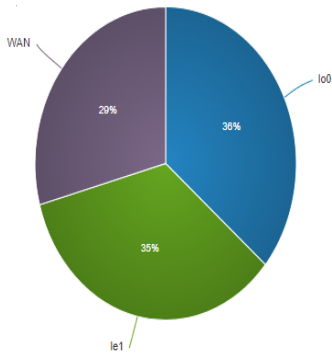
| Action | Time | Interface | Source | Destination | Protocol |
|--------|----------------|-----------|--------------------|----------------------|----------|
| ✗ | Apr 7 11:17:07 | le1 | i 192.168.40.1:137 | i 192.168.40.255:137 | UDP |
| ✗ | Apr 7 11:17:07 | le1 | i 192.168.40.1:137 | i 192.168.40.255:137 | UDP |
| ✗ | Apr 7 11:17:08 | le1 | i 192.168.40.1:137 | i 192.168.40.255:137 | UDP |
| ✗ | Apr 7 11:17:08 | le1 | i 192.168.40.1:137 | i 192.168.40.255:137 | UDP |
| ✗ | Apr 7 11:17:08 | le1 | i 192.168.40.1:137 | i 192.168.40.255:137 | UDP |
| ✗ | Apr 7 11:17:08 | le1 | i 192.168.40.1:137 | i 192.168.40.255:137 | UDP |
| ✗ | Apr 7 11:17:08 | le1 | i 192.168.40.1:137 | i 192.168.40.255:137 | UDP |
| ✗ | Apr 7 11:17:08 | le1 | i 192.168.40.1:137 | i 192.168.40.255:137 | UDP |
| ✗ | Apr 7 11:17:08 | le1 | i 192.168.40.1:137 | i 192.168.40.255:137 | UDP |

این بخش هم مثل قسمت نرمال است با این تفاوت به صورت متناوب در سطح نمایش بروز می شود و از تکنولوژی AJAX استفاده می کند. برای غیرفعال کردن حالت بروزرسانی شدن باید گزینه pause را به که در بخش بالای این قسمت است را انتخاب کنید، این گزینه در شکل زیر نمایش داده شده است:

Last 50 Firewall Log Entries. (Maximum 50) Pause

در قسمت پایانی از این بخش شما می توانید خلاصه وضعیتی را از کل گزارش به صورت نموداری مشاهده کنید که این بخش برای ارایه کردن گزارشات pfsense بسیار مفید و کاراتس که شما در شکل زیر بخشهای این گزارش را مشاهده می کنید:

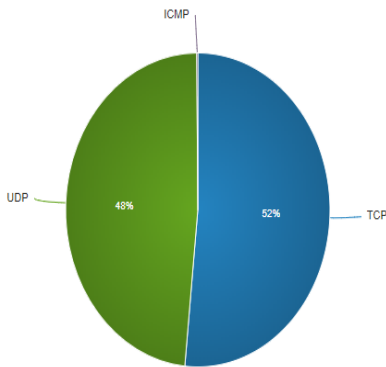
Interfaces



| Interfaces | Data points |
|------------|-------------|
| lo0 | 1164 |
| le1 | 1112 |
| WAN | 941 |

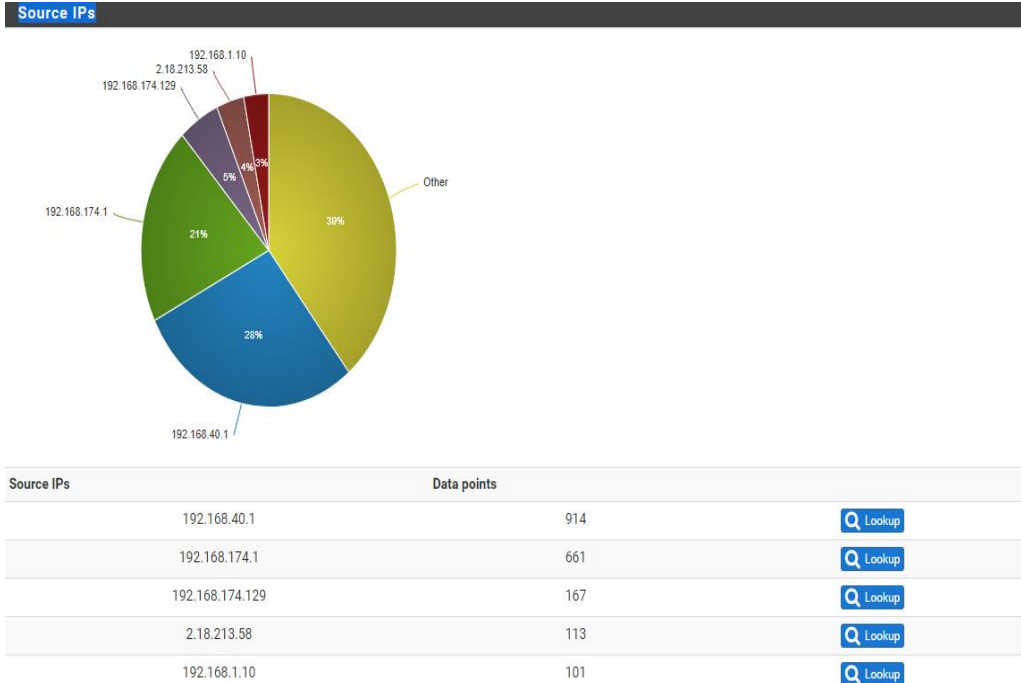
بخش مربوط به پروتکلها:

Protocols



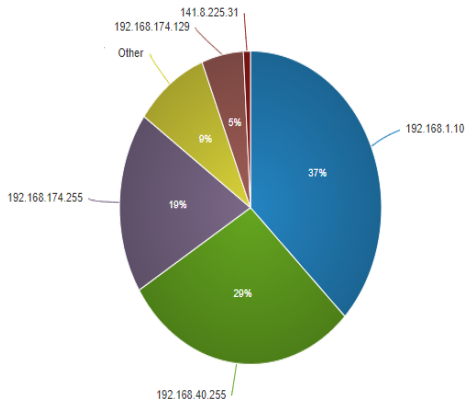
| Protocols | Data points |
|-----------|-------------|
| TCP | 1659 |
| UDP | 1554 |
| ICMP | 4 |

بخش Source IPs



بخش Destination IPs

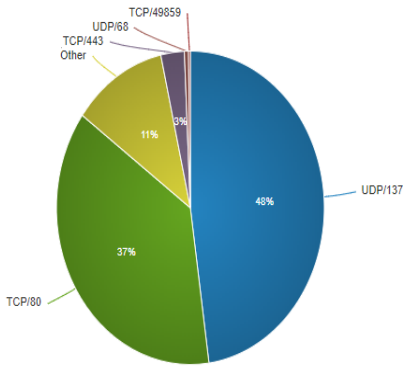
Destination IPs



| Destination IPs | Data points | |
|-----------------|-------------|--------------------------|
| 192.168.1.10 | 1197 | Q Lookup |
| 192.168.40.255 | 932 | Q Lookup |
| 192.168.174.255 | 602 | Q Lookup |
| 192.168.174.129 | 166 | Q Lookup |
| 141.8.225.31 | 28 | Q Lookup |

بخش Source Ports

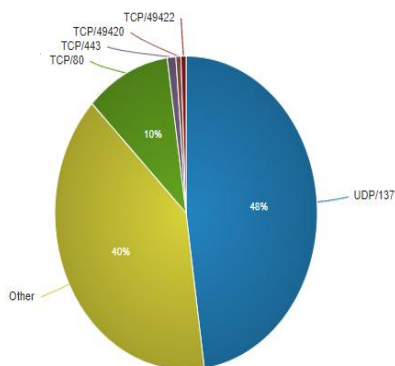
Source Ports



| Source Ports | Data points |
|---------------------|-------------|
| UDP/137: netbios-ns | 1537 |
| TCP/80: http | 1199 |
| TCP/443: https | 91 |
| UDP/68: bootpc | 16 |
| TCP/49859 | 7 |

بخش Destination Ports

Destination Ports



| Destination Ports | Data points |
|---------------------|-------------|
| UDP/137: netbios-ns | 1537 |
| TCP/80: http | 335 |
| TCP/443: https | 34 |
| TCP/49420 | 20 |
| TCP/49422 | 20 |

بخش های دیگر در این قسمت بسته به استفاده شما از pfSense دارای گزارشات بوده و شما با وارد شدن به هر بخش می توانید گزارشات مخصوص آن بخش را مشاهده کنید.

اما قسمت مهم و پرکاربرد این بخش قسمت تنظیمات یا setting است که خود به دو بخش General Logging و Remote Logging Options برای اعمال تنظیمات برای گزارشگیری های محلی استفاده می شود و بخش Options که از طریق آن می توانید گزارشات را به سمت یک سرور syslog دیگر ارسال کنید، در ادامه بخش های مختلف موجود در این قسمت را توضیح خواهیم داد.

زیر بخش های General Logging Options :

بخش اول Forward/Reverse Display اگر قصد دارید که برای نمایش گزارشات log در نمایش از جدید به قدیم باشد باید این بخش را فعال کنید.

بخش دوم **GUI Log Entries to Display**: در زمانی که این سیستم لاگ وضعیت را برای شما نمایش میدهد در صفحه نمایش به صورت پیش فرض 50 فیلد را نمایش میدهد که برای افزایش این تعداد و یا کاهش آن می توانید از این بخش استفاده کنید.

بخش سوم **Log File Size**: هر فایل لاگی که بر روی سیستم شما ایجاد می شود باید دارای سایز خاصی باشد که از فضای سیستم شما به صورت بهینه استفاده شود و فایل‌های بزرگ لاگ برای شما درد سرساز نشود، در سیستم عامل **FreeBSD** برای این بخش به صورتی طراحی شده است که بعد از رسیدن سایز یک فایل به اندازه مشخص این فایل بسته شود و فایل جدید ایجاد می شود و تا مقداری مشخص از این فایلها بر روی سیستم شما ذخیره میشود، در این بخش و با استفاده از آن می توانید حجم فایل لاگ خود را مشخص کنید. در این بخش شما در خط آخر هم یک گزارشی از حجم فایل‌های لاگ خود را در حالت کلی مشاهده کنید ، محاسبه این بخش به تعداد پردازش های که گزارش گرفته می شود و حجمی که شما تعیین می کنید قابل محاسبه است.

بخش سوم **Log firewall default blocks**: با فعال کردن این بخش در بخش فایروال بسته هایی که به رول پیش فرض که همان **block** کنند کل ترافیک است **match** می شود را برای شما لاگ گیری می کند، این بخش در زمان راه اندازی اولیه برای شما مفید خواهد بود که شما بتوانید رولهای که عمل نمیکنند را پیدا کنید و یا ترافیک هایی را که شما قصد عبور آنها دارید ولی به رول پیش فرض بلاک برخورد میکنند را پیدا کنید و رول مناسب را اعمال کنید ولی در زمانیکه شما به صورت حرفه ای رول ها را می نویسد دیگر نیاز به گزارش گیری این بخش را نخواهید داشت و بهتر است که آنها حذف کنید.

بخش چهارم **Web Server Log**: در صورت فعال بودن این بخش لاگهای سرور وب و بخش **Captive portal** هم برای شما در ساختار گزارشگیری ذخیره می شود.

بخش پنجم **Raw Logs**: بخش نمایش لاگهای فایروال در صورت پیش فرض برای شما قسمتهایی را نمایش میدهد که البته شما می توانید در بخش رول نویسی هم از آن استفاده کنید که در بخش مورد نظر با آن آشنا می شوید، در زمان نمایش هم به صورت زیر گزارشات را برای شما نمایش میدهد:

| Action | Time | Interface | Source | Destination | Protocol |
|--------|----------------|-----------|------------------|--------------------|----------|
| ✘ | Apr 7 11:40:22 | le1 | 192.168.40.1:137 | 192.168.40.255:137 | UDP |
| ✘ | Apr 7 11:40:22 | le1 | 192.168.40.1:137 | 192.168.40.255:137 | UDP |

در صورتی که شما این بخش را فعال کنید نمایش گزارشات فایروال به صورت خاص بوده و به صورت زیر برای شما نمایش داده می شود:

| Last 50 Firewall Log Entries. (Maximum 50) | |
|--|---|
| Time | Message |
| Apr 7 11:40:22 | filterlog: 5,16777216,,1000000103,le1,match,block,in,4,0x0,128,2154,0,none,17,udp,78,192.168.40.1,192.168.40.255,137,137,58 |
| Apr 7 11:40:22 | filterlog: 5,16777216,,1000000103,le1,match,block,in,4,0x0,128,2153,0,none,17,udp,78,192.168.40.1,192.168.40.255,137,137,58 |
| Apr 7 11:40:21 | filterlog: 5,16777216,,1000000103,le1,match,block,in,4,0x0,128,2152,0,none,17,udp,78,192.168.40.1,192.168.40.255,137,137,58 |
| Apr 7 11:36:40 | filterlog: 5,16777216,,1000000103,le1,match,block,in,4,0x0,128,2151,0,none,17,udp,78,192.168.40.1,192.168.40.255,137,137,58 |

همانطوری که مشاهده میکنید این بخش اطلاعات خام را برای شما نمایش میدهد.

بخش IGMP Proxy: اگر شما برای برقرار ارتباط بین شبکه ها از IGMP Proxy استفاده کنید برای فعال کردن گزارشگیر این بخش را فعال کنید.

بخش Where to show rule descriptions: هر رولی که شما در بخش لاگ مشاهده می کنید یک بخش توضیحات دارد که به صورت پیش فرض نمایش داده نمی شود، با استفاده از این بخش شما می توانید محل نمایش توضیحات رولهای بخش لاگ را تعیین کنید شما می توانید آنرا در یک سطر جدا یا در یک ستون قرار دهید، در جلو منوی انتخاب شما دو حالت زیر را مشاهده میکنید:



Where to show rule descriptions

Display as column
▼

- Dont load descriptions
- Display as column
- Display as second row

Use with large rule sets.

با انتخاب کردن بخش row گزایش به صورت زیر تغییر می کند:

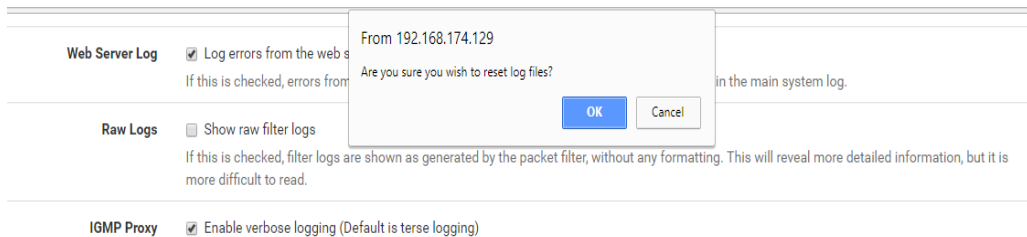
| Last 50 Firewall Log Entries. (Maximum 50) | | | | | | |
|--|----------------|-----------|--|--|----------|--|
| Action | Time | Interface | Source | Destination | Protocol | |
| ✘ | Apr 7 11:40:22 | le1 |  192.168.40.1:137 |  192.168.40.255:137 | UDP | |
| Default deny rule IPv4 (1000000103) | | | | | | |

و در صورتی که گزینه column را انتخاب کنید گزارش توضیحات بخش لاگ به صورت زیر نمایش داده می شود:

| Last 50 Firewall Log Entries. (Maximum 50) | | | | | | |
|--|----------------|-----------|-------------------------------------|------------------|--------------------|----------|
| Action | Time | Interface | Rule | Source | Destination | Protocol |
| ✘ | Apr 7 11:40:22 | le1 | Default deny rule IPv4 (1000000103) | 192.168.40.1:137 | 192.168.40.255:137 | UDP |
| ✘ | Apr 7 11:40:22 | le1 | Default deny rule IPv4 (1000000103) | 192.168.40.1:137 | 192.168.40.255:137 | UDP |

بخش Local Logging: برای غیرفعال کردن ذخیره شده گزارشات بر روی هارد دیسک سیستم شما و ارسال آن به سمت سرور مرکزی log شما می توانید نوشته شدن لاگ بر روی هارد دیسک را از طریق این منو غیر فعال کنید. البته شما می توانید هر دو این بخش ها را یعنی ذخیره کردن بر روی هارد و ارسال به سمت سرور بیرونی را داشته باشد. در صورتی که حجم فایل های لاگ شما زیاد است و بر روی سیستم شما پردازشی ایجاد می کند می توانید آنرا از این بخش هم غیرفعال کنید.

بخش Reset Log Files: با استفاده از این بخش شما می توانید همه فایل های لاگ را پاک کرده و در زمان انتخاب این گزینه شما پیغامی را به صورت زیر مشاهده می کنید که در بالای مرورگر وب شما نمایش داده می شود و در صورت تایید این پیغام همه فایل های لاگ شما پاک خواهد شد:



بخش Remote Logging Options:

از این گزینه شما می توانید در جهت ارسال لاگ های به سمت سرور syslog دیگری که در شبکه شما وجود دارد استفاده کنید که بعد از فعال کردن این بخش شما با زیر منوی زیر مواجه می شوید:

Remote Logging Options

Enable Remote Logging Send log messages to remote syslog server

Source Address Default (any)

This option will allow the logging daemon to bind to a single IP address, rather than all IP addresses. If a single IP is picked, remote syslog servers must all be of that IP type. To mix IPv4 and IPv6 remote syslog servers, bind to all interfaces.

NOTE: If an IP address cannot be located on the chosen interface, the daemon will bind to all addresses.

IP Protocol IPv4

This option is only used when a non-default address is chosen as the source above. This option only expresses a preference; If an IP address of the selected type is not found on the chosen interface, the other type will be tried.

Remote log servers IP[:port] IP[:port] IP[:port]

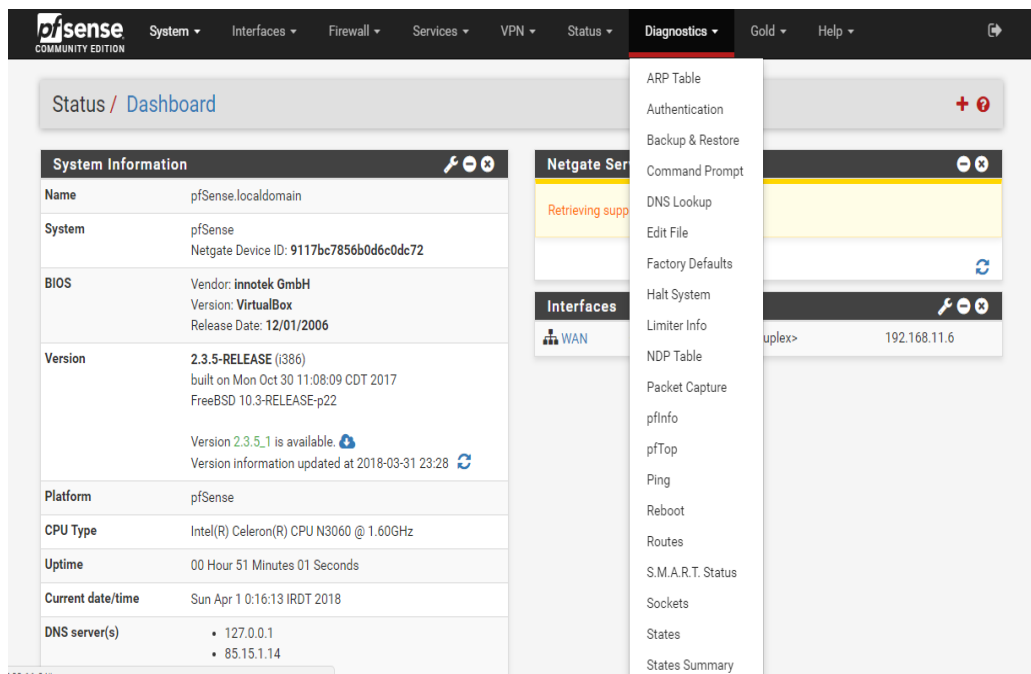
Remote Syslog Contents

- Everything
- System Events
- Firewall Events
- DNS Events (Resolver/unbound, Forwarder/dnsmasq, filterdns)
- DHCP Events (DHCP Daemon, DHCP Relay, DHCP Client)
- PPP Events (PPPoE WAN Client, L2TP WAN Client, PPTP WAN Client)
- Captive Portal Events
- VPN Events (IPsec, OpenVPN, L2TP, PPPoE Server)
- Gateway Monitor Events
- Routing Daemon Events (RADVD, UPnP, RIP, OSPF, BGP)
- Server Load Balancer Events (relayd)
- Network Time Protocol Events (NTP Daemon, NTP Client)
- Wireless Events (hostapd)

Syslog sends UDP datagrams to port 514 on the specified remote syslog server, unless another port is specified. Be sure to set syslogd on the remote

در بخش **Source Address** شما می توانید آدرس ip کارت شبکه ای را که قصد دارید از طریق آن گزارشات ارسال شود را مشخص کنید. در بخش بعدی شما می توانید ورژن 4 یا 6 بودن مورد استفاده برای ارسال را مشخص کنید. در قسمت **Remote log servers** شما می توانید آدرسهای ip سرور ها به همراه شماره پورت ها را مشخص کنید) شما در این بخش می توانید همزمان چندین سرور را مشخص کنید) در بخش **Remote Syslog Contents** شما می توانید محتوایی را که شما قصد دارید به سمت سرور ارسال شود را مشخص کنید.

سلام دوستان در این بخش شما با منوی عیب یابی یا همون **Diagnostics** آشنا می شوید که در حقیقت شما با استفاده از زیر منوی این بخش می توانید وضعیت بخشهای مختلف شبکه و سیستم را مشاهده کنید و در صورت نیاز تصمیمات لازم را در خصوص عیب یابی سیستم خود بگیرید، با استفاده این بخش شما می توانید از وضعیت فایروال خود **backup** گرفته و فایل های **backup** گرفته شده را هم بازگردانی کنید در بخش فرمانهای مقدماتی شما به بخشهای فرمانی این زیر منو ها آشنا شده اید در بخش پیش رو با رابط وبی این فرمان ها که در فایروال **pfSense** طراحی ایجاد و پیاده سازی شده است آشنا می شوید.



The screenshot shows the pfSense web interface. The top navigation bar includes 'System', 'Interfaces', 'Firewall', 'Services', 'VPN', 'Status', 'Diagnostics', 'Gold', and 'Help'. The 'Diagnostics' menu is open, showing options like 'ARP Table', 'Authentication', 'Backup & Restore', 'Command Prompt', 'DNS Lookup', 'Edit File', 'Factory Defaults', 'Halt System', 'Limiter Info', 'NDP Table', 'Packet Capture', 'pInfo', 'pTop', 'Ping', 'Reboot', 'Routes', 'S.M.A.R.T. Status', 'Sockets', 'States', and 'States Summary'. The main content area shows the 'Status / Dashboard' with a 'System Information' table.

| System Information | |
|--------------------|---|
| Name | pfSense.localdomain |
| System | pfSense Netgate Device ID: 9117bc7856b0d6c0dc72 |
| BIOS | Vendor: innotek GmbH Version: VirtualBox Release Date: 12/01/2006 |
| Version | 2.3.5-RELEASE (i386) built on Mon Oct 30 11:08:09 CDT 2017 FreeBSD 10.3-RELEASE-p22 Version 2.3.5_1 is available. Version information updated at 2018-03-31 23:28 |
| Platform | pfSense |
| CPU Type | Intel(R) Celeron(R) CPU N3060 @ 1.60GHz |
| Uptime | 00 Hour 51 Minutes 01 Seconds |
| Current date/time | Sun Apr 1 0:16:13 IRDT 2018 |
| DNS server(s) | <ul style="list-style-type: none"> 127.0.0.1 85.15.1.14 |

زیر منوی **ARP Table**:

در قسمت فرمانی شما با فرمان **arp** رو روشهای استفاده از آن آشنا شده اید در این بخش به صورت تحت وبی شما خروجی فرمان **arp** را مشاهده می کنید:

The screenshot shows the pfSense web interface. The top navigation bar includes System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, Gold, and Help. The main content area is titled "Diagnostics / ARP Table". Below the title is a table with the following data:

| Interface | IP address | MAC address | Hostname | Actions |
|-----------|-----------------|-------------------|----------|---------|
| WAN | 192.168.174.2 | 00:50:56:e5:ad:d4 | | |
| WAN | 192.168.174.1 | 00:50:56:c0:00:08 | | |
| WAN | 192.168.174.129 | 00:0c:29:b1:74:4f | | |
| WAN | 192.168.174.254 | 00:50:56:f1:49:d4 | | |

Below the table, there is a blue information banner that reads: "Local IPv6 peers use NDP instead of ARP."

زیر منوی Authentication:

شما می توانید روشهای مختلف Authentication را در فایروال pfSense راه اندازی کنید و برای چک کردن معتبر بودن نام کاربری و رمز عبور از این زیر منو استفاده کنید، بعد از وارد شدن به این بخش شما با بخش زیر مواجه می شوید.

The screenshot shows the pfSense web interface for the Authentication Test page. The top navigation bar is the same as in the previous screenshot. The main content area is titled "Diagnostics / Authentication". Below the title is a form for testing authentication:

Authentication Test

Authentication Server: Local Database (dropdown menu)
Select the authentication server to test against.

Username: Username (text input field)

Password: Password (text input field)

Test (button with a play icon)

شما نوع سرور این بخش را می توانید انتخاب کنید، اگر سرور را تنظیم نکرده باشید در این بخش فقط local Database را باید انتخاب کنید فقط کاربران محلی را می توانید چک کنید که امکان وارد شدن و یا عدم ورود به

سیستم را خواهند داشت، بعد از وارد کردن نام کاربری و رمزعبور با استفاده از کلید **test** می توانید صحت یک کاربر را تست کنید.

زیر منوی Backup & Restore:

ساختار **pfSense** بر اساس یک فایل **xml** کار می کند و همه تنظیمات را در قالب این فایل برای شما ذخیره می کند با استفاده از این روش **backup** گیری و **restore** کردن بسیار ساده و کم هزینه خواهد بود، در این زیر منوی شما می توانید به راحتی از این زیر منوی این کار را انجام دهید که در بخشی در این زمینه توضیحاتی بیان خواهیم کرد، در شکل زیر شما این زیر منو را مشاهده می کنید:

| Backup Configuration | |
|--|---|
| Backup area | All |
| Skip packages | <input type="checkbox"/> Do not backup package information. |
| Skip RRD data | <input checked="" type="checkbox"/> Do not backup RRD data (NOTE: RRD Data can consume 4+ megabytes of config.xml space!) |
| Encryption | <input type="checkbox"/> Encrypt this configuration file. |
| <input type="button" value="Download configuration as XML"/> | |
| Restore Backup | |
| Open a pfSense configuration XML file and click the button below to restore the configuration. | |
| Restore area | All |
| Configuration file | <input type="button" value="Choose File"/> No file chosen |
| Encryption | <input type="checkbox"/> Configuration file is encrypted. |
| <input type="button" value="Restore Configuration"/> | |
| The firewall will reboot after restoring the configuration. | |

زیر منوی Command Prompt:

شما با استفاده از رابط وبی هم می تونید فرمانهایی را که دوست دارید اجرا کنید، برای وارد شدن به این بخش کفایت که وارد این زیر منو شوید که در شکل زیر آنرا مشاهده می کنید:

Advanced Users Only

The capabilities offered here can be dangerous. No support is available. Use them at your own risk!

Execute Shell Command



Download File



Upload File

 No file chosen


Execute PHP Commands

این بخش شامل چهار زیر بخش است که در ادامه با همه آنها را توضیح خواهیم داد، در ابتدا بعد برای استفاده از این بخش به شما پیغامی داده شده که استفاده از این بخش فقط برای کاربران حرفه ای است و در صورت نداشتن دانش کافی از این بخش استفاده نکنید.

بخش اول درمخصوص اجرا کردن فرمان هایی است که شما در خط فرمان هم از آن استفاده کرده اید ، برای راه اندازی فرمان کافیست که در باکس command فرمان را وارد کنید و بعد بر روی execute کلیک کنید تا فرمان اجرا شده و خروجی بعد از بروز شدن صفحه در بالا باکس فرمان برای شما نمایش داده شود، در شکل زیر فرمان ps که برای نمایش پردازش های سیستم است را اجرا و خروجی را برای شما نمایش داده شده است:

Diagnostics / Command Prompt



Shell Output - ps

| PID | TT | STAT | TIME | COMMAND |
|-------|----|------|---------|-------------------------|
| 12868 | v0 | I+ | 0:00.72 | /bin/tcsh |
| 38736 | v0 | Is | 0:00.30 | login [pam] (login) |
| 38874 | v0 | I | 0:00.26 | -sh (sh) |
| 39148 | v0 | I | 0:00.00 | /bin/sh /etc/rc.initial |

Execute Shell Command



بعد از اجرا بخشی به نام Shell Output برای نمایش خروجی فرمان در صفحه اضافه می شود، با استفاده از کلید های زیرین بخش command شما می توانید باک فرمان را پاک کنید، فرمان ها را با دو کلید جهت چپ و راست تغییر داده (این بخش فرمان های اجرا شده را برای شما ذخیره کرده تا دیگر شما تایپ را انجام ندهید)، اکنونهای این بخش را شما در زیر مشاهده می کنید:



دو بخش دیگر از این قسمت برای دانلود کردن و آپلود کردن فایلها استفاده می شود، برای دانلود کردن فایلهای مختلف شما حتما باید مسیر کامل فایل را تایپ کنید و برای آپلود کردن شما باید فایل مورد نظر خود را انتخاب کنید و بعد از آپلود کردن فایل در زیر شاخه /tmp قرار می گیرد. در شکل زیر ما فایل rc.conf که در زیر شاخه etc قرار گرفته است را دانلود می کنیم:

Download File

`/etc/rc.conf`

Download

Upload File

No file chosen

Upload

Execute PHP Commands

Command

rc (1).conf ^

در شکل زیر هم با فایلی را آپلود کرده و بعد از اتمام مسیر این فایل را برای شما نمایش می دهد:

Uploaded file to /tmp/unins000.exe.

Upload File

No file chosen

Upload

در بخش پایانی از این قسمت هم شما می توانید فرمانهای موجود در php را اجرا کنید که بعد از اجرا کردن این بخش باکسی جداگانه برای نمایش جواب درخواست شما باز خواهد شد به صورت نمایش داده شده در شکل زیر :

PHP Response

Hello World!

Execute PHP Commands

```
print("Hello World!");
```

⚡ Execute Example: `print("Hello World!");`

زیر منوی DNS Lookup:

در بخش شما می توانید اطلاعات DNS هر دامنه ای را که می خواهید مشاهده کنید و از ابزارهای مثل ping و tracert هم به صورت تحت وب استفاده کنید، زیر منوی اولیه این بخش را در شکل زیر مشاهده میکنید:

Diagnostics / DNS Lookup ?

DNS Lookup

Hostname

🔍 Lookup

بعد از وارد کردن یک نام در بخش Hostname to look up و lookup کردن گزارشی به صورت نمایش داده می شود:

| Results | |
|--------------------------|-------------|
| Result | Record type |
| 172.217.23.206 | A |
| 2a00:1450:4005:80a::200e | AAAA |

| Timings | |
|---------------|------------|
| Name server | Query time |
| 127.0.0.1 | 3 msec |
| 192.168.174.2 | 80 msec |

| More Information | |
|--|--|
| Ping | |
| Traceroute | |
| NOTE: The following links are to external services, so their reliability cannot be guaranteed. | |
| IP WHOIS @ DNS Stuff | |
| IP Info @ DNS Stuff | |

در بخش Result گزارش این دامنه را مشاهده می کنید، در بخش Timings شما می توانید سرور هایی که از آن جستجو شده است را مشاهده می کنید. برای دریافت اطلاعات بیشتر شما می توانید از ابزارهای Ping و Traceroute استفاده کند دو منوی زیر هم اطلاعات کامل دامین مورد نظر شما را نمایش می دهند که البته اگر این لینکها در دسترس نباشد به pfsense مربوط نمی شود.

زیر منوی Edit File:

از این بخش هم به دقت استفاده کنید و فقط برای کاربران حرفه ای در نظر گرفته شده است. با استفاده از این زیر منو می توانید فایلهایی که بر روی فایروال خود دارید را ویرایش کنید برای شروع کفایت که مسیر کامل فایل را انتخاب کنید و فایل های متنی را در این ویرایشگر برای شما بارگذاری شود، در زمان وارد شدن به این بخش شما با بخشی به صورت زیر مواجه می شوید:

Diagnostics / Edit File ?

Advanced Users Only

The capabilities offered here can be dangerous. No support is available. Use them at your own risk!

Save / Load a File from the Filesystem

Path to file to be edited

اگر شما مسیر فایل مورد نظر را می دانید در بخش مسیر آنرا وارد کنید و از گزینه load استفاده کنید اگر شما مسیر را نمی دانید می توانید از بخش Browse استفاده کنید و فایل را باز کنید بعد از انتخاب کردن گزینه browse در کادر پایین شما همه فایلها و شاخه های موجود را مشاهده می کنید که می توانید با استفاده از کلیک کردن آنها را انتخاب کنید:

Save / Load a File from the Filesystem

Path to file to be edited

Load Browse Save GoTo Line #

- /
- .snap
- bin
- boot
- cf
- conf
- conf.default
- dev
- etc
- home
- lib
- libexec
- media
- mnt
- proc
- rescue
- root
- sbin
- scripts
- tmp
- usr
- var
- .cshrc
- profile

0.88 KiB
12 KB

حال یک فایل را انتخاب کنید، بعد از انتخاب فایل در کارد مورد نظر برای شما باز خواهد شد که در شکل زیر مشاهده می کنید:

Save / Load a File from the Filesystem

/var/etc/resolv.conf

Load Browse Save GoTo Line #

```
nameserver 127.0.0.1
search localdomain
nameserver 192.168.174.2
```

حال بعد از اعمال ویرایش شما می توانید از **Save** برای ذخیره کردن تغییرات استفاده کنید در صورتی که خطوط فایل شما زیاد باشد و شما قصد داشته باشید که به یک خط با شماره خاص مراجعه کنید می توانید از آیکون زیر برای این بخش استفاده کنید:

GoTo Line #

زیر منوی Factory Defaults

با استفاده از این زیر منو شما می توانید تنظیمات خود را به حالت اولیه بازگردانی کنید، این بخش هم از طریق منوی کنسول قابل اجراست، بعد از وارد شدن به این بخش شما با منوی به صورت زیر مواجه می شوید:

The screenshot shows the 'Diagnostics / Factory Defaults' page. It features a 'Factory Defaults Reset' section with a warning: 'Resetting the system to factory defaults will remove all user configuration and apply the following settings:'. A list of settings follows, including LAN IP address (192.168.1.1), DHCP server configuration, and admin credentials. At the bottom, there are two buttons: 'Factory Reset' (red) and 'Keep Configuration' (green).

برای ریست کردن بروی گزینه **factory Reset** کلیک کرده و در صورتی که قصد تغییر ندارید گزینه **keep Configuration** را انتخاب کنید که شما را وارد بخش داشبورد می کند، در بخش بالایی از این قسمت هم تغییراتی که در زمان این ریستارت اتفاق می افتد را برای شما نمایش می دهد.

زیر منوی Halt System

Halt برای خاموش کردن سیستم استفاده می شود که بعد از وارد شدن به این بخش شما با منوی به شکل زیر مواجه می شوید:

Diagnosics / Halt System ?

System Halt Confirmation

Click "Halt" to halt the system immediately, or "Cancel" to go to the system dashboard. (There will be a brief delay before the dashboard appears.)

برای خاموش کردن از halt استفاده کنید و برای رفتن به منوی داشبورد از cancel.

زیرمنوی Limiter Info:

Pfsense از قابلیت ipfw برای مدیریت کردن محدودیت ترافیک داده های شبکه استفاده می کند که از این بخش شما می توانید اطلاعات موجود در این بخش را مشاهده کنید:

Diagnosics / Limiter Info ? [icon] [icon]

Limiter Information

Limiters:
No limiters were found on this system.

بدلیل فعال نبودن این بخش شما هیچ گزارشی را در این قسمت مشاهده نمی کنید.

زیر منوی NDP Table:

این بخش مربوط به آدرس ip ورژن 6 است که در حقیقت همان قابلیتی که در arp برای نمایش هاست های فعال در شبکه lan را دارید با استفاده از این بخش هم می توانید اطلاعات هاست های موجود در شبکه را که از آدرس v6 از ip استفاده می کنند را مشاهده کنید:

Diagnosics / NDP Table ?

NDP Table

| IPv6 address | MAC address | Hostname | Interface | Expiration | Actions |
|------------------------------|-------------------|----------|-----------|------------|---------|
| fe80::20c:29ff:feb1:744f%le0 | 00:0c:29:b1:74:4f | | WAN | permanent | |

زیر منوی Packet Capture:

شما با استفاده از این بخش می توانید از قابلیت tcpdump برای کپچر کردن بسته ها در قالب وب استفاده کنید، این بخش شامل گزینه های زیر می باشد:

Diagnostics / Packet Capture ?

Packet Capture Options

Interface ▼
Select the interface on which to capture traffic.

Promiscuous Enable promiscuous mode
The packet capture will be performed using promiscuous mode.
 Note: Some network adapters do not support or work well in promiscuous mode.
 More: [Packet capture](#)

Address Family ▼
Select the type of traffic to be captured.

Protocol ▼
Select the protocol to capture, or 'Any'.

Host Address
This value is either the Source or Destination IP address or subnet in CIDR notation. The packet capture will look for this address in either field. Matching can be negated by preceding the value with '!'. Multiple IP addresses or CIDR subnets may be specified. Comma (',') separated values perform a boolean 'AND'. Separating with a pipe ('|') performs a boolean 'OR'. If this field is left blank, all packets on the specified interface will be captured.

Port
The port can be either the source or destination port. The packet capture will look for this port in either field. Leave blank if not filtering by port.

در این بخش شما می توانید کارت شبکه خود را انتخاب کنی، در بخش بعد برای اینکه کارت شبکه شما بسته ای را بروی شبکه ارسال نکند می توانید از حالت Promiscuous استفاده کنید، در قسمت Address Family شما می توانید از هر دو ورژن 4 و 6 آدرس ip استفاده کنید. در بخش پروتکل هم می توانید پروتکل های مختلف را انتخاب کنید.

بخش Host address و بخش port فقط برای ذخیره کردن یک هاست خاص استفاده می شود، در ادامه این بخش شما با گزینه های دیگری هم مواجه می شوید:

Packet Length

The Packet length is the number of bytes of each packet that will be captured. Default value is 0, which will capture the entire frame regardless of its size.

Count

This is the number of packets the packet capture will grab. Default value is 100. Enter 0 (zero) for no count limit.


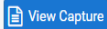

Level of detail

This is the level of detail that will be displayed after hitting "Stop" when the packets have been captured. This option does not affect the level of detail when downloading the packet capture.

Reverse DNS Lookup
 Do reverse DNS lookup

The packet capture will perform a reverse DNS lookup associated with all IP addresses. This option can cause delays for large packet captures.

در ادامه شما می توانید اندازه طول بسته و تعداد بسته ها را هم مشخص کنید که بعد از رسیدن به این دو مقدار عمل capture متوقف شود، شما می توانید از این بخش سطح دریافت اطلاعات را نیز مشخص کنید و از جستجوی نامی از طریق DNS را هم غیرفعال کنید. برای شروع به کار هم کافیست که بر روی start کلیک کنید تا بعد از رسیدن به حد تعیین شده گزارشی از بسته های دریافتی به صورت زیر نمایش داده شود:

 Start
 View Capture
 Download Capture

Packets Captured

```

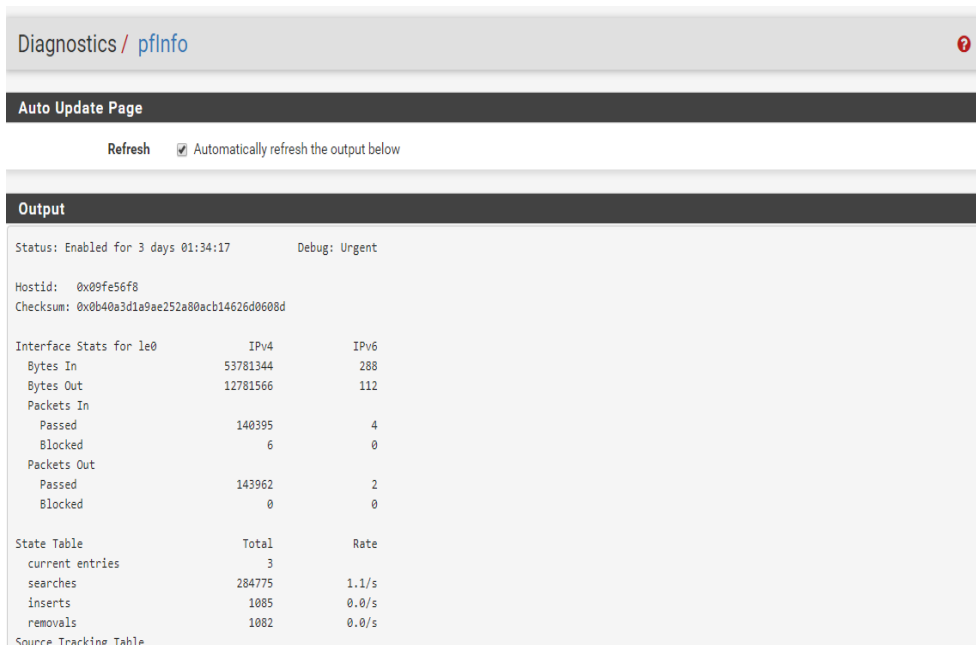
17:17:17.878732 IP 192.168.174.129 > 192.168.174.2: ICMP echo request, id 19226, seq 47158, length 8
17:17:17.906465 IP 192.168.174.129 > 192.168.174.2: ICMP echo request, id 51634, seq 5168, length 8
17:17:17.906581 IP 192.168.174.2 > 192.168.174.129: ICMP echo reply, id 19226, seq 47158, length 8
17:17:17.906694 IP 192.168.174.2 > 192.168.174.129: ICMP echo reply, id 51634, seq 5168, length 8
17:17:18.418651 IP 192.168.174.129 > 192.168.174.2: ICMP echo request, id 19226, seq 47159, length 8
17:17:18.418810 IP 192.168.174.129 > 192.168.174.2: ICMP echo request, id 51634, seq 5169, length 8
17:17:18.419004 IP 192.168.174.2 > 192.168.174.129: ICMP echo reply, id 19226, seq 47159, length 8
17:17:18.419064 IP 192.168.174.2 > 192.168.174.129: ICMP echo reply, id 51634, seq 5169, length 8
17:17:18.635367 ARP, Request who-has 192.168.174.2 tell 192.168.174.1, length 46
17:17:18.934694 IP 192.168.174.129 > 192.168.174.2: ICMP echo request, id 51634, seq 5170, length 8
17:17:18.935136 IP 192.168.174.2 > 192.168.174.129: ICMP echo reply, id 51634, seq 5170, length 8
17:17:18.935344 IP 192.168.174.129 > 192.168.174.2: ICMP echo request, id 19226, seq 47160, length 8
17:17:18.935911 IP 192.168.174.2 > 192.168.174.129: ICMP echo reply, id 19226, seq 47160, length 8
17:17:19.450679 IP 192.168.174.129 > 192.168.174.2: ICMP echo request, id 19226, seq 47161, length 8
17:17:19.450922 IP 192.168.174.129 > 192.168.174.2: ICMP echo request, id 51634, seq 5171, length 8
17:17:19.450987 IP 192.168.174.2 > 192.168.174.129: ICMP echo reply, id 19226, seq 47161, length 8
17:17:19.451075 IP 192.168.174.2 > 192.168.174.129: ICMP echo reply, id 51634, seq 5171, length 8
17:17:19.548033 ARP, Request who-has 192.168.174.2 tell 192.168.174.1, length 46
17:17:19.966122 IP 192.168.174.129 > 192.168.174.2: ICMP echo request, id 51634, seq 5172, length 8
17:17:19.966971 IP 192.168.174.2 > 192.168.174.129: ICMP echo reply, id 51634, seq 5172, length 8

```

شما می توانید فایل capture را دانلود کنید که در زمان مورد نیاز با برنامه هایی که برای این کار تهیه شده است مورد آنالیز قرار دهید.

زیر منوی pfInfo:

برای دریافت گزارش وضعیت از pf شما می توانید از این بخش استفاده کنید که در شکل زیر قسمت بالایی این گزارش را مشاهده می کنید:



The screenshot shows the pfSense Diagnostics / pfInfo page. It includes a 'Refresh' button and a checkbox for 'Automatically refresh the output below'. The main content area displays the following information:

```

Status: Enabled for 3 days 01:34:17      Debug: Urgent
Hostid: 0x09fe56f8
Checksum: 0x0b40a3d1a9ae252a80acb14626d0608d

Interface Stats for le0
  IPv4          IPv6
Bytes In       53781344      288
Bytes Out      12781566      112
Packets In
  Passed       140395        4
  Blocked      6             0
Packets Out
  Passed       143962        2
  Blocked      0             0

State Table
  Total      Rate
current entries 3
searches     284775  1.1/s
inserts      1085    0.0/s
removals     1082    0.0/s

Source Tracking Table
    
```

زیر منوی pfTop:

با فرمان pftop در بخش خط فرمان آشنا شده اید، این بخش را شما در این زیر منو در دسترس دارید و بعد از وارد شدن با تصویر زیر مواجه می شوید:

pfTop Configuration

View:

Sort by:

Maximum # of States:

Output

pfTop: Up State 1-5/5, View: default, Order: bytes

| PR | DIR | SRC | DEST | STATE | AGE | EXP | PKTS | BYTES |
|------|-----|-----------------------|---------------------|-------------------------|----------|----------|--------|---------|
| icmp | Out | 192.168.174.129:19226 | 192.168.174.2:19226 | 0:0 | 07:16:53 | 00:00:09 | 101777 | 2849756 |
| icmp | Out | 192.168.174.129:51634 | 192.168.174.2:51634 | 0:0 | 01:16:32 | 00:00:09 | 17840 | 499520 |
| tcp | In | 192.168.174.1:62835 | 192.168.174.129:443 | FIN_WAIT_2:FIN_WAIT_2 | 00:06:20 | 00:00:48 | 549 | 309565 |
| tcp | In | 192.168.174.1:62842 | 192.168.174.129:443 | ESTABLISHED:ESTABLISHED | 00:00:40 | 24:00:00 | 74 | 30095 |
| tcp | In | 192.168.174.1:62841 | 192.168.174.129:443 | FIN_WAIT_2:FIN_WAIT_2 | 00:00:40 | 00:00:50 | 12 | 1209 |

شما در بخش pfTop Configuration می توانید تغییراتی در نمایش بخش OutPut اعمال کنید.

زیر منوی ping:

شما برای ping کردن یک هاست می توانید از طریق خط فرمان، منوی کنسول و این زیر منوی در رابط وب هم استفاده کنید که در شکل زیر بخش اصلی این زیر منو را مشاهده می کنید:


Ping

Hostname:

IP Protocol:

Source address:
Select source address for the ping.

Maximum number of pings:
Select the maximum number of pings.



زیر منوی Reboot:

با استفاده این زیر منوی می توانید سیستم را راه اندازی مجدد کنید که این روش هم از طریق فرمان و هم منوی کنسول در دسترس است، در شکل زیر شما این زیر منو را مشاهده می کنید:

Diagnostics / Reboot ?
System Reboot Confirmation

Click "Reboot" to reboot the system immediately, or "Cancel" to go to the system dashboard without rebooting. (There will be a brief delay before the dashboard appears.)


زیر منوی Routes:

شما در این بخش می توانید وضعیت rout های موجودی که pfSense آنها را تشخیص داده است را مشاهده کنید:

Routing Table Display Options

Resolve names Enable

Enabling name resolution may cause the query to take longer. It can be stopped at any time by clicking the Stop button in the browser.

Rows to display

Filter

Use a regular expression to filter the tables.


IPv4 Routes

| Destination | Gateway | Flags | Use | Mtu | Netif | Expire |
|------------------|-------------------|-------|------|-------|-------|--------|
| default | 192.168.174.2 | UGS | 79 | 1500 | le0 | |
| 127.0.0.1 | link#6 | UH | 152 | 16384 | lo0 | |
| 192.168.174.0/24 | link#1 | U | 1133 | 1500 | le0 | |
| 192.168.174.2 | 00:0c:29:b1:74:4f | UHS | 3208 | 1500 | le0 | |
| 192.168.174.129 | link#1 | UHS | 0 | 16384 | lo0 | |

IPv6 Routes

| Destination | Gateway | Flags | Use | Mtu | Netif | Expire |
|---------------|---------|-------|-----|-------|-------|--------|
| ::1 | link#6 | UH | 2 | 16384 | lo0 | |
| fe80::%le0/64 | link#1 | U | 0 | 1500 | le0 | |

زیر منوی S.M.A.R.T. Status

اگر هارد سیستمی که بر روی آن pfSense را نصب کرده اید از قابلیت SMART در این بخش می‌توانید هارد خود را تست کنید، اطلاعات سخت افزاری آنرا چک کنید و در نهایت هاردی را که به آن احتیاج ندارید از سیستم خود جدا کنید، این زیر منو در شکل زیر نمایش داده شده است:

The screenshot shows the pfSense S.M.A.R.T. Status configuration page. It is divided into two main sections: "Information" and "Perform self-tests".

Information Section:

- Info type: Radio buttons for Info, Health, S.M.A.R.T. Capabilities (selected), Attributes, and All.
- Device: /dev/ ada0 (dropdown menu)
- View button (blue icon)

Perform self-tests Section:

- Test type: Radio buttons for Offline, Short (selected), Long, and Conveyance.
- Text: Select "Conveyance" for ATA disks only.
- Device: /dev/ ada0 (dropdown menu)
- Test button (blue icon)

زیر منوی States

در این بخش شما لیستی از وضعیت فعال ارتباط pfSense را مشاهده میکنید و می‌تواندی در بخش بالایی ان از قابلیت فیلتر کردن هم استفاده کنید، این بخش در شکل زیر قابل نمایش است:

Diagnostics / States / States

States **Reset States**

State Filter

Interface: all

Filter expression: Simple filter such as 192.168, v6, icmp or ESTABLISHED

Filter

States

| Interface | Protocol | Source (Original Source) -> Destination (Original Destination) | State | Packets | Bytes |
|-----------|----------|--|-------|---------------------|---------------------|
| WAN | icmp | 192.168.174.129:19226 -> 192.168.174.2:19226 | 0:0 | 55.565 K / 55.522 K | 1.48 MiB / 1.48 MiB |
| WAN | icmp | 192.168.174.129:51634 -> 192.168.174.2:51634 | 0:0 | 13.575 K / 13.575 K | 371 KiB / 371 KiB |

برای **Reset** کردن این وضعیت به بخش **reset states** در قسمت بالایی از این منو وارد شوید تا شکلی به صورت زیر برای شما باز می شود:

Diagnostics / States / **Reset States**

States **Reset States**

State reset options

State Table Reset the firewall state table

Resetting the state tables will remove all entries from the corresponding tables. This means that all open connections will be broken and will have to be re-established. This may be necessary after making substantial changes to the firewall and/or NAT rules, especially if there are IP protocol mappings (e.g. for PPTP or IPv6) with open connections.

The firewall will normally leave the state tables intact when changing rules.

NOTE: Resetting the firewall state table may cause the browser session to appear hung after clicking "Reset". Simply refresh the page to continue.

Reset

کافیست چک باکس **reset the firewall state table** را انتخاب کرده و بروی گزینه **Reset** کلیک کنید.

زیر منوی States Summary

در یک نگاه شما می توانید کل وضعیت ارتباطی موجود را مشاهده کنید ، این منو در شکل زیر نمایش داده شده است:

| Diagnostics / States Summary ? | | | | | |
|---|----------|----------|-----------------|--------------|-------------|
| By Source IP | | | | | |
| IP | # States | Protocol | Protocol counts | | |
| | | | # States | Source Ports | Dest. Ports |
| 192.168.174.1 | 5 | tcp | 5 | 5 | 1 |
| 192.168.174.129 | 2 | icmp | 2 | 2 | 2 |
| By Destination IP | | | | | |
| IP | # States | Protocol | Protocol counts | | |
| | | | # States | Source Ports | Dest. Ports |
| 192.168.174.2 | 2 | icmp | 2 | 2 | 2 |
| 192.168.174.129 | 5 | tcp | 5 | 5 | 1 |
| Total per IP | | | | | |
| IP | # States | Protocol | Protocol counts | | |
| | | | # States | Source Ports | Dest. Ports |
| 192.168.174.1 | 5 | tcp | 5 | 5 | 1 |
| 192.168.174.2 | 2 | icmp | 2 | 2 | 2 |
| 192.168.174.129 | 7 | icmp | 2 | 2 | 2 |

دسته بندی در چهار قالب است: Source IP ، Destination IP ، Per IP و IP Pair که هر کدام به تفکیک قابل نمایش است.

زیر منوی System Activity

شما در قسمتهای فرمانها با فرمان **top** آشنا شده اید که در این بخش این فرمان به صورت وبی هم برای شما نمایش داده می شود که خروجی این بخش به صورت زیر است:

Diagnostics / System Activity

CPU Activity

last pid: 53215; load averages: 0.18, 0.26, 0.21 up 0+08:04:29 18:36:32
 107 processes: 3 running, 88 sleeping, 16 waiting

Mem: 17M Active, 87M Inact, 89M Wired, 59M Buf, 277M Free
 Swap: 1024M Total, 1024M Free

| PID | USERNAME | PRI | NICE | SIZE | RES | STATE | TIME | WCPU | COMMAND |
|-------|----------|-----|------|--------|--------|--------|--------|--------|---|
| 11 | root | 155 | ki31 | 0K | 8K | RUN | 474:19 | 89.99% | [idle] |
| 300 | root | 39 | 0 | 65600K | 38856K | pipefd | 0:26 | 2.98% | php-fpm: pool nginx (php-fpm) |
| 12 | root | -60 | - | 0K | 128K | WAIT | 1:18 | 0.00% | [intr{swi4: clock}] |
| 12 | root | -92 | - | 0K | 128K | WAIT | 0:36 | 0.00% | [intr{irq19: le0}] |
| 19226 | root | 20 | 0 | 10632K | 1864K | nanslp | 0:35 | 0.00% | [dpinger{dpinger}] |
| 15 | root | -16 | - | 0K | 8K | - | 0:24 | 0.00% | [rand_harvestq] |
| 0 | root | -16 | - | 0K | 88K | swpin | 0:23 | 0.00% | [kernel{swapper}] |
| 301 | root | 52 | 0 | 61504K | 32528K | accept | 0:22 | 0.00% | php-fpm: pool nginx (php-fpm) |
| 4 | root | -16 | - | 0K | 16K | - | 0:19 | 0.00% | [cam{doneq0}] |
| 299 | root | 52 | 0 | 61504K | 34528K | accept | 0:16 | 0.00% | php-fpm: pool nginx (php-fpm) |
| 5 | root | -16 | - | 0K | 8K | pftm | 0:14 | 0.00% | [pf_purge] |
| 12 | root | -88 | - | 0K | 128K | WAIT | 0:11 | 0.00% | [intr{irq18: whci0 ehc}] |
| 27839 | root | 20 | 0 | 23952K | 6236K | kqread | 0:10 | 0.00% | nginx: worker process (nginx) |
| 51634 | root | 20 | 0 | 10632K | 1856K | nanslp | 0:10 | 0.00% | [dpinger{dpinger}] |
| 19 | root | 16 | - | 0K | 8K | syncer | 0:06 | 0.00% | [syncer] |
| 12 | root | -88 | - | 0K | 128K | WAIT | 0:06 | 0.00% | [intr{irq15: atal}] |
| 29146 | root | 20 | 0 | 13060K | 13092K | select | 0:05 | 0.00% | /usr/local/sbin/ntpd -g -c /var/etc/ntpd.conf |
| 27569 | root | 20 | 0 | 23952K | 6212K | kqread | 0:05 | 0.00% | nginx: worker process (nginx) |

زیر منوی Tables:

در pfSense قابلیت وجود دارد به نام tables که از آن برای ذخیره سازی مقادیر زیادی آدرس ip استفاده می شود که برای سهولت در اجرا و رول نویسی به کار می رود، در این زیر منو شما می توانید وضعیت این جدول را مشاهده کنید، در زیر این زیر منو را مشاهده می کنید:

Diagnostics / Tables

Table to Display

Table

Select a user-defined alias name or system table name to view its contents.

Aliases become Tables when loaded into the active firewall ruleset. The contents displayed on this page reflect the current addresses inside tables used by the firewall.

No entries exist in this table.

یک سری جدول پیش فرض در این بخش وجود دارد که چون این بخش در حال حاضر پیکربندی نشده است شما نمی توانید خروجی در این بخش را مشاهده کنید.

زیرمنوی Test Port:

یک برنامه ساده است که شما می توانید با استفاده از آن یک پورت خاص را مورد تست در دسترس بودن قرار دهید، این زیر منو را شما در شکل زیر مشاهده می کنید:

This page performs a simple TCP connection test to determine if a host is up and accepting connections on a given port. This test does not function for UDP since there is no way to reliably determine if a UDP port accepts connections in this manner.

| Test Port | |
|-------------------------------------|---|
| Hostname | <input type="text" value="Hostname to look up."/> |
| Port | <input type="text" value="Port to test."/> |
| Source Port | <input type="text" value="Typically left blank."/> |
| Remote text | <input type="checkbox"/> Show remote text Shows the text given by the server when connecting to the port. If checked it will take 10+ seconds to display in a panel below this form. |
| Source Address | <input type="text" value="Any"/> Select source address for the trace. |
| IP Protocol | <input type="text" value="IPv4"/> If IPv4 or IPv6 is forced and a hostname is used that does not contain a result using that protocol, it will result in an error. For example if IPv4 is forced and a hostname is used that only returns an AAAA IPv6 IP address, it will not work. |
| <input type="button" value="Test"/> | |

زیر منوی Traceroute:


آخرین زیر منوی که در این بخش وجود دارد و برای چک کردن مسیر بین فایروال شما و سیستم مقصد مورد نظر استفاده می شود. در شکل زیر شما این زیر منو را مشاهده می کنید:

Diagnostics / Traceroute



Traceroute

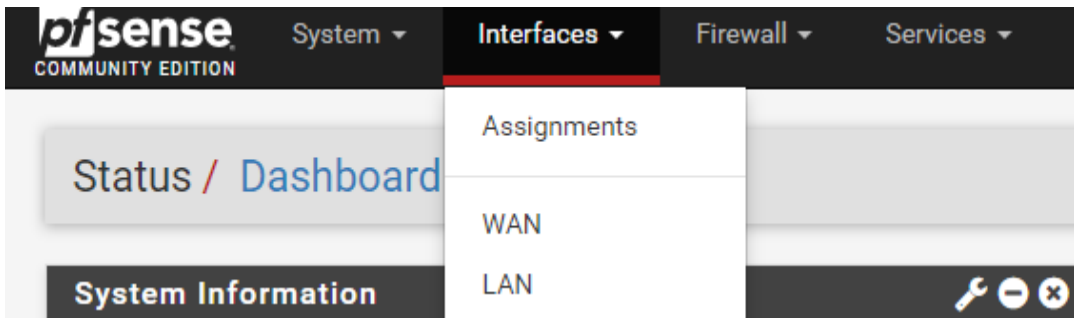
| | |
|------------------------|---|
| Hostname | <input type="text" value="yahoo.com"/> |
| IP Protocol | <input type="text" value="IPv4"/> Select the protocol to use. |
| Source Address | <input type="text" value="Any"/> Select source address for the trace. |
| Maximum number of hops | <input type="text" value="18"/> Select the maximum number of network hops to trace. |
| Reverse Address Lookup | <input type="checkbox"/> When checked, traceroute will attempt to perform a PTR lookup to locate hostnames for hops along the path. This will slow down the process as it has to wait for DNS replies. |
| Use ICMP | <input checked="" type="checkbox"/> By default, traceroute uses UDP but that may be blocked by some routers. Check this box to use ICMP instead, which may succeed. |

 Traceroute

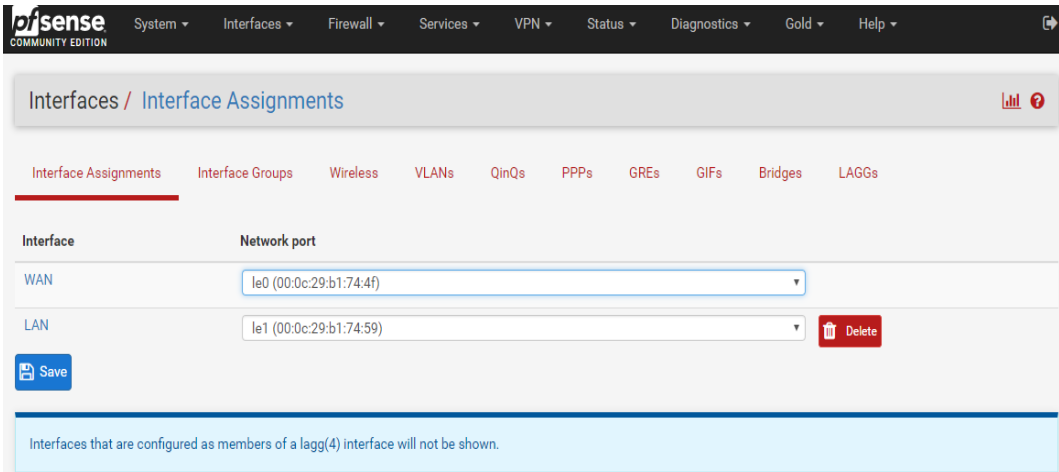
در برخی از مسیر یاب ها پروتکل UDP برای استفاده نکردن از این فرمان مسدود شده است که شما در بخش آخر می توانید از icmp برای این منظور استفاده کنید.

فصل ششم بخش کارت شبکه در رابط وب pfSense

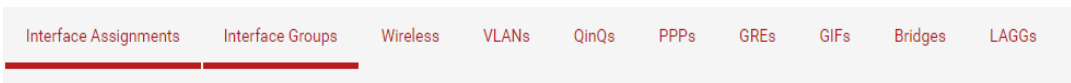
یکی از منوهای پر کاربرد در راه اندازی اولیه و یا در زمانی که شما قصد ایجاد تغییرات اساسی در ساختار شبکه ای خود را دارید منوی interface است که این منو خود شامل بخشهای زیر است:



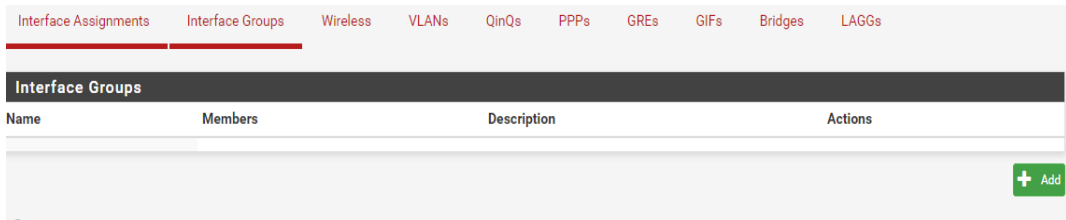
در زمان نصب کردن شما با روش تعیین کردن کارتهای شبکه lan و wan آشنا شده اید در بخش Assignments شما می توانید کارتهای شبکه قبلی خود را تغییر دهید و یا به آن کارتهای شبکه ای جدید اضافه کنید، در شکل زیر بخش Assignments نمایش داده شده است:




اگر pfSense کارتهای شبکه جدیدی را تشخیص دهد در این لیست برای شما نمایش داده می شود تا به ساختار آن اضافه شود. در این بخش شما آدرس mac هر کارت شبکه را مشاهده می کنید تا بتوانید تصمیم درستی در این زمینه بگیرید. برای پاک کردن هر کارت شبکه هم از لیست Assignments شما کافیست آنرا Delete کنید. همانطوری که مشاهده می کنید در این بخش شما گزینه های دیگری هم برای تنظیم کردن در اختیار دارید که در شکل زیر این منوها را مشاهده می کنید:



در این بخش با این منوی ها آشنا می شوید، در بخش اول گاهی شما نیاز دارید که یک سری تنظیمات به چندین کارت شبکه به صورت هم زمان اعمال شود، برای این منظور شما باید از گزینه Interface Groups استفاده کنید و کارتهای شبکه مورد نظر را در زیر یک لیست قرار دهید، در شکل زیر شما با این بخش آشنا می شوید:



برای شروع به کار در این بخش کافیست که بر روی  کلیک کنید تا منوی برای انتخاب کردن چندین کارت شبکه به صورت زیر برای شما باز شود:

Interfaces / Interface Groups / Edit 🔍 📄 ⓘ

Interface Group Configuration

| | |
|--------------------------|---|
| Group Name | <input type="text" value="Group Name"/> |
| | No numbers or spaces are allowed. Only characters: a-zA-Z |
| Group Description | <input type="text" value="Group Description"/> |
| | A group description may be entered here for administrative reference (not parsed). |
| Group Members | <input type="text" value="WAN"/> |
| | NOTE: Rules for WAN type interfaces in groups do not contain the reply-to mechanism upon which Multi-WAN typically relies. More Information |



در این بخش شما باید در ابتدا یک نام برای گروه خود انتخاب کنید تا در زمان نوشتن رو از آن استفاده کنید، برای توضیحات بیشتر هم می توانید از بخش توضیحات استفاده کنید و در کارد پایین می توانید کارتهای شبکه ای را که قصد دارید در یک گروه قرار دهید را انتخاب کرده و بعد save کنید.

بخش Wireless :

از ورژن 2.4 به بعد در pfSense شما برای تعریف کردن کارتهای شبکه بی سیم باید از این بخش اقدام کنید هم همانطوری که در شکل زیر مشاهده می کنید در این بخش یک کارت شبکه بی سیم اضافه شده است:

Interface Assignments Interface Groups **Wireless** VLANs QinQs PPPs GREs GIFs Bridges LAGGs

Wireless Interfaces

| Interface | Mode | Description | Actions |
|--------------|----------------------|-------------|---|
| urtwn0_wlan1 | Infrastructure (BSS) | |   |

اگر شما کارت شبکه بی سیمی بر روی سیستم داشته باشید با استفاده از کلید Add می توانید آنرا اضافه کنید تا در بخش Assignments بتوانید به سیستم آنرا اضافه کنید مثل بخش نمایش داده شده در شکل زیر:

Interfaces / Interface Assignments [Menu] [Help]

[Interface Assignments](#)
[Interface Groups](#)
[Wireless](#)
[VLANs](#)
[QinQs](#)
[PPPs](#)
[GREs](#)
[GIFs](#)
[Bridges](#)
[LAGGs](#)

| Interface | Network port |
|--------------------------|---|
| WAN | le0 (00:0c:29:b1:74:4f) ▼ |
| LAN | le1 (00:0c:29:b1:74:59) ▼ Delete |
| Available network ports: | urtwn0 (84:16:f9:1e:c3:26) ▼ + Add |

Save

بخش VLAN:

یکی از بخشهای موجود در pfSense استفاده کردن از قابلیت vlan و vlan trunk است که شما در این بخش می توانید کارتهای شبکه ای که قصد استفاده کردن از آنها را دارید در این بخش انتخاب کنید، منوی اولیه این بخش را در شکل زیر مشاهده می کنید:

Interfaces / VLANs [Menu] [Help]

[Interface Assignments](#)
[Interface Groups](#)
[Wireless](#)
[VLANs](#)
[QinQs](#)
[PPPs](#)
[GREs](#)
[GIFs](#)
[Bridges](#)
[LAGGs](#)

| VLAN Interfaces | | | | |
|--|----------|----------|-------------|---------|
| Interface | VLAN tag | Priority | Description | Actions |
| + Add | | | | |

i

برای اضافه کردن کارت شبکه بررروی گزینه Add کلیک کنید تا منوی به صورت شکل زیر برای شما باز شود تا تنظیمات کارت شبکه را وارد کنید:

Interfaces / VLANs / Edit 🔍 📄 ?

VLAN Configuration

Parent Interface ▼
Only VLAN capable interfaces will be shown.

VLAN Tag
802.1Q VLAN tag (between 1 and 4094).

VLAN Priority
802.1Q VLAN Priority (between 0 and 7).

Description
A group description may be entered here for administrative reference (not parsed).

بخش QinQ Interfaces

برای استفاده کردن از پروتکل 802.11q در ساختار vlan شما می توانید کارتهای شبکه این بخش را از این قسمت به pfSense معرفی کنید و به این نکته هم توجه داشته باشید که کارت شبکه شما باید از پروتکل پشتیبانی کند.

بخش PPP Interfaces

شما در pfSense می توانید از پرتکلهای ppp و pppoe برای برقراری ارتباط با مودم های خطوط DSL و غیره هم استفاده کنید از این بخش شما می توانید پرتکلهای مختلفی که برای استفاده از شبکه های pptp غیر استفاده می شوند را تنظیم کنید در شکل زیر شما این بخش را مشاهده می کنید :

PPP Configuration

Link Type

Link Interface(s)

Select at least two interfaces for Multilink (MLPPP) connections.

Description

A description may be entered here for administrative reference. Description will appear in the "Interfaces Assign" select lists.

Username

Password

Confirm

Service name Configure NULL service name

This field can usually be left empty. Service name will not be configured if this field is empty. Check the "Configure NULL" box to configure a blank Service name.

Advanced options

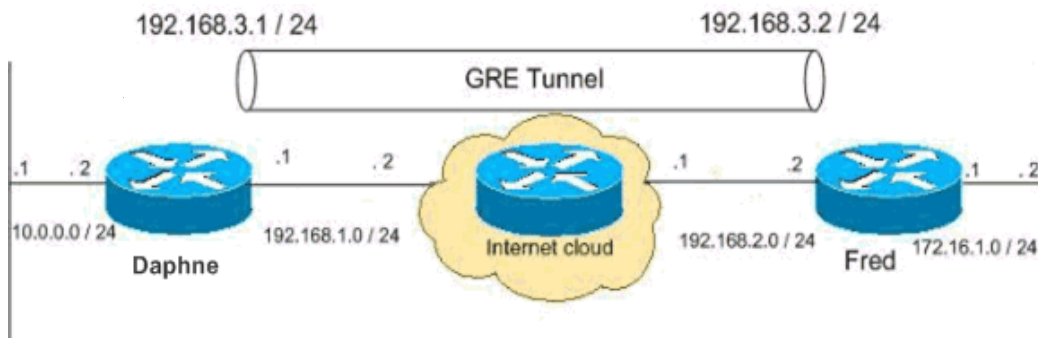
پروتکل‌هایی که در این بخش وجود دارد و pfSense از آنها پشتیبانی می‌کند شامل لیست زیر است:



Select at least two interfaces for Multilink (MLPPP) connections.

بخش GREs:

بسیاری از تولید کنندگان محصولات شبکه از تانل GREs برای انتقال اطلاعات مسیریابی استفاده می‌کنند و در شکل زیر این تانل را مشاهده می‌کنید:



در pfSense هم شما می توانید این تانل را ایجاد کنید که در شکل زیر منو های مختلف برای تنظیمات این تانل را مشاهده می کنید:

| GRE Configuration | |
|-------------------------------------|---|
| Parent Interface | WAN <small>This interface serves as the local address to be used for the GRE tunnel.</small> |
| GRE Remote Address | <input type="text"/> <small>Peer address where encapsulated GRE packets will be sent.</small> |
| GRE tunnel local address | <input type="text"/> <small>Local GRE tunnel endpoint.</small> |
| GRE tunnel remote address | <input type="text"/> <small>Remote GRE address endpoint.</small> |
| GRE tunnel subnet | 128 <small>The subnet is used for determining the network that is tunnelled.</small> |
| Add Static Route | <input type="checkbox"/> Add an explicit static route for the remote inner tunnel address/subnet via the local tunnel address |
| Description | <input type="text"/> <small>A description may be entered here for administrative reference (not parsed).</small> |
| <input type="button" value="Save"/> | |

بخش GIFs:

شما از GIFs برای تانل کردن اطلاعات برای دو پروتکل ورژن 6 و ورژن 4 از آدرس ip می توانید استفاده کنید، در این بخش شما به راحتی می توانید این تانل را ایجاد کنید که حداقل شما به دو سیستم در این بخش نیاز دارید، در این روش شما باید فیلدهای زیر را وارد کنید:

| GIF Configuration | |
|-------------------------------------|---|
| Parent Interface | WAN <small>This interface serves as the local address to be used for the GIF tunnel.</small> |
| GIF Remote Address | <input type="text"/> <small>Peer address where encapsulated gif packets will be sent.</small> |
| GIF tunnel local address | <input type="text"/> <small>Local gif tunnel endpoint.</small> |
| GIF tunnel remote address | <input type="text"/> <small>Remote GIF address endpoint.</small> |
| GIF tunnel subnet | 128 <small>The subnet is used for determining the network that is tunnelled.</small> |
| ECN friendly behavior | <input type="checkbox"/> ECN friendly behavior violates RFC2893. This should be used in mutual agreement with the peer. |
| Outer Source Filtering | <input type="checkbox"/> Disable automatic filtering of the outer GIF source which ensures a match with the configured remote peer. When disabled, martian and inbound filtering is not performed which allows asymmetric routing of the outer traffic. |
| Description | <input type="text"/> <small>A description may be entered here for administrative reference (not parsed).</small> |
| <input type="button" value="Save"/> | |

بخش Bridges:

با استفاده از این بخش شما می توانید دو یا چند کارت شبکه را در لایه دوم از شبکه به هم متصل کنید، بعد از وارد شدن به این بخش شما می توانید کارتهای شبکه را انتخاب کنید:

Interfaces / Bridges / Edit 🔍 📊 ⓘ

Bridge Configuration

Member Interfaces

Interfaces participating in the bridge.

Description

Advanced Options [⚙️ Display Advanced](#)

[💾 Save](#)

بخش LAGG:

در سیستم عامل FreeBSD قابلیت وجود دارد که شما می توانید با استفاده از آن چندین کارت شبکه را در یک گروه به صورت failover همدیگر در قالب یک کارت شبکه مجازی ایجاد کنید. در شکل زیر شما می توانید تنظیمات این بخش را مشاهده کنید:

LAGG Configuration

Parent Interfaces

Choose the members that will be used for the link aggregation.

LAGG Protocol

- **NONE**
This protocol is intended to do nothing: it disables any traffic without disabling the lagg interface itself.
- **LACP**
Supports the IEEE 802.3ad Link Aggregation Control Protocol (LACP) and the Marker Protocol. LACP will negotiate a set of aggregable links with the peer in to one or more Link Aggregated Groups. Each LAG is composed of ports of the same speed, set to full-duplex operation. The traffic will be balanced across the ports in the LAG with the greatest total speed, in most cases there will only be one LAG which contains all ports. In the event of changes in physical connectivity, Link Aggregation will quickly converge to a new configuration.
- **FAILOVER**
Sends and receives traffic only through the master port. If the master port becomes unavailable, the next active port is used. The first interface added is the master port; any interfaces added after that are used as failover devices.
- **FEC**
Supports Cisco EtherChannel. This is a static setup and does not negotiate aggregation with the peer or exchange frames to monitor the link.
- **LOADBALANCE**
Balances outgoing traffic across the active ports based on hashed protocol header information and accepts incoming traffic from any active port. This is a static setup and does not negotiate aggregation with the peer or exchange frames to monitor the link. The hash includes the Ethernet source and destination address, and, if available, the VLAN tag, and the IP source and destination address.
- **ROUNDROBIN**
Distributes outgoing traffic using a round-robin scheduler through all active ports and accepts incoming traffic from any active port.

Description

Enter a description here for reference only (Not parsed).

شما در این بخش می توانید از حالت‌های مختلف LAGG استفاده کنید که هر کدام به صورت مختصر در این بخش بیان شده است.

تنظیمات هر کارت شبکه

در زیر منوی **Interface** علاوه بر بخشی که به **Assignments** معروف است و برای دسته بندی کردن کارت‌های شبکه استفاده می شود شما می توانید هر کارت شبکه ای را که دارید را مدیریت کنید، به تعداد کارت‌های شبکه موجود در این بخش شما زیر منوی در اختیار خواهید داشت که با کلیک کردن بر روی هر کدام می توانید به تنظیمات هر کارت شبکه وارد شوید، در بخش زیر شما به قسمتهای مختلف آن آشنا می شوید.

به صورت کلی شما می توانید اطلاعات قابل تنظیم در این منو را به دسته های زیر تقسیم کنید:

- بخش **General Configuration**

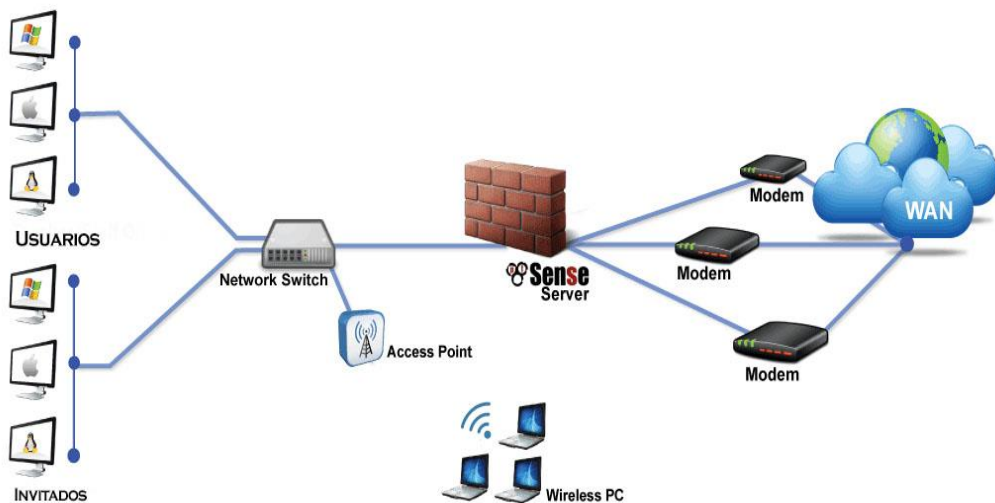
• بخش Reserved Networks

در صورت اعمال تنظیمات ip از طریق dhcp دو بخش زیر هم به این تنظیمان اضافه می شود:

- بخش DHCP6 Client Configuration
- بخش DHCP Client Configuration

تنظیمات کار شبکه Lan:

این کارت شبکه در بخش شبکه LAN شما قرار دارد، در شکل زیر شما یک طرح کلی از شبکه مبتنی بر Pfsense را مشاهده می کنید که در این طراحی مقدماتی هدف برقراری ارتباط بین شبکه درونی شما با شبکه بیرونی که اینترنت است می باشد با این هدف که نظارت بیشتری بر روی ترافیک و سطح دسترسی هر کاربر داشته باشید:



در این عکس نکته ای وجود دارد و آن این است که شما می توانید در Pfsense هم زمان از چند ارتباط اینترنتی استفاده کنید و pfsense آنها را برای استفاده کاربران lan مدیریت می کند. در ادامه شما با بخشهای پیکربندی

کارت شبکه Lan آشنا می شوید. بعد از وارد شدن به بخش lan شما با بخش هایی مواجه شده که در این بخش به صورت قسمت به قسمت توضیح داده خواهد شود، بخش General از این قسمت را در شکل مشاهده می کنید:

| General Configuration | |
|-------------------------|--|
| Enable | <input type="checkbox"/> Enable interface |
| Description | <input type="text" value="LAN"/> Enter a description (name) for the interface here. |
| IPv4 Configuration Type | <input type="text" value="None"/> |
| IPv6 Configuration Type | <input type="text" value="None"/> |
| MAC Address | <input type="text" value="xxxxxxxxxxxx"/> This field can be used to modify ("spoof") the MAC address of this interface. Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank. |
| MTU | <input type="text"/> If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances. |
| MSS | <input type="text"/> If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect. |
| Speed and Duplex | <input type="text" value="Default (no preference, typically autoselect)"/> Explicitly set speed and duplex mode for this interface. WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced. |

برای فعال فعال و غیر فعال کردن کارت های شبکه از بخش اول این قسمت استفاده کنید، در عکس بالا بخش enable تیک نخورده است و کارت شبکه lan در این قسمت غیرفعال است. در بخش توضیحات شما می توانید در مورد این کارت شبکه توضیح دهید که به صورت پیش فرض چون این بخش lan است در توضیحات هم Lan وارد شده است. اگر کارت شبکه شما در شبکه wan قرار داشته باشد این بخش wan نام گذاری شده است به صورت خودکار که شما می توانید آنرا تغییر دهید.

دو بخش در ادامه به نام های IPv4 Configuration Type و IPv6 Configuration Type دارد که شما می توانید نوع تنظیمات کارت شبکه را تنظیم کنید که در شکل زیر منوی ها آنرا مشاهده می کنید و با انتخاب کردن هر بخش شما در ادامه برای شما بخش مکملی باز می شود که شما می توانید به تناسب انتخاب خود کار را انجام دهید.

| | |
|-------------------------|---|
| IPv4 Configuration Type | None |
| IPv6 Configuration Type | None |
| MAC Address | Static IPv4 DHCP PPP PPPoE PPTP L2TP |

Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.

اگر در این بخش None را انتخاب کرده باشید در حقیقت هیچ تنظیمی برای کارت شبکه خود در نظر نگرفته اید. در ادامه بخشهای این قسمت را توضیح خواهیم داد. در بخش MAC Address شما می توانید آدرس مک هر کارت شبکه را برای انجام مقاصد خاصی تغییر دهید ،

در تنظیمات کارت شبکه در pfSense شما می توانید با تغییر در فیل MTU مقدار بیشتر سائز انتقال فایل را تغییر دهید که پیش فرض این بخش 1500 بایت است . در بخش MSS شما می توانید maximum segment size را هم مشخص و تنظیم کنید که این دو بخش برای تنظیمات حرفه شما.

یکی از قابلیت های کارت شبکه در سیستم عامل های مبتنی بر BSD این است که شما می توانید Speed and Duplex هر کارت شبکه را هم تعیین کنید که از این بخش قابل تنظیم است و شما می توانید حالت هایی را که در شکل زیر مشاهده می کنید را انتخاب کنید:

| | |
|------------------------|---|
| Speed and Duplex | Default (no preference, typically autoselect) |
| Reserved Networks | Default (no preference, typically autoselect) |
| Block private networks | Media Supported by this interface |
| loopback addresses | 10base5/AUI full-duplex |
| | 10base5/AUI |
| | 10baseT/UTP full-duplex |
| | 10baseT/UTP |
| | autoselect full-duplex |
| | autoselect |

RFC 4193 (fc00::/7) as well as loopback addresses (127/8). This option should generate private address space, too.

حالت پیش فرض این بخش به تناسب شبکه شما خود تنظیمات سرعت و روش ارسال و دریافت را تنظیم خواهد کرد که به صورت پیش فرض برای شما اعمال خواهد شد مگر شما قصد داشته باشید که آنرا دستی تغییر دهید.

بخش Reserved Networks:

در بخش اتنهایی از این صفحه شما می توانید به صورت خودکار ترافیکهای شبکه هایی که در RFC 1918 مشخص شده است را بلاک کنید که البته این تنظیمات در شبکه lan اعمال نمی شود و در شبکه wan اعمال می شود، این آدرسها شامل 10/8, 172.16/12, 192.168/16 هستند که شما می توانید تردد این آدرسها را مسدود کنید.



برای اعمال شدن تغییرات در این بخش شما باید از کلید استفاده کنید.

تنظیمات خاص آدرس IP هر بخش:

همانطوری که در بخش های قبل به آن اشاره کرده ایم شما برای تنظیم کردن آدرسهای ip کارت شبکه خود می توانید حالت های مختلفی را انتخاب کنید که در ادامه تنظیمات و منو های اضافه شده به این بخش را مرور خواهیم کرد، اگر شما حالت Static IPv4 را انتخاب کرده باشید بخشی در زیر تنظیمات کلی برای شما باز خواهد شد به نام Static IPv4 Configuration که منو های آنرا در شکل زیر مشاهده می کنید:

Static IPv4 Configuration

IPv4 Address / 32

IPv4 Upstream gateway None + Add a new gateway

If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button.
On local area network interfaces the upstream gateway should be "none". Gateways can be managed by [clicking here](#).

شما می توانید در این بخش به صورت دستی آدرس ip را تنظیم کنید و حتی gateway خود را هم تعیین کنید.

اگر شما در بخش قبل حالت DHCP را انتخاب کنید بخش جدید به نام DHCP Client Configuration برای شما اضافه می شود که در شکل زیر بخشهای آنرا مشاهده می کنید:

DHCP Client Configuration

Options Advanced Configuration Configuration Override

Use advanced DHCP configuration options. Override the configuration from this file.

Hostname

The value in this field is sent as the DHCP client identifier and hostname when requesting a DHCP lease. Some ISPs may require this (for client identification).

Alias IPv4 address /

The value in this field is used as a fixed alias IPv4 address by the DHCP client.

Reject leases from

To have the DHCP client reject offers from specific DHCP servers, enter their IP addresses here (separate multiple entries with a comma). This is useful for rejecting leases from cable modems that offer private IP addresses when they lose upstream sync.

در این بخش شما می توانید بخش **hostname** را انتخاب کنید تا در **DHCP** سرور نامی برای شما تنظیم شود. اگر بخش **Advanced Configuration** را انتخاب کنید بخش های دیگری به صورت زیر به تنظیمات شما اضافه می شود:

Protocol timing

Timeout Retry Select timeout Reboot Backoff cutoff Initial interval

Presets FreeBSD default Clear pfSense Default Saved Cfg

The values in these fields are DHCP protocol timings used when requesting a lease.
[See here more information](#)

شما در این بخش می توانید زمان هایی را که در **DHCP** استفاده می شود را تعیین کنید، اگر کارت شبکه شما از روش **ppp** برای دریافت کردن آدرس **ip** استفاده می کند بعد از انتخاب کردن این بخش شما با منوی زیر برای اعمال تنظیمات مواجه می شوید:

| PPP Configuration | |
|-------------------|---|
| Country | <input type="text"/> |
| Provider | <input type="text"/> |
| Plan | <input type="text"/> Select to fill in service provider data. |
| Username | <input type="text"/> |
| Password | <input type="password"/> Password <input type="password"/> Password Confirm |
| Phone number | <input type="text"/> Typically *99# for GSM networks and #777 for CDMA networks. |
| Access Point Name | <input type="text"/> |
| Modem port | <input type="text"/> None |
| Advanced PPP | <input type="button" value="Advanced PPP"/> Create a new PPP configuration. |

در بخش بعدی شما می توانید از pppoe برای دریافت ip استفاده کنید که این بخش هم به صورت زیر نمایش داده می شود:

| PPPoE Configuration | |
|---------------------|---|
| Username | <input type="text"/> |
| Password | <input type="password"/> *Password <input type="password"/> *Password Confirm |
| Service name | <input type="text"/> This field can usually be left empty. |
| Dial on demand | <input type="checkbox"/> Enable Dial-On-Demand mode |
| Idle timeout | <input type="text"/> If no qualifying outgoing packets are transmitted for the specified number of seconds, the connection is brought down. An idle timeout of zero disables this feature. |
| Periodic reset | <input type="text"/> Disabled Select a reset timing type. |
| Advanced and MLPPP | <input type="button" value="Advanced and MLPPP"/> Click for additional PPPoE configuration options. Save first if changes have been made. |

برای تنظیمات این بخش شما حتما باید نام کاربری و رمز عبور را وارد کنید.

دو روش PPTP/L2TP را هم شما می توانید انتخاب کنید که منوی به صورت شکل زیر برای شما باز خواهد شد تا شما بتوانید اطلاعات مورد نظر این بخش را وارد کنید:

PPTP/L2TP Configuration

| | | |
|-------------------------------|--|---|
| Username | <input type="text"/> | |
| Password | <input type="password" value="*Password"/> | <input type="password" value="*Password"/> Confirm |
| Local IP address | <input type="text"/> | / 128 ▾ |
| Remote IP address | <input type="text"/> | |
| Dial on demand | <input type="checkbox"/> Enable Dial-On-Demand mode <small>This option causes the interface to operate in dial-on-demand mode, allowing it to be a virtual full time connection. The interface is configured, but the actual connection of the link is delayed until qualifying outgoing traffic is detected.</small> | |
| Idle timeout (seconds) | <input type="text"/> <small>If no qualifying outgoing packets are transmitted for the specified number of seconds, the connection is brought down. An idle timeout of zero disables this feature.</small> | |
| Advanced and MLPPP | <input type="button" value="Advanced and MLPPP"/> | |

Click for additional PPTP and L2TP configuration options. Save first if changes have been made.

کارت شبکه در بخش wan هم دارای بخشهای بیان شده است با این تفاوت که در این بخش DHCP به صورت پیش فرض فعال است.

راه اندازی کردن ssh در pfsense

با فصل چهارم در خدمت شما دوستان عزیز و مشتاقان به استفاده از pfSense در خدمت شما دوستان هستیم، در این بخش قصد داریم که در خصوص راه اندازی کردن سرویسهای مهمی مثل DHCP DNS و NTP صحبت کنیم و در قدم اول روش فعال کردن و استفاده کردن از ssh یکی از راه های برقرار ارتباط با pfSense را برای شما بیان کنم.

راه اندازی کردن ssh در pfSense :

پروتکل ارتباطی ssh به صورت Client/Server کار می کند و هدف اصلی آن هم برقراری یک ارتباط امن از راه دور با سرور است، در بسیاری از موارد شما می توانید با استفاده از این خط فرمان راه دور امن با سیستم pfSense ارتباط برقرار کنید و اعمال مورد نیاز برای مدیریت کردن سیستم را انجام دهید. این راه اندازی خود به 3 بخش کلی تقسیم می شود، بخش اول راه اندازی کردن سرور ssh بخش دوم هم تولید کردن کلیده های مورد نیاز برای ارتباط و بخش پایانی هم ایجاد کردن کاربر برای دسترسی.

راه اندازی کردن سرور ssh:

سرور ssh را شما می توانید از دو طریق فعال کنید، روش اول در منوی کنسول بیان شده است و در روش دوم شما با استفاده از رابط وب این عمل را انجام می دهید، در ادامه با بخش راه اندازی از طریق رابط وب آشنا می شوید، ابتدا وارد رابط وب شوید و از منوی System بخش Advanced وارد شوید و بخش Secure Shell را پیدا کنید که این بخش را در شکل زیر مشاهده میکنید:

| Secure Shell | |
|-----------------------|---|
| Secure Shell Server | <input type="checkbox"/> Enable Secure Shell |
| Authentication Method | <input type="checkbox"/> Disable password login for Secure Shell (RSA/DSA key only) When enabled, authorized keys need to be configured for each user that has been granted secure shell access. |
| SSH port | <input type="text" value="22"/> Note: Leave this blank for the default of 22. |

این منو شامل سه گزینه است که با انتخاب کردن Enable Secure Shell شما می توانید ssh را فعال کنید. به صورت پیش فرض سرور ssh بر روی پورت 22 در شبکه به کاربران راه دور سرویس می دهد که برای بالا بر امنیت

سرور خود این شماره پورت را تغییر دهید و از اعداد بالاتر از 1024 استفاده کنید تا برنامه های اسکنر پورت به سرعت شماره پورت شما را پیدا کنند و بروی پورت شما حمله انجام ندهد، این بخش را شما می توانید با وارد کردن عددی در کادر زیر تغییر دهید:

SSH port

Note: Leave this blank for the default of 22.

شما به دو روش می توانید از ssh استفاده کنید، روش اول استفاده نام کاربری و رمز عبور است که در ادامه با روش ایجاد کردن کاربر برای استفاده از این روش در ssh و pfSense بیان خواهد شد و روش دوم استفاده از کلید برای برقراری ارتباط است، روش دوم یعنی استفاده از کلید دارای امنیت بالاتری است ولی شما باید کلید اصلی را در اختیار داشته باشید تا بتوانید از این روش استفاده کنید، برای غیرفعال کردن دسترسی از طریق رمز عبور و ورود از طریق کلید های نامتقارن RSA/DSA می توانید منوی زیر را انتخاب کنید و Save کنید:

Authentication Method Disable password login for Secure Shell (RSA/DSA key only)

When enabled, authorized keys need to be configured for each user that has been granted secure shell access.

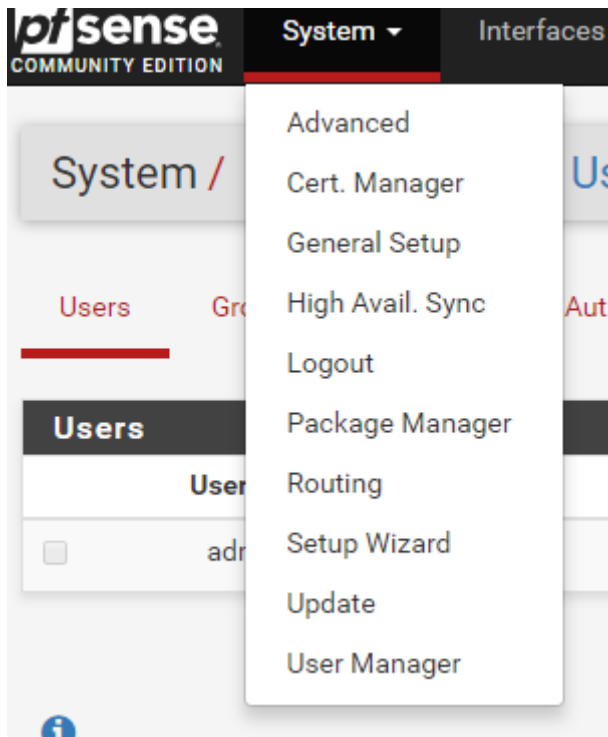
بعد از فعال کردن این سرویس وارد بخش Diagnostics شوید و زیر منوی Sockets را انتخاب کنید و دنبال sshd در خروجی این برنامه گشته تا مشاهده کنید که بروی چه پورتهی سرور ssh شما فعال شده است، این بخش را در شکل زیر مشاهده می کنید:

| | | | | | | |
|------|------|-------|---|------|------|----|
| root | sshd | 15005 | 5 | tcp4 | *:22 | ** |
|------|------|-------|---|------|------|----|

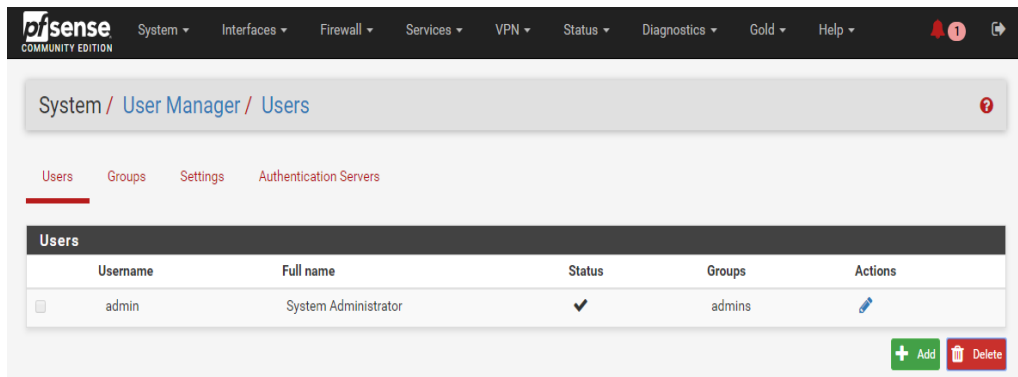
در خروجی بالا این سرور بروی همه آدرسهای IP و بروی پورت 22 فعال است.

روش اضافه کردن کاربر در Pfsense :

برای ادامه کار شما باید روش اضافه کردن کاربر آشنا شوید. برای وارد شده به بخش کاربری باید از منوی System وارد بخش User manager شوید که این منو را شما در شکل زیر مشاهده می کنید:



بعد از وارد شدن به این بخش شما با منویی به صورت زیر مواجه می شوید:



این بخش خود شامل زیر منوی های است به نام Users که همه کاربران را نمایش می دهد و بخش وردی به این قسمت است، بخش Groups که گروه های کاربران را نمایش میدهد و بخش setting که شما می توانید نوع

Authentication خود را تست و مشاهده کنید و در صورتی که شما علاوه بر روش دسترسی local قصد استفاده از سایر روش ها رو سرورها را دارید می توانید از بخش اخر استفاده کنید. این بخشها در ادامه توضیح داده خواهد شد.

بخش Users:

هر عمل و اقدامی را که شما قصد دارید انجام دهید نیاز به یک نام کاربری دارد که کاربر پیش فرض برای وارد شدن به سیستم کاربر admin است که شما در این بخش مشاهده می کنید که مدیر کل سیستم است و همه سطح دسترسی را دارد عضو گروه Admins است برای ویرایش کردن اطلاعات آن می توانید بروی بخش actions بروی مداد کلیک کنید تا منوی به صورت زیر برای شما نمایش داده شود که خود شامل بخشهای User Properties ، Effective Privileges ، User Certificates و Keys است که در شکل زیر شما بخش User Properties را مشاهده می کنید:

User Properties

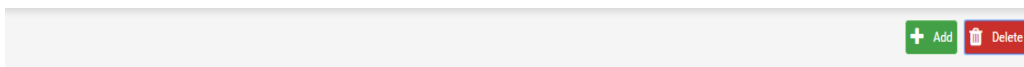
| | | |
|-------------------------|---|---|
| Defined by | SYSTEM | |
| Disabled | <input type="checkbox"/> This user cannot login | |
| Username | <input type="text" value="admin"/> | |
| Password | <input type="password" value="Password"/> | <input type="password" value="Confirm Password"/> |
| Full name | <input type="text" value="System Administrator"/> <small>User's full name, for administrative information only</small> | |
| Expiration date | <input type="text"/> <small>Leave blank if the account shouldn't expire, otherwise enter the expiration date as MM/DD/YYYY</small> | |
| Custom Settings | <input type="checkbox"/> Use individual customized GUI options and dashboard layout for this user. | |
| Group membership | <input type="text" value="Not member of"/> | <input type="text" value="admins"/> <small>Member of</small> |
| | <input type="button" value="» Move to 'Member of' list"/> | <input type="button" value="« Move to 'Not member of' list"/> |

Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.

این کاربر توسط سیستم ایجاد شده است و عضو گروه admins است. این کاربر به صورت پیش فرض در زمان نصب ایجاد شده است و شما می توانید رمزعبور آنرا از این بخش تغییر دهید، به این نکته هم توجه داشته باشید که برای

این کار باید رمز عبور را دوبار به صورت درست در بخش password وارد کنید، کاراکترهای این بخش برای شما نمایش داده نمی شود.

برای ایجاد کردن یک کاربر جدید کافیست که بعد از وارد شدن به بخش کاربر شما بر روی گزینه Add که در شکل زیر مشاهده می کنید کلیک کنید:



بعد از وارد شدن به این بخش منوی اضافه شدن کاربر برای شما نمایش داده می شود که در شکل زیر مشاهده می کنید که خود شامل دو بخش User Properties و Keys است . در شکل زیر بخش مشخصات کاربر را مشاهده می کنید:

User Properties

| | | |
|-------------------------|---|---|
| Defined by | USER | |
| Disabled | <input type="checkbox"/> This user cannot login | |
| Username | <input type="text"/> | |
| Password | <input type="password" value="Password"/> | <input type="password" value="Confirm Password"/> |
| Full name | <input type="text"/> | |
| | <small>User's full name, for administrative information only</small> | |
| Expiration date | <input type="text"/> | |
| | <small>Leave blank if the account shouldn't expire, otherwise enter the expiration date as MM/DD/YYYY</small> | |
| Custom Settings | <input type="checkbox"/> Use individual customized GUI options and dashboard layout for this user. | |
| Group membership | <input type="text" value="admins"/> | <input type="text"/> |
| | <small>Not member of</small> | <small>Member of</small> |
| | » Move to 'Member of' list | « Move to 'Not member of' list |
| | <small>Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.</small> | |
| Certificate | <input type="checkbox"/> Click to create a user certificate | |

در این قسمت از دسته‌ها می‌توانید یک کاربر را غیر فعال کنید که این بخش هم در زمان ایجاد کردن یک کاربر فعال است و هم در زمانی که شما قصد غیرفعال کردن یک کاربر را داشته باشید.

در کادر **username** نام کاربری که قصد ایجاد کردن آنرا دارید را وارد کنید که باید کاربر منحصر بفردی باشد، در کادر **password** هم باید به صورت دوبرابر پشت سر هم رمز عبور را وارد کنید که این دو فیلد اجباری است.

شما می‌توانید اسمی کامل برای کاربر وارد کنید و زمانی که قصد دارید کاربر غیرفعال شود را هم مشخص کنید.

اگر قصد دارید که تنظیمات نمایشی یک کاربر را هم تغییر دهید می‌توانید از گزینه **Custom Settings** استفاده کنید تا منویی به صورت شکل زیر برای شما باز شود تا بتوانید تم‌های ورود کاربر به سیستم را هم انتخاب کنید:

| | | | | |
|---|---|---|---|--|
| Custom Settings | <input checked="" type="checkbox"/> Use individual customized GUI options and dashboard layout for this user. | | | |
| Theme | pfSense ▼ <small>Choose an alternative css file (if installed) to change the appearance of the webConfigurator. css files are located in /usr/local/www/css/</small> | | | |
| Top Navigation | Scrolls with page ▼ <small>The fixed option is intended for large screens only.</small> | | | |
| Hostname in Menu | Default (No hostname) ▼ <small>Replaces the Help menu title in the Navbar with the system hostname or FQDN.</small> | | | |
| Dashboard Columns | 2 | | | |
| Interfaces Sort | <input type="checkbox"/> Sort Alphabetically <small>If selected, lists of interfaces will be sorted by description, otherwise they are listed wan,lan,optn...</small> | | | |
| Associated Panels Show/Hide | <input type="checkbox"/> Available Widgets <small>Show the Available Widgets panel on the Dashboard.</small> | <input type="checkbox"/> Log Filter <small>Show the Log Filter panel in System Logs.</small> | <input type="checkbox"/> Manage Log <small>Show the Manage Log panel in System Logs.</small> | <input type="checkbox"/> Monitoring Settings <small>Show the Settings panel in Status Monitoring.</small> |
| <small>These options allow certain panels to be automatically hidden on page load. A control is provided in the title bar to un-hide the panel.</small> | | | | |
| Left Column Labels | <input type="checkbox"/> Active <small>If selected, clicking a label in the left column will select/toggle the first item of the group.</small> | | | |
| Browser tab text | <input type="checkbox"/> Display page name first in browser tab <small>When this is unchecked, the browser tab shows the host name followed by the current page. Check this box to display the current page followed by the host name.</small> | | | |

این بخش در زمان ایجاد کردن یک کاربر اختیاری بوده و اجباری نیست.

در بخش Group membership شما می توانید کاربر را عضو گروه های دیگری کنید که به صورت پیش فرض فقط یک گروه Admins وجود دارد . با انتخاب کردن نام گروه و کلیک بر روی شکل زیر کاربر را به گروه اضافه کنید:

Not member of

» Move to "Member of" list

برای غیرفعال کردن عضویت هم کفایت که گروه های سمت چپ را انتخاب کنید و از گزینه زیر استفاده کنید:

Member of

« Move to "Not member of" list

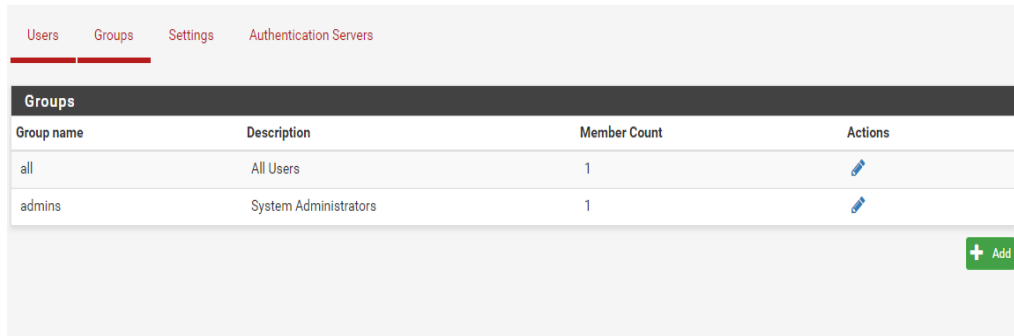
در بخش Keys شما می توانید کلید هایی که یک کاربر برای اتصال به آن نیاز دارد را مشخص کنید که در شکل زیر این بخش را مشاهده می کنید:

| Keys | |
|----------------------|---|
| Authorized SSH Keys | <input type="text"/> |
| | Enter authorized SSH keys for this user |
| IPsec Pre-Shared Key | <input type="text"/> |



در بخش Authorized SSH Keys شما باید کلید مربوط به ssh کاربر را وارد کنید که در این بخش به آن نیاز دارید و در بخش IPsec Pre-Shared Key شما می توانید از کلید ipsec این بخش استفاده کنید.

اضافه کردن گروه در pfSense:

در pfSense ما دو گروه کلی و عمده داریم که بعد از وارد شدن به بخش گروه‌ها شما منویی به صورت زیر را مشاهده می‌کنید که مشخصات گروه‌ها را می‌بینید:



The screenshot shows the pfSense web interface with the 'Groups' tab selected. It displays a table with the following data:

| Group name | Description | Member Count | Actions |
|------------|-----------------------|--------------|--|
| all | All Users | 1 |  |
| admins | System Administrators | 1 |  |

At the bottom right of the table, there is a green '+ Add' button.

گروهی به نام **all** وجود دارد که همه کاربران در آن قرار می‌گیرند و گروهی هم به نام **Admins** به صورت پیش فرض هست که مدیران فایروال pfSense را می‌توانید در این گروه قرار دهید و کاربر **Admin** هم یکی از اعضای این گروه است. در بخش **member count** شما تعداد کاربرانی که در هر گروه وجود دارد را مشاهده می‌کنید. برای اضافه کردن یک گروه اضافی کافیست که بر روی **add** کلیک کنید تا منوی جدید به صورت زیر برای شما باز شود:

Users **Groups** Settings Authentication Servers

Group Properties

Group name

Scope Local

Description
Group description, for administrative information only

Group membership

admin

Not members Members

» Move to "Members" « Move to "Not members"

Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.

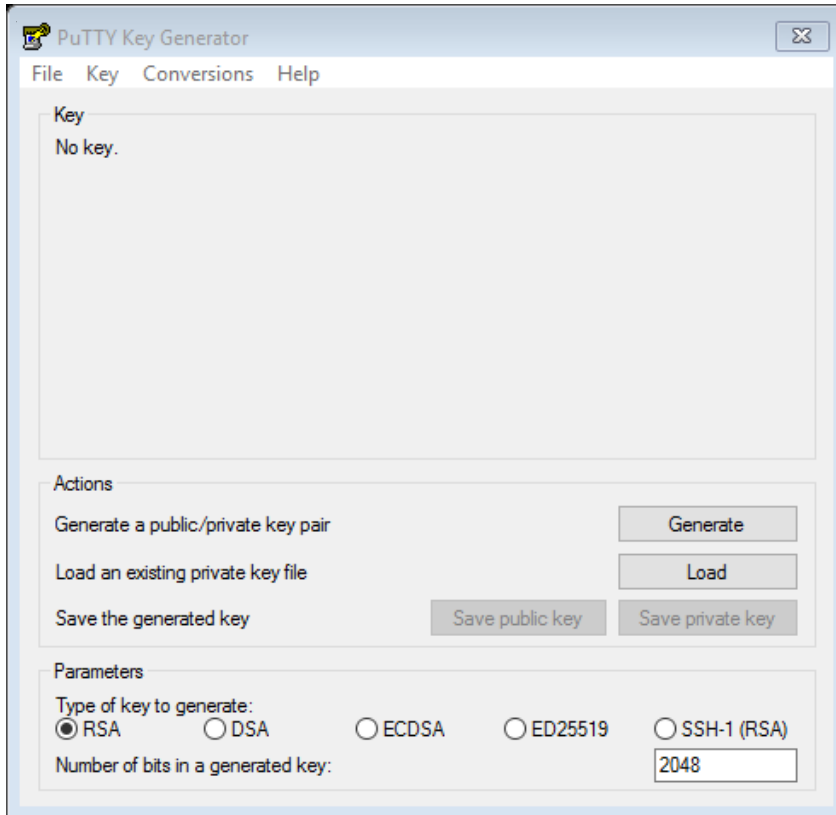
برای تعریف کردن گروه شما باید دو بخش اجباری آنرا حتما وارد کنید یکی بخش مربوط به نام گروه است و دیگری Scope گروه است. در بخش توضیحات شما می توانید توضیحاتی را وارد کنید و می توانید با استفاده از بخش Group Membership اعضای گروه را مشخص کنید که در این بخش شما نام کاربران را مشاهده می کنید.

اتصال به Pfsense از طریق کلید در ssh:

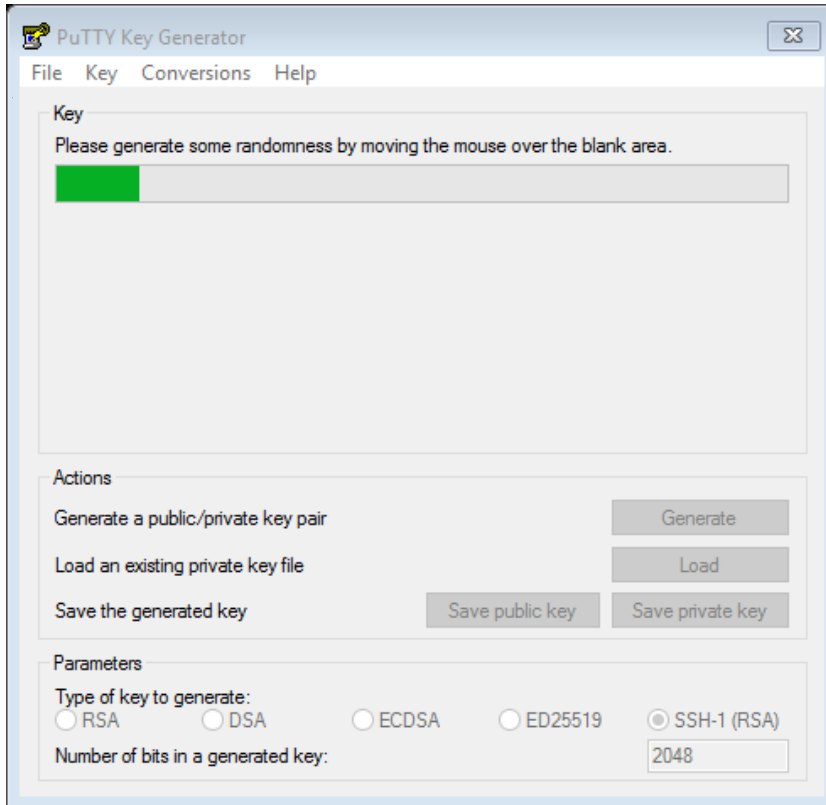
تا این بخش شما با فعال کردن ssh و روش ایجاد کردن کاربر در آن آشنا شدید، در این قسمت قصد دارم که روش برقرار اتصال از طریق کلیده های عمومی و خصوصی را به سرور ssh موجود در pfsense را برای شما بیان کنم. در قدم اول فرض بر این است که شما از سیستم عامل ویندوز برای اتصال استفاده می کنید و به دلیل اینکه در این سیستم عامل قابلیت ssh به صورت پیش فرض وجود دارد و شما باید از برنامه های جانبی استفاده کنید در این قسمت با یک برنامه معروف به نام putty آشنا می شوید که یکی از پرکاربردترین برنامه ها برای مدیریت کردن سرور های لینوکسی از طریق سیستم عامل ویندوز با استفاده از ssh است. این برنامه را می توانید از سایت <https://www.putty.org> دانلود کنید.

در این قسمت در بخش اول شما نیاز به ایجاد کردن کلیده های ارتباطی دارید که برای اینکار باید برنامه (puttygen.exe (a RSA and DSA key generation utility را دانلود کنید.

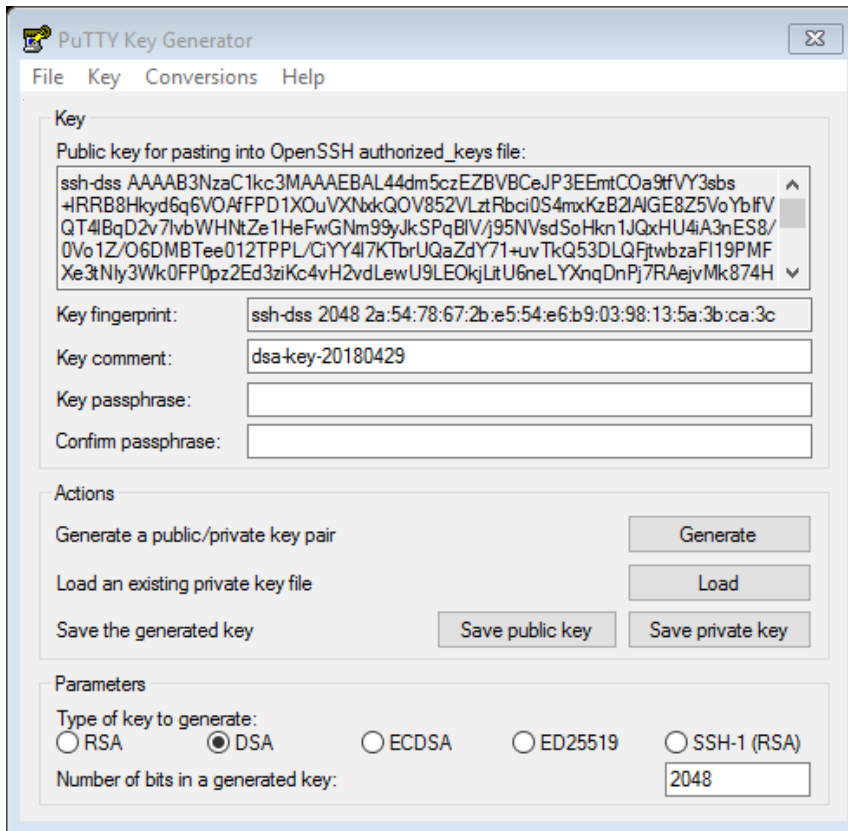
بعد دانلود کردن این بخش شما با اجرا این نرم افزار وارد محیط زیر می شوید:



همانطوری که مشاهده می کنید در این برنامه فعلا هیچ کلیدی وجود ندارد. یکی از بهترین کلید های که شما می توانید از ان استفاده کنید ssh-1(rsa) است . در بخش actions شما می توانید دو عمل انجام دهید برای تولید کردن کلید از Generate استفاده کنید و برای باز کردن کلید های موجود و نمایش کلید عمومی و خصوصی از Load استفاده کنید، در این بخش ما قصد داریم اولین کلید را ایجاد کنیم که باید بعد از انتخاب کردن نوع آن بر روی Generate کلیک کنید تا همانطوری که مشاهده می کنید یک نمایش بار به صورت زیر برای شما در صفحه نمایش داده شود و کلید مورد نظر شما ایجاد شود ، این بخش را در شکل زیر مشاهده می کنید:



این برنامه برای ایجاد کردن کلیدها یک مدت زمانی طول می کشد که بسته به نوع کلیدی که شما انتخاب کرده اید می توانید متغییر باشد بعد از اتمام ای بخش شما با شکل زیر مواجه می شوید:



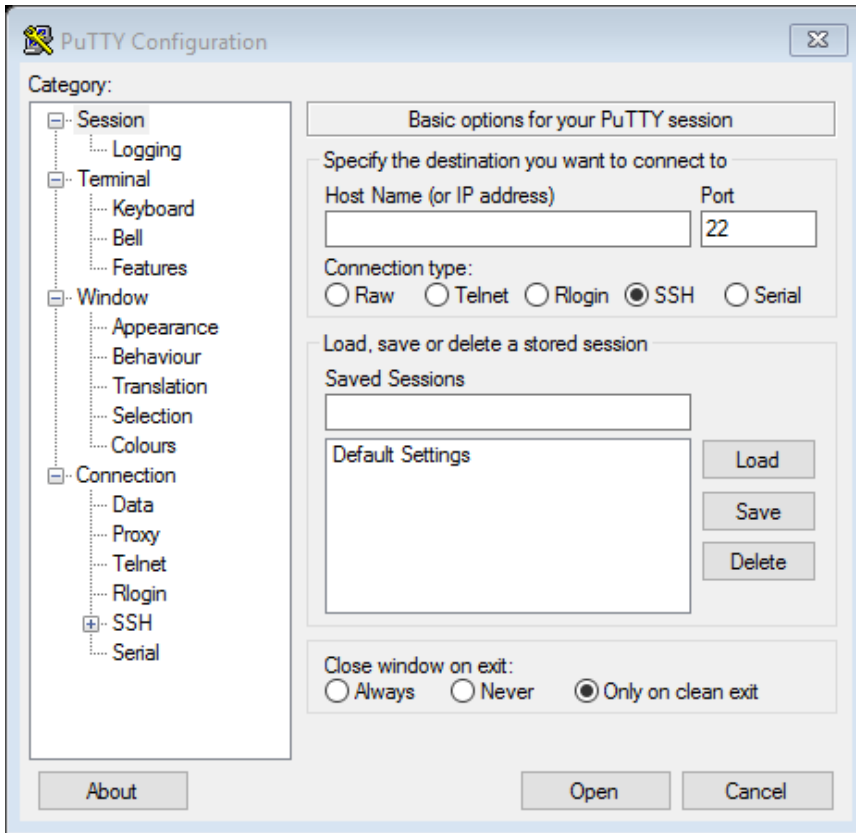
در این بخش کلید public را مشاهده می کنید و برای اتصال به سرور هم fingerprint را هم مشاهده میکنید .
بخش Save کردن شما می توانید کلید public و private راه هم ذخیره کنید، کلید private را در محلی امن
ذخیره کنید. در مرحله بعد باید کلید ایجاد شده و نمایش داده شده است را کپی کنید و در بخش کاربر آنرا کپی کنی
به صورت زیر :

Authorized SSH Keys

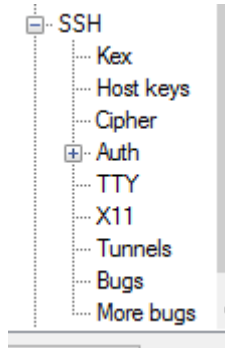
```
ssh-dss
AAAAB3NzaC1kc3MAAAEBAL44dm5czEZBVBCeJP3EEmtCOa9tfVY3sb
s+IRRB8Hkyd6q6VOAfFPD1XOuVXNkQOV852VLztRbc10S4mxKzB21
A1GE8Z5VoYbIFVQT41BqD2v7IvbWHntZe1HeFwGNm99yJkSPqB1V/j
95WsdSoHkn1JQxHU4iA3nES8/0Vo1Z/06DMBTee012TPPL/CiYY41
```

Enter authorized SSH keys for this user

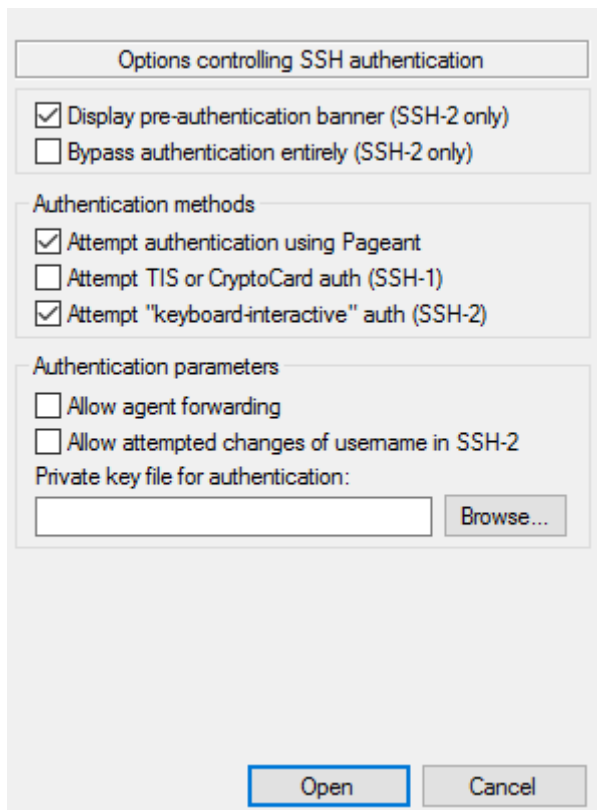
در مرحله بعد شما باید از برنامه putty استفاده کنید برای اتصال به سرور در این بخش شما نیاز به کلید private و آدرس ip سرور و شماره پورت فعال سرور ssh برروی سرور دارید که همه این بخش ها را باید در برنامه زیر وارد کنید بعد از دانلود کردن این برنامه و اجرا کردن آن شما وارد صفحه این برنامه می شوید به صورت زیر:



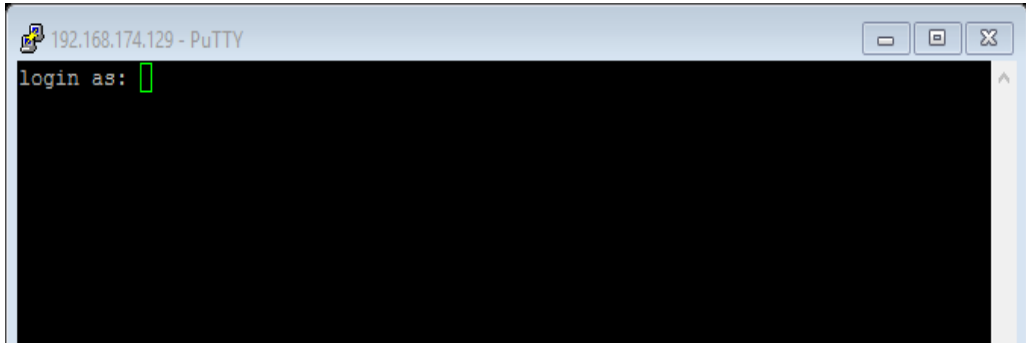
در باکس Host name نام و یا آدرس ip سرور را وارد کنید در باکس port شماره پورت را وارد کنید، در منوی سمت راست برنامه در زیر منوی Connection وارد بخش SSH شوید تا با منوی زیر مواجه شوید:



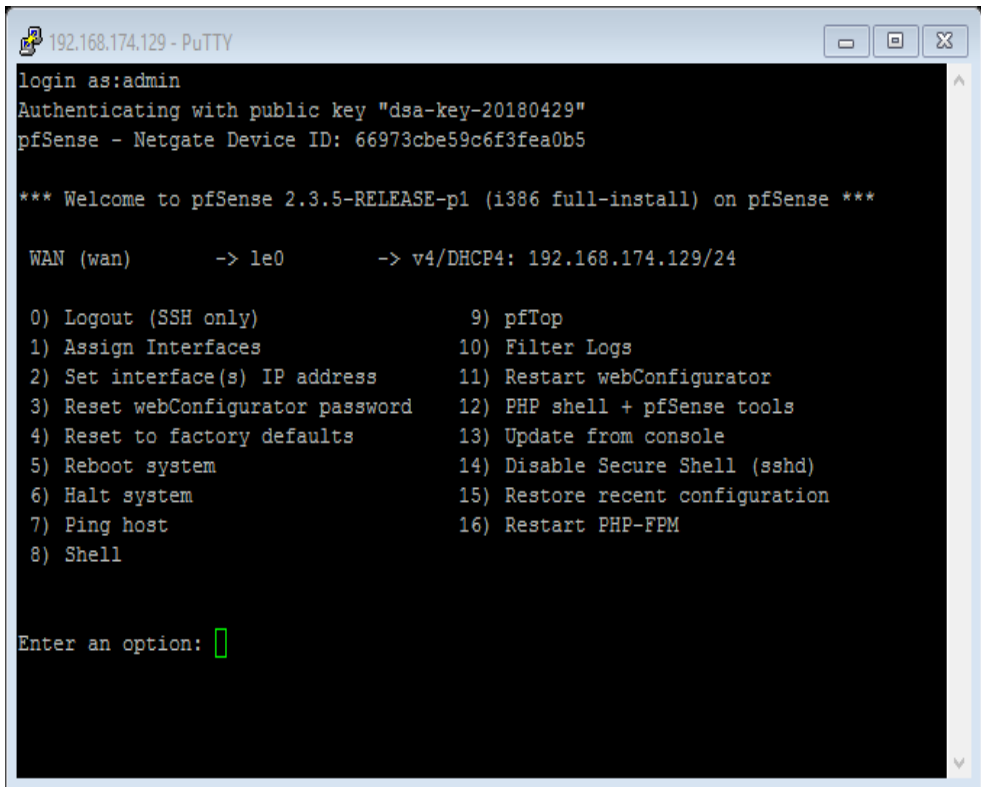
وارد زیر منوی Auth شوید تا بخش سمت راست به صورت زیر برای شما تغییر پیدا کند:



در مقابل باکس Private key file for authentication کلید را Browse کنید و مسیر فایل کلید را انتخاب کنید، بعد بخش Open را کلیک کنید تا صفحه اتصال به سرور برای شما باز شود:



در مقابل نام کاربری اسم کاربر را که کلید را بر روی پروفایلش ست کردین را وارد کنید و بعد از Enter کردن کلید به سمت سرور ارسال شده و بدون وارد کردن رمزعبور شما به سرور متصل می شود که در شکل زیر منوی کنسول pfSense را مشاهده می کنید:



```
192.168.174.129 - PuTTY
login as:admin
Authenticating with public key "dsa-key-20180429"
pfSense - Netgate Device ID: 66973cbe59c6f3fea0b5

*** Welcome to pfSense 2.3.5-RELEASE-p1 (i386 full-install) on pfSense ***

WAN (wan)      -> le0      -> v4/DHCP4: 192.168.174.129/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults    13) Update from console
5) Reboot system              14) Disable Secure Shell (sshd)
6) Halt system                15) Restore recent configuration
7) Ping host                  16) Restart PHP-FPM
8) Shell

Enter an option: █
```

همان طوری که مشاهده می کنید شما به سرور متصل شده اید و با انتخاب کردن منوی 0 می توانید ارتباط خود را قطع کنید.

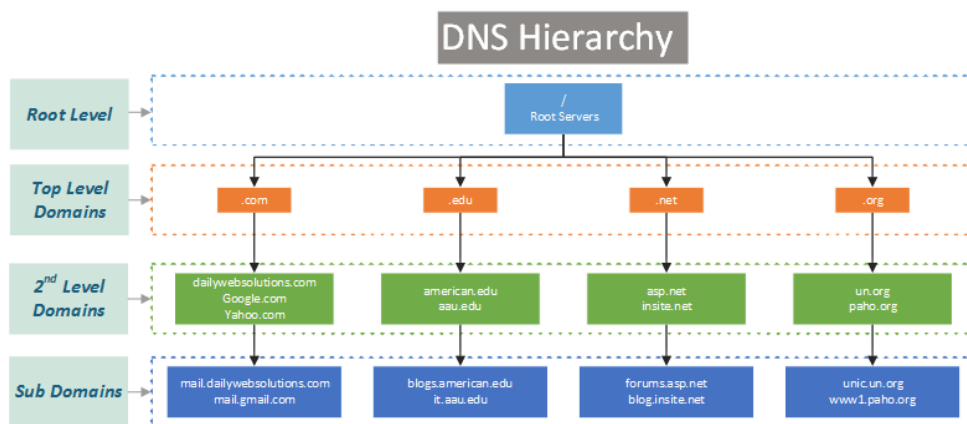
راه اندازی کردن DNS در pfSense

راهاندازی سرور DNS در Pfsense

در این بخش شما با راهاندازی کردن سرور DNS در pfsense آشنا می‌شوید. یکی از سرویس‌های مهم در شبکه اینترنت که باعث برقرار ارتباط شما با سایت‌های مختلف می‌شود سرور DNS است که داشتن یک سرور DNS در شبکه علاوه بر کاهش ترافیک‌های این سرویس، سرعت شما را هم در باز کردن سایت‌های مختلف بالا می‌برد. در تنظیمات شبکه هر سیستمی شما می‌توانید دو آدرس مربوط به سرورهای DNS معروف دنیا را وارد کنید تا از طریق آن‌ها بتوانید عمل تبدیل کردن نام به آدرس IP را برای برقرار کردن ارتباط با سرویس‌های مختلف در شبکه را انجام دهید. در ادامه این بخش شما با ساختار و روش جستجوی اسمی در اینترنت آشنا می‌شوید.

ساختار سلسله مراتبی سرورهای DNS:

ساختار موجود در شبکه جهانی برای استفاده کرده از سرویس DSN به صورت سلسله مراتبی است و در شکل زیر شما با نمایی از این ساختار آشنا می‌شوید:



همه چیز از سرور root شروع می‌شود که به نقطه یا (.) معروف است، تعداد این سرورها در اینترنت مشخص است و آدرس‌های IP خاصی دارند که به صورت فراگیر در شبکه جهانی اینترنت وجود دارند. در رده دوم از این بخش اول نام دامنه قرار دارد که به صورت 3 حرفی برای دامنه‌های معروف و به صورت دوحرفی برای هر کشور در نظری گرفته شده است برای مثال .com. برای ثبت دامنه‌های تجاری استفاده می‌شود و .ir هم برای دامنه‌هایی که در کشور ایران است

استفاده می‌شود، وظیفه فروش و مدیریت کردن دامنه‌های هر کشور به عهده همان کشور است. در این سطح شما می‌توانید بخش دولتی و شخصی نام هر دامنه را جدا کنید.

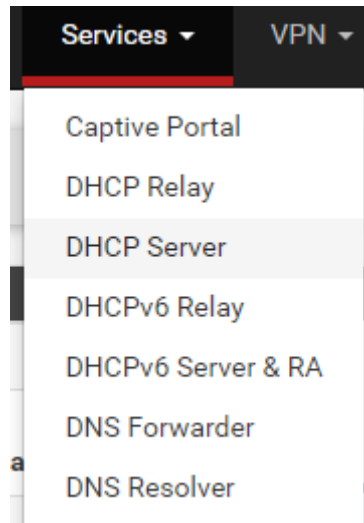
در سطح دوم یک نام وجود دارد که این نام خاص و منحصر به فرد است و برای شخصی که درخواست می‌شود ثبت شده و برای خرید آن هزینه پرداخت می‌کند. در ادامه همین نام شما می‌توانید Sub Domain هم ایجاد کرده و نام اصلی خود را به زیر دامنه‌ها خاص هم تقسیم‌بندی کنید، این ساختار کلی نام دهی در اینترنت است.

راه‌اندازی کردن سرور DNS در pfSense:

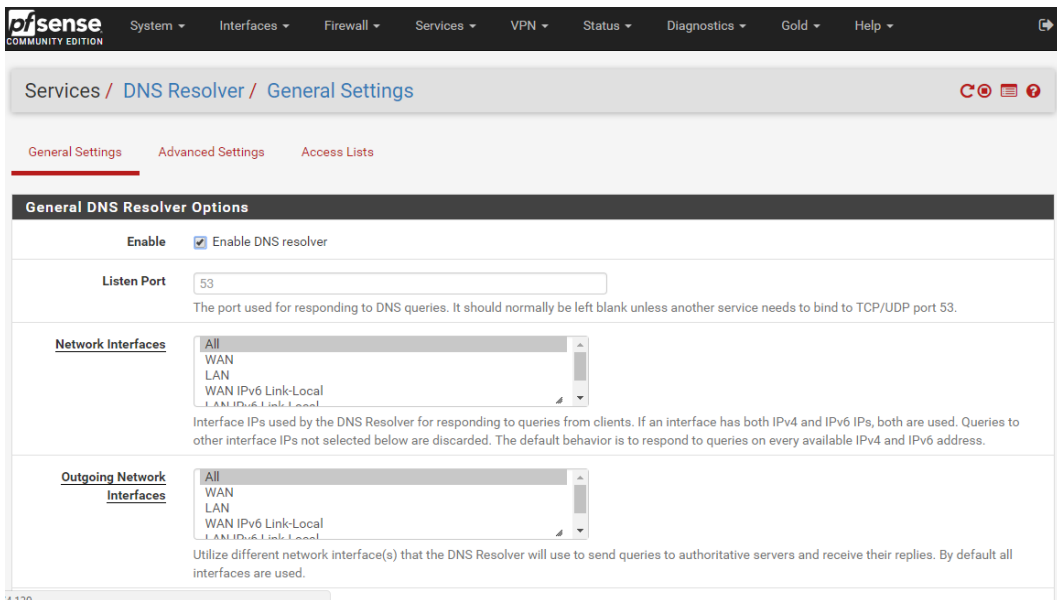
در فایروال pfSense شما با دو سرویس DNS مواجه هستید. یکی از این سرویس‌ها به resolver معروف است که مسئول کش کردن درخواست‌هایی است که از سمت کلاینت‌ها شبکه داخلی شما ارسال می‌شود و کلاینت‌های شما نیاز به برقراری ارتباط با سرورهای راه دور خود از طریق نام به جای آدرس IP دارند، به صورت پیش‌فرض در سرویس‌دهنده‌های اینترنتی چندین سرور کش DNS وجود دارد که شما می‌توانید از آن‌ها استفاده کنید و یا از آدرس‌های معروف مثل 4.2.2.4 و 8.8.8.8 استفاده کنید که باز هم باعث افزایش ترافیک شبکه شما می‌شود. برای کاهش این بخش کافی است که شما سرور Resolver را در pfSense فعال کنید که به صورت پیش‌فرض فعال است و DNS سرور سیستم‌های شبکه داخلی خود را به آدرس ip فایروال داخلی خود تنظیم کنید، در ادامه شما با روش فعال کردن و بخش‌های مختلف آن آشنا می‌شوید.

فعال کردن DNS Resolver:

همان‌طوری که می‌دانید و در بخش‌های قبلی به آن پرداختیم همه سرویس‌ها چه آن‌هایی که به صورت پیش‌فرض نصب هستند و چه آن‌هایی که بعداً نصب می‌شود در زیرشاخه service قرار دارند. برای وارد شدن به این بخش کافی است که از منوی service وارد بخش زیر شوید:



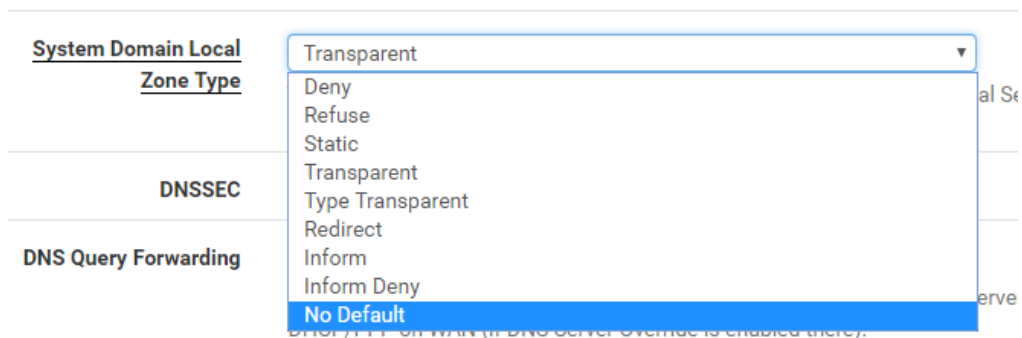
بعد از وارد شدن به بخش DNS Resolver شما با منوی به صورت نمایش داده شده در شکل زیر مواجه می شوید:



به صورت پیش فرض این سرویس فعال بوده و شما می توانید از آن استفاده کنید، برای غیرفعال کردن آن کافی است که تیک بخش enable را برداشته و Save کنید تا سرویس غیرفعال شود، در ادامه شما می توانید حتی شماره پورت

سرویس را تغییر دهید که البته شماره پورت پیش فرض آن 53 است. این بخش همچنین به شما این اجازه را می دهد که کارت های شبکه ای را که شما قصد دارید از طریق آن سرویس دهید و یا اینکه از کدام شبکه برای ارسال درخواست های خود استفاده کند را مشخص کنید.

در بخش شما با مفهوم **local zone** آشنا می شوید که در سرور **unbound** پیاده سازی می شود. در پاسخ دادن به درخواست های کاربران حالت هایی وجود دارد که از دیتابیس داخلی هم می تواند برای پاسخگویی استفاده کند که البته در ادامه با روش اضافه کردن رکوردها در بخش **local** آشنا می شوید. در برخی از موارد شما دامینهایی دارید که به صورت محلی بر روی **pfsense** خود تعریف می کنید و قصد دارید که اولویت با آن ها در پاسخ گویی باشد در این حالت شما باید گزینه **transparent** را از میان این گزینه انتخاب کنید که حالت پیش فرض دی این بخش است. در شکل زیر شما حالت های موجود در این بخش را مشاهده می کنید.



در حالت **Deny** همه درخواست های **DNS** از سمت کلاینت پاسخ داده نمی شود مگر اینکه در دیتابیس محل متغیر داشته باشد.

در حالت مثل حالت **Deny** است با این تفاوت که به سمت کلاینت یک کد **REFUSED** ارسال می شود در زمانی که خطایی ایجاد شده است.

در حالت **transparent** اول دیتابیس اسمی محلی چک می شود که اگر در آن متغیر متناسب بانام درخواستی باشد به آن پاسخ داده می شود و اگر هم نباشد مراحل جستجوی نامی از سرورهای دیگر انجام می شود.

حالت **redirect** زمانی استفاده می شود که شما قصد داشته باشید که یک نام را به نام دیگری **Redirect** کنید.

برای redirect کردن یک هاست خاص به یک آدرس ip خاص کافی است که شما حالت های redirect یا transparent را انتخاب کنید و بعد در بخش زیرین این صفحه وارد قسمت Host Overrides یا Domain Overrides شوید که در شکل زیر آن ها مشاهده می کنید:

The screenshot shows two configuration tables in the pfSense interface. The first table is titled 'Host Overrides' and has columns for Host, Domain, IP, Description, and Actions. It contains one entry: Host 'www', Domain 'mabedini.com', and IP '4.2.2.1'. The second table is titled 'Domain Overrides' and has columns for Domain, IP, Description, and Actions. Both tables have a '+ Add' button at the bottom right.

| Host Overrides | | | | |
|----------------|--------------|---------|-------------|---------|
| Host | Domain | IP | Description | Actions |
| www | mabedini.com | 4.2.2.1 | | |

| Domain Overrides | | | |
|------------------|----|-------------|---------|
| Domain | IP | Description | Actions |
| | | | |

با رفتن بر روی گزینه Add شما می توانید در هر کدام از این دو بخش هاست و یا دامین برای تغییر دادن آدرس اصلی ایجاد کنید، همان طوری که در شکل بالا مشاهده می کنید هاست www از دامین mabedini.com را به آدرس ip شماره 4.2.2.1 redirect کرده ایم که در شکل زیر با استفاده nslookup تغییرات اعمال شده را مشاهده می کنید:

```

Name:   www.mabedini.com
Address: 4.2.2.1
> mabedini.com
Server:   127.0.0.1
Address:  127.0.0.1#53

Non-authoritative answer:
Name:   mabedini.com
Address: 89.39.208.119
>

```

همان طوری که مشاهده می کنید ip دامین mabedini.com به آدرس اصلی برگشت داده می شود هاست www از این دامین به آدرس تنظیم شده در بخش قبل بازگردانی می شود. شما در بخش Domain Overrides می توانید کلیه زیر دامین های و هاست های یک دامین را به آدرسی خاص redirect کنید.

سرور زمان در Pfsense

سرور زمان در Pfsense

یکی از سرورهای مهمی که در شبکه‌های کامپیوتری وجود دارد سرویس NTP است که توسط سرورهای مختلفی در شبکه‌های کامپیوتری و اینترنت ارائه می‌شوند، هدف اصلی این سرویس قرار دادن زمان درست به سیستم‌های درون شبکه است، زمان بخش مهمی است که شما حتماً باید سیستم‌های داخل شبکه شما زمان یکسانی داشته باشند تا هم سرویس‌های شما به درستی کار کند و هم در زمان بروز خطا و گزارش‌های خرابی و یا خرابکاری بتوانید زمان را درست ارزیابی کنید.

زمان با استفاده از پروتکل NTP که مخفف Network Time Protocol در شبکه ارائه می‌شود، که قالب اصلی آن در قالب Client/server است، هر سرور می‌توانید کلاینت برای سرور بالاتر خود باشد و خود این سرور هم می‌تواند زمان را در بین سیستم‌های شبکه خود به اشتراک بگذارد. این سرورها در 3 دسته اصلی طبقه‌بندی می‌شود که بسته به دریافت زمان از سرور اصلی تقسیم‌بندی می‌شوند.

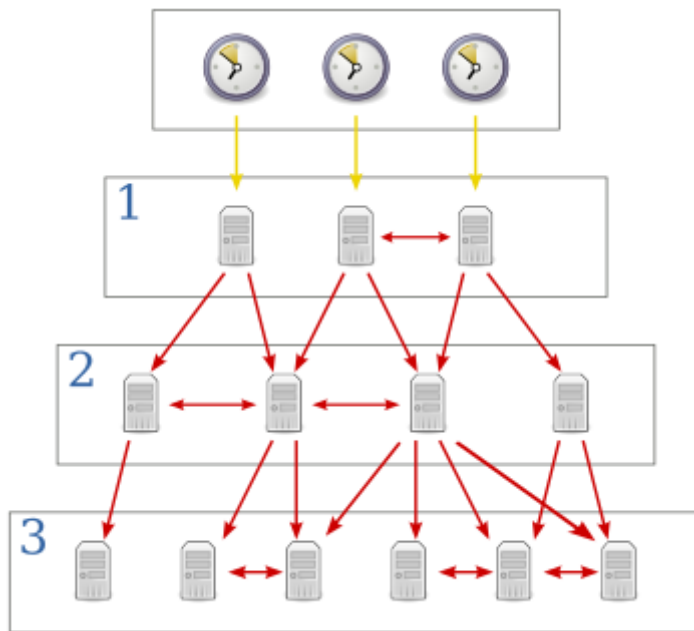
زمان در قدم اول در ساعت‌های مختلف ذخیره می‌شود مثل ساعت اتمی ، ساعت‌های رادیویی و ساعت‌های GPS دار که هر کدام مستقیم زمان را در خود حفظ می‌کند، در شکل زیر نمونه‌ای از ساعت اتمی را مشاهده می‌کنید:



شکل بالا ساعت FOCS 1، یک ساعت اتمی فسفر سزیم سرد در سوئیس است که در سال 2004 با عدم اطمینان آن‌یک ثانیه در 30 میلیون سال شروع به کار کرد.



شکل بالا هم یک ساعت GPS است که با قابلیت ارائه پروتکل NTP در شبکه است، این نوع از دستگاهها در شبکه به Stratum 0 معروف هستند. در شکل زیر این تقسیم‌بندی را مشاهده می‌کنید:



سرورهای در این بخش Stratum 0 هستیم که به زمان اصلی را در دسترس دارند. در این بخش سرورهایی که از این سیستمها ساعت را درخواست می‌کنند به Stratum1 می‌گویند. به همین ترتیب سرورها به ترتیب در سطوح مختلف تقسیم‌بندی می‌شوند. برای برقراری ارتباط با این سرورها از پروتکل NTP استفاده می‌شود. در این میان سایت وجود دارد که شما می‌توانید از طریق آن سرورهای نزدیک به خود را پیدا کنید نام این سایت <http://www.pool.ntp.org/en/> است که صفحه اصلی این سایت را در زیر مشاهده می‌کنید:

pool.ntp.org: the internet's time server

www.pool.ntp.org/en

JOIN THE POOL USE THE POOL MANAGE SERVERS

pool.ntp.org: public ntp time server for everyone

Introduction

The pool.ntp.org project is a big virtual cluster of timeservers providing reliable easy to use NTP service for millions of clients.

The pool is being used by millions or tens of millions of systems around the world. It's the default "time server" for most of the major Linux distributions and many networked appliances (see [information for vendors](#)).

Because of the large number of users we are in need of more servers. If you have a server with a static IP address always available on the internet, please consider [adding it to the system](#).

The project is maintained and developed by Ask Bjørn Hansen and a great group of contributors on the mailing lists. The source code for the system is available.

Hosting and bandwidth for the "hub" servers are provided by Developer and Phyber Communications.

Active Servers

| | |
|------------------|------|
| Africa | 32 |
| Antarctica | 0 |
| Asia | 232 |
| Europe | 2773 |
| North America | 929 |
| Oceania | 119 |
| South America | 45 |
| Global | 3823 |
| All Pool Servers | 4130 |

As of 2018-03-31

News

Subscribe in a reader

- May 21, 2017 **How to Configure NTP for Use in the NTP Pool Project**
Daniel Ziegenberg wrote a tutorial for Digital Ocean on configuring NTP for the NTP Pool on Ubuntu.
Oliver Nadler has another tutorial covering non-Ubuntu, too.
- January 1, 2017 **NTP Pool Forum**
There's a new forum for discussion related to the NTP Pool at [community.ntppool.org](#). Please come join us. There are a

این سایت به شما آدرس‌های سرورهای NTP در بخش‌های مختلف را می‌دهد که شما می‌توانید به ترتیب منطقه جغرافیایی خود آن‌ها را انتخاب کنید.

در این سایت سه سرور برای ایران ذکر شده است در لیست زیر:

```
server 2.ir.pool.ntp.org
server 3.asia.pool.ntp.org
server 2.asia.pool.ntp.org
```

سرور شماره یک به آدرس 82.99.215.102 در شرکت پارس آنلاین قرار دارد. در این سرور رسمی برای این کار نداریم و بسیار جالب است که سایتی در ایران وجود دارد به نام time.ir که فقط زمان محلی ایران را نمایش می‌دهد و سرور NTP نیست.

با این توضیحات شما برای تنظیم کردن سرور NTP در Pfsense آماده هستید و در قسمت بعدی با روش تنظیم کردن این سرور آشنا می‌شوید، قبل از وارد شدن به این بخش شما حتماً باید آشنایی با منوی اصلی رابط وب در pfsense داشته باشید.

را اندازی کردن سرور NTP در Pfsense :

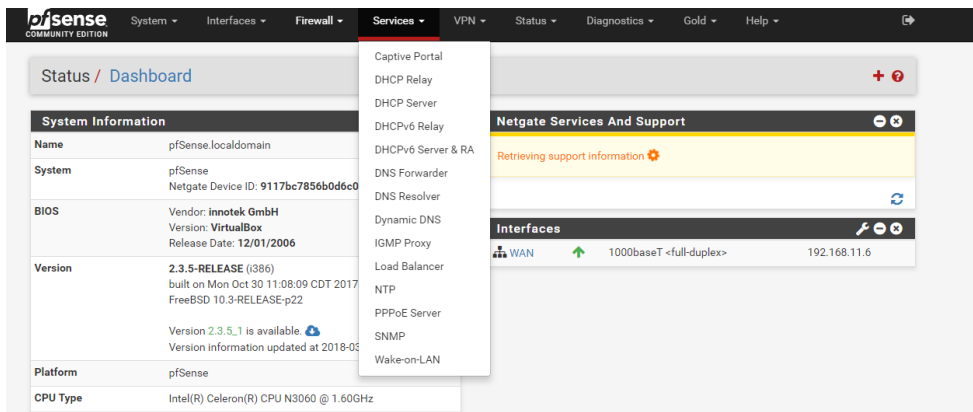
تمام سروریس ها در Pfsense از زیر منوی سرویس Services قابل دسترسی و تنظیم است برای این کار به زیر منوی NTP در این منو مراجعه کنید، در شکل زیر شما این بخش را مشاهده می کنید:

Localization

Timezone ▼
 Select the timezone or location within the timezone to be used by this system. Usually choose a "Continent/City". Only choose a special or "Etc" entry if you understand why you need to use it.

Timeservers
 Use a space to separate multiple hosts (only one required). Remember to set up at least one DNS server if a host name is entered here!

Language ▼
 Choose a language for the webConfigurator



برای وارد شدن به بخش سرور NTP شما بر روی این گزینه کلیک کنید تا بخش تنظیمات سرور برای شما به صورت زیر باز شود:

Settings ACLs Serial GPS PPS

NTP Server Configuration

Interface: WAN

Interfaces without an IP address will not be shown.
 Selecting no interfaces will listen on all interfaces with a wildcard.
 Selecting all interfaces will explicitly listen on only the interfaces/IPs specified.

Time Servers: 0.pfsense.pool.ntp.org Prefer No Select

Add:

For best results three to five servers should be configured here.
 The prefer option indicates that NTP should favor the use of this server more than all others.
 The no select option indicates that NTP should not use this server for time, but stats for this server will be collected and displayed.

Orphan Mode: 12

Orphan mode allows the system clock to be used when no other clocks are available. The number here specifies the stratum reported during orphan mode and should normally be set to a number high enough to insure that any other servers available to clients are preferred over this server (default: 12).

NTP Graphs: Enable RRD graphs of NTP statistics (default: disabled).

در قسمت بالایی از این بخش شما می‌توانید کارت شبکه‌ای را که بر روی آن این سرویس راه‌اندازی شود را انتخاب کنید که در این باکش شما فهرستی از کارت‌های شبکه را مشاهده می‌کنید، در قسمت بعدی شما می‌توانید سرورهای Time که از آن زمان پرسیده شود را انتخاب کنید که در بخش‌های قبل در خصوص روش پیدا کردن آن و سایت مرجع توضیحاتی داده شده است با استفاده از کلید add هم می‌توانید به تعداد این سرورها اضافه کنید تا در صورتی که یکی از آن‌ها پاسخ‌گو نباشد به سرور دیگر بتوان متصل شود و از آن زمان را پرس‌وجو کند.

با تنظیم کردن حالت orhan اگر سرورهای اصلی در دسترس نباشد سیستم می‌تواند به صورت موقت از زمان محلی خود پاسخ‌گویی درخواست‌های شبکه داخلی باشد. عدد بالا در این بخش بیانگر این مطلب است که ابتدا سرورهای دیگر چک شود و در صورتی که در دسترس نباشد از این حالت استفاده کند که عدد این بخش 12 است.

به صورت پیش‌فرض گزارش دهی از طریق گراف برای NTP غیرفعال است و شما در صورت لزوم می‌توانید این بخش را هم فعال کنید. در فایروال pfsense به صورت پیش‌فرض گزارش‌گیری از سیستم لاگ برای NTP غیرفعال شده است و شما در صورت لزوم می‌توانید گزارش‌گیری را از طریق بخش Logging فعال کنید.

برای داشتن یک لاگ فایل جداگانه شما می‌توانید بخش Statistics Logging را فعال کنید. اگر هم سرور شما دست‌اول باشد می‌توانید گزینه Leap seconds را فعال کنید.

بعد از فعال شدن این بخش شما می‌توانید بخش منوی Status بخش NTP بخش وضعیت را مشاهده کنید که در شکل زیر آن‌ها مشاهده می‌کنید:

| Status / NTP | | | | | | | | | | |
|------------------------------|-------------|----------------|---------|------|------|------|-------|--------|--------|--------|
| Network Time Protocol Status | | | | | | | | | | |
| Status | Server | Ref ID | Stratum | Type | When | Poll | Reach | Delay | Offset | Jitter |
| Unreach/Pending | 5.144.132.2 | 194.225.150.25 | 3 | u | 1 | 64 | 13 | 50.066 | 18.209 | 27.231 |

یکی از روش‌های قدیمی و مؤثر در مورد مانیتورینگ کردن سیستم‌ها در شبکه استفاده از پروتکلی است به نام `snmp` که در فایروال `pfSense` هم قابل پیاده‌سازی است. این برنامه در حالت کلاینت/ سروری کار می‌کند و اطلاعات دریافت شده از سیستم را به سمت سرور منتقل کرده و پردازش را از این طریق در سمت سرور انجام می‌شود، این پروتکل در ورژن‌های اولیه آن به صورت متن‌های رمز نشده اطلاعات را به سمت سرور ارسال می‌کند ولی در ورژن‌های جدید امکان ارسال امن هم برای شما ایجاد شده است.

در فایروال `pfSense` شما می‌توانید بخش کلاینتی `SNMP` را فعال کنید تا بتوانید این اطلاعات را سمت سرور ارسال کنید که این سرورهای می‌تواند `cacti` و یا `Check_MK` باشد. برای فعال کردن این بخش شما نیاز دارید که به رابط وب فایروال خود متصل شوید و از منوی سرویس وارد بخش `snmp` شوید که در شکل زیر این منو را مشاهده می‌کنید:

The screenshot shows the pfSense web interface with the 'Services' menu open. The menu items are: Captive Portal, DHCP Relay, DHCP Server, DHCPv6 Relay, DHCPv6 Server & RA, DNS Forwarder, DNS Resolver, Dynamic DNS, IGMP Proxy, Load Balancer, NTP, PPPoE Server, SNMP, UPnP & NAT-PMP, and Wake-on-LAN. In the background, the 'Interfaces' tab is active, showing a table for 'Dynamic DNS Status' and 'Services Status'.

| Int. | Service | Hostn |
|------|---------|---------|
| | | All Dyn |

| Service | Descriptio |
|---|------------|
| <input checked="" type="checkbox"/> dpinger | Gateway I |
| <input checked="" type="checkbox"/> ntpd | NTP clocl |
| <input checked="" type="checkbox"/> syslogd | System L |
| <input checked="" type="checkbox"/> unbound | DNS Resc |

بعد از وارد شدن به منوی موردنظر شما با صفحه‌ای به صورت زیر برای انجام تنظیمات آشنا می‌شوید:

The screenshot shows the 'Services / SNMP' configuration page in pfSense. It includes sections for 'SNMP Daemon', 'SNMP Daemon Settings', and 'SNMP Traps Enable'.

SNMP Daemon

Enable Enable the SNMP Daemon and its controls

SNMP Daemon Settings

Polling Port:
Enter the port to accept polling events on (default 161).

System Location:

System Contact:

Read Community String:
The community string is like a password, restricting access to querying SNMP to hosts knowing the community string. Use a strong value here to protect from unauthorized information disclosure.

SNMP Traps Enable

Enable Enable the SNMP Trap and its controls

برای فعال‌سازی کافی است که بخش **Enable the SNMP Daemon and its controls** را انتخاب کنید و بعد **save** کنید. در بخش دوم از این بخش شما می‌توانید شماره پورت شبکه سمت سرور را تعیین کنید که به صورت

پیش فرض 161 است. در بخش شما می‌توانید اطلاعات اضافه‌ای مثل محل سیستم و آدرس تماس را هم مشخص کنید که بخشی است اختیاری، بخش مهم در این زمینه پیکربندی سخت کلمه **Read Community String** است که در حقیقت مثل یک رمز عبور برای برقرار ارتباط عمل می‌کند در نتیجه تلاش کنید که کلمه‌ای سخت برای این بخش انتخاب کنید.

اگر قصد فعال کردن سرویس traps را داشته باشید می‌توانید در شکل زیر این بخش را فعال کنید و باید تنظیمات زیر را اعمال کنید:

SNMP Traps Enable

Enable Enable the SNMP Trap and its controls

SNMP Trap Settings

Trap server
Enter the trap server name

Trap Server Port
Enter the port to send the traps to (default 162)

SNMP Trap String

در بخش پایانی از این شما می‌توانید ماژول‌های که قصد دارید اطلاعات در سمت سرور را مشخص کنید این بخش‌ها را در شکل زیر مشاهده می‌کنید:

SNMP Modules

SNMP modules

- MibII
- Netgraph
- PF
- Host Resources
- UCD
- Regex

در بخش پایانی هم شما می‌توانید کارت شبکه‌ای را که قصد دارید از طریق آن اطلاعات را ارسال کنید را انتخاب کنید. بعد از باز کردن این بخش شما لیست کارت‌های شبکه را مشاهده می‌کنید.

نصب کردن برنامه در FreeBSD

در این بخش قصد داریم که در مورد نصب کردن برنامه در Pfsense با شما دوستان عزیز صحبت کنیم، علاوه بر قابلیت‌های پیش فرضی که در Pfsense وجود دارد شما می‌توانید با استفاده از نصب کردن بسته‌ها قابلیت‌های جدید هم به این فایروال پر قدرت اضافه کنید. در این بخش شما ابتدا با روش نصب برنامه در FreeBSD آشنا می‌شوید و در بخش بعد هم با روش نصب کردن برنامه‌ها در دو قالب خط فرمان و استفاده از رابط وب برای نصب کردن برنامه‌های مختلف در pfsense آشنا می‌شوید.

نصب کردن برنامه در FreeBSD

در سیستم عامل FreeBSD شما به سه روش می‌توانید برنامه‌های کاربردی را نصب کردن که در دو حالت شما از طریق کد منبع برنامه را نصب می‌کنید و در روشی دیگر از برنامه‌های از پیش کامپایل شده برای این کار استفاده می‌کنید. قبل از شروع به استفاده کردن از این دو روش شما نیاز به آشنا با نصب برنامه از کد منبع و برنامه کامپایل شده دارید.

هر برنامه به صورت مجموعه از فایل‌هایی است که در یک زبان برنامه‌نویسی خاصی ایجاد شده است، بسیاری از این برنامه در دنیای سیستم عامل‌های BSD به صورت رایگان در اختیار همگان قرار دارد و شما به راحتی می‌توانید از طریق سایت ایجادکننده برنامه این کدها را دانلود کردن و آن‌ها نصب کنید. این روش در هر سیستم عامل متن‌باز خط فرمانی وجود دارد. این روش به دانش شما در مورد برنامه‌هایی که باید قبل از نصب کردن آن استفاده کنید بستگی دارد و در سایت سازنده هم برای شما این توضیحات نوشته شده است. این روش بسیار حساس، حرفه‌ای و زمان‌بر است و کامپایل کردن هر برنامه می‌تواند برای شما زمان‌بر باشد و شما با خطاهایی آشنا شوید.

در مقابل روش نصب ذکر شده روشی دیگر وجود دارد که در این روش به سیستم عامل شما بستگی دارد و هر سیستم عاملی از یک مدیریت کننده برای نصب کردن بسته‌های کامپایل شده استفاده می‌کند که در سیستم عامل جدید FreeBSD شما از فرمان pkg برای این کار استفاده می‌کنید و برنامه‌هایی که از قبل کامپایل شده و بر روی سرورهای ftp سایت قرار دارند دانلود کرده که البته می‌توانید فرآیند دانلود را هم به صورت خودکار انجام دهید، و بعد برنامه را بدون کامپایل کردن نصب کنید.

این بسته‌های از پیش کامپایل شده از دل روش نصبی در FreeBSD ایجاد می‌شوند به نام سیستم ports که در ادامه در مورد آن صحبت خواهیم کرد.

در ادامه این دو روش را باهم مقایسه خواهیم کرد:

در روش نصب از کد منبع شما می‌توانید قابلیت‌ها های بیشتری و موردنظر خود را در برنامه فعال کنید که بسته‌های کامپایل شده این برنامه‌ها وجود ندارد.

در روش نصب برنامه از کد منبع شما باید زمان زیادی صرف کامپایل کردن برنامه‌ها صرف کنید که در روش بسته‌های کامپایل شده شما به راحتی این کار را انجام می‌دهد.

در روش دستی نصب بسته‌ها شما باید به پیش نیازهای برنامه نصبی توجه کنید که در روش استفاده از فرمان `pkg` این کار به صورت خودکار انجام می‌شود.

در روش نصب از کد منبع برای بروز رسانی کرده برنامه‌های نصبی شما باید از ابتدا برنامه را کامپایل کنید که در سیستم بسته‌های کامپایل شده شما از این قبیل مشکلات ندارد.

در میان این دو روش روشی وجود دارد که به سیستم `ports` در `FreeBSD` معروف است و شما در این روش برنامه‌ها را از کد منبع نصب می‌کنید ولی نگران پیش برنامه‌های نصبی، دریافت کردن فایل‌ها هر برنامه نبوده و به شما هم این امکان را می‌دهد که امکانات برنامه را به تناسب درخواست خود کم یا زیاد کنید و از همه بهتر برای خود بسته‌های نصبی خاصی ایجاد کنید.

نصب کردن برنامه در `FreeBSD` با استفاده از فرمان `pkg`

در این روش شما باید از سلسله پیرایند موجود در فرمان `pkg` استفاده کنید و برنامه‌های از پیش کامپایل شده را نصب می‌کنید، شما می‌توانید در این روش ابتدا فایل موردنظر را دانلود کنید که باید از بسته‌های جانبی نصبی هم اطلاعات داشته باشید و آن‌ها را نصب کنید و یا از طریق سوئیچ ۲ از این فرمان به صورت خودکار از طریق اینترنت و سایت `FreeBSD` این کار را انجام دهید که در این روش دیگر شما نگران تقدم و تاخر بسته‌ها نخواهید بود. در شکل زیر خروجی نصبی با استفاده از برنامه `pkg` را مشاهده می‌کنید:


```

Terminal
File Edit View Terminal Tabs Help
root@OpenBSD:/usr # pkg install wget
Updating FreeBSD repository catalogue...
FreeBSD repository is up-to-date.
All repositories are up-to-date.
The following 1 package(s) will be affected (of 0 checked):

New packages to be INSTALLED:
  wget: 1.18

Number of packages to be installed: 1

The process will require 3 MiB more space.
557 KiB to be downloaded.

Proceed with this action? [y/N]: y
Fetching wget-1.18.txz: 100% 557 KiB 570.3kB/s   00:01
Checking integrity... done (0 conflicting)
[1/1] Installing wget-1.18...
[1/1] Extracting wget-1.18: 100%
root@OpenBSD:/usr #

```

در این روش برای جستجو کردن نام یک برنامه خاص برای نصب می‌توانید از `search` بعد از فرمان `pkg` استفاده کنید که خروجی به صورت زیر برای شما نمایش داده می‌شود:

```

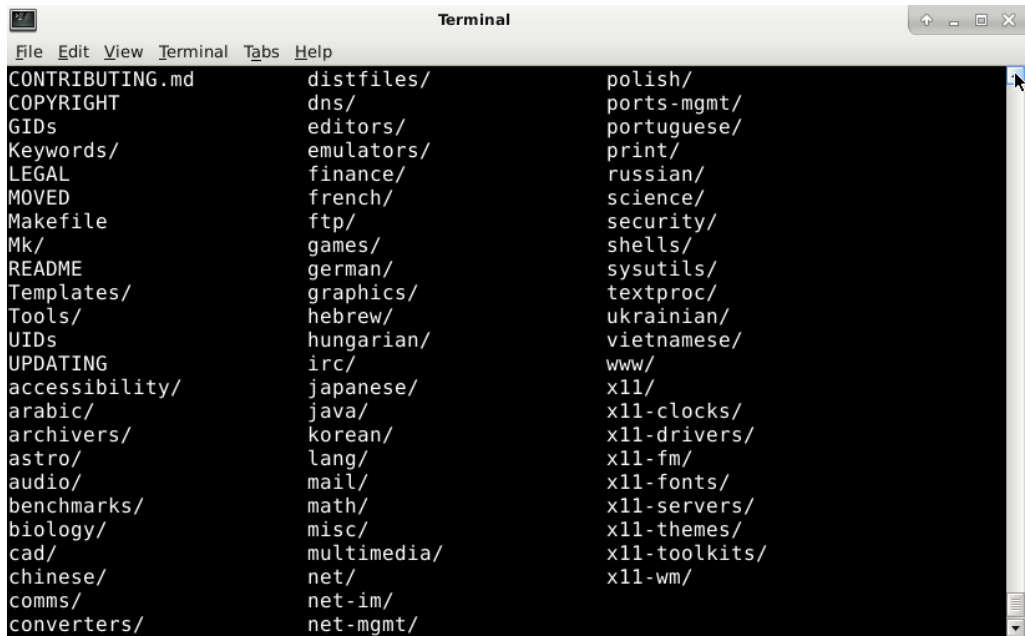
Terminal
File Edit View Terminal Tabs Help
root@OpenBSD:~ # pkg search ftp | less
aftp-1.0          Ftp-like shell for accessing Apple II disk images
atftp-0.7_3      Advanced tftp server and client
bareftp-0.3.12  FTP client made in C sharp
bbftp-3.0.2     Multiple stream file transfer protocol optimized
for large files
bftpd-4.4       Very configurable FTP server that can do chroot e
asily
bsdftpd-ssl-1.1.0_4 Secure FTP client/server with TLS/SSL support
cftp-0.12_3     Comfortable FTP, a full screen ftp client
cmdftp-0.9.8   Command line shell-like ftp client
dkftpbench-0.45_2 FTP benchmark program
ftpcopy-0.6.7  Command line ftp tools for listing and mirroring
ftpfind-0.996  Find directory&file on a ftp server
ftplib-4.0_1   Set of routines that implement the FTP protocol
ftpmirror-1.96_5 Utility to mirror directory hierarchy with FTP
ftpproxy-1.2.3_1 ftp proxy
ftpsesame-0.95 Helper for pf firewall to pass FTP protocol

```

نصب کردن برنامه‌ها در FreeBSD با استفاده از سیستم ports

سیستم ports مجموعه‌ای از فایل‌هایی به نام Makefile است که در خود patch ها امنیتی و توضیحات در مورد هر برنامه را در شاخه `usr/ports/` قرار داده این شاخه به صورت دسته‌بندی شده هر برنامه را به دسته‌های مختلف جدا کرده است برای مثال شما برای نصب برنامه‌هایی که به زبان برنامه‌نویسی جاوا مربوط می‌شود باید وارد شاخه `java`

شويد، يا براي نصب برنامه‌هايي كه به فهرست‌هاي پستي يا همان mail مربوط مي‌شود به شاخه mail وارد شويد، براي برنامه‌هاي مربوط به برنامه‌هاي مديريتي شبكه به شاخه net-mgmt مراجعه كنيد، در زير ليست كامل اين شاخه‌ها را در شكل زير مشاهده مي‌كنيد:



```

Terminal
File Edit View Terminal Tabs Help
CONTRIBUTING.md    distfiles/         polish/
COPYRIGHT          dns/              ports-mgmt/
GIDs               editors/          portuguese/
Keywords/         emulators/        print/
LEGAL             finance/          russian/
MOVED            french/           science/
Makefile          ftp/              security/
Mk/              games/            shells/
README           german/           sysutils/
Templates/       graphics/         textproc/
Tools/           hebrew/           ukrainian/
UIDs             hungarian/        vietnamese/
UPDATING         irc/              www/
accessibility/   japanese/         x11/
arabic/          java/             x11-clocks/
archivers/       korean/           x11-drivers/
astro/           lang/             x11-fm/
audio/           mail/             x11-fonts/
benchmarks/      math/             x11-servers/
biology/         misc/             x11-themes/
cad/             multimedia/       x11-toolkits/
chinese/         net/              x11-wm/
comms/           net-im/
converters/      net-mgmt/
    
```

براي جستجو كردن برنامه خاص كافي است كه وارد شاخه ports شويد و از فرمان زير استفاده كنيد:

```

Terminal
File Edit View Terminal Tabs Help
root@OpenBSD:~ # cd /usr/ports/
root@OpenBSD:/usr/ports # make search name=lsof
Port:      lsof-4.90.e,8
Path:     /usr/ports/sysutils/lsof
Info:     Lists information about open files (similar to fstat(1))
Maint:    ler@lerctr.org
B-deps:
R-deps:
WWW:      http://people.freebsd.org/~abe/

Port:     p5-Unix-Lsof-0.0.5_2
Path:    /usr/ports/sysutils/p5-Unix-Lsof
Info:    Unix::Lsof -- a wrapper to the Unix lsof utility
Maint:   gjvc@gjvc.com
B-deps:  p5-IPC-Run3-0.048_1 perl5-5.20.3_13
R-deps:  p5-IPC-Run3-0.048_1 perl5-5.20.3_13
WWW:     http://search.cpan.org/dist/Unix-Lsof/

root@OpenBSD:/usr/ports # █

```

برای نصب کردن برنامه کافی است که وارد شاخه برنامه موردنظر شوید و فرمان **make install** را اجرا کنید به صورت نمایش داده شده در شکل زیر:

```

Terminal
File Edit View Terminal Tabs Help
root@OpenBSD:/usr/ports/sysutils/lsof # make install
==> Installing for lsof-4.90.e,8
==> Checking if lsof already installed
==> Registering installation for lsof-4.90.e,8
Installing lsof-4.90.e,8...
==> SECURITY REPORT:
    This port has installed the following binaries which execute with
    increased privileges.
/usr/local/sbin/lsof                                     ⓘ

    If there are vulnerabilities in these programs there may be a security
    risk to the system. FreeBSD makes no guarantee about the security of
    ports included in the Ports Collection. Please type 'make deinstall'
    to deinstall the port if this is a concern.

    For more information, and contact details about the security
    status of this software, see the following webpage:
http://people.freebsd.org/~abe/
root@OpenBSD:/usr/ports/sysutils/lsof # █

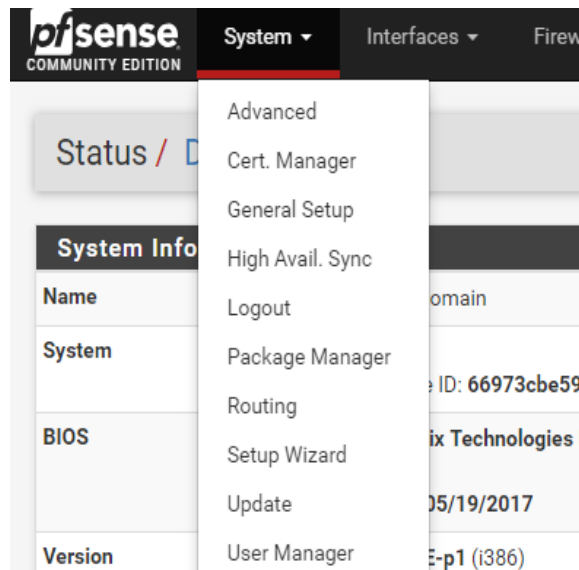
```

نصب کردن برنامه‌های موجود در مخازن pfSense با استفاده از رابط وب

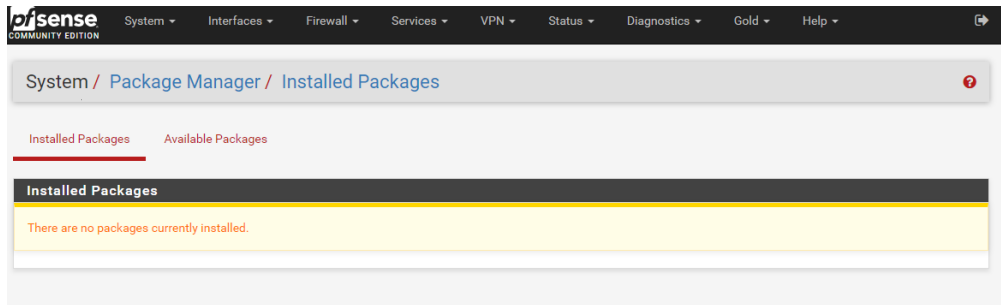
نصب کردن برنامه‌های موجود در مخازن pfSense با استفاده از رابط وب

در فایروال pfSense این امکان وجود دارد که برنامه‌های موردنظر را با استفاده از رابط وبی که در آن وجود دارد نصب کنید که در قدم اول باید شما ابتدا ارتباط با شبکه اینترنت خود را چک کنید چون این بخش نیاز به اینترنت دارد و بسته‌هایی که در مخازن سایت pfSense است را برای شما نصب می‌کند، پس در قدم اول در شل از ping برای چک کردن ارتباط خود استفاده کنید.

برای وارد شدن به منوی نصب برنامه باید از منوی system وارد بخش package manager شوید که در شکل زیر این زیر منو برای شما نمایش داده شده است:



بعد از ورود به این بخش شما با منوی به صورت زیر مواجه می‌شوید:



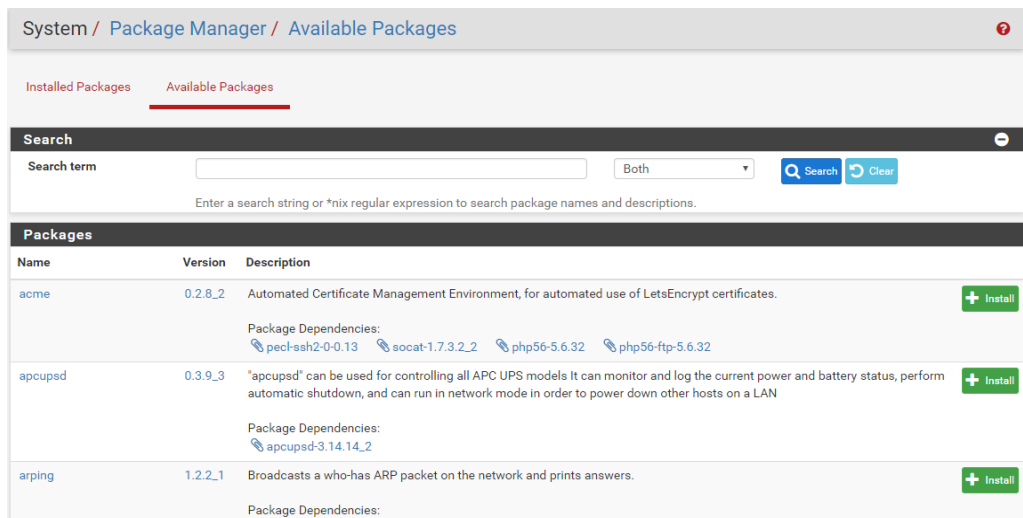
System / Package Manager / Installed Packages

Installed Packages Available Packages

Installed Packages

There are no packages currently installed.

این قسمت به دو بخش اصلی تقسیم می‌شود بخش اول برنامه‌های نصب‌شده را برای شما نمایش می‌دهد که در شکل بالا همان‌طوری که مشاهده می‌کنید هیچ برنامه‌ای وجود ندارد و بخش دو برنامه‌های موجود است که با کلید کردن بر روی آن بخش شما لیست برنامه‌هایی که می‌توانید نصب کنید را مشاهده می‌کنید به صورت زیر :



System / Package Manager / Available Packages

Installed Packages Available Packages

Search

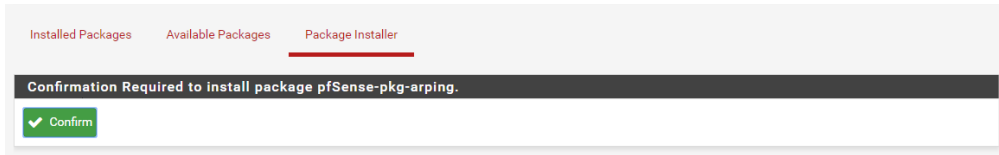
Search term Both

Enter a search string or *nix regular expression to search package names and descriptions.

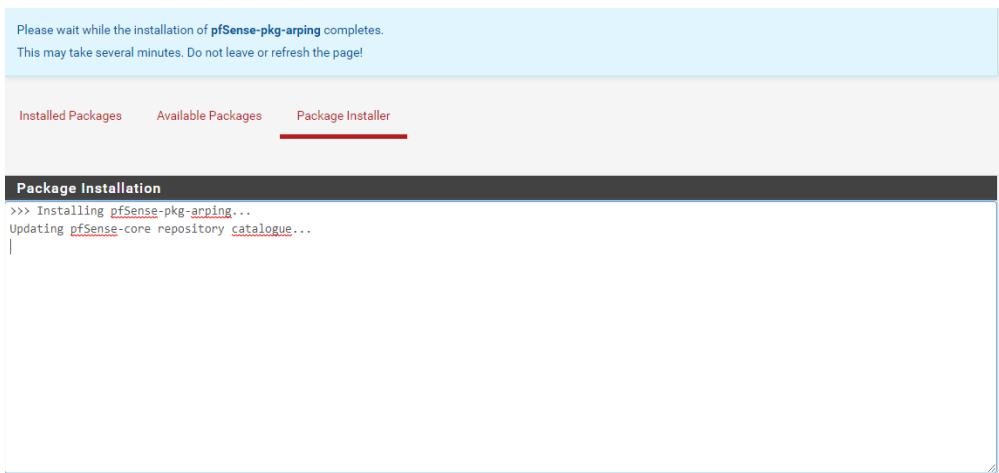
Packages

| Name | Version | Description | |
|--------|---------|--|--|
| acme | 0.2.8_2 | Automated Certificate Management Environment, for automated use of LetsEncrypt certificates. Package Dependencies: pecl-ssh2-0-0.13 socat-1.7.3.2_2 php56-5.6.32 php56-ftp-5.6.32 | <input type="button" value="+ Install"/> |
| apcpsd | 0.3.9_3 | "apcpsd" can be used for controlling all APC UPS models It can monitor and log the current power and battery status, perform automatic shutdown, and can run in network mode in order to power down other hosts on a LAN Package Dependencies: apcpsd-3.14.14_2 | <input type="button" value="+ Install"/> |
| arping | 1.2.2_1 | Broadcasts a who-has ARP packet on the network and prints answers. Package Dependencies: | <input type="button" value="+ Install"/> |

در این بخش شما اگر اسم برنامه خاصی را می‌دانید می‌توانید در بخش **Search** آن‌ها وارد کنید که این بخش هم در بخش نام وهم در بخش توضیحات به دنبال برنامه شما می‌گردد و هم می‌توانید در لیست زیر یک برنامه خاص را نصب کنید که البته هم شما ورژن را مشاهده می‌کنید و هم توضیحات برنامه موردنظر را برای نصب کافی است بر روی دکمه **install** کلیک کنید تا به صورت زیر برنامه برای شما نصب شود:



شما وارد بخش نصب می‌شود که باید نصب کردن بسته را ابتدا تأیید کنید این تأیید در شکل بالا نمایش داده شده است، بعد از کلیک کردن مراحل نصب به صورت شکل زیر آغاز می‌شود:



زمان نصب در این بخش به سرعت شما و بسته‌های قبل از نصب بسته موردنظر شما بستگی دارد.

pfSense-pkg-arping installation successfully completed.

Installed Packages Available Packages Package Installer

Package Installation

```
>>> Installing pfSense-pkg-arping...
Updating pfSense-core repository catalogue...
pfSense-core repository is up to date.
Updating pfSense repository catalogue...
pfSense repository is up to date.
All repositories are up to date.
The following 3 package(s) will be affected (of 0 checked):

New packages to be INSTALLED:
  pfSense-pkg-arping: 1.2.2_1 [pfSense]
  arping: 2.15_1 [pfSense]
  libnet: 1.1.6_5,1 [pfSense]

Number of packages to be installed: 3
```

در این بخش برنامه به صورت کامل نصب شده است ، در پیغام‌هایی که در باکس نصب مشاهده می‌کنید فهرستی از بسته‌هایی که باید برای شما نصب شود را مشاهده می‌کنید که بسته به برنامه نصبی شما می‌تواند متنوع باشد، در ادامه مراحل دانلود و نصب را مشاهده می‌کنید به صورت نمایش داده شده است:

Package Installation

```
[1/3] Installing libnet-1.1.6_5,1...
[1/3] Extracting libnet-1.1.6_5,1: ..... done
[2/3] Installing arping-2.15_1...
[2/3] Extracting arping-2.15_1: ..... done
[3/3] Installing pfSense-pkg-arping-1.2.2_1...
Extracting pfSense-pkg-arping-1.2.2_1: ..... done
Saving updated package information...
done.
Loading package configuration... done.
Configuring package components...
Loading package instructions...
Custom commands...
Menu items... done.
Writing configuration... done.
*** Cleaning up cache... done
```

بعد از نصب حال در زیر منوی برنامه نصب شده برنامه را مشاهده می‌کنید به صورت زیر:

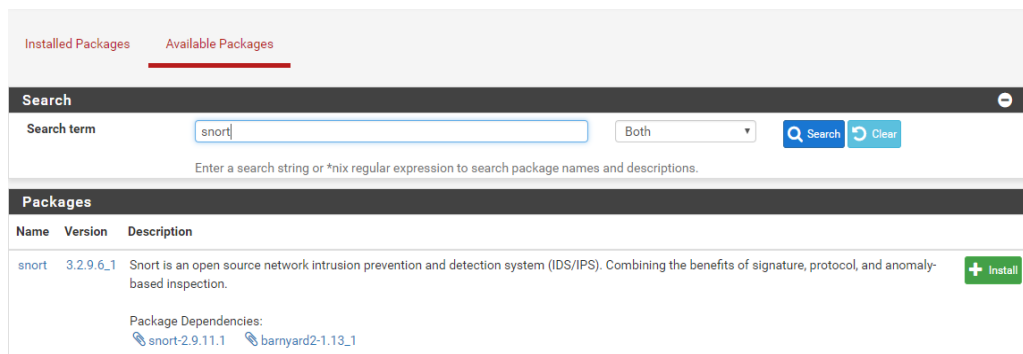
Installed Packages

| Name | Category | Version | Description | Actions |
|---|----------|---------|--|---------|
| ✓ arping | net | 1.2.2_1 | Broadcasts a who-has ARP packet on the network and prints answers. | |
| Package Dependencies: arping-2.15_1 | | | | |
| Update = Update ✓ = Current = Remove = Information = Reinstall Newer version available Package is configured but not (fully) installed or deprecated | | | | |

برای پاک کردن برنامه نصب شده از دکمه **remove** و برای دوباره نصب کردن از **Reinstall** در زیر برنامه می توانید استفاده کنید.

در این مرحله برنامه شما نصب شده است. این برنامه نصب شده هیچ منوی برای پیکربندی ندارد، ولی کاربردی کردن **pfsense**

در این است که برای برنامه های کاربردی منوهای را ایجاد کرده است که کاربری برنامه را برای شما جذاب زیبا و ساده و کاربردی می شود، در ادامه برای شما نصب برنامه **IDS** معروف **snort** را در **pfsense** نصب خواهیم کردن و مختصری در مورد روش پیکربندی آن توضیحاتی را برای شما دوستان عزیز بیان می کنم، در این بخش فرض بر آن است که شما **snort** را نصب کرده اید، برای نصب باید برنامه زیر را از لیست نصب کنید:



The screenshot shows the 'Available Packages' tab in the pfSense package manager. A search bar contains the text 'snort'. Below the search bar, there is a table of packages. The first row shows the package 'snort' with version '3.2.9.6_1'. The description reads: 'Snort is an open source network intrusion prevention and detection system (IDS/IPS). Combining the benefits of signature, protocol, and anomaly-based inspection.' To the right of the description is a green '+ Install' button. Below the package name, it lists 'Package Dependencies: snort-2.9.11.1, barnyard2-1.13.1'.

این برنامه **IDS/IPS** است که می تواند با استفاده از **pfsense** جلوی ترافیک های ناخواسته شما را مسدود کند البته شما برای کاربری بهتر باید در سایت آن ثبت نام کنید و آخرین پترهای روز را دانلود کنید و همه ترافیک وارد و یا خارج شده در شبکه را اسکن کنید، این برنامه نیاز به نصب برنامه **barnyard** هم دارد. در ادامه فرض بر این است که برنامه **snort** را نصب کرده و برای ادامه مراحل آماده هستید.

بعد از نصب در زیر منوی **services** شما می توانید وارد بخش **snort** شوید این زیر منو را شما در شکل زیر مشاهده می کنید:

System / Package Manager / Package Installation

pfSense-pkg-snort installation successfully completed.

Installed Packages Available Packages Package Installation

Package Installation

Configuration files are located in /usr/local/etc/snort

Please note that, by default, snort will truncate packet default snaplen of 15158 bytes. Additionally, LRO may Stream5 target-based reassembly. It is recommended to your card supports it.

This can be done by appending '-lro' to your ifconfig_

 Message from pfSense-pkg-snort-3.2.9.6_1:
 Please visit Services - Snort - Interfaces tab first to add an interface, then select your desired rules packages at the Services - Snort - Global tab. Afterwards visit the Updates tab to download your configured rulesets.
 >>> Cleaning up cache... done.
 Success

Services menu items: Captive Portal, DHCP Relay, DHCP Server, DHCPv6 Relay, DHCPv6 Server & RA, DNS Forwarder, DNS Resolver, Dynamic DNS, IGMP Proxy, Load Balancer, NTP, PPPoE Server, SNMP, Snort, UPnP & NAT-PMP, Wake-on-LAN

بعد از کلید شما می‌توانید از طریق منوی وبی برنامه را مدیریت کنید:

Services / Snort / Interfaces

Snort Interfaces Global Settings Updates Alerts Blocked Pass Lists Suppress IP Lists SID Mgmt Log Mgmt Sync

Interface Settings Overview

| Interface | Snort Status | Pattern Match | Blocking | Barnyard2 Status | Description | Actions |
|-----------|--------------|---------------|----------|------------------|-------------|---------|
| + Add | | | | | | |

Warning: New settings will not take effect until interface restart

Click on the icon to edit an interface and settings.
 Click on the icon to delete an interface and settings.
 Click on the icon to clone an existing interface.

icons will show current snort and barnyard2 status
 Click on the or icons to start/stop Snort and Barnyard2.

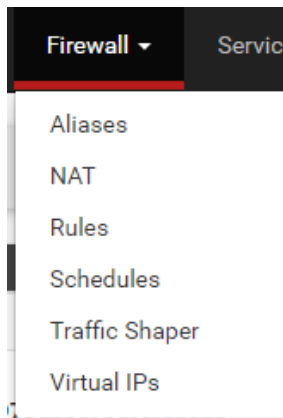
نوشتن رول با استفاده از فایروال pfsense

نوشتن رول با استفاده از فایروال pfSense:

در بخش پایانی از این کتاب شما با روش نوشتن رول در فایروال pfSense آشنا می‌شوید. در این فصل شما با سه مفهوم rule Alias و Nat آشنا می‌شوید. این بخش‌ها در زیر منوی firewall قرار دارد که در ادامه این بخش با موارد استفاده آن آشنا می‌شوید.

معرفی کردن منوی فایروال:

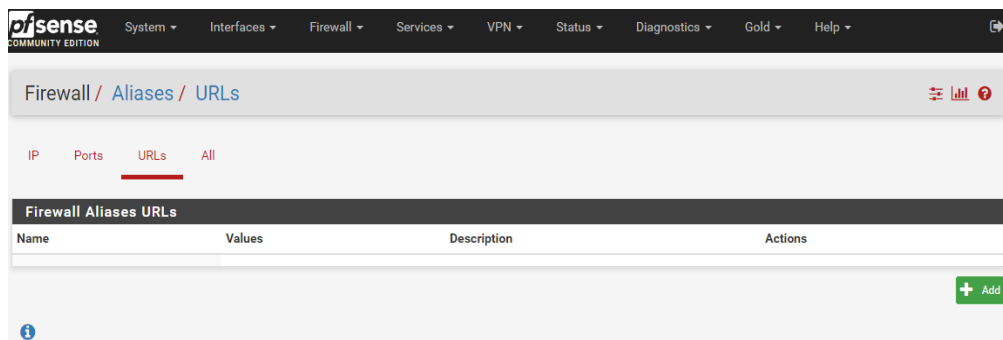
یکی از اعمال اصلی در pfSense ارائه کردن خدمات فایروال است که این اعمال به صورت دسته‌بندی شده در زیر منوی Firewall در دسترس است که زیر منوی این منوی اصلی را در شکل زیر مشاهده می‌کنید:



بخش Aliases:

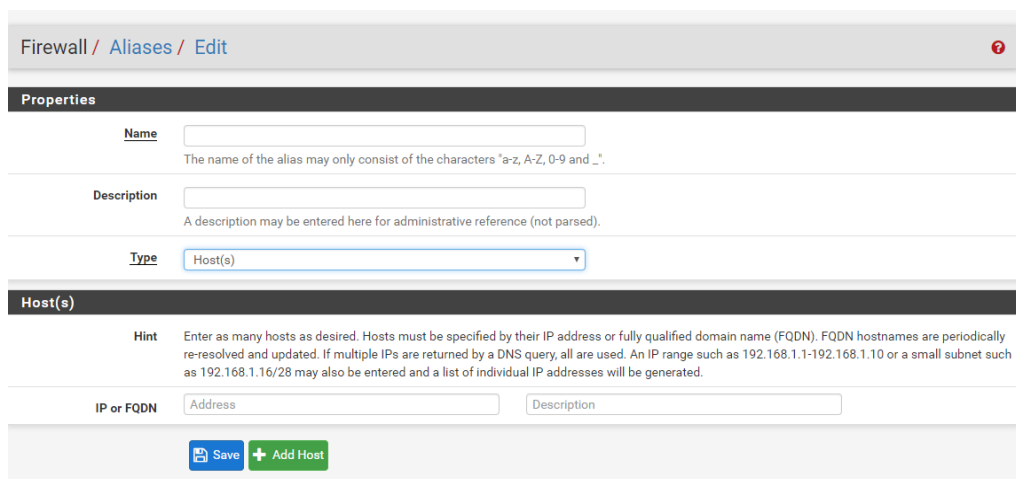
یکی از قابلیت‌های خوب پیاده‌سازی شده در pfSense بخش Aliases است که شما را در نوشتن رول‌های تکراری برای مشخصات مشترک کمک می‌کند. برای مثال فرض کنید که قصد دارید به یک رنج آدرس IP یا آدرس‌های مختلف و یا شماره پورت دسترسی خاصی دهید. اگر در این بخش از alias استفاده نکنید باید برای هر آدرس ip و یا هر پورت یک رول بنویسید که باعث ایجاد تعداد رول‌های زیاد شده و سرعت پردازش بسته‌ها را کند می‌کند و یا برای

اعمال تغییرات باید همه رول‌ها را تغییر دهید. با استفاده از این قابلیت شما به راحتی می‌توانید یک نام برای این دسته از اطلاعات انتخاب کنید و در این گروه هر مشخصه‌ای را وارد کنید و به راحتی از آن در رول‌ها استفاده کنید. بعد از وارد شدن به این بخش شما با منوی به صورت شکل زیر مواجه می‌شوید:



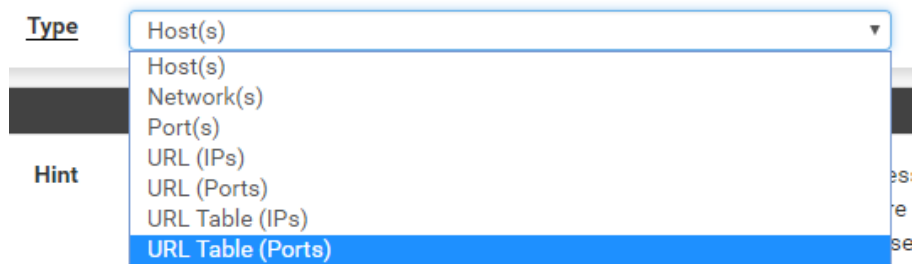
همان طوری که در شکل بالا مشاهده می‌کنید شما در سه دسته‌بندی کلی می‌توانید نام مستعار تعریف کنید بخش **ip** که شما در این بخش می‌توانید آدرس‌های **ip** را قرار دهید، بخش **ports** که شما می‌توانید عدد پورت‌های مورد نیاز خود را وارد کنید و بخش **URL** شما می‌توانید از قابلیت جدول برای تعریف کردن تعداد زیادی آدرس و یا شماره پورت استفاده کنید. در ادامه با روش تعریف کردن هر کدام از این بخش‌ها آشنا می‌شوید.

برای تعریف کردن آدرس‌های **IP** کافی است که در بخش **IP** بر روی گزینه **add** کلیک کنید تا منوی به صورت نمایش داده شده در شکل زیر هم برای شما باز شود:



همان طوری که مشاهده می کنید شما در این بخش هم می توانید آدرس ip وارد کنید و هم نام. برای شروع هم باید یک اسم انتخاب کنید که می تواند فقط شامل حروف کوچک و بزرگ باشد هم اعداد و _ بعد از وارد کردن نام در بخش name حال باید نوع را انتخاب کنید، این بخش به صورت پیش فرض بسته به انتخاب شما در منوی قبلی انتخاب شده است و شما در این بخش حتی می توانید سایر aliases را هم تعریف کنید که تفاوت اصلی آن ها وارد کردن نوع اطلاعاتی است که در بخش دوم ورود اطلاعات وجود دارد، در این بخش می توانید آدرس ip و یا نام host را وارد کنید در صورتی که تعداد بیشتری نیاز داشته باشید می توانید از کلید Add Host هم استفاده کنید. شما در این بخش هم می توانید یک رنج از آدرس ها را هم به صورت 192.168.1.1-192.168.1.10 هم تعریف کنید.

برای تعریف کردن سایر موارد هم به همین صورت می توانید اقدام کنید انواع آنرا در شکل زیر مشاهده می کنید:



در pf ما مفهوم به نام جدول برای تعریف کردن تعداد زیادی متغیر همسان داریم که در pfSense هم برای تعریف کردن آن از URL استفاده می شود که شما در نوع های URL این موضوع را مشاهده می کنید.

از این بخش می توانید در رول ها استفاده کنید که در بخش نوشتن رول ها در ادامه به آن ها می پردازیم.

بخش NAT:

به صورت پیش فرض اگر شما یک کارت شبکه LAN و یک کارت شبکه از نوع WAN داشته باشید و در زمان نصب کردن آن ها به pfSense معرفی کردن باشید و تنظیمات آن ها انجام داده باشید حالت NAT برای کاربرانی که در شبکه lan دارید فعال است و شما نیازی به تنظیمات اضافه ای ندارید. بعد از انتخاب کردن این بخش از منوی firewall شما با منویی به صورت زیر مواجه می شوید که دارای بخش هایی است که در ادامه در مورد آن ها صحبت خواهد شد:

pfSense COMMUNITY EDITION System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Gold ▾ Help ▾

Firewall / NAT / Port Forward

Port Forward 1:1 Outbound NPT

| Interface | Protocol | Source Address | Source Ports | Dest. Address | Dest. Ports | NAT IP | NAT Ports | Description | Actions |
|--|----------|----------------|--------------|---------------|-------------|--------|-----------|-------------|---------|
| <input type="button" value="Add"/> <input type="button" value="Add"/> <input type="button" value="Delete"/> <input type="button" value="Save"/> <input type="button" value="Separator"/> | | | | | | | | | |

همان طوری که مشاهده می کنید این بخش دارای 4 زیر منوی است که اولین آن ها منوی port Forward است که برای منتقل کردن درخواست ها بر روی یک پورت خاص در شبکه بیرونی برای انتقال به شبکه داخلی استفاده می شود، بعد از اضافه کردن این بخش به صورت خودکار رول فایروال برای باز کردن دسترسی به سمت سیستم داخلی برای شما در pfSense ایجاد می شود. برای ایجاد کردن یک رول در این بخش بر روی گزینه Add کلیک کنید تا منوی به صورت زیر برای شما باز شود:

Edit Redirect Entry

Disabled Disable this rule

No RDR (NOT) Disable redirection for traffic matching this rule
This option is rarely needed. Don't use this without thorough knowledge of the implications.

Interface
Choose which interface this rule applies to. In most cases "WAN" is specified.

Protocol
Choose which protocol this rule should match. In most cases "TCP" is specified.

Source

Destination Invert match. Type /

Destination port range From port Custom To port Custom
Specify the port or port range for the destination of the packet for this mapping. The 'to' field may be left empty if only mapping a single port.

Redirect target IP
Enter the internal IP address of the server on which to map the ports.
e.g.: 192.168.1.12

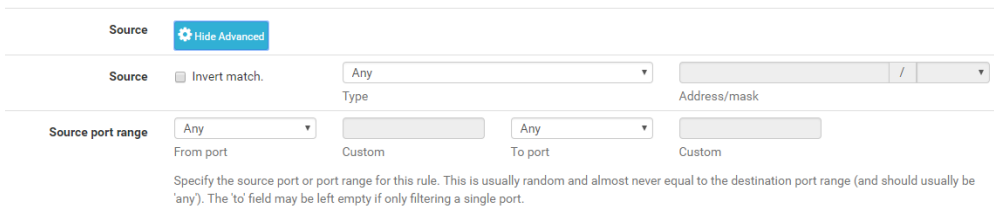
Redirect target port Port Custom

بخش اول گزینه disable است که برای غیرفعال کردن رول مورد نظر بدون اینکه رول را پاک کنید در نظر گرفته شده است.

گزینه NO RDR برای غیرفعال کردن حالت redirect استفاده می‌شود که به صورت پیش فرض استفاده نمی‌شود و در زمانی که شما آن‌ها فعال کنید بخش Redirect از منوی های زیرین حذف می‌شود.

در بخش Interface شما می‌توانید کارت شبکه‌ای را که قصد فعال کردن port Forward را بر روی آن دارید را انتخاب کرده که به صورت پیش فرض کارت شبکه wan برای این بخش انتخاب می‌شود.

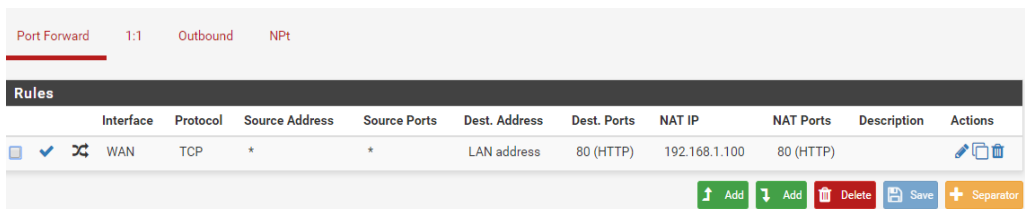
در این بخش گزینه source برای شما به صورت پیش فرض نمایش داده نمی‌شود، در این بخش شما می‌توانید محل ارسال بسته را مشخص کنید که در حالتی که شما قصد فعال کردن برای همه را دارید به بخش به صورت any تعریف می‌شود. در صورتی که نیاز به انتخاب آدرس‌های مبدأ خاصی دارید بر روی این بخش کلیک کنید تا بخشی به صورت زیر برای شما باز شود و شما بتوانید تنظیمان مبدأ را هم اعمال کنید:





همان طوری که در شکل بالا مشاهده می‌کنید تنظیمات پیش فرض در این بخش any است.

در ادامه بخش‌های این رول شما می‌توانید آدرس ip سیستم مورد نظر در شبکه LAN را انتخاب کنید. یکی از تنظیمات جالبی که در این بخش وجود دارد این است که هم می‌توانید به صورت دستی شماره پورت را وارد کنید و هم می‌توانید از نام‌هایی که در باکسی که با other مشخص شده‌اند استفاده کنید.

در بخش Redirect target IP شما باید آدرس ip مورد نظر خود را وارد کنید و در بخش زیرین این بخش هم باید شماره پورت را وارد کنید و بعد از Save کردن شما به صفحه قبل بازمی‌گردید با این تفاوت که یک رول جدید به صورت زیر برای شما در این بخش اضافه شده است:

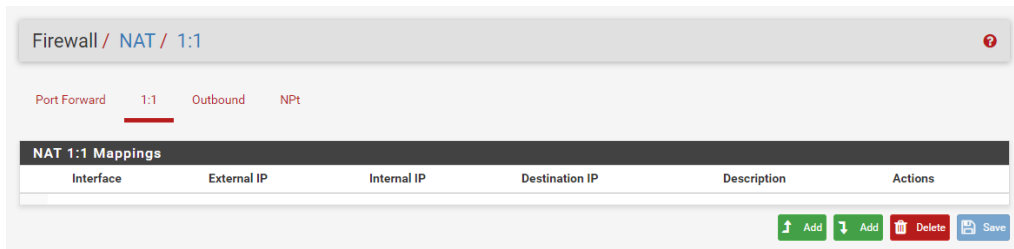


| Interface | Protocol | Source Address | Source Ports | Dest. Address | Dest. Ports | NAT IP | NAT Ports | Description | Actions |
|-----------|----------|----------------|--------------|---------------|-------------|---------------|-----------|-------------|---|
| WAN | TCP | * | * | LAN address | 80 (HTTP) | 192.168.1.100 | 80 (HTTP) | |   |

شما می‌توانید با استفاده از Add که فلش رو به بالا دارد بالاتر از این رول یک رول جدید اضافه کنید و یا به سمت پایین این رول هم بیکرو جدید اضافه کنید.

حالت nat 1:1

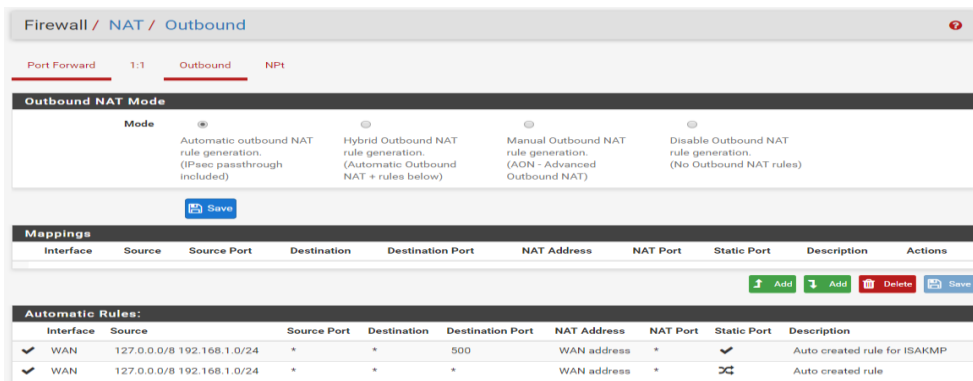
در این حالت اگر شما نیاز داشته باشید که یک رنج آدرس LAN را به یک رنج از آدرس WAN اختصاص داده و برای هر یک از این آدرس‌های داخلی یک آدرس خارجی خاص در نظر بگیرید از حالت Nat1:1 باید استفاده کنید. این بخش را در شکل زیر مشاهده می‌کنید:



The screenshot shows the 'NAT 1:1 Mappings' configuration page in pfSense. It includes a breadcrumb 'Firewall / NAT / 1:1' and tabs for 'Port Forward', '1:1', 'Outbound', and 'NPT'. Below the tabs is a table with columns: Interface, External IP, Internal IP, Destination IP, Description, and Actions. At the bottom right, there are buttons for 'Add', 'Add', 'Delete', and 'Save'.

بخش NAT Outbound:

در ابتدای بخش NAT برای شما توضیح دادم که pfSense به صورت خودکار NAT را برای کاربران LAN شما فعال می‌کند، این بخش در حقیقت همان جایی است که این تنظیمات به صورت خودکار اعمال می‌شود. این بخش دارای منوهای زیر است که در شکل زیر مشاهده می‌کنید:



The screenshot shows the 'Outbound NAT Mode' configuration page in pfSense. It includes a breadcrumb 'Firewall / NAT / Outbound' and tabs for 'Port Forward', '1:1', 'Outbound', and 'NPT'. Below the tabs is a section for 'Outbound NAT Mode' with four radio button options: 'Automatic outbound NAT rule generation (IPsec passthrough included)', 'Hybrid Outbound NAT rule generation (Automatic Outbound NAT + rules below)', 'Manual Outbound NAT rule generation (AGN - Advanced Outbound NAT)', and 'Disable Outbound NAT rule generation (No Outbound NAT rules)'. Below this is a 'Mappings' table with columns: Interface, Source, Source Port, Destination, Destination Port, NAT Address, NAT Port, Static Port, Description, and Actions. At the bottom, there is an 'Automatic Rules' table with columns: Interface, Source, Source Port, Destination, Destination Port, NAT Address, NAT Port, Static Port, and Description. The 'Automatic Rules' table shows two rules for the WAN interface.

| Interface | Source | Source Port | Destination | Destination Port | NAT Address | NAT Port | Static Port | Description |
|-----------|-------------|----------------|-------------|------------------|-------------|----------|-------------|------------------------------|
| ✓ WAN | 127.0.0.0/8 | 192.168.1.0/24 | * | * | 500 | * | ✓ | Auto created rule for ISAKMP |
| ✓ WAN | 127.0.0.0/8 | 192.168.1.0/24 | * | * | WAN address | * | ✗ | Auto created rule |

این منو خود به سه بخش تقسیم می‌شود که در شکل بالا مشاهده می‌کنید، بخش اول Outbound NAT Mode است که شما می‌توانید حالت‌های nat خروجی را مشخص کنید. در بخش Mappings شما می‌توانید رول‌های اختصاصی خود را بنویسید که البته باید در بخش بالایی حالتی را انتخاب کرده که این رول‌ها اعمال شود و در بخش سوم از این قسمت شما رول‌هایی که به صورت خودکار ایجاد شده‌اند را مشاهده می‌کنید.

در بخش Outbound NAT Mode شما می‌توانید چهار حالت را انتخاب کنید که در ادامه شما با آن‌ها آشنا می‌شوید.

حالت Automatic outbound NAT:

در این حالت که حالت پیش فرض است به صورت خودکار بخش nat فعال شده و رول‌های مربوطه را هم ایجاد کرده است.

حالت Hybrid Outbound NAT rule generation:

در این حالت علاوه بر حالت قبلی شما می‌توانید از بخش mapping رول‌های خود را هم به حالت NAT اضافه کنید.

حالت Manual Outbound NAT:

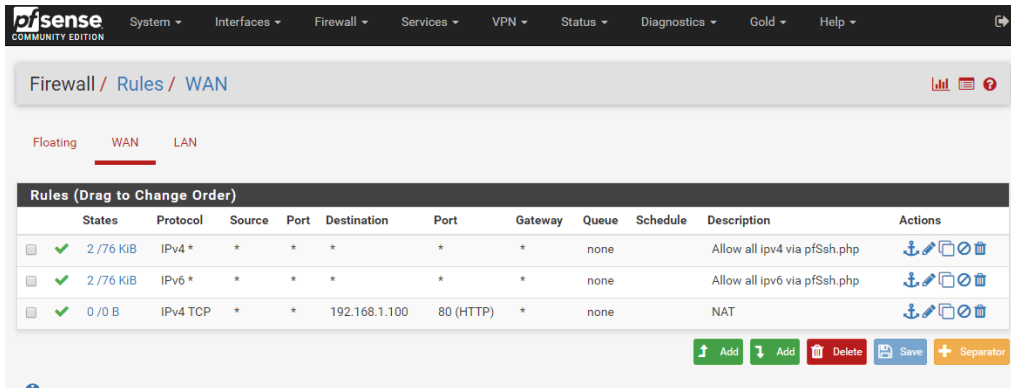
با انتخاب این بخش شما حالت خودکار را غیرفعال کرده‌اید و باید به صورت دستی رول‌های مربوط به nat را ایجاد کنید.

حالت Disable Outbound NAT:

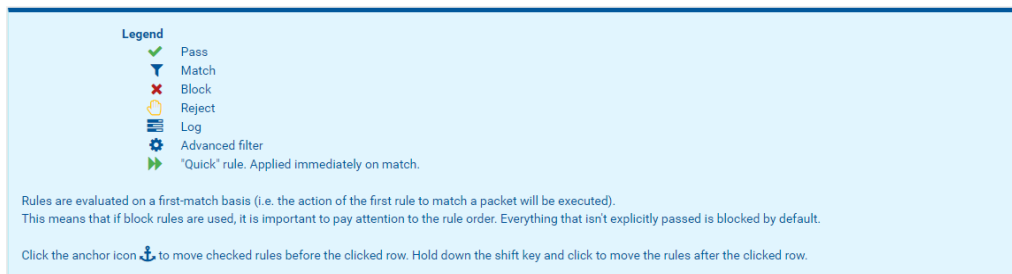
برای غیرفعال کردن حالت NAT شما باید این گزینه را انتخاب کنید و save کنید تا حالت NAT غیرفعال شود، در برخی از موارد شما قصد دارید که از pfSense به عنوان یک روتر استفاده کنید که باید این بخش را غیرفعال کنید.

بخش rule در pfSense:

یکی از بخش‌هایی که شما با آن بسیار کار داشته و در حقیقت مرکز اصلی فایروال pfSense است بخش rules است که با استفاده از آن شما می‌توانید سیاست‌های خاصی را برای ترافیک‌های ردوبدل شده در شبکه خود اعمال کنید. برای وارد شدن به این بخش باید از منوی firewall وارد بخش Rules شوید. این بخش را در شکل زیر مشاهده می‌کنید:



این بخش دارای ای کون‌هایی است که در شکل زیر توضیحات آن‌ها مشاهده می‌کنید:



همانطوری که مشاهده می‌کنید برای حالت‌های log Block Reject pass و غیره‌ای کون‌های خاصی در نظر گرفته شده است. در بخش Actions شما با آی‌کون‌هایی به صورت زیر مواجه هستید:



آی‌کون اول علامت لنگر است که کاربرد جالبی دارد، رول‌ها در این بخش به ترتیب از بالا به پایین مورد بررسی قرار می‌گیرد، برای انتقال دادن یک‌رو به پایین باید آن رو را انتخاب کنید که بخش در قسمت سمت راست هر رول یک

باکس مربعی کوچکی قرار دارد بعد از انتخاب آن می‌توانید از لنگر استفاده کنید تا با استفاده از حالت درک کردن بتوانید رول‌ها را به سمت پایین و یا بالا رول‌های دیگر منتقل کنید.



برای ویرایش کردن رو ایجاد شده از علامت مداد استفاده کنید و برای کپی کردن یکترو از علامت کناری مداد

استفاده کنید و در صورتی که نیاز دارید رول را فقط غیرفعال کنید از علامت استفاده کنید که رول شما را پاک نمی‌کند و فقط غیرفعال می‌کند. برای پاک کردن رول شما می‌توانید از آیکون سطل آشغال استفاده کنید. به این نکته توجه داشته باشید که در همه این موارد شما باید رول مورد نظر را انتخاب کنید. برای اعمال تغییرات باید از گزینه **save** استفاده کنید و بعد از اعمال هر تغییر شما باید از گزینه زیر برای اعمال کردن تغییرات مورد نظر خود استفاده کنید:

The firewall rule configuration has been changed.
The changes must be applied for them to take effect.

Apply Changes

بعد از کلیک کردن بر روی **Apply Changes** تغییرات مورد نظر شما اعمال می‌شود، برای مثال در شکل زیر مشاهده می‌کنید که رول انتهایی در این بخش را غیرفعال کرده‌ایم و هم‌رنگ آن تغییر کرده است و هم آیکون در بخش **Actions** ایجاد شده است، این تغییرات را در شکل زیر مشاهده می‌کنید:

| Rules (Drag to Change Order) | | | | | | | | | | |
|-------------------------------------|------------|----------|------|-------------|---------------|-----------|-------|----------|------------------------------|---------|
| States | Protocol | Source | Port | Destination | Port | Gateway | Queue | Schedule | Description | Actions |
| <input checked="" type="checkbox"/> | 6 / 38 KiB | IPv4 * | * | * | * | * | none | | Allow all ipv4 via pfSsh.php | |
| <input checked="" type="checkbox"/> | 6 / 38 KiB | IPv6 * | * | * | * | * | none | | Allow all ipv6 via pfSsh.php | |
| <input checked="" type="checkbox"/> | 0 / 0 B | IPv4 TCP | * | * | 192.168.1.100 | 80 (HTTP) | * | none | NAT | |

Add
 Add
 Delete
 Save
 Separator

برای ایجاد کردن یک رول جدید شما می‌توانید دو مسیر را انتخاب کنید در مسیر اول شما می‌توانید یکترو را انتخاب کنید و آن‌ها کپی کنید تا رول جدید ب همان مشخصات رول قبلی ایجاد شود و بعد آن‌ها ویرایش کنید و یا از ای



کون‌های استفاده کنید تفاوت این دو در محل ایجاد رول است که اگر قصد دارید رول شما در بالای لیست قرار گیرد از فلش رو به بالا و در صورتی که قصد دارید رول شما در زیر آن رو اعمال شود از آیکون

فلش سمت پایین استفاده کنید. بعد از کلیک کردن بر روی یکی از این دو آیکن صفحه‌ای برای ایجاد کردن یک رول جدید برای شما نمایش داده می‌شود که دارای بخش‌های مختلفی است به نام های زیر است

Edit Firewall Rule برای مشخص کردن رفتار رول موردنظر

Source مشخص کردن مبدأ رول

Destination برای مشخص کردن مقصد رول

Extra Options برای فعال کردن گزارش گیر بر روی رول و نوشتن توضیحات برای رول و بخش‌های پیشرفته.

قبل از نوشتن یک رول باید به زبانه بالایی این بخش توجه کنید که شما به تعداد کارت‌های شبکه موجود بر روی pfSense خود می‌توانید رول تعریف کنید برای مثال در شکل زیر مشاهده می‌کنید که سه کارت شبکه در این بخش وجود دارد :



با کلیک بر روی هر بخش شما می‌توانید رول‌های مربوط به هر کدام را مشاهده کنید بخش floating دارای رول‌هایی هستند که بر روی همه کارت‌های شبکه اعمال می‌شوند. در زمان ایجاد کردن یک رول شما می‌توانید کارت شبکه را انتخاب کنید و به تفکیک آن‌ها را در زیر این بخش‌ها مشاهده کنید.

ترتیب پردازش رول‌ها در pfSense به صورت زیر است:

در حالت کلی پردازش رول‌ها در pfSense به صورت زیر است:

Outbound NAT rules-1

Inbound NAT rules such as Port Forwards (including rdr pass and UPnP)-2

3- NAT rules for the Load Balancing daemon (relayd)

4- Rules dynamically received from RADIUS for OpenVPN and IPsec clients

5- Internal automatic rules (pass and block for various items like lockout, snort, DHCP,)

et

6- قواعد تعریف شده توسط کاربر که به ترتیب زیر پردازش می‌شوند .

1. قوانین تعریف شده در برگه floating
2. قوانین تعریف شده در هر یک از برگه های interface group و برگه OpenVPN
3. قوانین تعریف شده در برگه های مربوط به هر رابط شامل LAN, WAN, OPTx و ...

7- Automatic VPN rules

به این ترتیب اولویت پردازش را برای قواعد تعریف شده در برگه Floating در نظر می‌گیرد به بیان ساده‌تر ابتدا قوانین موجود در این برگه پردازش شده و پس از آن قواعد تعریف شده در هر یک از برگه های interface group و برگه OpenVPN و در نهایت قواعد تعریف شده در برگه های مربوط به هر رابط شامل LAN, WAN, OPTx و ... مورد پردازش قرار خواهند گرفت.

قوانین (Rules) تعریف شده در هر یک از برگه های LAN, WAN, OPTx و برگه های Interface Groups تنها بر ترافیک ورودی به رابط (Interface) مربوطه اعمال می‌شوند به بیان دیگر قواعد تعریف شده در این برگه ها ترافیک رسیده به رابط را تنها در جهت ورودی (Inbound) به رابط پردازش خواهند کرد. برای مثال برای کارت شبکه LAN ترافیک ورودی به بسته های گفته می‌شود که از سمت کاربران lan ارسال می‌شود و برای کارت شبکه wan ترافیکی است که از طریق کاربران شبکه دیگر که برای مثال کاربران شبکه اینترنت ارسال می‌شود ترافیک ورودی به این کارت شبکه است اعمال می‌شود.

چنانچه ترافیک رسیده به رابطها با هیچ یک از قوانین (Rules) تعریف شده توسط کاربر تطابق نداشته باشد و یا برای اجازه عبور یک ترافیک خاص از فایروال قانون صریحی توسط کاربر تعیین نشده باشد ، ترافیک مسدود شده و اجازه عبور از فایروال را نخواهد داشت. به بیان دیگر در این دو حالت قانون پیش فرض PfSense که ((قانون انسداد) Deny

Rule)) نامیده می‌شود بر ترافیک اعمال شده و ترافیک Block می‌گردد. به یاد داشته باشید که اقدام پیش‌فرض قانون Deny Rule اقدام Block است بنابراین قانون یادشده بسته‌ها بدون اطلاع به فرستنده حذف خواهد کرد.

حال در ادامه قصد داریم که یک رول ایجاد کنیم برای این کاربر روی زبانه lan بروید و از کلید Add استفاده کنید تا صفحه‌ای برای شما برای اضافه کردن رول باز شود، بخش‌های این بخش را در خطوط قبل بیان شده است، بخش اول صفحه را در شکل زیر مشاهده می‌کنید:

Edit Firewall Rule

Action Pass

Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled Disable this rule
Set this option to disable this rule without removing it from the list.

Interface LAN

Choose the interface from which packets must come to match this rule.

Address Family IPv4

Select the Internet Protocol version this rule applies to.

Protocol TCP

Choose which IP protocol this rule should match.

منوی اولیه این بخش Action است که در این بخش می‌توانید وضعیت رول را مشخص کنید که این بخش دارای 3 وضعیت است، حالت pass که اجازه عبور بسته را می‌دهد، دو حالت block و reject باعث عدم تردد بسته‌هایی می‌شوند که با رول موردنظر شما مطابقت دارند و تفاوت آن‌ها در این است که حالت reject برای ارسال‌کننده بسته یک بسته خطا ایجاد می‌کند و در حالت block این امر بدون ایجاد خطا ایجاد شده و ارسال‌کننده بسته هیچ اطلاعاتی از عدم ارسال بسته نخواهد داشت.

بخش disable زمانی برای شما کاربرد دارد که شما قصد دارید به‌طور موقت یک رول را بدون پاک کردن غیرفعال کنید تا در زمان موردنیاز دوباره آن‌ها فعال کنید.

در بخش interface شما فهرستی از کارت‌های شبکه بر روی pfSense را مشاهده می‌کنید و می‌توانید یک کارت شبکه را انتخاب کنید که به محلی که قصد دارید رول را ایجاد کنید بستگی دارد.

در بخش address family شما می‌توانید ورژن‌های 4 یا 6 یا هر دوی آن‌ها را انتخاب کنید برای نوع آدرس‌دهی. فایروال pfSense از ورژن 6 آدرس ip هم می‌تواند استفاده کند.

در بخش پروتکل هم شما نوع پروتکل موردنظر را انتخاب کنید که در شکل زیر لیست این پروتکل‌هایی که در pfSense قرار دارد را مشاهده کنید:



حالت any برای اعمال بر روی همه نوع از پروتکل‌ها استفاده می‌شود.

بخش Source و Destination شما می‌توانید آدرس و پورت را تعیین کنید که قصد محدود کردن یا تردد آن را دارید را تعیین کنید که در شکل زیر این دو بخش را مشاهده می‌کنید:

Source

Source Invert match. any Source Address /

⚙ Display Advanced

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any.

Destination

Destination Invert match. any Destination Address /

Destination Port Range (other) (other)

From Custom To Custom

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

پیش‌فرض این بخش به صورت any to any است که قابل تغییر برای نیاز و درخواست شماست.

در قسمت پایانی از ایجاد رول بخش Extra Options است که دارای بخش‌های پیش‌فرض زیر است:

Extra Options

Log Log packets that are handled by this rule
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).

Description
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Advanced Options [Display Advanced](#)

در بخش log شما می‌توانید مشخص کنید که از رول موردنظر شما در صورت استفاده شدن log گرفته شود و شما با استفاده از log بتوانید وضعیت را موردبررسی قرار دهید، در بخش Description می‌توانید یک توضیحات مختصری در مورد رولی که ایجاد کرده را بنویسید تا در بخش نمایش رول بتوانید از آن استفاده کنید.

یک بخش بسیار کاربردی و حرفه‌ای در این بخش وجود دارد که ب کلید بر روی Advanced Options در ادامه صفحه برای شما باز می‌شود که شما می‌توانید با استفاده از آن فیلدهای بیشتری را موردبررسی قرار دهید. یکی از قابلیت‌های کاربردی در این بخش این است که شما pfSense قابلیت شناسایی سیستم‌عامل‌های مختلف را دارد و شما می‌توانید از آن برای محدود کردن در رول‌ها استفاده کنید و حتی می‌توانید در این بخش TCP Flags خاصی را هم مدیریت کنید.

در شکل زیر برای مثال رولی اضافه‌شده است که جلوی ترافیک ICMP را برای کاربران شبکه LAN مسدود می‌کند. بعد از ایجاد کردن هر تغییر شما باید بر روی Apply Changes که در بالا صفحه‌نمایش داده می‌شود کلیک کنید:

| Floating | | WAN | | LAN | | Rules (Drag to Change Order) | | | | | |
|----------|----------|---------------|------|-------------|-----------------|------------------------------|-------|----------|-------------------|------------|--|
| States | Protocol | Source | Port | Destination | Port | Gateway | Queue | Schedule | Description | Actions | |
| ✓ | 0/0 B | * | * | LAN Address | 443 80 22 | * | * | * | Anti-Lockout Rule | ⚙️ | |
| ☐ | ✗ 0/0 B | IPv4 ICMP any | * | * | * | * | * | none | | 📄 🗑️ 🗑️ 🗑️ | |