دیوار آتش‌های متن‌باز

کد: APA-Semnan-Open-Source-Firewalls

طبقه‌بندی: عادی

http://cert.semnan.ac.ir
cert@semnan.ac.ir

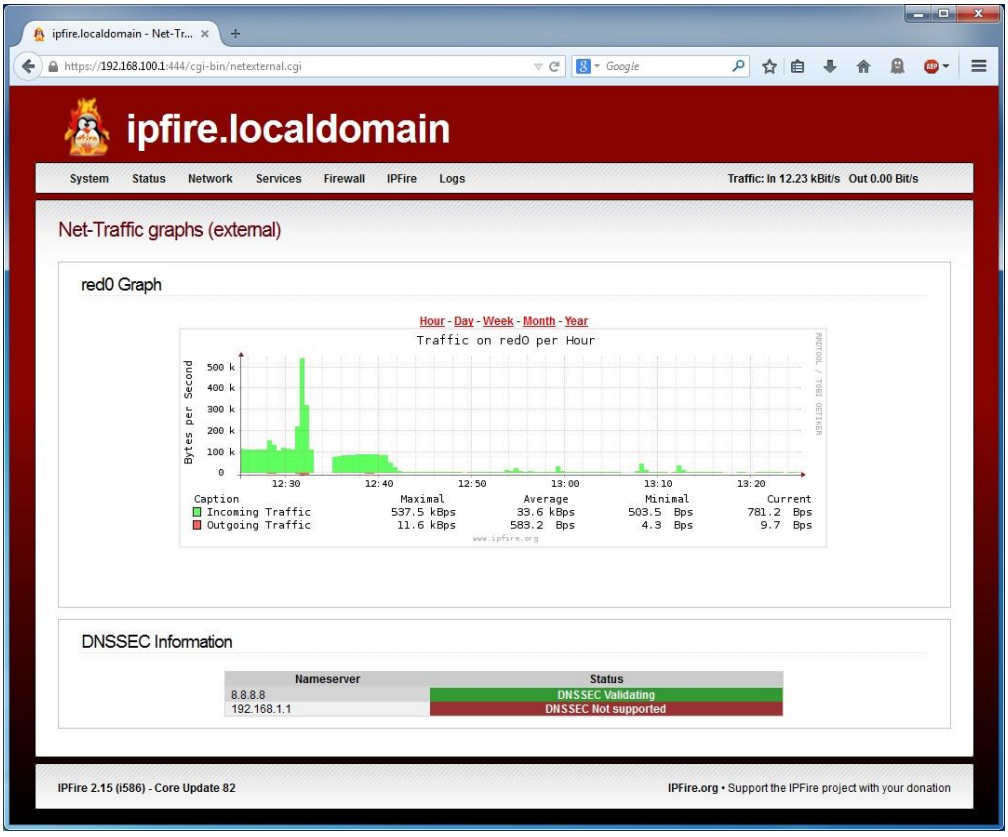
تابستان ۹۶

مقدمه

دیوار آتش[1] یک قطعه‌ی نرم‌افزاری یا سخت‌افزاری است که مانند دیواری از رایانه‌ی شما محافظت می‌کند. در واقع دیوار آتش با تمرکز بر روی شبکه و اتصال اینترنت، تسهیلات لازم در جهت عدم دستیابی کاربران غیرمجاز به شبکه و یا رایانه‌ی شما را ارائه می‌نماید. دیوار آتش‌های این اطمینان را ایجاد می‌نمایند که صرفاً پورت‌های ضروری برای کاربران و یا سایر برنامه‌های موجود در خارج از شبکه در دسترس و قابل استفاده می‌باشد. به منظور افزایش ایمنی، سایر پورت‌ها غیرفعال می‌گردد تا امکان سوء استفاده از آنان توسط مهاجمان وجود نداشته باشد. در این گزارش به بررسی دیوار آتش‌های متن‌باز عموماً شناخته‌شده پرداخته می‌شود.

IPFire –۱

IPFire یک توزیع برای استفاده دیوار آتش و مسیریاب[2] می‌باشد که شامل ابزارهای بسیار کارآمد برای مدیران سیستم و شبکه می‌باشد.



شکل ۱ – نمایی از بخش Net-traffic graphs در IPFire

از ویژگی مهم این دیوار آتش می‌توان به ۱- توزیع شده (Distributed) ۲- سطح Kernel اشاره کرد.

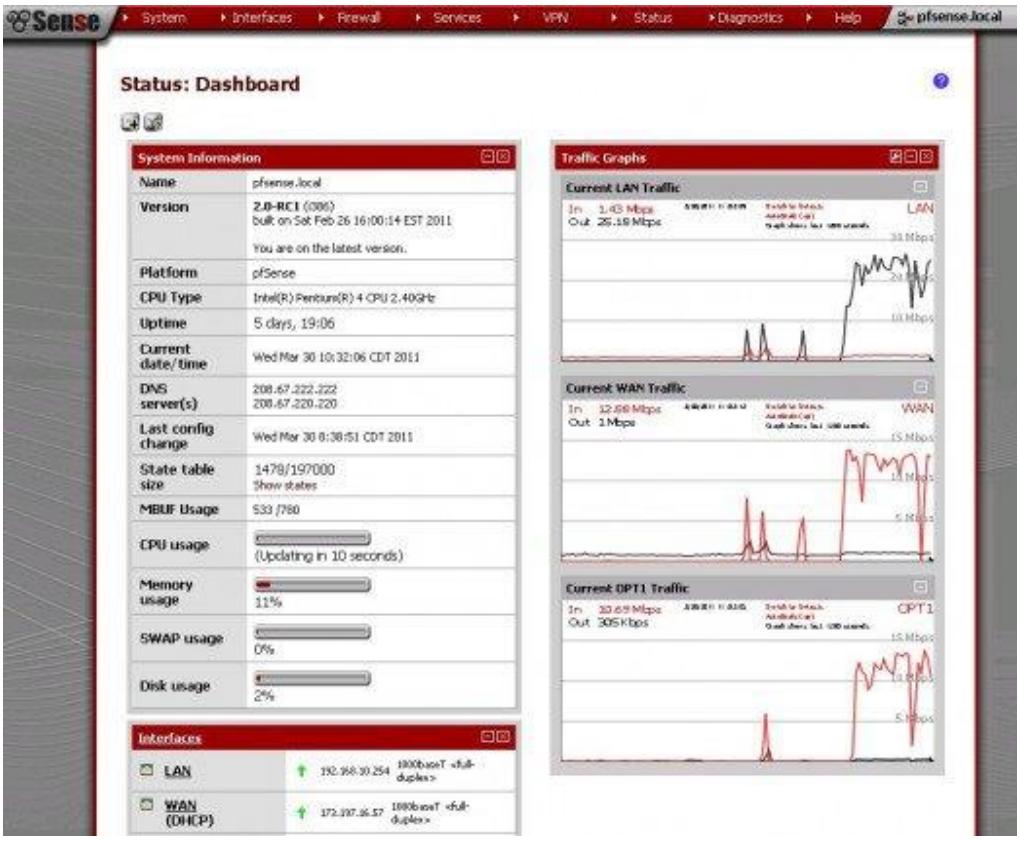
[1] Firewall
[2] Router

خصوصیات		توضیحات
Packfire		پکیج ها و بسته های مدیریتی زیادی برای آن توسعه یافته است.
Web Proxy	Security	ایجاد امنیت
	Authentication	احراز هویت
	Authorization	صحت اعتبار
	Logginig	سیستم ورود و خروج
	Bandwidth management	مدیریت پهنای باند برای هر کاربر
Content Filter		فیلتر کردن براساس آدرس سایت یا محتوای آن
Transparent mode		در این حالت در بسته ها هیچ تغییری ایجاد نمی شود و تنها به بررسی بسته ها برای یافتن بدافزار ها می پردازد.
VPN	IPSec	اتصال به وسیله‌ی پروتکل Ipsec
	OpenVPN	اتصال به وسیله‌ی پروتکل Open VPN
Wireless Access Point		تنظیمات مربوط به AP
System	Wireless Client	تنظیمات مربوط به wireless
	Mail Server	ارسال ایمیل از سیستم
	Ssh Access	دسترسی به وسیله ی SSH
	Backup	پشتیبان گیری از تمام تنظیمات وذخیره ی آن در قالب یک فایل ISO
Status	System	نمایش گراف استفاده از CPU
	Memory	نمایش گراف استفاده از حافظه و SWAP
	Services	وضعیت سرویس های فعال و مقدار استفاده آن ها از پردازنده
	Media	دمای سرور و حافظه و وضعیت آن ها
	Net-Traffic	جزئیات ترافیک
	Connections	وضعیت ارتباطات
	Hardware Graphs	نمایش گراف مربوط به استفاده از منابع سخت افزاری
	OpenVPN Clients	آمار VPN های متصل
	Network (other)	وضعیت شبکه های دیگر (DMZ و...)
	Network (internal)	وضعیت شبکه داخلی
	Network (external)	وضعیت شبکه خارجی
Network	Web Proxy Server	قابلیت پیکربندی Proxy Server
	DHCP Server	
	The Connection Scheduler	تعیین زمان بندی برای اتصال به شبکه
	Edit Hosts	اختصاص نام به IPها برای دسترسی ساده تر (سرویس نام دامنه ی داخلی)
	Static routes	مسیریابی بر اساس مسیریابی ایستا
	Aliases	اختصاص آدرس IP عمومی
	DNS Server	
	Assign MAC Address	تغییر آدرس مک
	Wake On LAN	قابلیت استفاده از این پروتکل در شبکه
	Bridge-Green-Blue	ترکیب دو شبکه‌ی مختلف و تبدیل آن به یک شبکه

	Network Modes	هر شبکه دارای ویژگی های خاص خود می باشد
Service	IPSec	
	OpenVPN	
	Dynamic DNS	پیاده سازی Dynamic DNS
	The Time Server	NTP Server
	Quality of Service	QoS
	Intrusion Detection System	IDS
	ExtraHD	قابلیت توسعه پذیری دیسک ها و حافظه ها
Logs	Summary	خلاصه وضعیت
	Setting	نمایش رخدادهای مربوط به تغییر تنظیمات
	Proxy-Logs	نمایش رخدادهای مربوط به پراکسی سرور
	Firewall	نمایش رخدادهای مربوط انتطباق یا عدم انتطباق با قوانین
	Attacks from IPs	حملات تشخیص داده شده توسط IPS
	IDS	حملات تشخیص داده شده توسط IDS
	Attacks to Ports	حملات پورت
	URL-Filter	فیلتر کردن آدرس
	System	

PfSense-۲

PfSense یک بستر مسیریابی و دیوار آتش انعطاف‌پذیر است که می‌تواند هم به عنوان دیوار آتش و هم به عنوان مسیریاب مورد استفاده قرار گیرد؛ این ابزار توزیعی رایگان و سفارشی از FreeBSD است و شامل فهرست طولانی از ویژگی‌های مربوطه بوده که امکان بسط بیشتر را نیز فراهم می‌کند. این ابزار از زمان انتشار یک میلیون بار بارگیری شده و یکی از پراستفاده‌ترین دیوار آتش‌های در دنیا به حساب می‌آید. شایان ذکر است که این پروژه سال ۲۰۰۴ آغاز شد و در حال حاضر محبوبیت زیادی کسب کرده است. یکی از ویژگی‌های مفید آن توانایی فیلترکردن براساس IP مبدأ و مقصد، پروتکل IP، پورت مبدأ و مقصد برای ترافیک TCP و UDP می‌باشد. با استفاده از این ابزار می‌توانید شبکه‌های کوچک و بزرگ خود را محافظت نمایید. این نرم‌افزار که یکی از پراستفاده‌ترین دیوار آتش‌های در دنیا به حساب می‌آید یک بستر مسیریابی و دیوار آتش انعطاف‌پذیر است که می‌تواند هم به عنوان دیوار آتش و هم به عنوان مسیریاب مورد استفاده قرار گیرد اما به دلیل فاصله‌ی زیاد نسخه تجاری و نسخه‌ی رایگان در برخی کشورها استفاده‌ی چندانی از آن نمی‌شود. این ابزار توزیعی رایگان و سفارشی از FreeBSD است و شامل فهرست طولانی از ویژگی‌های مربوطه بوده که امکان بسط بیشتر را نیز فراهم می‌کند.



شکل ۲ – نمایی از دیوار آتش PfSense

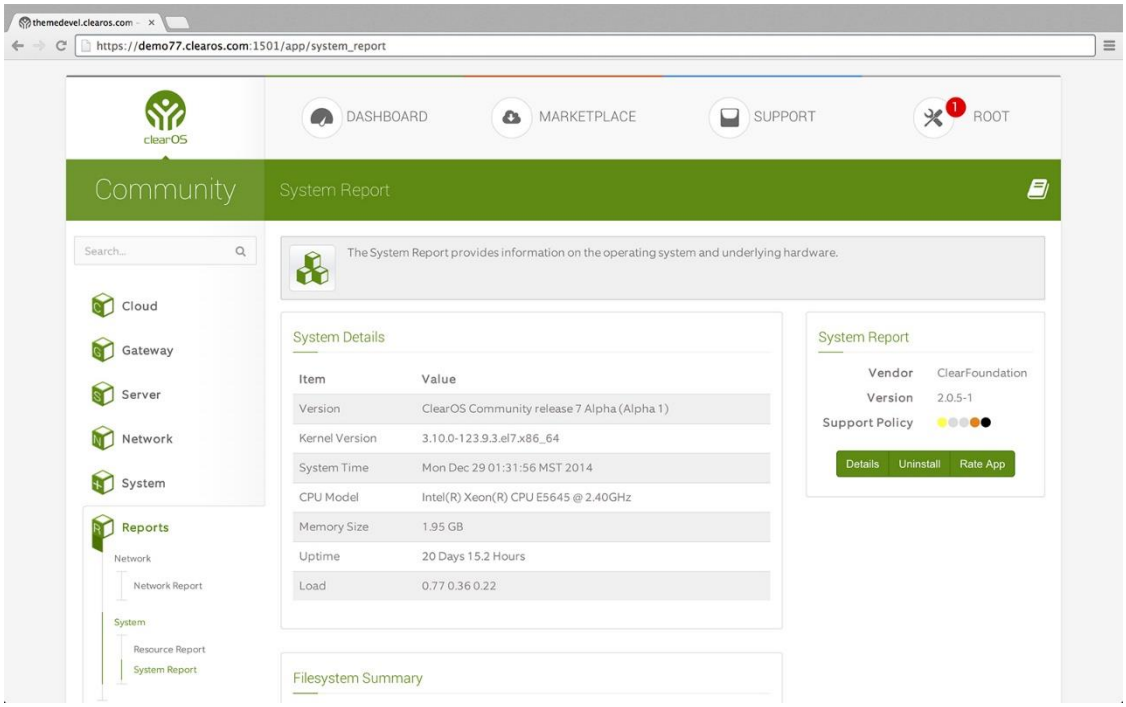
از مهمترین ویژگی این دیوار آتش می‌توان به حالت‌مند بودن آن اشاره کرد.

خصوصیات	توضیحات
Wireless Access Point	با اتصال چیپی که VAP/MBSS را پشتیبانی کند
Traffic Shaping	پشتیبانی از ALTQ، limiters، 802.1p match/set، DiffServ/DSCP
State Table Controls	بر اساس قوانین، زمان بندی، محدودیت ها...
Redundancy/High Availability	با استفاده از CARP+pfsync+XMLRPC Config syncمی تواند باعث کاهش از دست دادن تجهیزات شود. (حداقل دو فایروال نیاز است)
Nat	قابلیت Port Forwarding، NAT ۱:۱، Outbound NAT، NPT با استفاده از NAT
Multi-WAN	
Inbound Load Balancing	ایجاد تعادل در ترافیک ورودی
Network Diagnostic Utilities	با نصب پکیج‌ها
VPN	پشتیبانی از IPSec، Open VPN، L2TP
PPOE Server	
RRD Graphs	نمایش گراف تغییرات دما، استفاده از منابع و ...
Traffic Graphs	نمایش گراف ترافیک به صورت زنده
Dynamic DNS	
Captive Portal	نمایش پورتال قبل از دسترسی

DHCP Server	
SSH	دسترسی با SSH
Virtual Interfaces	پشتیبانی از VLAN، LAGG/LACP، GIF، GRE، QinQ ،PPPoE/PPTP/L2TP/PPP WANs
Dns Forwarder/Resolver	کَش و ذخیره کردن DNS
Proxy Server	با نصب پکیج

۳- ClearOS

این ابزار که همخوانی زیادی با سرورهای HPE داشته براساس نسخه‌ی RedHat لینوکس توسعه داده شده است و از آن می‌توان به عنوان یک مسیریاب نیز استفاده کرد. این ابزار در دو نسخه‌ی معمولی (رایگان) و نسخه‌ی تجاری (با پرداخت هزینه) ارائه شده است. از ویژگی‌های آن می‌توان به Gateway AntiVirus، Mail AntiVirus، Mail AntiSpam و... اشاره کرد.



شکل ۳ – نمایی از دیوار آتش ClearOS

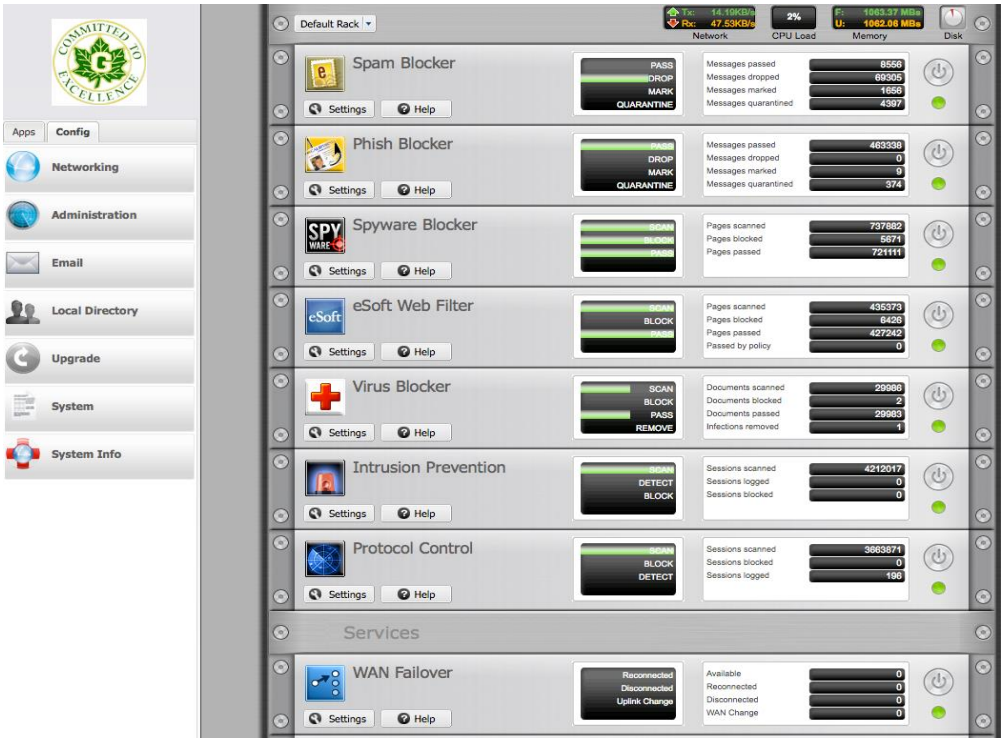
از مهمترین ویژگی آن می‌توان به حالت‌مند بودنش اشاره کرد.

خصوصیات	توضیحات
IDS	با استفاده از Snort
VPN	PPTP ،OpenVPN ،IPSec
Web Proxy	فیلتر کردن یک محتوای به خصوص و همچنین بررسی آن توسط ضد ویروس (با استفاده از Squid, DansGuardi)
E-Mail Services	پشتیبانی از Webmail, Postfix, SMTP, POP3, IMAP

Groupware	با استفاده از Kolab
File And Print Services	با استفاده از CUPS ،Samba
Flexshares	پشتیبانی از پروتکل های http، https، ftp، ftps، smb، smtp
WAF	
MultiWAN	طراحی شده برای کاهش از دست رفتن تجهیزات (High Availability)
Database And Web Server	پیاده سازی با استفاده از LAMP stack

Untangle-۴

Untangle نوعی UTM می‌باشد و تمام چیزهایی که شبکه شما برای سالم ماندن به آن نیاز دارد را در یک بسته جمع‌آوری کرده است. این بسته شامل: فیلترکردن محتوای وب و هرزنامه‌ها، ویروس‌یابی، VPN، قابلیت Failover بر روی چندین شبکه WAN و قابلیت‌های دیگر را پشتیبانی می‌کند.



شکل ۴ – نمایی از دیوار آتش Untangle

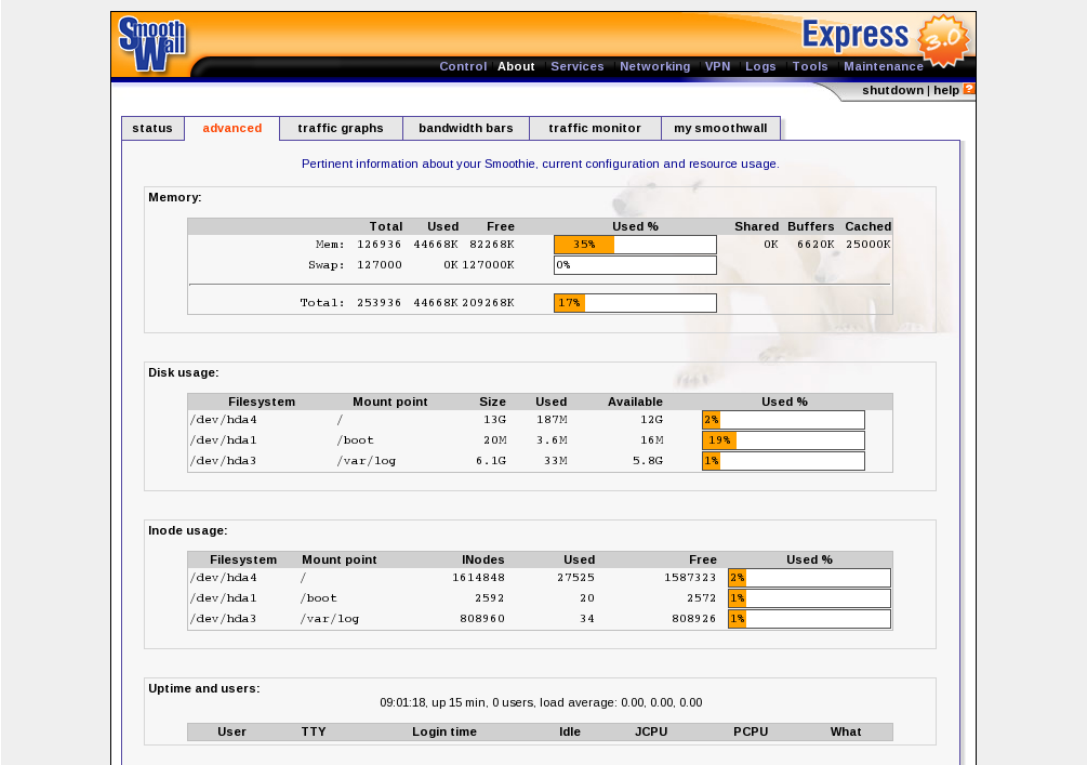
از مهمترین ویژگی‌های این دیوار آتش که آن را با دیگران متمایز می‌کند می‌توان به داشتن نسخه‌ی ویندوزی و امکان نصب اپلیکیشن‌های مختلف بر روی آن اشاره کرد.

خصوصیات	توضیحات
Web Filter	فیلترکردن محتوا و آدرس
SSL Inspector	رمزگشایی https و smtp برای بررسی محتوای آن
Policy Manager	ساخت سیاست‌های امنیتی مختلف

Branding Manager	بستن یک صفحه یا آدرس با توجه یک پیام خاص یا لگوی آن
WAN Failover	پشتیبانی از High Availability
WAN Balancer	Load Balancing
VPN	OpenVPN ،IPSec
Application Control	کنترل پروتکل‌ها و اپلیکیشن‌ها با استفاده از پیاده‌سازی قوانین پیچیده توسط اپلیکیشن‌های نصب شده
Web Cache	
Bandwidth Control	کنترل پهنای باند با توجه به کاربر و QoS
Virus Blocker	جلوگیری از نفوذ ویروس در شبکه به وسیله‌ی IPS
Spam Blocker	جلوگیری از ورود ایمیل های Spam در Mail Server
Directory Connector	گزارش گیری و اتصال براساس Active Directory
Web Monitor	
Phish Blocker	
Intrusion Prevention	IPS
Reports	دارای سیستم گزارش گیری
Ad Blocker	جلوگیری از تبلیغات
Captive Portal	

۵- Smoothwall

این دیوار آتش که به دلیل استفاده از IPChain غیر حالت‌مند بوده و از انواع توزیع‌شده می‌باشد براساس نسخه‌ی Redhat لینوکس توسعه یافته است.



شکل ۵ – نمایی از دیوار آتش Smoothwall

خصوصیات	توضیحات
External Connectivity	Static Ethernet, DHCP Ethernet, PPPoE, PPPoA
Filtering	باتوجه به Black List
Qos	
Traffic Stats	باتوجه به درگاه شبکه و IP
IDS	باتوجه به به‌روزرسانی خودکار قوانین Snort
UPnP	پشتیبانی از UPnP
Proxy	پشتیبانی از وب پروکسی برای افزایش سرعت بارگذاری وب، پشتیبانی از POP3 برای بررسی توسط ضدویروس، IM Proxy
Traffic Graphs	
Backup	دارای سیستم پشتیبان گیری
Updates	به‌روزرسانی خودکار
Time Service	زمان سرویس و تنظیم زمان دسترسی
مدیریت متمرکز	
رابط گرافیک کاربری با کنترل پنل Webmin	
پشتیبانی از ISPهای متعدد	

Shorewall-۶

دیوار آتش Shorewall یکی دیگر از محبوب‌ترین دیوار آتش‌های متن‌باز برای لینوکس GNU است. این دیوار آتش بر روی سیستم Netfilter ای که در هسته لینوکس درون ساخت است ایجاد شده و از IPv6 پشتیبانی می‌کند.

خصوصیات	توضیحات
Netfilter	فیلترکردن بسته‌ها
پشتیبانی از طیف گسترده از اپلیکیشن‌ها	Router , Firewall , Gateway
مدیریت متمرکز	
رابط گرافیک کاربری با کنترل پنل Webmin	
پشتیبانی از ISPهای متعدد	
Port Forwarding & Masquerading	
VPN	

IPcop -۷

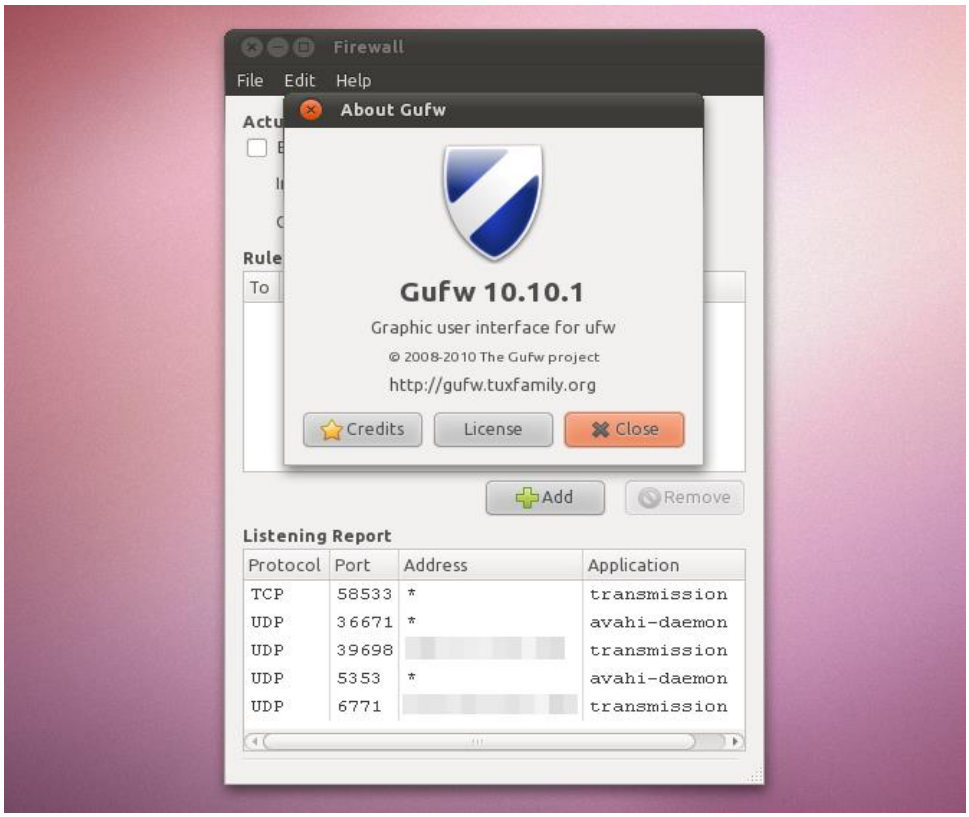
IPCop یکی از دیوار آتش‌های لینوکسی متن‌باز است. تیم IPCop به طور مداوم بر روی فراهم‌آوردن سیستم مدیریت کاربرپسند، امن، پایدار کار می کنند. رابط وب این دیوار آتش به خوبی طراحی شده و مدیریت آن را ساده‌تر می‌سازد. این دیوار آتش برای کسب و کارهای کوچک و رایانه‌های محلّی مفید خواهد بود. شما می‌توانید رایانه قدیمی خود را به عنوان یک VPN امن پیکربندی کنید تا محیط امنی را ایجاد نمایید. این گزینه اطلاعاتی که اخیراً استفاده شده است را حفظ می‌کند تا تجربه بهتری برای کاربران فراهم آورد.

شکل ۶ – نمایی از دیوار آتش IPCop

خصوصیات	توضیحات
رابط وب رنگی این فایروال به شما اجازه می دهد عملکرد کارت گرافیکی را برای CPU، حافظه و دیسک مانیتور کنید.	
پشتیبانی از زبان‌های متعدد	
ارتقای بسیار امن و آسان	

UFW –۸

UFW دیوار پیش‌فرض برای سرورهای Ubuntu می‌باشد. این گزینه اساساً برای کاهش پیچیدگی IP Table طراحی شده است و آن را کاربرپسندتر می‌سازد. رابط گرافیک کاربری این دیوار آتش، برای سرورهای Ubuntu و Debian موجود است.

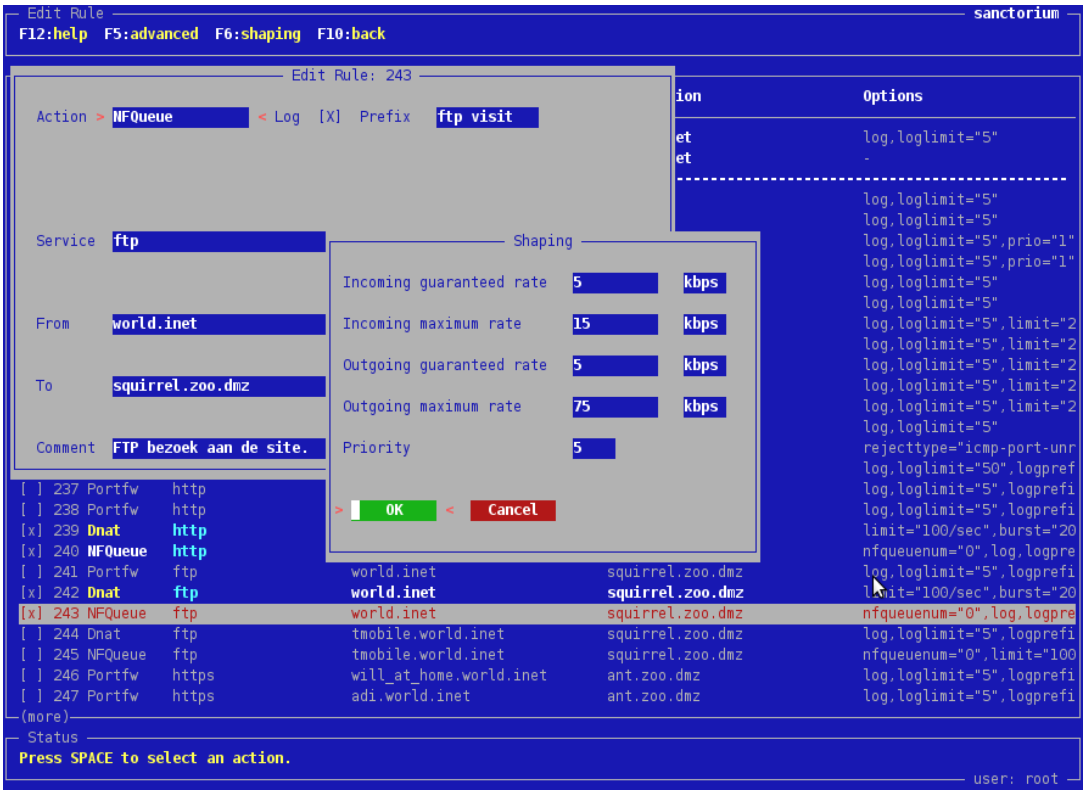


شکل ۷ – نمایی از دیوار آتش UFW

خصوصیات	توضیحات
پشتیبانی از IPv6	
گزینه های Logging متعدد با امکانات On/Off	
مانیتورکردن وضعیت	
فریم‌ورک توسعه‌پذیر	
قابلیت ادغام با اپلیکشین‌ها	
اضافه‌کردن/ حذف‌کردن و اصلاح‌نمودن قوانین براساس نیازهای شرکت	

۹-Vuurmuur

Vuurmuur یکی دیگر از دیوار آتش‌های لینوکسی قدرتمند برای سرور یا شبکه است. این گزینه برای ادمین ها نیز بسیار کاربرپسند است. ادمین ها برای کار کردن با این فایروال نیازمند دانش قبلی در مورد iptables نیستند.

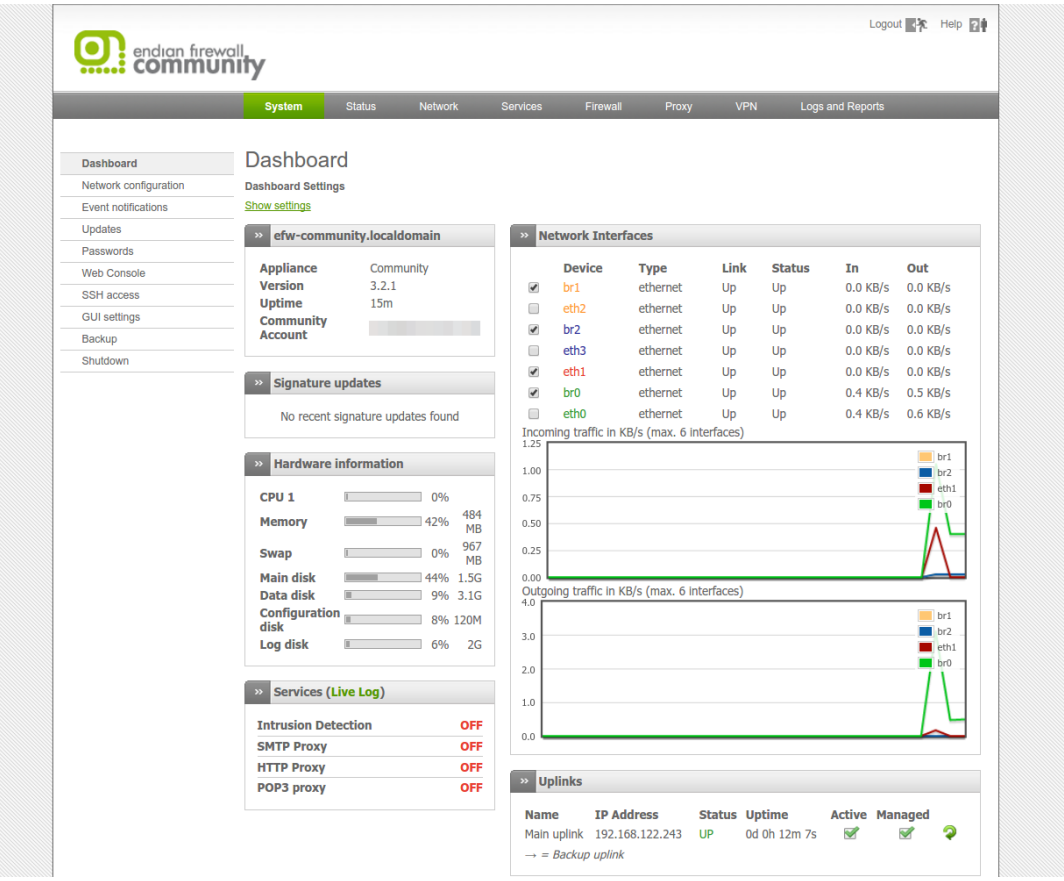


شکل ۸ – نمایی از دیوار آتش Vuurmuur

خصوصیات	توضیحات
پشتیبانی از IPv6	
شکل‌دهی به ترافیک	
قابلیت‌های مانیتورینگ پیشرفته	
مانیتورینگ زمان واقعی ارتباط و مصرف پهنای باند	
پیکربندی آسان با NAT	
قابلیت Anti-Spoofing	

Endian –۱۰

Endian، دیوار آتش مبتنی بر مفهوم بررسی بسته های Stateful است که می توان به عنوان مسیریاب، پروکسی و Gateway VPN با OpenVPN توسعه داد.

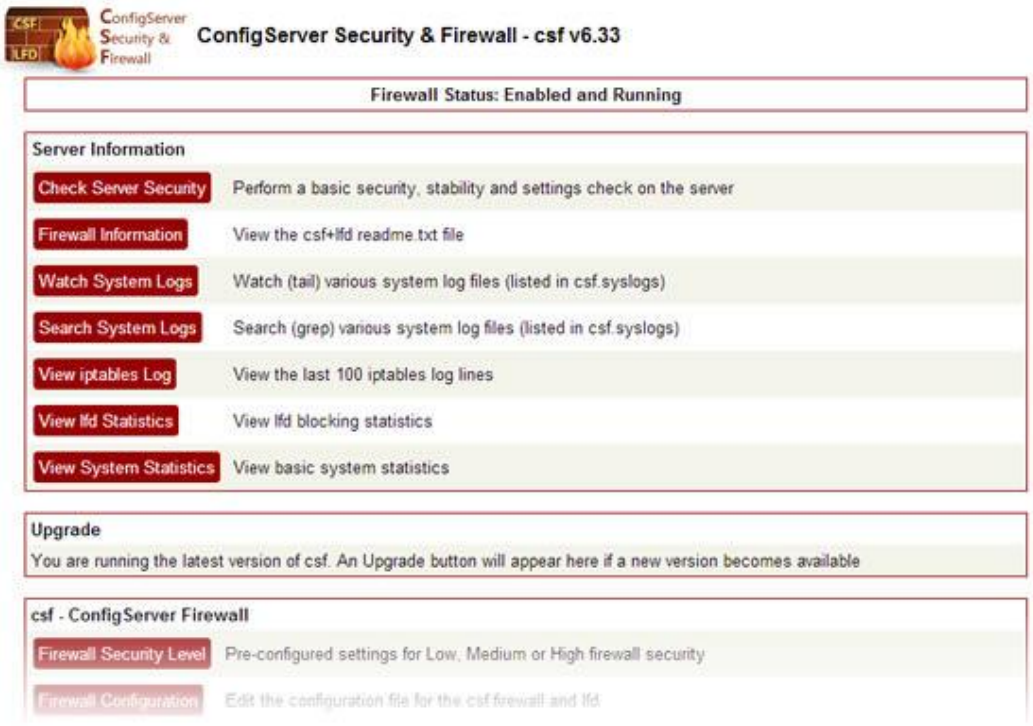


شکل ۹ – نمایی از دیوار آتش Endian

خصوصیات	توضیحات
دیوار آتش دوطرفه	
پیشگیری از نفوذ	Snort
مکان امن کردن وب سرور با پروکسی های FTP و HTTP ، آنتی ویروس و بلک لیست URL ها	
امکان امن‌کردن میل‌سرور با پراکسی	POP3 و SMTP، Greylisting
VPN	IPSec
لاگ زمان واقعی شبکه	

۱۱- CSF [1]

این گزینه یکی از دیوار آتش‌های تطبیق‌پذیر است. CSF مبتنی بر مفهوم Stateful Packet Inspection (SPI) کار می‌کند. این گزینه تقریباً تمامی محیط‌های مجازی‌سازی همچون XEN، Vmware، OpenVZ، KVM و Virtual Box را پشتیبانی خواهد کرد.



شکل ۱۰ – نمایی از دیوار آتش CSF

خصوصیات	توضیحات
بررسی مشکلات ورود در سرورهای حساس نظیر SSH	Login Failure Daemon
پیکربندی Alertهای ایمیلی	
ادغام با کنترل‌پنل‌های محبوب	Cpanel, Webmin, Direct Admin
نمایش فرآیندهای مشکوک و استفاده بیش از حد منابع	از طریق پست الکترونیک
داشتن سیستم Intrusion detection پیشرفته	
محافظت از لینوکس باکس	
بررسی سوء استفاده از سرور	
آسان بودن عملیات Start، Restart و Stop	

[1] ConfigServer Security Firewall