دژافزار نت
DEZHAFZAR CORPORATION

ARIYADEZH

Ariadezh UTM

سامانه مدیریت یکپارچه تهدیدات آریادژ

آریـــادژ، امنیتـــ پایدار شبکه شمـــا

ARIYADEZH

info@dezhafzar.com http://www.dezhafzar.com

فهرست :

۱. احراز هویت (Authentication)

به منظور جلوگیری از دسترسی‌های غیرمجاز و سوء استفاده‌های احتمالی محصول آریادژ از دو سطح احراز هویت پشتیبانی می‌کند. احراز هویت ترافیک شبکه (Data Plane) و احراز هویت واسط کاربری سامانه. احراز هویت ترافیک شبکه امکان تشخیص کاربر ارسال‌کننده ترافیک را می‌دهد، به صورتی که کاربر در صورتی مجاز به ارسال ترافیک است که پیش‌تر تصدیق هویت شده باشد. احراز هویت واسط کاربری به منظور جلوگیری از دسترسی غیر مجاز به پنل مدیریتی استفاده می‌گردد.

۱.۱. قابلیت‌های احراز هویت ترافیک:

- پشتیبانی از کاربران LDAP(Active Directory)، RADIUS و کاربران تعریف شده در سامانه
- تشخیص کاربرانی که مجوز ارسال ترافیک را دارند
- شخصی سازی قالب صفحه احراز هویت (Captive Portal)
- سازگاری با انواع ویندوز سرورها
- نمایش لیست کاربران و مدیریت آن‌ها
- مدیریت و تشخیص کاربران غیرفعال و خارج‌شده از سیستم

۲.۱. قابلیت‌های احراز هویت واسط کاربری:

- احراز هویت دو مرحله‌ای (Two Step Authentication) در پنل مدیریت با استفاده از کلمه عبور و SMS
- قابلیت غیرفعال کردن پورت‌های HTTP، HTTPS و فعال شدن خودکار آن‌ها در صورتی که کاربر ارتباط SSH برقرار نماید. با کمک این ویژگی واسط کاربری تحت وب دیواره آتش در معرض حمله مهاجمان قرار نمی‌گیرد.
- امکان SSH preauthentication برای جلوگیری از دسترسی به واسط کاربری تا اولین لاگین موفقیت آمیز در کنسول SSH.

۱ .۳. ورود یک باره (Single Sing On)

دیواره آتش آریادژ با استفاده از قابلیت احراز هویت Active Directory کاربرانی را که به عضویت دامنه در آمده‌اند شناسایی می‌کند. از این رو دیواره آتش توسط این ویژگی، از ورود و خروج کاربران آگاه می‌شود و دیگر نیازی به احراز هویت مجدد کاربران نیست.

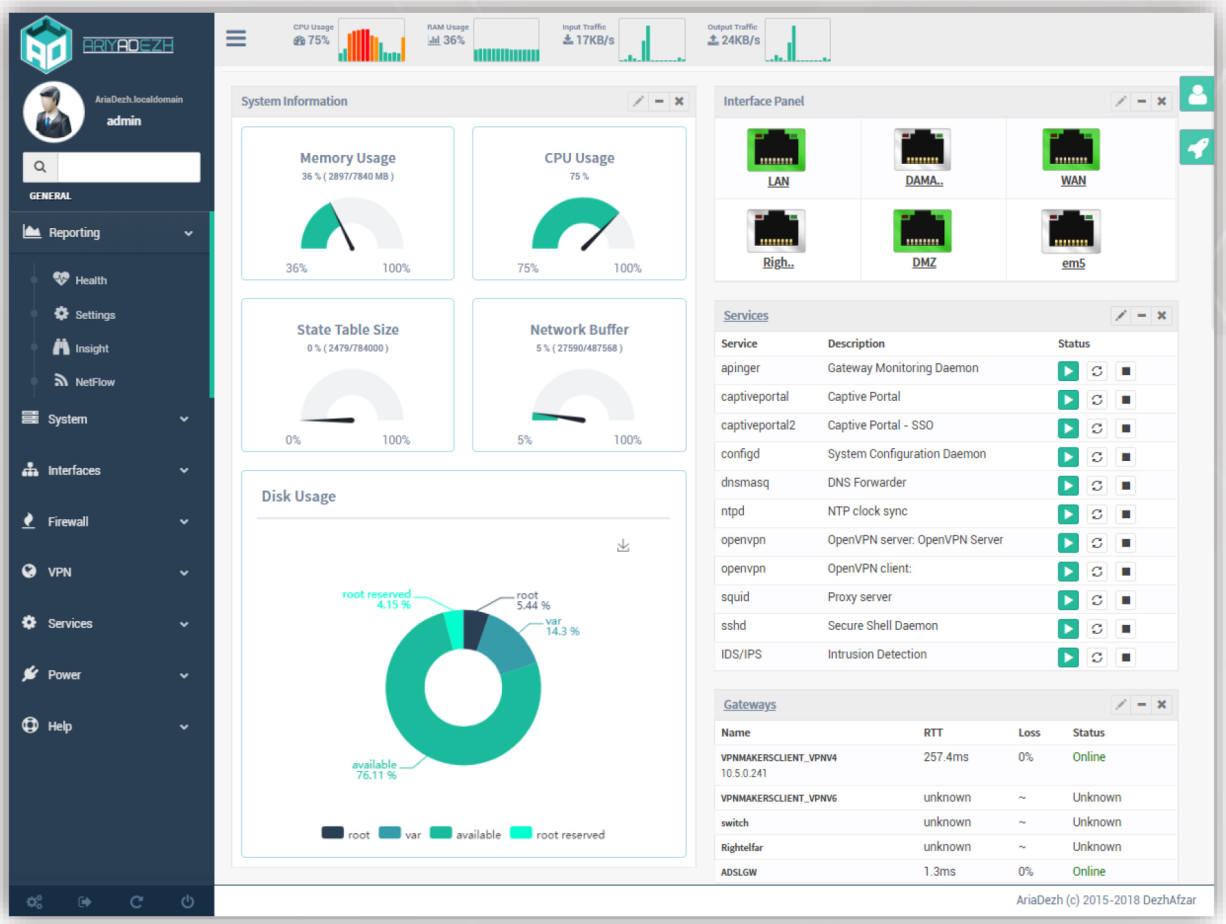
یکی از ویژگی های مهم در این قابلیت امکان تشخیص کاربران Log off شده می‌باشد، که این قابلیت در بسیاری از دیواره‌های آتش با چالش روبرو هستند.

۲. داشبورد

در داشبورد شما می‌توانید آخرین وضعیت سیستم را در چند ستون با قابلیت Drag & Drop داشته باشید. محیط داشبورد مبتنی بر ابزارک (widget) است به صورتی که کاربر می‌تواند با توجه به نیازهایش ابزارک‌های متفاوتی را اضافه نماید، از جمله:

- High Availability
- Dynamic DNS
- Interface Statistics
- IPsec
- Load Balancer
- Firewall Logs
- Network Time
- SSL VPN
- Picture
- RSS
- System Log
- Thermal Sensors
- Traffic Graph
- Wake On Lan

ویژگی فوق به صورت کاملاً پویا است و قابلیت سفارشی سازی داشبورد برای کاربران وجود دارد.

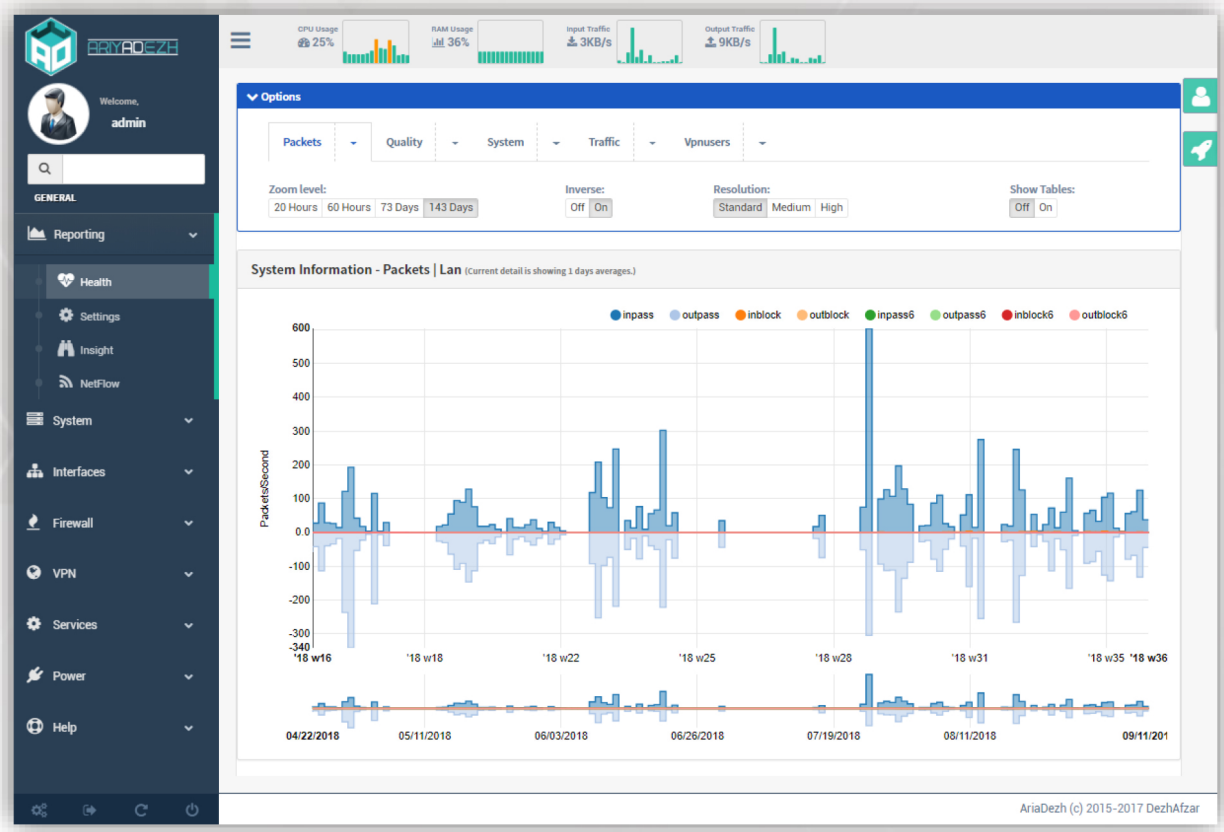


شکل ۱- در این صفحه وضعیت کلی دیواره آتش و سرویس های آن در یک نگاه قابل مشاهده است

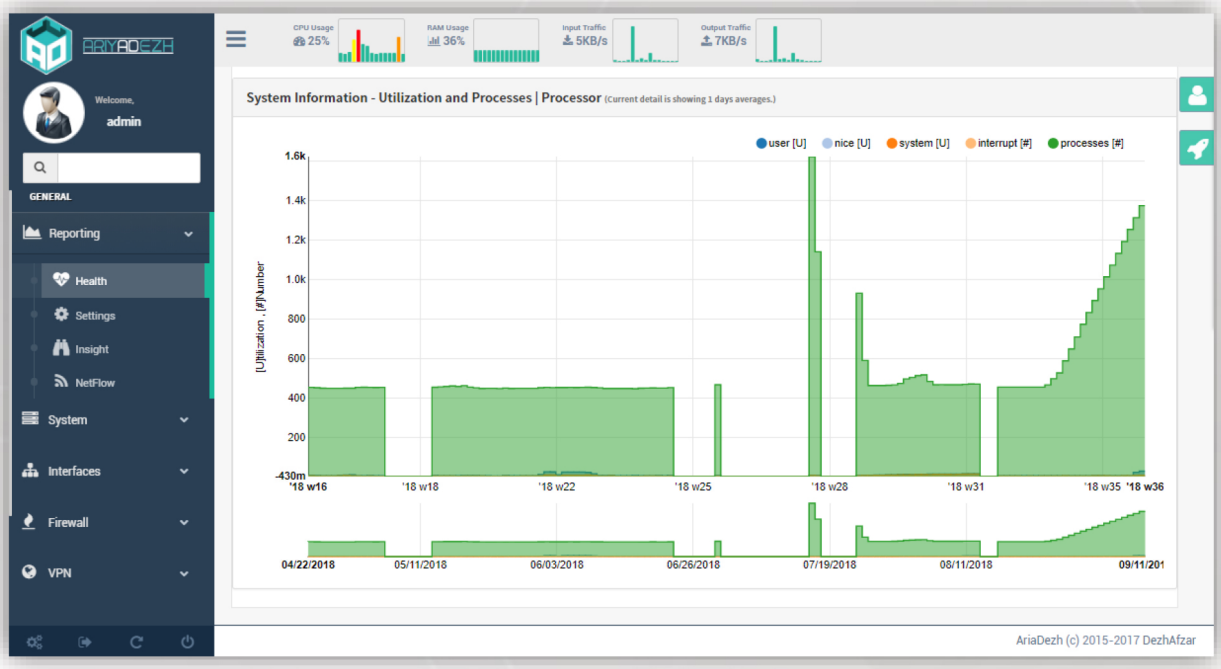
۳.گزارش گیری

قسمت گزارش گیری قابلیت و نظارت و بررسی تمام رخدادها در شبکه و دیواره آتش را فراهم می‌کند.

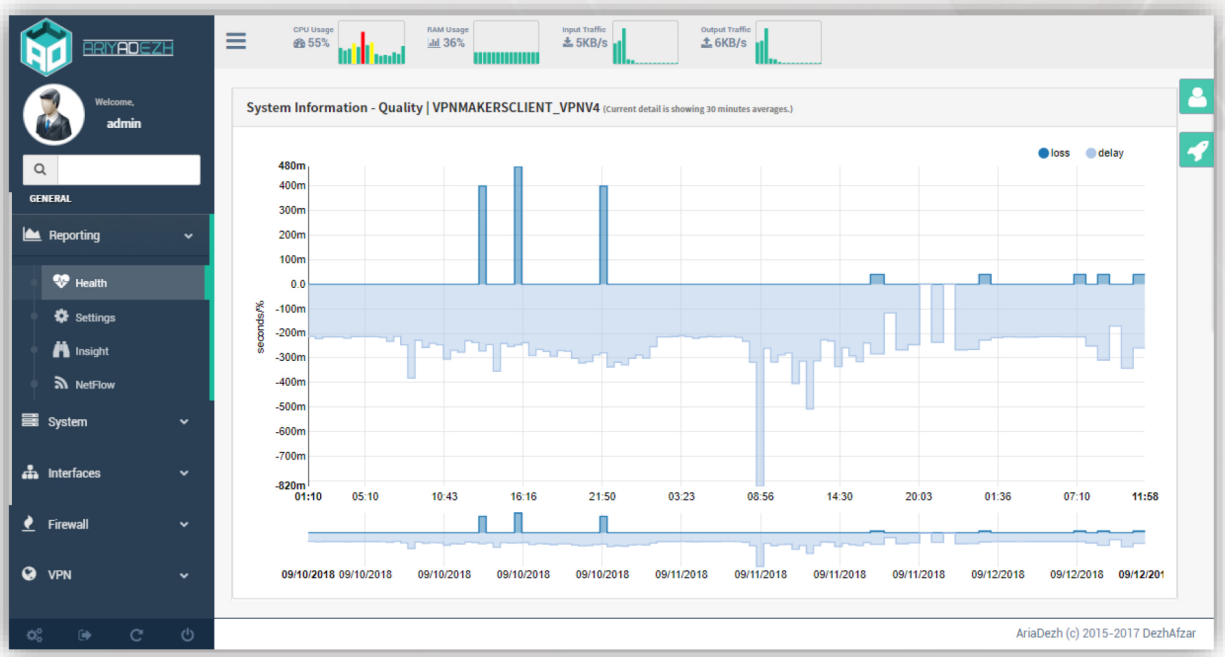
- گزارش گیری از فعالیت پروتکل‌های مختلف:TCP,UDP, ICMP, IGMP و ...
- گزارش گیری ترافیک عبوری بر اساس واسط‌های شبکه (interfaces)
- گزارش گیری بر اساس IP های مبدأ و مقصد به صورت تفکیک‌شده
- گزارش گیری بر اساس درگاه‌های (Port) مبدأ و مقصد به صورت تفکیک‌شده
- گزارش گیری کامل و جزئی از خصوصیات و رخدادهای واسط‌های شبکه



شکل ۲- نمودار وضعیت بسته های مشاهده شده در دیواره آتش



شکل ۳- نمودار وضعیت پردازه های سیستم در طول زمان

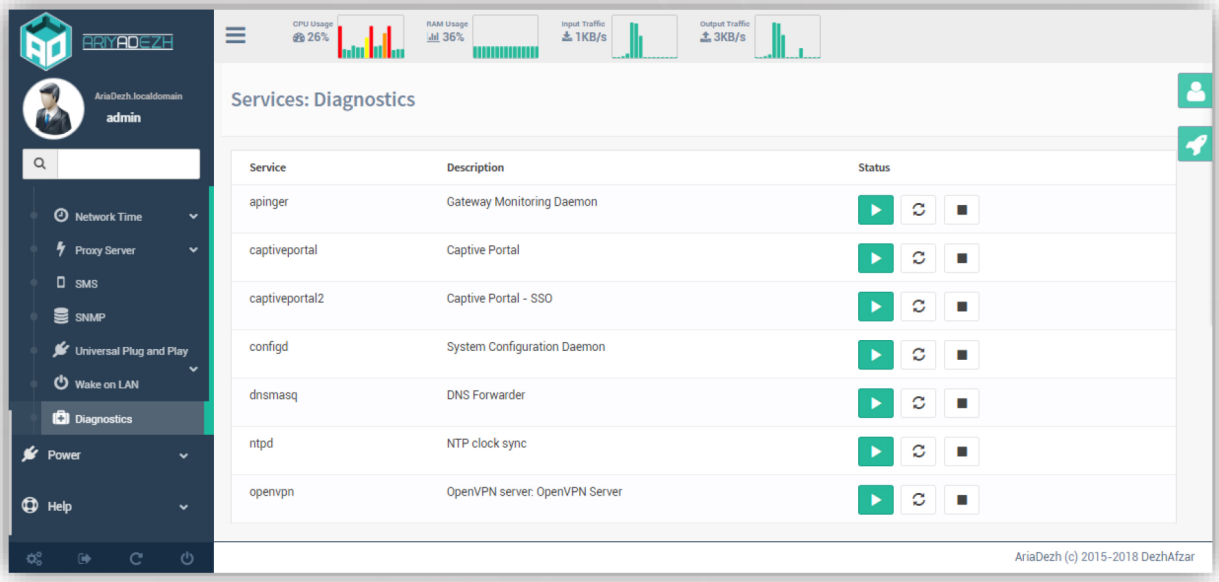


شکل ۴- نمودار وضعیت بسته های مشاهده شده در دیواره آتش در واسط شبکه WAN

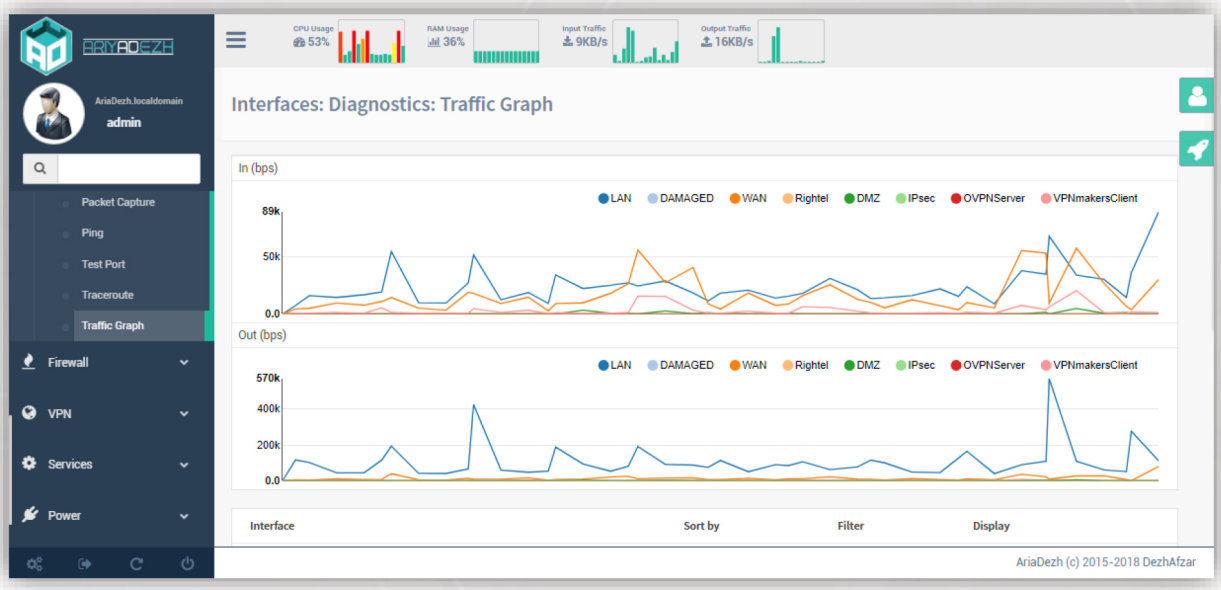
٤. ابزارهای عیب‌یابی

پشتیبانی کامل از ابزارهای تشخیص و عیب‌یابی همچون:

ARP Table	هنگامی‌که آدرس اینترنتی (IP) مشخص باشد با استفاده از ARP آدرس فیزیکی را به دست می‌آوریم. جهت مشاهده لیست آدرس‌های اینترنتی (IP) و فیزیکی (MAC) در ارتباط با دیواره آتش می‌توان از ARP Table استفاده نمود.
NDP Table	این قابلیت به صورت کامل، مشابه ARP Table است با این تفاوت که برای IPv6 به کاربر می‌رود.
Packet Capture	به منظور گرفتن و بازرسی بسته‌های عبوری از دیواره آتش می‌توان از این قابلیت استفاده و طیف وسیعی از فیلترها را برای گرفتن بسته‌ها اعمال نمود.
Test Port	به منظور بررسی اینکه آیا یک سرویس بر بروی سیستم میزبان بالا است و قادر به پذیرش بسته از یک پورت خاص است می‌توان از این ابزار استفاده کرد. این ابزار از پروتکل TCP استفاده می‌کند.
Traffic Graph	مشاهده نموداری ترافیک عبوری بر روی واسط‌ها
Filter Reload	جهت اعمال قوانین در دیواره آتش و مشاهده خطاهای احتمالی در تنظیم و اعمال قوانین
Afinfo, AfTop and AfTables	نمایش وضعیت بر خط دیواره آتش که شامل مواردی همچون: آمارهای مربوط به ترافیک واسط‌ها استفاده می شود.
States Dump	دیواره آتش برای هر ارتباط یک وضعیت (state) ایجاد می‌نماید. در این قسمت می‌توان وضعیت تمامی ارتباطات را مشاهده و بررسی نمود.
States Reset	به منظور ساخت مجدد وضعیت ارتباطات
States Summary	نمایش وضعیت اتصالات جاری شبکه در دیواره آتش
Ping Traceroute	بررسی وضعیت اتصال



شکل ۵- امکان فعال و غیر فعال کردن سرویس ها در این صفحه فراهم است.



شکل ۶- نمودار مصرف ترافیک بر روی واسط شبکه های واقعی و مجازی

۵. بازرسی پروتکل لایه اپلیکیشن

در آریادژ قابلیت بررسی ترافیک لایه ۷ وجود دارد که به وسیله این ویژگی می‌توانیم پروتکل‌های لایه‌ی کاربرد را شناسایی و نوع ترافیک عبوری مجاز را مشخص کنیم و بدین وسیله اطمینان حاصل کنیم که امکان عبور ترافیک با پروتکل‌های نامطلوب وجود ندارد.

انواع پروتکل‌های قابل‌تشخیص:

- HTTP
- FTP
- IMAP
- SMTP
- SSL/TLS: برای پروتکل‌هایی مانند HTTPS, IMAPS, SMTPS, FTPS و... که به صورت Implicit از پروتکل TLS استفاده می‌کنند باید گزینه SSL/TLS انتخاب شود.
- SSH: برای پروتکل SSH, SFTP, SCP, RSH, FISH و هر پروتکلی که از تونل SSH استفاده کند باید گزینه SSH انتخاب شود.

با وجود موتور کاوش و واکاوی پروتکل‌های لایه ۷ (کاربرد) امکان اضافه نمودن پروتکل‌های اختصاصی و سفارشی آن‌ها برای مشتری فراهم است.

۶. SNMP

پشتیبانی از نسخه‌های مختلف پروتکل SNMP

قابلیت‌ها:

- نظارت بر ارتباطات شبکه به صورت لحظه‌ای
- سازگاری با انواع برنامه‌های مدیریت و نظارت شبکه
- نظارت بر عملکرد کارگزاران: میزان پهنای باند مصرفی، مثل وضعیت بر خط بودن و ...
- اطلاع‌رسانی لحظه‌ای در مورد وضعیت کارایی دیواره آتش، خطاهای محتمل و رخدادهای شبکه و دیواره آتش

۷. Web Proxy

به منظور کنترل و نظارت ترافیک‌های HTTP، HTTPS و FTP می‌توانید از این سرویس استفاده نماید. Proxy ارائه‌شده توسط آریادژ دارای امکاناتی همچون web-filtering دسته‌ای و کنترل دسترسی می‌باشد. این سرویس می‌تواند در حالت شفاف اجرا شود. می‌توان با ترکیب پروکسی، دیواره آتش و captive portal نظارت بسیار خوبی بر روی کاربران و اعمال آن‌ها داشت به صورتی که به وسیله captive portal می‌توان دسترسی کاربران را کنترل نمود، با استفاده از قوانین دیواره آتش مبدأ و مقصد ترافیک، پروتکل‌های مورد استفاده و ... را مدیریت نمود و همچنین با استفاده از پروکسی می‌توان ترافیک HTTP و HTTPS را کنترل کرد. به طور مثال می‌توان دسترسی یک کاربر را به یک وب سایت یا آدرس محدود نمود. همچنین، امکان یکپارچه شدن این ویژگی با ضد ویروس‌هایی که دارای واسط ICAP هستند وجود دارد.

سایر قابلیت‌ها:

- اعمال قوانین محدود سازی دسترسی برای کاربران
- ثبت رخدادهای کاربران
- ثبت ترافیک وب کاربران

۸. حالت پراکسی برای SIP و H.323

آریا دژ می تواند همچون یک دروازه و یا پراکسی برای پروتکل H.323 عمل کند. این ویژگی امکان کنترل بیشتر بر روی ترافیک های VOIP در شبکه را فراهم نماید. همچنین می تواند مسائل و مشکلاتی که H.323 و SIP در فایروال های عمومی دارند را برطرف نماید.

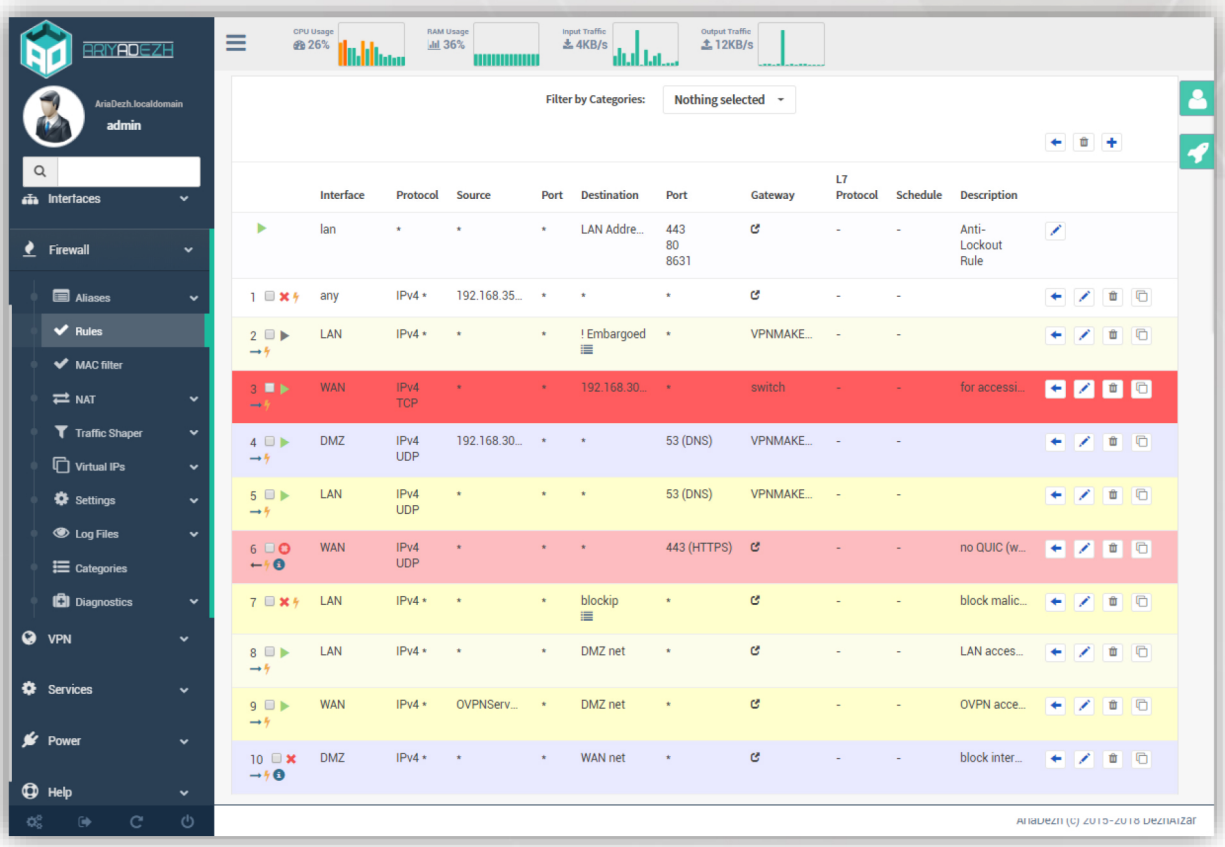
۹. دیواره آتش

دیواره آتش آریادژ یک دیواره آتش حالتمند است که در آن مسیر و حالت اتصالات شبکه مانند جریان‌های TCP و ارتباطات UDP نگهداری می‌شود. دیواره آتش آریادژ امکان دسته‌بندی و مدیریت قوانین را به کاربر می‌دهد. تمامی بسته‌هایی که قصد ورود به و یا خروج از شبکه را دارند، ممکن است بسته‌های سالمی نباشند و برخی از آن‌ها ممکن است دارای یک سری نقایص عمدی و یا غیر عمدی باشند که موجب صدمه به میزبان گردند. فرایند بازسازی بسته‌ها و دسته‌بندی آن‌ها به وسیله خصوصیتی به نام نرمال سازی صورت می‌پذیرد.

فرایند نرمال سازی بسته‌ها به صورتی می باشد که مقصد نهایی دچار ابهامات در تفسیر بسته‌ها نمی‌گردد. این قابلیت همچنین در بازسازی بسته‌ها، دور انداختن بسته‌هایی که پرچم (flag) TCP نادرستی دارند و محافظت از سیستم عامل در مقابل برخی از حملات به دیواره آتش کمک می‌کند.

سایر قابلیت ها:

- امکان دسته بندی و رنگ بندی قوانین
- امکان تعریف زمانبندی برای قوانین
- امکان جستجو در قوانین
- امکان محدود سازی تعداد اتصالات و نود ها
- امکان نوشتن قانون بر اساس نام کاربر
- SYN Proxy برای مقابله با حملات مبتنی بر SYN



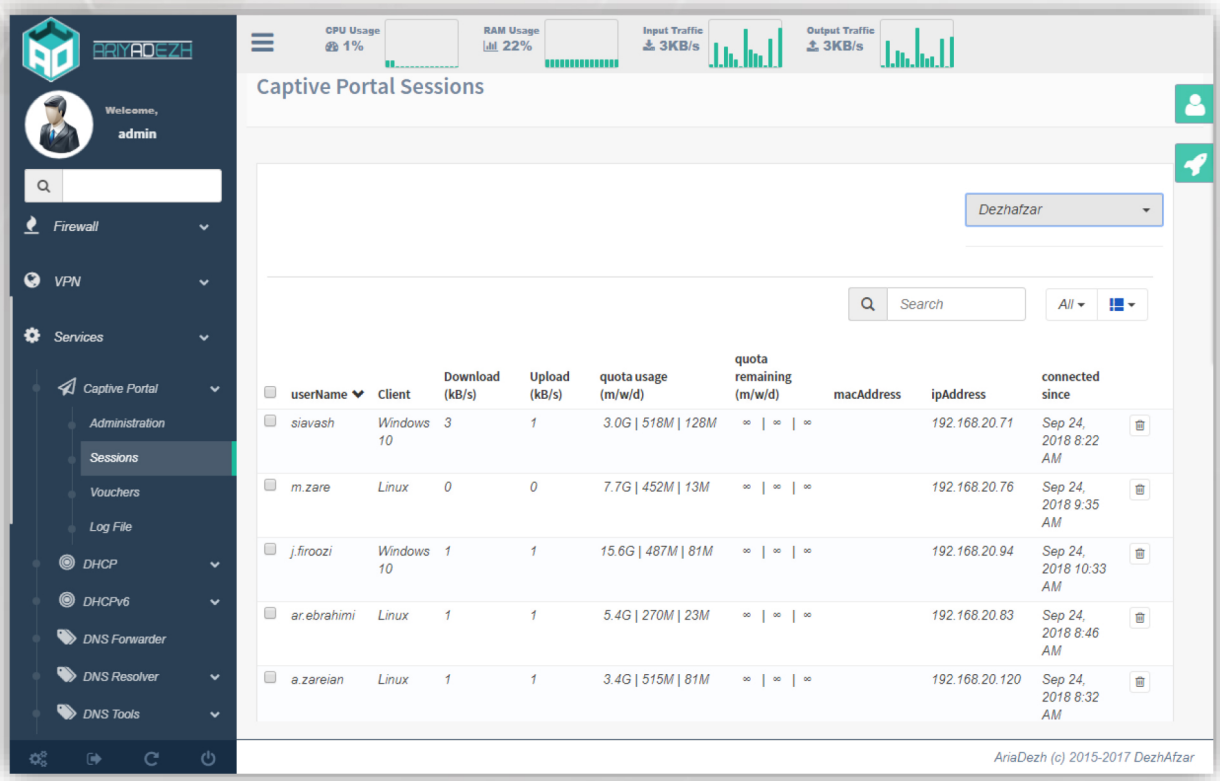
شکل ۷- صفحه اصلی تعریف قوانین دیواره آتش که در آن امکان رنگ بندی و دسته بندی وجود دارد.

Captive Portal .۱۰

Captive Portal به شما اجازه می‌دهد که احراز هویت را در شبکه اجباری کنید، یا اینکه برای دسترسی به شبکه کاربر به یک صفحه دیگر که نیاز به کلیک دارد ارجاع داده شود. این ویژگی معمولاً در شبکه‌های Hotspot مورد استفاده قرار می‌گیرد، به طور گسترده در شبکه‌هایی یکپارچه برای ایجاد یک لایه‌ی اضافه امنیتی روی شبکه بی‌سیم یا اینترنت استفاده می‌شود. علاوه بر آن آریادژ از Voucher نیز پشتیبانی می‌کند. قابلیت Voucher رمزهای تصادفی را تولید می‌نماید که کاربران با استفاده از آن‌ها می‌توانند از طریق Captive Portal به اینترنت دسترسی داشته باشند و تا زمانی که به Voucher اعتبار داده باشیم دسترسی آن‌ها برقرار خواهند ماند. این قابلیت در رستوران و هتل‌ها جهت دسترسی کاربران به اینترنت مورد استفاده قرار می‌گیرد.

قابلیت‌ها:

- پشتیبانی از ویژگی Single Sign On خودکار با استفاده از پروتکل Integrated Windows Authentication (IWA)
- سازگاری با انواع ویندوز سرورها
- پشتیبانی و سازگاری با LDAP و Radius
- تشخیص و مدیریت کاربران Log off شده
- نمایش وضعیت کاربران متصل شده براساس حجم ترافیک مصرف شده، پهنای باند کنونی و سیستم عامل



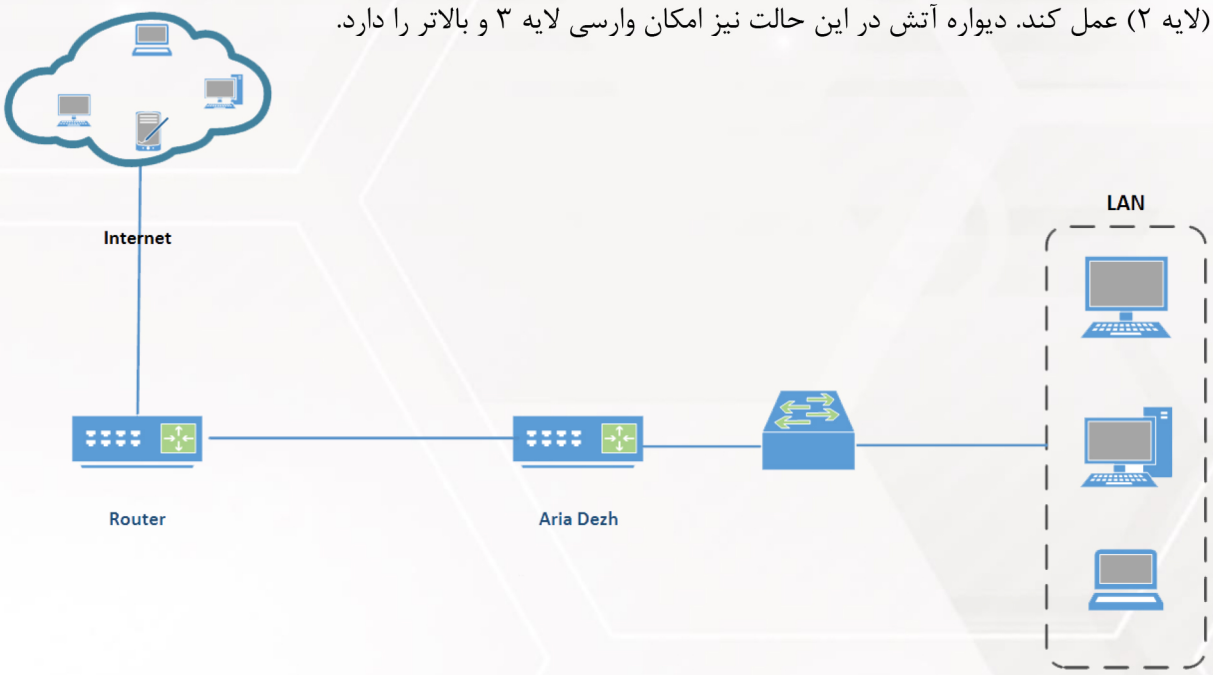
شکل ۸- لیست کاربران احراز هویت شده در آریا دژ

۱۱. حالت‌های استقرار

محصول آریادژ دارای وضعیت های مختلف استقرار است از جمله:

Bridge.۱.۱۱

اگر دیواره آتش آریادژ در حالت Bridge راه اندازی شود این قابلیت را دارد که به صورت Transparent Bridge (لایه ۲) عمل کند. دیواره آتش در این حالت نیز امکان وارسی لایه ۳ و بالاتر را دارد.



شکل ۹- در این حالت دیواره آتش به صورت Transparent یا Bridge مستقر شده است.

در این حالت آریادژ میان ارتباط شبکه داخلی و مسیریاب قرار می‌گیرد و بدون نیاز به تغییرات در معماری شبکه اقدام به بازرسی ترافیک می‌نماید.

NAT/Route.۲.۱۱

در این حالت دیواره آتش به عنوان یک دروازه و یا مسیریاب میان دو شبکه مستقر می‌شود. در بیشتر مواقع، مابین شبکه امن و اینترنت قرار می‌گیرد و علاوه بر عملکرد ترجمه آدرس، عملیات مسیریابی را نیز انجام خواهد داد.

۱۲. Accounting

در اینجا می توان حجم ترافیک و مصرف پهنای باند کاربران را کنترل و نظارت نمود.

قابلیت ها:

- امکان تعریف حجم مصرفی بر اساس روز، هفته و ماه برای کاربران و یا گروه کاربران
- امکان مشاهده حجم مصرف شده و باقی مانده حجم کاربران
- نمایش حجم ترافیک مصرف شده برای هر کاربر

۱۳. نام‌های مستعار

مدیریت قوانین دیواره‌آتش کار آسانی نیست. با استفاده از نام‌های مستعار شما می‌توانید چند IP، میزبان، شبکه و یا شماره درگاه را در یک گروه برای استفاده در قوانین دیواره‌آتش فهرست کنید. نام های مستعار همان بخش definition در دیواره آتش خارجی است.

۱۴. پایگاه داده IP بر اساس موقعیت جغرافیایی

امکان استفاده و اضافه نمودن لیست آدرس‌های IP بر اساس موقعیت جغرافیای آن‌ها. این امکان اجازه مسدود و یا عبور ترافیک را بر اساس کشور مبدأ یا مقصد ترافیک می‌دهد. این پایگاه داده مداوم در حال به روز رسانی است.

۱۵. مدیریت کاربران

در این قسمت می‌توانیم کاربران و گروه های مختلفی را تعریف و مدیریت کنیم.

قابلیت‌ها:

- تخصیص کاربران به گروه های متفاوت و یکسان
- مدیریت زمان نشست‌های کاربران
- تعریف سرورهای مختلف: LDAP، Radius، Voucher و...
- امکان تعریف شماره همراه جهت ارسال پیامک
- امکان تعریف حجم ترافیک مصرفی به صورت روزانه، هفتگی و ماهانه
- امکان مدیریت دسترسی به بخش های مختلف آریادژ

۱۶. ترجمه آدرس شبکه Network Address Translation (NAT)

پشتیبانی کامل از ویژگی NAT:

- Port Forwarding (Destination NAT)

امکان برقراری ارتباط مستقیم برای سرویسی خاص در سمت شبکه امن که بر روی یک میزبان بدون آدرس IP عمومی

- Outbound NAT (Source NAT)

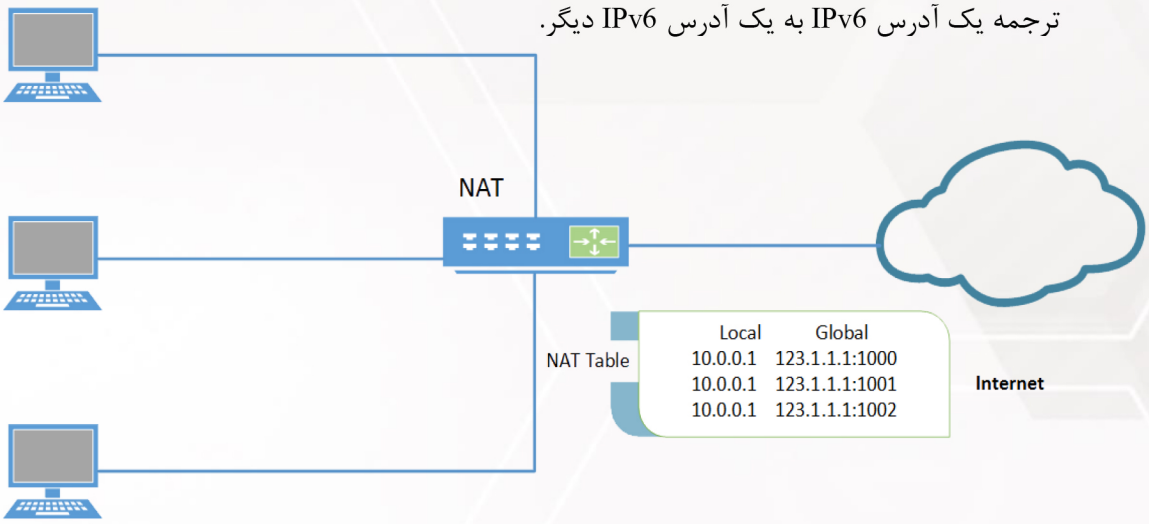
ترافیک خروجی را بر اساس IP مبدأ ترجمه می‌کند

- One-To-One

ترجمه یک آدرس خاص به یک آدرس معین دیگر.

- NPT(IPv6)

ترجمه یک آدرس IPv6 به یک آدرس IPv6 دیگر.

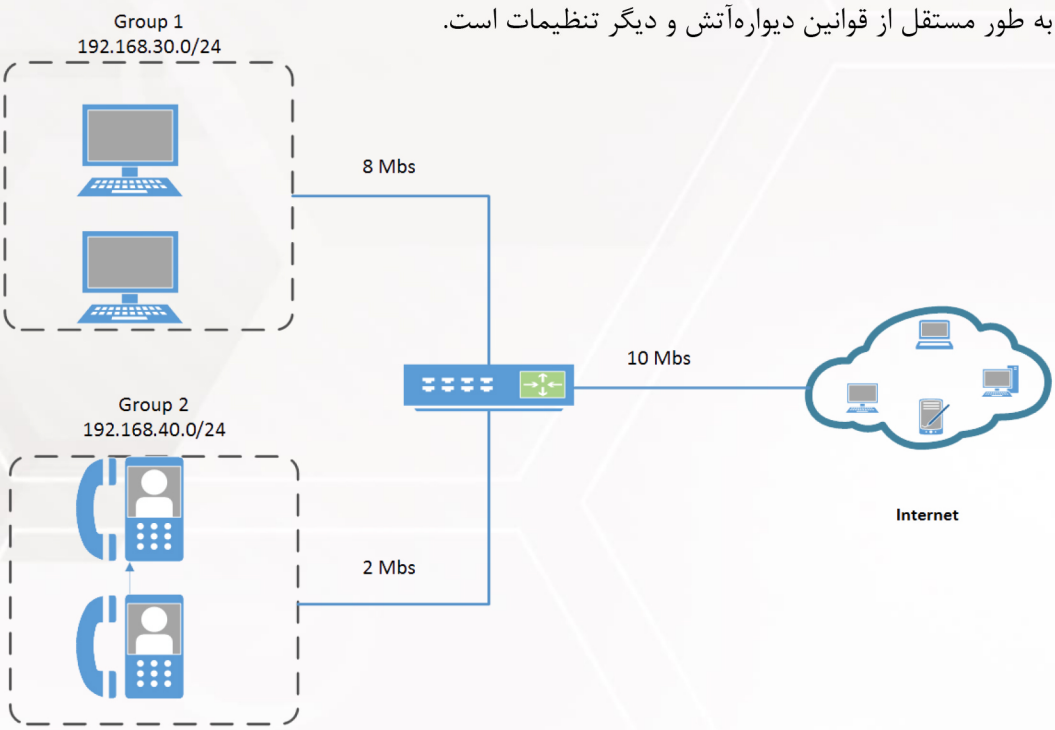


شکل ۱۰- ترجمه آدرس شبکه (NAT)

۱۷. تسهیم ترافیک (Traffic Shaper)

یکی از ویژگی مورد نیاز در شبکه ویژگی تسهیم ترافیک است. این ویژگی پهنای باند ترافیک مجاز، جهت عبور از لینک‌ها را کنترل می‌کند. در واقع با استفاده از این قابلیت شما به داده‌ها و ترافیک تان سرعت مجاز را می‌دهید و یا می‌تواند محدودیت‌هایی را در ترافیک‌های ارسالی اعمال کنید.

تسهیم ترافیک در آریادژ بسیار انعطاف‌پذیر است و پیرامون شریان ها (pipe)، صف‌ها و قوانین مربوطه سازمان‌دهی شده است. pipe پهنای باند مجازی را تعریف می‌کنند و صف‌ها می‌توانند برای تنظیم اولویت ترافیک داخل هر pipe مورد استفاده قرار گیرند و در نهایت قوانین برای شکل دادن به یک جریان بسته خاص استفاده می‌شود. قوانین تسهیم ترافیک به طور مستقل از قوانین دیواره‌آتش و دیگر تنظیمات است.



شکل ۱۱- در شکل فوق پهنای باند اینترنت برای کاربران گروه ۱ با 8Mbs و کاربران گروه ۲ با 2Mbs تقسیم شده است.

۱۸. پشتیبانی از DNS

- DNS Forwarder

قابلیتی جهت ارسال درخواست‌های (پرس و جوهای) DNS به سرورهای DNS خارج از شبکه داخلی.

- DNS Resolver

قابلیتی به منظور پاسخ دادن به پرس و جوهای میزبان‌ها و تبدیل نام دامنه به IP

- DNS Tools

مجموعه‌ای از ابزارها برای کنترل و بهره‌گیری بهتر از DNS، مانند DNS Lookup، Dynamic DNS، DNS Filter و...

- DNS Crypt

قابلیتی جهت حفظ محرمانگی ترافیک DNS

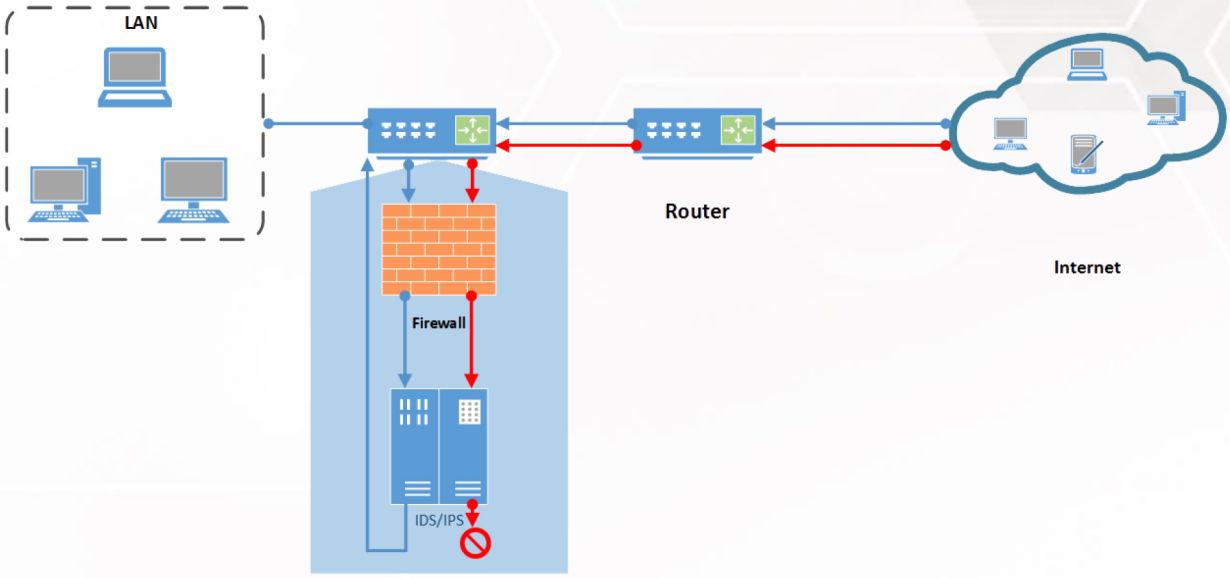
۱۹. سامانه تشخیص و پیشگیری از نفوذ (IPS/IDS)

تکنولوژی‌های IDS و IPS ترافیک شبکه را با جزئیات بیشتر نسبت به دیواره آتش تحلیل می‌کنند. مشابه سیستم‌های آنتی ویروس، ابزارهای IDS و IPS ترافیک را تحلیل و هر بسته اطلاعات را با پایگاه داده‌ای از مشخصات حملات شناخته‌شده مقایسه می‌کنند. هنگامی که حملات تشخیص داده می‌شوند، این ابزار وارد عمل می‌شود و مسؤولین را از وقوع یک حمله مطلع می‌سازند؛ ابزارهای IPS یک گام جلوتر می روند و به صورت خودکار ترافیک آسیب‌رسان را مسدود می‌کنند. مؤلفه IPS در آریادژ در دو مرحله به دفاع از شبکه می‌پردازد:

- با تشخیص رفتارهای غیرطبیعی در شبکه از رخ دادن حملات پخش وسیع (DDOS) و پویش درگاه‌ها جلوگیری می‌کند.
- با استفاده از الگوی حملات، با حملاتی چون Backdoor ها و Exploit ها مقابله می‌کند.

سایر قابلیت ها:

- امکان نوشتن قوانین پیچیده IDS توسط کاربران
- امکان مسدود نمودن سایت های HTTP و HTTPS
- امکان مشاهده لاگ ها با فیلترینگ بسیار سریع
- مدیریت هوشمند لاگ های ذخیره شده برای جلوگیری از پر شدن دیسک
- استفاده از فایل سیستم ZFS برای بالا بردن کارایی در ذخیره و بازیابی لاگ ها



شکل ۱۲- سامانه تشخیص و پیشگیری از نفوذ (IPS/IDS)

۲۰. مسدود سازی سایت های HTTP و HTTPS

در اینجا امکان مسدود سازی این سایت ها از طریق IPS فراهم می گردد. تفاوت این مسدود سازی با استفاده از Web Proxy در آن است که مسدود سازی با سرعت گیگا بیت و بدون رمز گشایی ترافیک HTTPS صورت می گیرد.

۲۱. شبکه خصوصی مجازی VPN

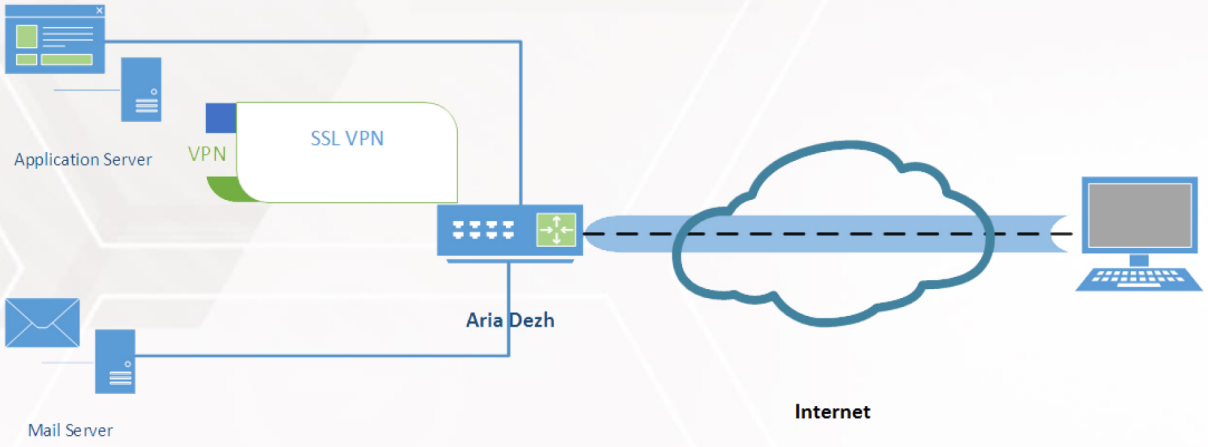
VPNمخفف Virtual Private Network می‌باشد که در لغت به معنی شبکه خصوصی مجازی می‌باشد. VPN جهت ارتباط دو شبکه یا زیر شبکه به صورت امن به کار می‌رود.

IPSec مخفف و کوتاه شده عبارت IP Security است که به مجموعه‌ای از پروتکل‌ها اشاره‌کرده و تبادل امن بسته‌ها در لایه IP را پشتیبانی می‌کند IPSec. به طور گسترده در تکنولوژی VPN جهت احراز هویت، محرمانگی، یکپارچگی و مدیریت کلید در شبکه‌های مبتنی بر IP ، مورد استفاده قرار می‌گیرد.

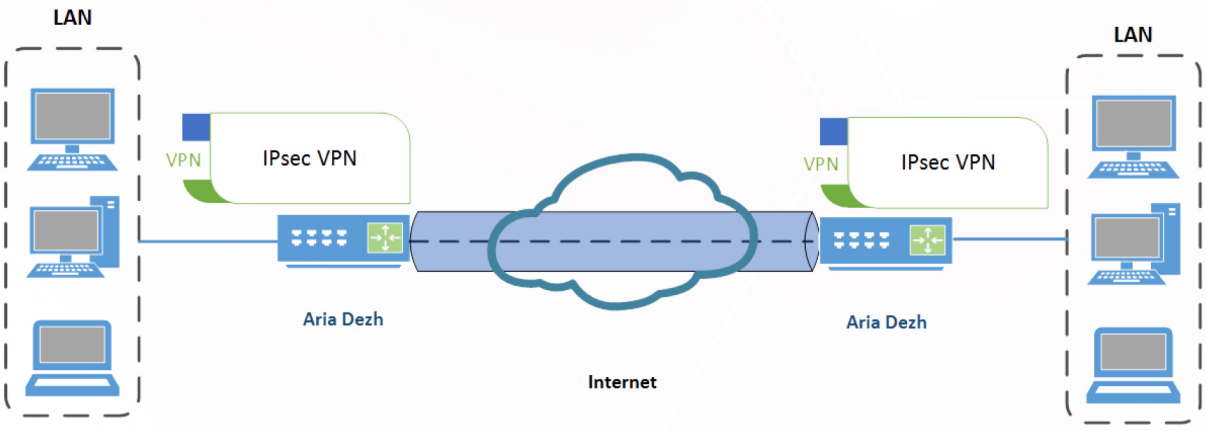
آریادژ طیف گسترده‌ای از فناوری‌های VPN اعم از SSL VPN امروزی تا تکنولوژی های قدیمی تر همچون IPsec وPPTP و L2TP را ارائه می‌دهد. تنظیمات Site-to-Site و Roadwarriar با وجود ویژگی export تنظیمات کاربر در عرض چند دقیقه قابل انجام هستند.

سایر قابلیت‌ها:

- قابلیت اعمال و پشتیبانی از الگوریتم‌های رمزنگاری سفارش مشتری



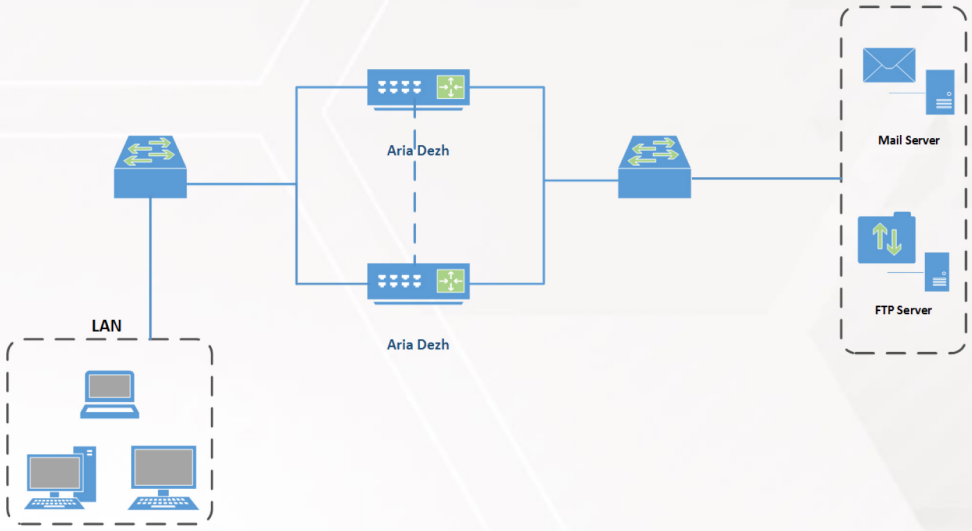
شکل ۱۳- نحوه قرارگیری VPN به صورت Host to Net



شکل ۱۴- نحوه قرارگیری VPN به صورت Net to Net

High Availability/Hardware Failover .۲۲

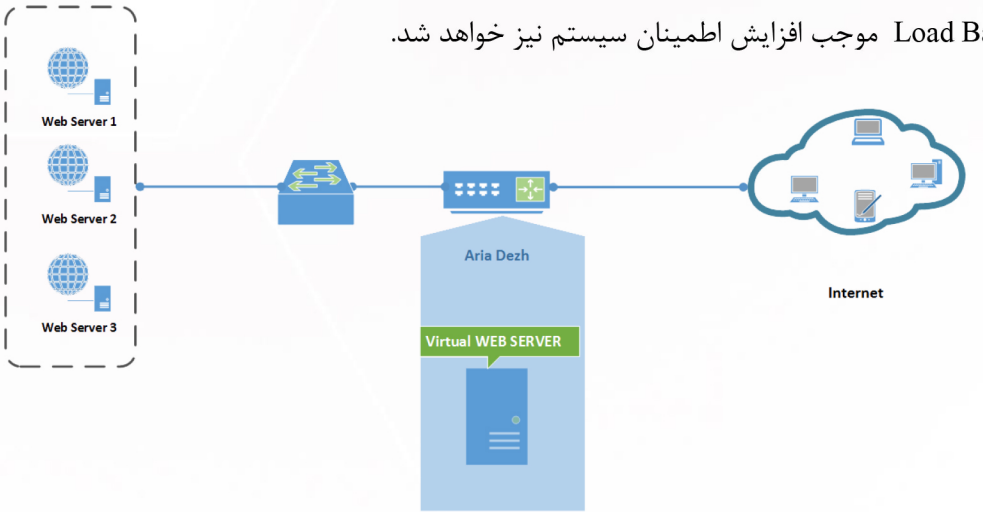
آریادژ دارای ویژگی تشخیص خرابی سخت‌افزار سامانه است. به صورتی که دو یا چند دیواره‌آتش می‌توانند به عنوان یک گروه Failover پیکربندی شوند. اگر یک واسط شبکه در دیواره آتش اولیه قطع شود یا دیواره آتش اولیه به طور کامل خراب شود، دیواره آتش ثانویه فعال می‌شود. به‌کارگیری این ویژگی قدرتمند آریادژ را به یک دیواره آتش پایدار و بدون خرابی مبدل می‌نماید. در طی انتقال خودکار به نسخه پشتیبان، ارتباط شبکه با کمترین وقفه برای کاربران فعال باقی خواهد ماند.



شکل ۱۵- نحوه قراگیری دیواره آتش در حالت High Availability/Hardware Failover

Load Balance .۲۳

به منظور توازن و عدم تحمیل بار اضافی برروی یک سرور از تکنیک Load Balance استفاده می‌شود. با استفاده از این قابلیت در صورت قطع شدن یک سرور، ترافیک عبوری بر روی دیگر سرورها پخش خواهد شد. بنابراین استفاده از Load Balance موجب افزایش اطمینان سیستم نیز خواهد شد.



شکل ۱۶- نحوه قرارگیری دیواره آتش در حالت Load Balance

۲۴. قابلیت پشتیبانی همزمان High Availability و Load Balance

با این ویژگی احتمال قطع شدن دیواره آتش و سرورها در شبکه به پایین‌ترین حد ممکن می‌رسد.

۲۵. پروتکل پیکربندی پویای میزبان (DHCP)

پشتیبانی کامل از سرویس DHCP در حالات:

- DHCP Server

تخصیص خودکار آدرس‌های IP به میزبان‌های شبکه

- DHCP Relay

جهت ارسال و دریافت درخواست‌های DHCP میان میزبان‌ها و سرورهای که در یک زیر شبکه نیستند (دامنه‌های پخش وسیع یا broadcast domains)

- DHCPv6 Server and Relay

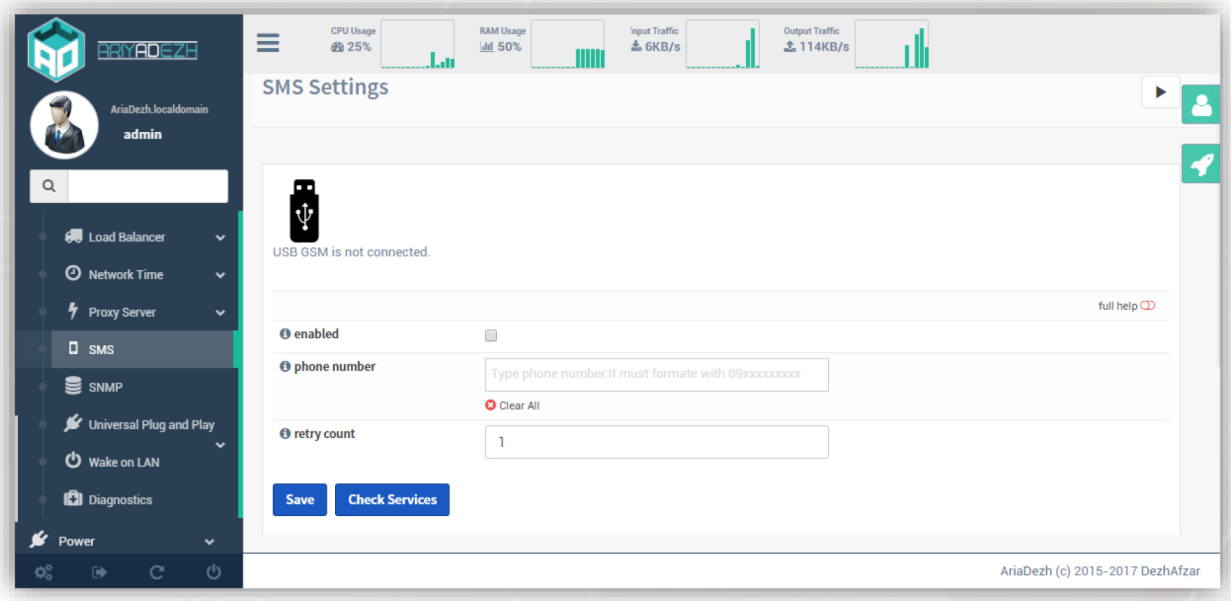
تخصیص خودکار آدرس‌های IPv6 به میزبان‌های شبکه. قابلیت Relay نیز همانند IPv4 است با این تفاوت که برای IPv6 به کار می‌رود.

سایر قابلیت‌ها:

- قابلیت نمایش IP های اختصاص داده‌شده توسط سرور به کارگزاران همراه با اطلاعات کامل کارگزاران
- قابلیت گزارش گیری از سرویس DHCP
- پشتیبانی از سرویس DHCP Static Mapping: جهت تخصیص آدرس های IP ایستا به میزبان های مورد نظر.

۲۶. ماژول ارسال SMS

با کمک این ویژگی رخدادهای اساسی دیواره آتش از طریق یک ماژول GSM به شماره تلفن‌های تعریف شده پیامک می شود.



شکل ۱۷- صفحه ای که در آن ارسال SMS وجود دارد.

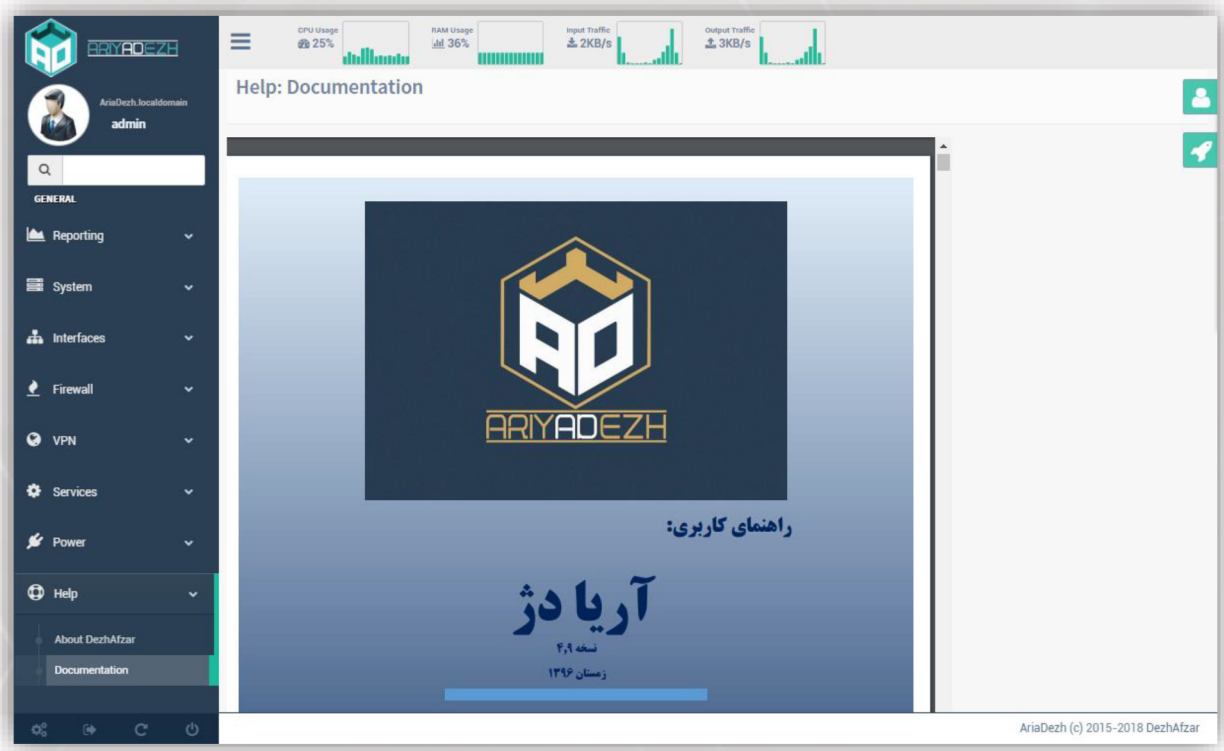
۲۹. توکن آریا کی:

از آنجایی که ذخیره امن داده های حساس همچون کلید های رمزنگاری یک چالش جدی است. وجود توکن بومی آریا کی در کنار آریا دژ می تواند بسیاری از دغدغه های امنیت را با حضور سخت افزار های خارجی برآورده کند. همچنین این توکن علاوه بر ذخیره امن داده امکان رمزنگاری متقارن را دارد.

شکل ۱۸- توکن سخت افزاری آریا کی

۲۷. راهنمای کاربری پیشرفته

راهنمای کاربری از ملزومات هر محصولی است. راهنمای کاربری آریادژ دارای تفاوتی اساسی با دیگر محصولات مشابه است. این راهنما کاملا کاربردی بوده و مبتنی بر سناریو است. به صورتی که برای فعال نمودن هر سرویسی یک سناریو آزمایش‌شده به صورت قدم به قدم ارائه گردیده است.



شکل ۱۹- صفحه اول راهنمای کاربری

۲۸. مدیریت واسط‌های شبکه

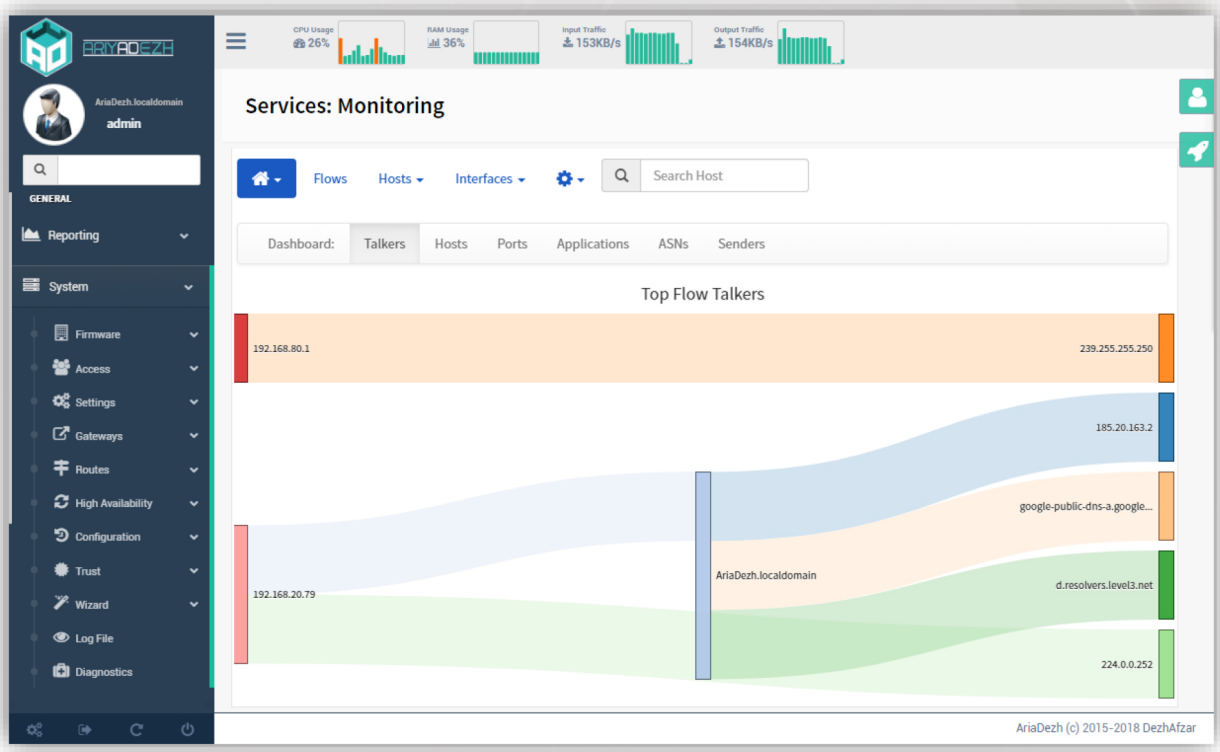
در این بخش امکان تخصیص، تنظیم و کنترل واسط‌های مختلف شبکه وجود دارد. انواع واسط‌های شبکه:

Bridge	لایه دوم Bridgeبه منظور اتصال دو یا چند واسط به یک دیگر در حالت (broadcast/collision domain)
GIF	ایجاد یک تونل منطقی برای ترافیک‌های IPv4 و IPv6
GRE	جهت ایجاد یک ارتباط (تونل) نقطه به نقطه میان میزبان‌ها
Group	جهت دسته‌بندی گروهی از واسط‌ها و اعمال قوانین بر روی آن‌ها به منظور جلوگیری از نوشتن دوباره قوانین
LAGG	امکان تجمیع چندین واسط و تبدیل آن‌ها به عنوان یک واسط مجازی به منظور افزایش سرعت لینک‌ها و بالا بردن تحمل خطا
VLAN	ایجاد شبکه محلی مجازی

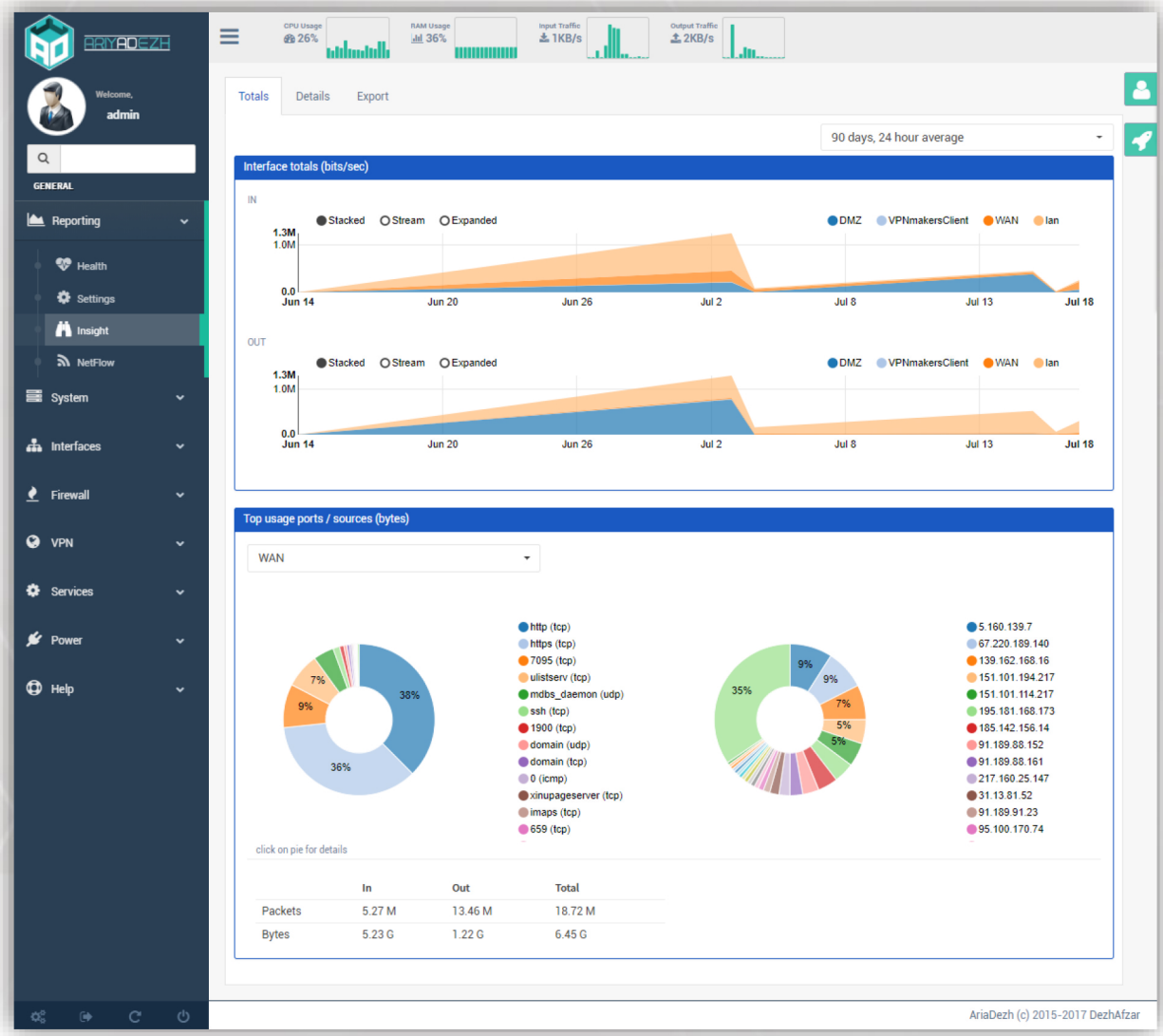
۳۰. سرویس نظارت برشبکه در لایه کاربرد

یکی از قابلیت‌های منحصربه‌فرد آریادژ وجود یک سرویس نظارت است که می‌تواند به صورت کاملاً جزئی ترافیک شبکه را تحلیل و آن را به صورت آنلاین به مدیر ارائه دهد. این سرویس توانایی نمایش وضعیت ترافیک به صورت‌های زیر را دارد:

- مرتب‌سازی ترافیک شبکه با توجه به معیارهای مختلف از جمله آدرس IP، پورت، پروتکل L7 و ...
- نمایش ترافیک شبکه، IPv4 و IPv6
- تولید گزارش‌های جامع در مورد معیارهای مختلف شبکه مانند توان عملیاتی، پروتکل‌ها
- ارائه گزارش برای هر جریان ارتباطی شبکه از جمله گزارش تأخیر RTT، آمار TCP، بایت/ بسته
- ذخیره مداوم آمار ترافیک بر روی دیسک با فرمت RRD
- گزارش‌ها بر اساس موقعیت‌های جغرافیایی میزبان
- کشف پروتکل‌های کاربردی با کاوش عمیق در ترافیک شبکه (Deep Packet Inspection)
- کاوش گواهینامه های TLS/SSL در ارتباطات رمز شده
- نمایش توزیع ترافیک IP در میان پروتکل‌های مختلف
- آنالیز ترافیک IP و مرتب کردن آن با توجه به مبدأ / مقصد
- نمایش ترافیک IP زیر شبکه ماتریس (مشخص کردن دو طرف ارتباط)
- گزارش استفاده از پروتکل IP مرتب شده بر اساس نوع پروتکل
- تولید آمار ترافیک شبکه HTML5 /Ajax



شکل ۲۰- نمودار وضعیت ارسال ترافیک از داخل شبکه به بیرون و بالعکس



شکل ۲۱- مشاهده اتصالات مربوط به هر IP

۳۱. مسیریابی (Routing)

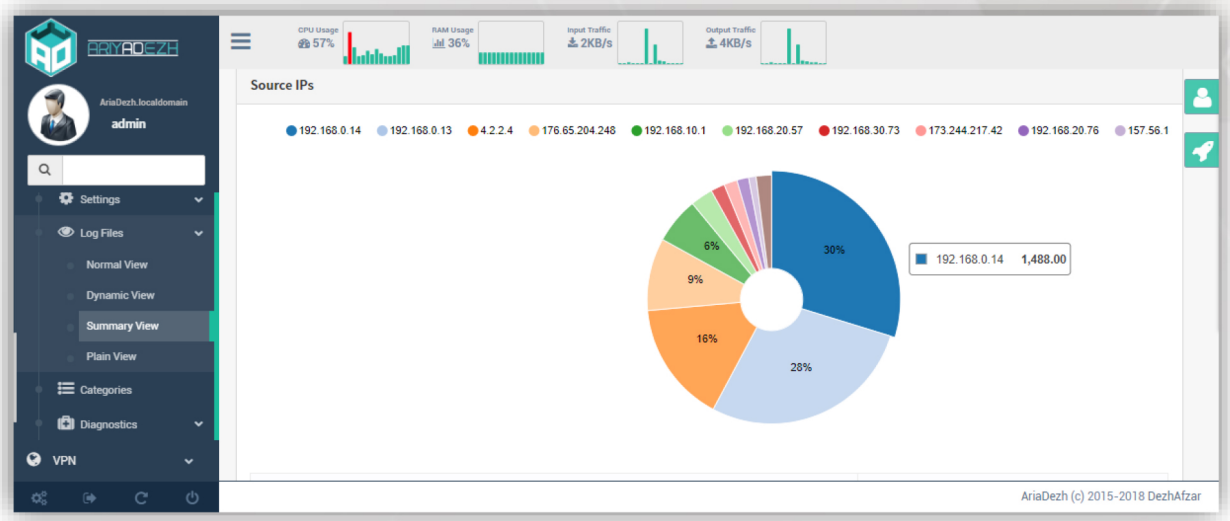
مسیریابی ایستا (Static Routing): با این ویژگی مدیر شبکه می‌تواند مسیریابی را براساس IP مقصد تعریف نماید.

مسیریابی بر اساس سیاست (Policy Based Routing): در این روش می توان مسیریابی را بر اساس سایر مؤلفه‌های یک بسته IP همچون IP مبدأ، پورت مبدأ و مقصد تعریف نمود. این قابلیت امکان مسیر یابی را با کمک قوانین دیواره آتش فراهم می کند. هر قانون دیواره آتش اجازه انتخاب یک درگاه Gateway را می دهد و اگر درگاهی انتخاب نشود جریان از درگاه پیش فرض و یا با توجه به جدول مسیریابی عبور می کند.

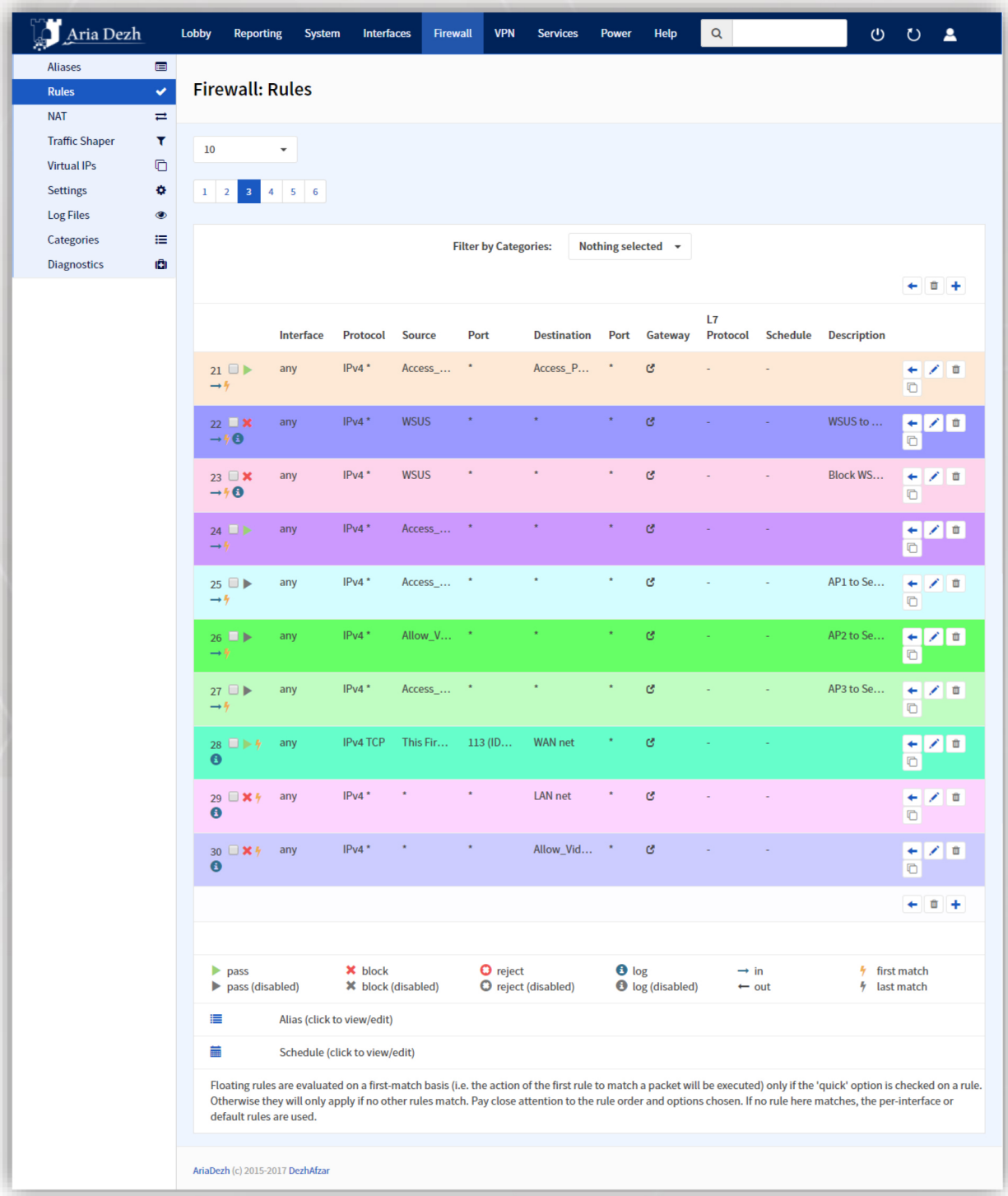
مسیر یابی پویا (Dynamic Routing): در اینجا انواع پروتکل های مسیریابی پویا همچون RIP, BGP, OSPF قابل پیکربندی و استفاده می باشند.

۳۲. واسط گرافیکی (Web UI)

واسط گرافیگی تحت وب آسان و طبقه‌بندی شده آریادژ این امکان را به مدیر شبکه می‌دهد تا بتواند بدون پیچیدگی، نظارتی کامل بر تمامی بخش‌های این محصول فوق داشته باشد.



شکل ۲۲- مشاهده وضعیت اتصالات جاری شبکه



شکل ۲۳- جدول قوانین دیواره آتش

یادداشت:

info@dezhafzar.com http://www.dezhafzar.com