معرفینامه شرکت پویش داده نوین

www.pdnsoft.com

تابستان ۹۸

کلیه حقوق مادی و معنوی این مستند به شرکت مهندسی شبکه پویش داده نوین تعلق دارد.

فهرست مندرجات

آدرس
تهران، خیابان آزادی، خیابان حبیب زادگان، پلاک ۳۶، طبقه ۲
یزد، خیابان مطهری، مرکز فناوری اقبال، واحد ۲۲۵

کدپستی
۱۴۵۸۸۸۷۱۵۴
۸۹۱۷۶۹۷۹۹۸

تلفن
۰۲۱۶۶۱۹۸۶۸۰
۰۳۵۳۷۲۶۵۳۴۳

فکس
۰۲۱۶۶۱۹۸۶۷۸
۰۳۵۳۷۲۴۵۰۸۷

پویش داده نوین
PDNSOFT.COM | INFO@PDNSOFT.COM

فهرست تصاویر

آدرس
تهران، خیابان آزادی، خیابان حبیب زادگان، پلاک ۳۶، طبقه ۲
یزد، خیابان مطهری، مرکز فناوری اقبال، واحد ۲۲۵
کدپستی
۱۴۵۸۷۷۷۱۵۴
۸۹۱۷۶۹۷۹۹۸
تلفن
۰۲۱۶۶۱۹۸۶۸۰
۰۳۵۳۷۲۶۵۳۴۳
فکس
۰۲۱۶۶۱۹۸۶۷۸
۰۳۵۳۷۲۴۵۰۸۷
پویش داده نوین
PDNSOFT.COM | INFO@PDNSOFT.COM

چکیده

شرکت پویش داده نوین در سال ۱۳۸۴ با هدف کاربردی نمودن ابزار و بسط و گسترش فرهنگ استفاده از فناوری اطلاعات (IT) تأسیس گردید. این شرکت با انجام تحقیقات طولانی‌مدت توانسته است به موفقیت‌های قابل توجهی در زمینه طراحی و توسعه نرم‌افزارهای حیاتی سازمانی و در نتیجه بومی سازی محصولات استراتژیک حوزه زیرساختی دست یافته و به سهم خویش، گامی را هر چند کوچک در امر قطع وابستگی خارجی و افزایش ضریب امنیت اطلاعات بردارد.

مستند حاضر به معرفی شرکت پویش داده نوین و تشریح مهمترین فعالیت‌های این شرکت می‌پردازد.

کلید واژه ها

شرکت پویش داده نوین، اهداف شرکت، فعالیت‌های شرکت

۱ معرفی شرکت

شرکت پویش داده نوین در سال ۱۳۸۴ توسط جمعی از متخصصین و مهندسین خلاق و جوان تأسیس گردیده و به شماره ثبت ۷۶۹۲ در اداره ثبت شرکتهای استان یزد به ثبت رسیده است. اهداف تاسیس این شرکت در پرتو اهداف و چشم‌انداز مشخص شده زیر می‌باشند:

- دستیابی به جایگاهی برتر و تأثیرگذار در عرصه صنعت نرم‌افزار و شبکه
- دستیابی به محصولی زیرساختی، استراتژیک و قابل رقابت در سطح کشوری و جهانی
- تلاش در جهت کارآفرینی و ایجاد اشتغال
- تلاش در جهت کاربردی نمودن قابلیت‌های فناوری اطلاعات در حوزه‌های مختلف کسب

آدرس
تهران، خیابان آزادی، خیابان حبیب زادگان، پلاک ۳۶، طبقه ۲
یزد، خیابان مطهری، مرکز فناوری اقبال، واحد ۲۲۵
کدپستی
۱۴۵۸۸۷۱۵۴
۸۹۱۷۶۹۷۹۹۸
تلفن
۰۲۱۶۶۱۹۸۶۸۰
۰۳۵۳۷۲۶۵۳۴۳
فکس
۰۲۱۶۶۱۹۸۶۷۸
۰۳۵۳۷۲۴۵۰۸۷
پویش داده نوین
PDNSOFT.COM | INFO@PDNSOFT.COM

- همکاری با مراکز پژوهشی و تحقیقاتی به منظور تبادل تجربیات و افزایش توان فنی

۲ رسالت شرکت

شرکت پویش داده نوین از بدو تاسیس، رسالت خود را براساس مسئولیت‌های ذیل بنا کرده است:

- معرفی برند ملی و رفع وابستگی کشور به نرم‌افزارهای خارجی
- ایجاد یک هسته تخصصی برپایه سیستم عامل لینوکس جهت معرفی راه‌کاری امنیتی متن باز
- معرفی راهکارهای بهینه بهره‌برداری از منابع سخت‌افزاری و نرم‌افزاری تحت شبکه
- کاربردی نمودن فناوری‌های نوین و ارتقاء زیرساخت‌های نرم افزاری بر پایه نرم‌افزارهای متن باز

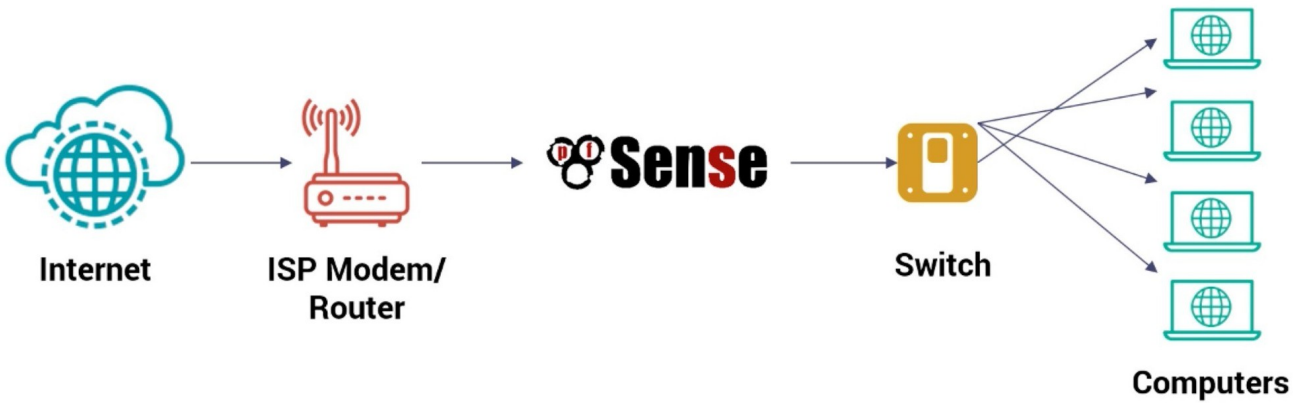
لازم به ذکر است این شرکت در اواخر سال ۹۷ امتیاز و حق بهره برداری از محصول تولیدی خود بـه نـام *PVM* (مجازی سازی سرورها) به شرکت رایانش ابری آوید فروخته است.

آدرس
تهران، خیابان آزادی، خیابان حبیب زادگان، پلاک ۳۶، طبقه ۲
یزد، خیابان مطهری، مرکز فناوری اقبال، واحد ۲۲۵
کدپستی
۱۴۵۸۸۸۷۱۵۴
۸۹۱۷۶۹۷۹۹۸
تلفن
۰۲۱۶۶۱۹۸۶۸۰
۰۳۵۳۷۲۶۵۳۴۳
فکس
۰۲۱۶۶۱۹۸۶۷۸
۰۳۵۳۷۲۴۵۰۸۷
پویش داده نوین
PDNSOFT.COM | INFO@PDNSOFT.COM

۳ مهمترین فعالیت‌های تخصصی شرکت

۱.۳ سامانه *UTM* حرفه‌ای مخصوص شبکه‌های پرسرعت

UTM از مهمترین ابزارهای تدافعی در شبکه ها محسوب می‌شود و نام عمومی برنامه‌هایی است که از دستیابی غیر مجاز به یک سیستم یا شبکه رایانه‌ای جلوگیری می‌کند و دارای انواع متفاوتی است که هریک دارای ویژگیها و امکانات مختلفی هستند. *Pfsesnse* یکی از معروف ترین فایروال های متن باز است که روی سیستم عامل FreeBSD پیاده سازی شده است.



تصویر ۱: فایروال

تیم فنی پویش داده سابقه ده ساله کار با این فایروال متن باز را در کارنامه خود دارد. یکی از مهم‌ترین فاکتورهای موفقیت در به کار گیری از این نرم‌افزار استقرار صحیح سامانه و نیز راه اندازی دقیق و درست آن بر اساس نیازهای مشتری میباشد.

آدرس
تهران، خیابان آزادی، خیابان حبیب زادگان، پلاک ۳۶، طبقه ۲
یزد، خیابان مطهری، مرکز فناوری اقبال، واحد ۲۲۵
کدپستی
۱۴۵۸۷۷۷۱۵۴
۸۹۱۷۶۹۷۹۹۸
تلفن
۰۲۱۶۶۱۹۸۶۸۰
۰۳۵۳۷۲۶۵۳۴۳
فکس
۰۲۱۶۶۱۹۸۶۷۸
۰۳۵۳۷۲۴۵۰۸۷
پویش داده نوین
PDNSOFT.COM | INFO@PDNSOFT.COM

در مجموع دیواره های آتش در شبکه های رایانه ای معمولا از امور چالش‌زا به حساب می آیند. کنترل دسترسی کاربران در فضای سایبر و همچنین جلوگیری از افت پهنای باند شبکه به دلیل پردازش‌های متعدد از سوی دیواره آتش از جمله مهمترین موارد بحث در این زمینه می‌باشند.

برخی از قابلیت های اصلی این *UTM* به شرح زیر است:

- VPN Server
- High Availability
- Load Balancing
- Traffic Shaping
- Captive Portal
- UTM Device
- Firewall / Router
- DNS / DHCP Server
- IDS / IPS
- Transparent Caching Proxy
- Web Content Filter

برای آشنایی بیشتر با قابلیت‌ها و امکانات فنی این سامانه و همچنین نحوه بکارگیری آن در سازمان‌ها میتوانید به قسمت ضمیمه این مستند مراجعه کنید.

آدرس
تهران، خیابان آزادی، خیابان حبیب زادگان، پلاک ۳۶، طبقه ۲
یزد، خیابان مطهری، مرکز فناوری اقبال، واحد ۲۲۵
کدپستی
۱۴۵۸۸۸۷۱۵۴
۸۹۱۷۶۹۷۹۹۸
تلفن
۰۲۱۶۶۱۹۸۶۸۰
۰۳۵۳۷۲۶۵۳۴۳
فکس
۰۲۱۶۶۱۹۸۶۷۸
۰۳۵۳۷۲۴۵۰۸۷
پویش داده نوین
PDNSOFT.COM | INFO@PDNSOFT.COM

۲.۳ سامانه *Network Access Control*

این سامانه با استفاده از چند پروتکل مخصوص (شامل ۸۰۲.۱X) روشی امن برای اتصال سیستم ها به نودهای شبکه و سوئیچ معین میکند. البته این موضوع خلاصه به شبکه‌های کابلی نمیشود. این سامانه قابلیت کنترل کلیه دسترسی ها به شبکه‌های وایرلس سازمان را نیز دارد. در این سامانه کلیه سوئیچ ها و *Access Point* ها تعریف میشود.

نرم افزار *NAC* قادر است امنیت شبکه زیرساخت فیزیکی شما را به طرز چشمگیری افزایش داده و مدیریت آن را برای ادمین شبکه بسیار ساده‌تر کند. از نقاط برجسته استفاده از این سامانه مدیریت متمرکز کلیه تجهیزات ارتباطی شبکه در لایه *Access* به صورت متمرکز می باشد. مدیر شبکه لازم نیست به هر سوئیچ لاگین کرده و جداگانه به تغییرپیکربندی سوئیچ (به عنوان نمونه تغییر ویلن) یک کاربر بپردازد.

امکانات کلیدی نرم افزار:

- مدیریت متمرکز کلیه سوئیچ های شبکه به صورت متمرکز از طریق رابط تحت وب
- امکان تعریف *Roles* براساس نوع دستگاه (تلفن همراه- چاپگر و ...) / سوئیچ یا ترکیبی از آنها
- تغییر *VLAN* کاربران و *restart* پورت سوئیچ کاربر از طریق رابط تحت وب
- اختصاص شبکه و *VLAN* به کاربران بعد از تأیید هویت
- امکان احراز هویت کاربر از طریق *Active Directory – user local – MAC address – Captive Portal*
- امکان تعیین مدت زمان استفاده از شبکه
- امکان تعیین پهنای باند پورت براساس نام کاربر
- پشتیبانی از تجهیزات *VOIP*
- پشتیبانی از شبکه‌های وایرلس

برای آشنایی بیشتر با قابلیت‌ها و امکانات فنی این سامانه و همچنین نحوه بکارگیری آن در سازمان‌ها میتوانید به قسمت ضمیمه این مستند مراجعه کنید.

آدرس
تهران، خیابان آزادی، خیابان حبیب زادگان، پلاک ۳۶، طبقه ۲
یزد، خیابان مطهری، مرکز فناوری اقبال، واحد ۲۲۵
کدپستی
۱۴۵۸۸۸۷۱۵۴
۸۹۱۷۶۹۷۹۹۸
تلفن
۰۲۱۶۶۱۹۸۶۸۰
۰۳۵۳۷۲۶۵۳۴۳
فکس
۰۲۱۶۶۱۹۸۶۷۸
۰۳۵۳۷۲۴۵۰۸۷
پویش داده نوین
PDNSOFT.COM | INFO@PDNSOFT.COM

۳.۳ سیستم مانیتورینگ شبکه *Network Monitoring*

سیستم‌های مانیتورینگ قابلیت نظارت بر تمام تجهیزات اکتیو شبکه‌های کامپیوتری از جمله انواع کامپیوترها، چاپگرهای تحت شبکه، یو پی اس ها، سوئیچها و روترها، حسگرهای دما و رطوبت، کارت خوانها، دوربین های مدار بسته و ... را دارند و با توجه به قابلیت‌ها و مولفه‌های حیاتی و عملیاتی هر سامانه تحت شبکه، امکان مونیتورینگ و نظارت بر کارکرد آن فراهم شده و وضعیت هریک توسط سیستمهای مانیتورینگ بررسی و گزارش می‌گردد.

سیستمهای مانیتورینگ در لحظه وقوع خطا یا بحران می‌تواند به روشهای گوناگونی از جمله پیام کوتاه، ایمیل، پیجر و یا به صدا درآوردن آژیر خطر مسئول شبکه را مطلع نماید.

سیستمهای مورد استفاده توسط این شرکت قابلیت ارائه نمودار کارایی تجهیزات را داشته، به نحوی که مدیران شبکه می‌توانند از گلوگاههای شبکه خود در ساعات مختلف شبانه روز مطلع گردند. از جمله می‌توان به نمودار لود سیستم (پروسه های فعال و یا منتظر) و یا نمودار ترافیک شبکه به روی هر اینترفیس از سوئیچ های لایه ۳ اشاره کرد.. برخی از قابلیتهای این نرم‌افزار به شرح زیر میباشد:

- Log- and event-based monitoring
- Powerful agent-based monitoring and an agentless monitoring via HTTP, SNMP or by connecting directly to the APIs of many applications.
- Graphing and analytics
- Customizable GUI
- Reporting
- Business Intelligence
- Hardware and software inventory
- Notifications and alert handler
- Rule-based configuration, auto-discovery and agent deployment

برای آشنایی بیشتر با قابلیت‌ها و امکانات فنی این سامانه و همچنین نحوه بکارگیری آن در سازمان‌ها میتوانید به قسمت ضمیمه این مستند مراجعه کنید.

آدرس
تهران، خیابان آزادی، خیابان حبیب زادگان، پلاک ۳۶، طبقه ۲
یزد، خیابان مطهری، مرکز فناوری اقبال، واحد ۲۲۵
کدپستی
۱۴۵۸۸۷۱۵۴
۸۹۱۷۶۹۷۹۹۸
تلفن
۰۲۱۶۶۱۹۸۶۸۰
۰۳۵۳۷۲۶۵۳۴۳
فکس
۰۲۱۶۶۱۹۸۶۷۸
۰۳۵۳۷۲۴۵۰۸۷
پویش داده نوین
PDNSOFT.COM | INFO@PDNSOFT.COM

۴.۳ طراحی، راه اندازی و بهبود شبکه‌های کامپیوتری

در عصر ارتباطات شبکه‌های کامپیوتری شاهرگ بقای سازمانها و قوام مسیر رشد و توسعه آنها محسوب گردیده و لزوم ارائه خدمات تخصصی و کارآمد تحت شبکه باعث شده است تا مدیریت بهینه و اثربخش شبکه‌های کامپیوتری در اولویت قرار گیرد. بدیهی است که پیاده‌سازی مناسب بستر تبادل اطلاعات و انجام پیش‌بینی‌های لازم جهت رویارویی با هرگونه حوادث احتمالی امری ضروری است که عدم توجه به این مهم، هدر رفت منابع انسانی، تجهیزاتی و اتلاف زمان به عنوان با ارزشترین سرمایه هر سازمانی را به دنبال خواهد داشت.

با توجه به توضیحات فوق و در راستای ارائه خدمات برتر تحت شبکه که از مهمترین فرصتهای حفظ رقابت در عصر حاضر است این شرکت مشروح خدمات زیر را به مشتریان خود ارائه می نماید.

- ✔ طراحی ستون فقرات (*Back Bone*) فیزیکی شبکه های محلی (*LAN*)
- ✔ شبکه مجازی *VLAN*
- ✔ نصب و راه اندازی تجهیزات زیرساختی شبکه و سرور (*SAN, NAS, SAN Switch*,...)
- ✔ نصب، راه اندازی و تنظیم بهینه سرورهای شبکه بر مبنای انواع سیستم عاملهای خانواده *UNIX, Windows* (بخصوص *Linux* و *FreeBSD*)
- ✔ راه اندازی و تنظیم انواع سیستمهای جامع *Backup* تحت شبکه
- ✔ راه اندازی و تنظیم انواع سیستمهای مدیریت شبکه (*SNMP, DHCP, DNS, NIS, LDAP, Terminal Service*, ...)
- ✔ نصب، راه اندازی و تنظیم بهینه تجهیزات ارتباط شبکه با اینترنت (*Router, Gateway, xDSL*, ...)
- ✔ نصب و تنظیم انواع سیستمهای کنترل کننده امنیت شبکه (*Proxy, Filter, Firewall, NAT, PAT*)
- ✔ نصب و راه اندازی سیستم ارتباط با شبکه از بیرون (*VPN,Remote Access Server*)
- ✔ نصب و راه اندازی سرویسهای مورد نیاز جهت ارائه سرویس اینترنت (*HTTP Server, NNTP Server , SMTP Server, IMAP Server, Radius Server* ...)

آدرس
تهران، خیابان آزادی، خیابان حبیب زادگان، پلاک ۳۶، طبقه ۲
یزد، خیابان مطهری، مرکز فناوری اقبال، واحد ۲۲۵
کدپستی
۱۴۵۸۸۸۷۱۵۴
۸۹۱۷۶۹۷۹۹۸
تلفن
۰۲۱۶۶۱۹۸۶۸۰
۰۳۵۳۷۲۶۵۳۴۳
فکس
۰۲۱۶۶۱۹۸۶۷۸
۰۳۵۳۷۲۴۵۰۸۷
پویش داده نوین
PDNSOFT.COM | INFO@PDNSOFT.COM

برای آشنایی بیشتر با قابلیت‌ها و امکانات فنی این سامانه و همچنین نحوه بکارگیری آن در سازمان‌ها میتوانید بـه قسـمت ضمیمه این مستند مراجعه کنید.

۵.۳ خدمات مشاوره و برنامه‌ریزی *IT* درحوزه های زیرساخت و طراحی شبکه

بدون شک استفاده از کارشناسان و مشاوران زبده‌ی خارج از سازمان، در امـر بهبـود رونـد کـار سیسـتماتیک سازمانها، تأثیرات بسزایی داشته و موجبات هم افزایی فردی و گروهی را فراهم خواهد ساخت و به طور مشـخص بهره‌گیری از خدمات مشاوره در حوزه فناوری اطلاعات، خود فراهم‌آورنده یك رابطه تعاملی فزاینده اسـت کـه از بکارگیـــری تخصص‌های چندگانه نیروهای کار، برای حل مسائل و توانایی ترکیب و پیوند تخصص‌های موجود در شـبکه‌های کامپیوتری و هنر اداره آن شبکه‌ها، پدید می‌آید و در این راستا سازمانهایی که در حیطه انفورماتیـك و فناوری اطلاعات از همفکری مشاورین ذیصلاح استفاده می‌کرده اند، به موفقیتهای شگرفی نسـبت بـه سـازمانهای هم رده خودکه به این موضوع توجه کافی نداشته اند، نایل گشته‌اند.

شرکت پویش داده نوین با برخورداری از تجربیات یک دهه فعالیت تخصصی در حوزه فناوری اطلاعات بویژه در حوزه های زیرساختی حوزه فناوری اطلاعات اعم از: زیرساختها و سرویسهای تحت شـبکه، سـامانه مبتنـی بـر *open source* ، سیستمهای فایروال، مباحث امنیت، کنترل پروژه و... آمادگی دارد در جهت پیشبرد کسب و کار و اهداف شرکت‌ها و سازمان‌ها نسبت به ارائه خدمات مشاوره اقدام نماید.

ازجمله حوزه‌های خدمات مشاوره می‌توان به موارد ذیل اشاره نمود:

- مشاوره طراحی و پیاده‌سازی زیرساخت شبکه‌های کامپیوتری
- مشاوره مدیریت فناوری اطلاعات: استراتژی و برنامه‌ریزی
- نیازسنجی طرح‌های انفورماتیکی دستگاههای اجرایی و شرکتهای خصوصی
- سرویسهای شبکه
- ایمن‌سازی شبکه و استانداردهای امنیت اطلاعات
- طراحی و نظارت بر پیاده سازی مراکز داده

آدرس
تهران، خیابان آزادی، خیابان حبیب زادگان، پلاک ۳۶، طبقه ۲
یزد، خیابان مطهری، مرکز فناوری اقبال، واحد ۲۲۵
کدپستی
۱۴۵۸۸۷۱۵۴
۸۹۱۷۶۹۷۹۹۸
تلفن
۰۲۱۶۶۱۹۸۶۸۰
۰۳۵۳۷۲۶۵۳۴۳
فکس
۰۲۱۶۶۱۹۸۶۷۸
۰۳۵۳۷۲۴۵۰۸۷
پویش داده نوین
PDNSOFT.COM | INFO@PDNSOFT.COM

- نگهداری و بهینه‌سازی سیستمهای نرم‌افزاری
- تدوین استراتژی و طرحهای جامع انفورماتیکی

۶.۳ پیاده سازی سرور حسابرسی کاربران *Accounting*

حسابرسی کاربران شبکه معمولا از دغدغه‌های اساسی مدیران شبکه‌های کامپیوتری است. محدودیت پهنای باند و همچنین استفاده بهینه از پهنای باند موجود از جمله عوامل اصلی این موضوع به حساب می آیند. همچنین می‌توان در این مورد به رهگیری سایتهای مورد استفاده کاربران از شبکه اینترنت نیز اشاره کرد.

شرکت پویش داده نوین با داشتن متخصصان در عرضه و استفاده از محصولات متن بازی از جمله سیستم لینوکس تاکنون توانسته است با استفاده از راهکارهای امن، نیازهای حسابرسی سازمانها و ارگانهای گوناگونی را مرتفع سازد.

با توجه به استفاده از بستر سیستم عامل امن لینوکس، راهکارهای ارائه شده تضمین‌کننده خواستهای امنیتی سازمان نیز می‌باشند.

آدرس
تهران، خیابان آزادی، خیابان حبیب زادگان، پلاک ۳۶، طبقه ۲
یزد، خیابان مطهری، مرکز فناوری اقبال، واحد ۲۲۵
کدپستی
۱۴۵۸۸۸۷۱۵۴
۸۹۱۷۶۹۷۹۹۸
تلفن
۰۲۱۶۶۱۹۸۶۸۰
۰۳۵۳۷۲۶۵۳۴۳
فکس
۰۲۱۶۶۱۹۸۶۷۸
۰۳۵۳۷۲۴۵۰۸۷
پویش داده نوین
PDNSOFT.COM | INFO@PDNSOFT.COM

۷.۳ نرم‌افزار *LogServer*

لاگ سرور جعبه ی سیاه سفینه شماست! با جمع‌آوری تمام لاگ ها از کلیه ی تجهیزات تحت شبکه، لاگ سرور قادر است تا در زمان وقوع بحران، شما را از آخرین وضعیت تجهیزات آگاه کرده و در خروج از بحران و جلوگیری از تکرار آن به شما کمک کند. همچنین لاگ سرور با ارائه داشبورد فارسی قادر است به صورت گرافیکی لاگ های مهم را بر اساس نیاز سازمان به ادمین شبکه نمایش دهد.

امکانات نرم افزار:

- جمع‌آوری لاگ های تمامی سیستم‌ها شامل ویندوز، لینوکس، سوئیچ، روتر و فایروال
- امکان جستجو پیشرفته در میان لاگ ها، جستجو بر اساس کلمات کلیدی، *Source*، زمان دقیق
- امکان استخراج اطلاعات مهم از درون لاگ ها با در اختیار داشتند *Log extractor* های پیشرفته
- ساخت داشبورد گرافیکی برای مانیتورینگ لاگ ها و رصد لاگ های حساس و حیاتی
- امکان پیاده‌سازی به صورت مجازی و فیزیکی با هارد دیسک های مجزا برای نگه داشتن لاگ ها پس از وقوع بحران.

برای آشنایی بیشتر با قابلیت‌ها و امکانات فنی این سامانه و همچنین نحوه بکارگیری آن در سازمان‌ها میتوانید به قسمت ضمیمه این مستند مراجعه کنید.

آدرس
تهران، خیابان آزادی، خیابان حبیب زادگان، پلاک ۳۶، طبقه ۲
یزد، خیابان مطهری، مرکز فناوری اقبال، واحد ۲۲۵
کدپستی
۱۴۵۸۷۷۷۱۵۴
۸۹۱۷۶۹۷۹۹۸
تلفن
۰۲۱۶۶۱۹۸۶۸۰
۰۳۵۳۷۲۶۵۳۴۳
فکس
۰۲۱۶۶۱۹۸۶۷۸
۰۳۵۳۷۲۴۵۰۸۷
پویش داده نوین
PDNSOFT.COM | INFO@PDNSOFT.COM

۸.۳ سامانه جامع پشتیبان‌گیری / *Backup*

یکی از بزرگترین دغدغه های مدیران شبکه تهیه نسخه پشتیبان از داده‌ها میباشد. در کنار داده‌ها پیکربندی سرویس‌ها و سیستم عامل‌ها نیز از اهمیت زیادی برخوردار میباشد. در هنگام انتشار یک ویروس یا بروز یک خطای سخت‌افزاری اولین عامل آرامش بخش برای مدیر شبکه اطمینان از این است که یک نسخه از داده‌های مهم و به روز را در جایی مطمئن در اختیار دارد. این سامانه یک سیستم متمرکز پشتیبان گیری با بهره گیری از انواع روش‌های پشتیبان گیری در اختیار مدیران شبکه قرار میدهد.

در این سامانه یک سرور اصلی(لینوکسی) به عنوان سرور *backup* نصب و راه اندازی میشود. مدیر شبکه اقدام به نصب و راه اندازی نسخه کلاینت سامانه روی سرورهای خود خود میکند. سرور *backup* از طریق نسخه کلاینت اطلاعاتی که مد نظر مدیر سیستم هست را بک آپ گیری و ذخیره می کند.

برخی از قابلیت های این سامانه به شرح زیر میباشد:

۱. رابط تحت وب برای مشاهده وضعیت بک آپ ها و نیز *restore* کردن آن‌ها
۲. امکان اطلاع از وضعیت کلیه تسک های بک آپ از طریق میل یا داشبورد تحت وب
۳. پشتیبانی از انواع سیستم عامل ها *GNU/Linux-FreeBSD-Windows*
۴. پشتیبان گیری از انواع روش های بک آپ گیری : *Full, Differential, Incremental*,
۵. پشتیبانی از *Deduplication* و فشرده‌سازی جهت کاهش فضای ذخیره سازی
۶. امکان پشتیبان گیری از دیتابیس های *mysql,pgsql* و *MS SQL*
۷. پشتیبانی از *Volume Shadow Copy (VSS)*
۸. پشتیبانی از انواع ترکیب های زمان بندی جهت تنظیم خودکار عملیات پشتیبان گیری

برای آشنایی بیشتر با قابلیت‌ها و امکانات فنی این سامانه و همچنین نحوه بکارگیری آن در سازمان‌ها میتوانید به قسمت ضمیمه این مستند مراجعه کنید.

آدرس
تهران، خیابان آزادی، خیابان حبیب زادگان، پلاک ۳۶، طبقه ۲
یزد، خیابان مطهری، مرکز فناوری اقبال، واحد ۲۲۵
کدپستی
۱۴۵۸۸۸۷۱۵۴
۸۹۱۷۶۹۷۹۹۸
تلفن
۰۲۱۶۶۱۹۸۶۸۰
۰۳۵۳۷۲۶۵۳۴۳
فکس
۰۲۱۶۶۱۹۸۶۷۸
۰۳۵۳۷۲۴۵۰۸۷
پویش داده نوین
PDNSOFT.COM | INFO@PDNSOFT.COM

اسامی برخی از مراکزی که شرکت پویش داده نوین افتخار خدمت‌رسانی به آنها را داشته است به شـرح ذیل است:

- استانداری یزد
- استانداری خراسان جنوبی
- استانداری کهگیلویه و بویراحمد
- استانداری خوزستان
- استانداری مازندران
- سازمان پژوهش های علمی و صنعتی ایران
- دانشگاه علوم پزشکی یزد
- سازمان مدیریت و برنامه‌ریزی استان یزد
- فرمانداری یزد
- فرمانداری اردکان
- فرمانداری میبد
- فرمانداری مهریز
- فرمانداری بافق
- فرمانداری ابرکوه
- فرمانداری خاتم
- فرمانداری صدوق
- فرمانداری بهاباد
- فرمانداری تفت
- فرمانداری طبس
- فرمانداری بیرجند
- فرمانداری درمیان
- فرمانداری قائنات
- فرمانداری خوسف
- فرمانداری نهبندان
- فرمانداری زیرکوه
- فرمانداری سرایان
- فرمانداری بشرویه
- فرمانداری فردوس
- سازمان همیاری شهرداریهای استان یزد
- شهرداری یزد
- شهرداری رفسنجان
- شهرداری اردکان
- شهرداری میبد
- شهرداری تفت
- شهرداری بافق
- شهرداری ابرکوه

پویش داده نوین
PDNSOFT.COM | INFO@PDNSOFT.COM

آدرس: تهران، خیابان آزادی، خیابان حبیب زادگان، پلاک ۳۶، طبقه ۲
یزد، خیابان مطهری، مرکز فناوری اقبال، واحد ۲۲۵

کدپستی: ۱۴۵۸۸۸۷۱۵۴
۸۹۱۷۶۹۷۹۹۸

تلفن: ۰۲۱۶۶۱۹۸۶۸۰
۰۳۵۳۷۲۶۵۳۴۳

فکس: ۰۲۱۶۶۱۹۸۶۷۸
۰۳۵۳۷۲۴۵۰۸۷

- شهرداری اشکذر
- شهرداری زارچ
- شهرداری مهریز
- شهرداری احمدآباد
- شهرداری شاهدیه
- شهرداری مروست
- شهرداری عقدا
- شهرداری سربیشه
- اداره کل راهداری وحمل و نقل جاده ای اســـتان یزد
- اداره کل آموزش و پرورش استان یزد
- اداره کل هواشناسی استان یزد
- کانون اصلاح و تربیت استان یزد
- سازمان جهاد کشاورزی استان یزد
- اداره کل آموزش فنی و حرفه ای استان یزد
- اداره کل راه و شهرسازی استان یزد
- اداره کل استاندارد و تحقیقات صنعتی استان یزد
- اداره کل منابع طبیعی استان یزد
- اداره کل فرهنگ و ارشاد اسلامی استان یزد

بیمارستان افشار یزد

- اداره کل امور اقتصادی و دارایی استان یزد
- شرکت برق منطقه ای استان یزد
- دانشگاه آزاد اسلامی واحد تفت
- پارک علم و فناوری یزد
- شرکت جهان الکترونیک
- شرکت الکتروکویر
- شرکت صنایع کاشی نائین
- شرکت فولاد گستر یزد
- سازمان همیاری شهرداریهای خراسان رضوی
- مرکز تحقیقات مخابرات ایران
- اداره کل زندانهای استان یزد
- شهرداری سرایان
- مدیریت تولید برق آذربایجان غربی
- مدیریت توزیع برق آذربایجان غربی
- شهرداری طبس
- شهرداری ندوشن
- شهرداری ایذه
- شرکت نوین الکترود اردکان
- شرکت توزیع نیروی برق خراسان جنوبی
- سازمان مدیریت و برنامه‌ریزی خراسان جنوبی
- شهرداری بیرجند
- شهرداری باغستان

پویش داده نوین
PDNSOFT.COM | INFO@PDNSOFT.COM

آدرس: تهران، خیابان آزادی، خیابان حبیب زادگان، پلاک ۳۶، طبقه ۲
یزد، خیابان مطهری، مرکز فناوری اقبال، واحد ۲۲۵

کدپستی: ۱۴۵۸۸۸۷۱۵۴
۸۹۱۷۶۹۷۹۹۸

تلفن: ۰۲۱۶۶۱۹۸۶۸۰
۰۳۵۳۷۲۶۵۳۴۳

فکس: ۰۲۱۶۶۱۹۸۶۷۸
۰۳۵۳۷۲۴۵۰۸۷

- شرکت پردیس فناور ایساتیس
- اداره کل راهداری و حمل و نقل جاده ای اســتان گلستان
- اداره کل راهداری و حمل و نقل جاده ای اســتان کهگیلویه و بویراحمد
- اداره کل راهداری و حمل و نقل جاده ای ایلام
- اداره کل راهداری و حمل و نقل جاده ای اســتان خراسان جنوبی
- بیمارستان رهنمون یزد
- مرکز تحقیقات ناباروری یزد
- سازمان مدیریت و برنامه‌ریزی خراسان رضوی
- پارک علم و فناوری استان گیلان
- بیمارستان شهید صدوقی یزد
- بیمارستان فاطمه زهرا مهریز

آدرس
تهران، خیابان آزادی، خیابان حبیب زادگان، پلاک ۳۶، طبقه ۲
یزد، خیابان مطهری، مرکز فناوری اقبال، واحد ۲۲۵
کدپستی
۱۴۵۸۷۷۷۱۵۴
۸۹۱۷۶۹۷۹۹۸
تلفن
۰۲۱۶۶۱۹۸۶۸۰
۰۳۵۳۷۲۶۵۳۴۳
فکس
۰۲۱۶۶۱۹۸۶۷۸
۰۳۵۳۷۲۴۵۰۸۷
پویش داده نوین
PDNSOFT.COM | INFO@PDNSOFT.COM

۴ ضمیمه:

معرفی قابلیتهای نرم افزاری سرویس های ارائه شده توسط شرکت پویش داده نوین.

۱.۴ سامانه *UTM* حرفه‌ای مخصوص شبکه‌های پرسرعت

پروژه *pfsense* از سال ۲۰۰۴ میلادی در حال رشد و فعالیت است. این نرم‌افزار روی سیستم عامل حرفه‌ای *FreeBSD* توسعه یافته است. توسعه این نرم‌افزار به عهده شرکت *Netgate* میباشد. ویژگی مهم این نرم‌افزار آن است که به راحتی قابلیت نصب بر روی هر نوع سرور با هر سخت افزاری را داشته و میتواند هر سروری را به یک *UTM* قدرتمند تبدیل کند. لذا مدیران شبکه نیازی به تهیه یک سخت‌افزار ویژه با مشخصات خاص برای *UTM* نخواهند داشت. از این سامانه میتوان در راه اندازی موارد زیر بهره گرفت.

۱.۱.۴ سامانه تشخیص نفوذ (*IPS/IDS*)

با راه اندازی این سامانه در سرور *pfsense*، میتوان بسیاری از حملات شبکه را شناسایی و جلوگیری کرد. سرویس *IPS/IDS* در این سامانه با توجه به رول هایی که برای آن نوشته می‌شود میتواند اطلاعات ویژه موجود در بستههای شبکه را بازبینی کرده و نسبت به آن اقدام لازم را انجام دهد. برخی از قابلیتهای سامانه تشخیص نفوذ به شرح زیر است:

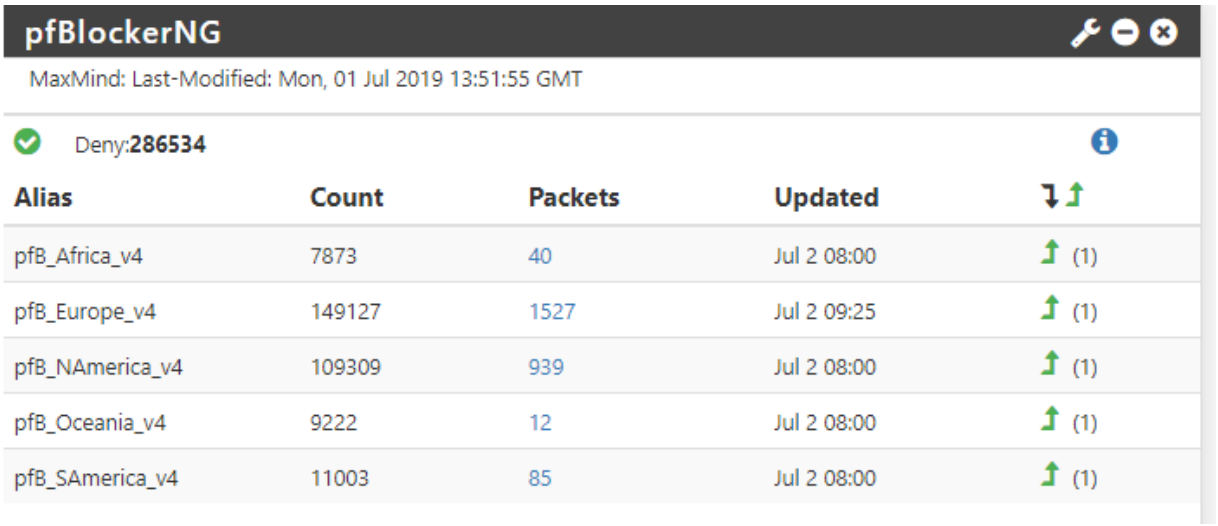
آدرس
تهران، خیابان آزادی، خیابان حبیب زادگان، پلاک ۳۶، طبقه ۲
یزد، خیابان مطهری، مرکز فناوری اقبال، واحد ۲۲۵
کدپستی
۱۴۵۸۸۷۱۵۴
۸۹۱۷۶۹۷۹۹۸
تلفن
۰۲۱۶۶۱۹۸۶۸۰
۰۳۵۳۷۲۶۵۳۴۳
فکس
۰۲۱۶۶۱۹۸۶۷۸
۰۳۵۳۷۲۴۵۰۸۷
پویش داده نوین
PDNSOFT.COM | INFO@PDNSOFT.COM

- *packet analyzer*
- *Layer ۷ application detection*
- *Multiple rules sources and categories*
- *Emerging threats database*
- *IP blacklist database*
- *Pre-set rule profiles*
- *Deep Packet Inspection (DPI)*
- *Suppressing false positive alerts*
- *Per-interface configuration*

سامانه های تشخیص نفوذ مانند *snort* و *suricata* شامل دیتابیس های جهانی هستند که هر ماه توسط سازمان های امنیتی بین‌المللی برای جلوگیری از حملات منتشر می شوند. برای مثال این دیتابیس‌ها شامل لیست *IP* های ماینرهای ارزهای دیجیتالی، لیست *IP* های بدافزارها ، جدیدترین الگوهای نفوذ باج افزارها، جدیدترین نحوه های دزدی اطلاعات از سازمان ها از طریق اینترنت و غیره بوده که این ماژول در صورت در اختیار داشتن آن‌ها، میتواند این حملات را شناسایی کرده و اقدام لازم را انجام دهد.

همچنین با استفاده از پکیج های متن باز موجود در این سامانه، میتوان دسترسی های تمامی کشورها به سرورهای داخل ایران را محدود کرد به طوری که سرور مورد نظر تنها برای کاربرانی که در داخل ایران هستند در دسترس باشد. با استفاده از این تکنیک، میتوان بسیاری از حملات سایبری که عموما از کشورهای خارجی انجام می‌پذیرد را به راحتی و با ضریب اطمینان بسیار بالا خنثی کرد، به نحوی که هیچ گونه حمله جدید کشف نشده‌ای نیز قابلیت ورود به سرور را نخواهد داشت. نمونه‌ای از عمل‌رد این قابلیت را در تصویر زیر مشاهده میکنید:

آدرس
تهران، خیابان آزادی، خیابان حبیب زادگان، پلاک ۳۶، طبقه ۲
یزد، خیابان مطهری، مرکز فناوری اقبال، واحد ۲۲۵
کدپستی
۱۴۵۸۸۸۷۱۵۴
۸۹۱۷۶۹۷۹۹۸
تلفن
۰۲۱۶۶۱۹۸۶۸۰
۰۳۵۳۷۲۶۵۳۴۳
فکس
۰۲۱۶۶۱۹۸۶۷۸
۰۳۵۳۷۲۴۵۰۸۷
پویش داده نوین
PDNSOFT.COM | INFO@PDNSOFT.COM



تصویر ۲: عملکرد سرویس *country block*

۲.۱.۴ روتر – فـایرواقدرتمند

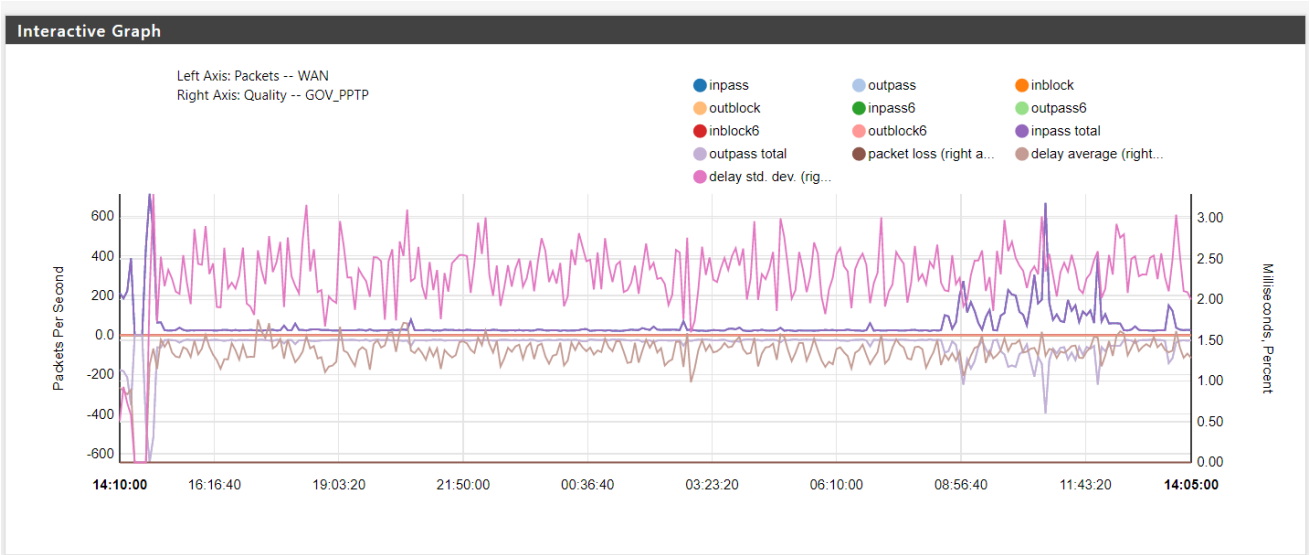
سامانه *pfsense* میتواند هر سروری را به یـک روتـر - فـایروال قدرتمنـد تبـدیل کنـد. قابلیت‌هـای نرم‌افزار *pfsene* به عنوان یک روتر - فایروال به شرح زیر است:

- *Stateful Packet Inspection (SPI)*
- *Anti-Spoofing*
- *Time based rules*
- *Connection limits*
- *Captive portal guest network*
- *NAT mapping (inbound/outbound)*
- *VLAN support (۸۰۲.۱q)*
- *Configurable static routing*
- *Multiple IP addresses per interface*
- *DHCP server*
- *DNS forwarding*
- *PPPoE Server*

آدرس
تهران، خیابان آزادی، خیابان حبیب زادگان، پلاک ۳۶، طبقه ۲
یزد، خیابان مطهری، مرکز فناوری اقبال، واحد ۲۲۵
کدپستی
۱۴۵۸۸۷۱۵۴
۸۹۱۷۶۹۷۹۹۸
تلفن
۰۲۱۶۶۱۹۸۶۸۰
۰۳۵۳۷۲۶۵۳۴۳
فکس
۰۲۱۶۶۱۹۸۶۷۸
۰۳۵۳۷۲۴۵۰۸۷
پویش داده نوین
PDNSOFT.COM | INFO@PDNSOFT.COM

سامانه *pfsense* به خوبی با سایر تجهیزات شبکه ارتباط برقرار کرده و می‌تواند کلیه نیازهای روتینگ و فایروالینگ شبکه و تجهیزات را برآورده کند. این فایروال، علاوه بر عملکرد به عنوان دروازه ای میان شبکه داخلی سازمان و شبکه اینترنت، میتواند به عنوان یک فایروال داخلی نیز ایفای نقش کرده و با شناسایی و مدیریت ارتباط بین شبکه‌های *LAN* و *VLAN*ها امنیت آن‌ها را تضمین کند. در شبکه‌های سازمانی، اجرای *VLAN* بندی برای جداسازی سرورها، کاربران رایانه، تلفن‌های *VoIP* ، شبکه دولت، شبکه‌های محلی راه دور (مانند مراکز شهرستان‌ها) و غیره یک امر حیاتی بوده و *pfsense* میتواند به عنوان یک روتر – فایروال قدرتمند، امنیت ارتباط میان این *VLAN* ها را تضمین کند.

این سامانه همچنین قادر است میزان پهنای باند، نوع ارتباط، سرعت و حجم کاربران، اینترفیس‌های شبکه، *VLAN*ها و غیره را در لحظه مانیتور و کنترل کرده و با استفاده از نمودارهای زیبا به نمایش بگذارد. تصویر زیرنمونه ای از این نمودارها را به نمایش میگذارد:



تصویر ۳: نمونه ای از گراف اطلاعات شبکه

آدرس
تهران، خیابان آزادی، خیابان حبیب زادگان، پلاک ۳۶، طبقه ۲
یزد، خیابان مطهری، مرکز فناوری اقبال، واحد ۲۲۵
کدپستی
۱۴۵۸۷۷۷۱۵۴
۸۹۱۷۶۹۷۹۹۸
تلفن
۰۲۱۶۶۱۹۸۶۸۰
۰۳۵۳۷۲۶۵۳۴۳
فکس
۰۲۱۶۶۱۹۸۶۷۸
۰۳۵۳۷۲۴۵۰۸۷
پویش داده نوین
PDNSOFT.COM | INFO@PDNSOFT.COM

۳.۱.۴ میزبانی *VPN* سرور امن

یکی از نیازهای شبکه‌های سازمانی، ایجاد دسترسی برای کاربرانی است که در خارج از محیط سازمان قرار دارند. همچنین شرکتهای نرم افزاری برای پشتیبانی سرویسهای خود در داخل سازمان، نیاز به دسترسی از راه دور دارند. در روشهای قدیمی برای ایجاد دسترسی برای کاربران خارج سازمانی از بازکردن پورت ریموت دسکتاپ(*remote desktop*) و یا دسترسی به وسیله نرم افزارهای جانبی مانند *anydesk* استفاده میشد. امروزه مخاطرات بسیاری پورت های *remote desktop* را تهدید میکند و همچنین باج افزارها نیز از همین طریق به سیستم‌ها نفوذ کرده و اطلاعات سرور را رمزنگاری میکنند. استفاده از پورت ریموت دسکتاپ در شبکه‌های اینترنتی بسیار خطرناک بوده و استفاده از نرم افزارهای جانبی مانند *anydesk* نیز با محدودیت‌ها و مخاطراتی همراه است. لذا *pfsense* میتواند با راه اندازی سرور *openvpn* که یک پروتکل *vpn* متن باز و رمزنگاری شده است، نیاز کاربران به دسترسی از راه دور را به صورت امن و به ساده‌ترین شکل (تنها با اجرا کردن یک فایل *exe*) برآورده کند.

همچنین با استفاده از *VPN* های منطقه‌ای (*site-to-site VPN*) ارتباط سازمان مرکزی با سازمان‌های زیر مجموعه‌ی آن (مانند استانداری و فرمانداری‌های شهرستان‌های تابعه) را می‌توان به صورت امن روی بستر اینترنت، شبکه دولت، فیبر و غیره برقرار کرد. به دلیل *site-to-site* بودن این نوع ارتباط، کاربران نیازی به انجام هیچگونه تنظیمات خاص و یا برقراری ارتباط *vpn* شخصی نداشته و میتوانند به صورت همزمان به شبکه محلی خود و شبکه‌ی سازمان مرکزی دسترسی داشته باشند. قابلیت‌های سامانه *pfsense* در برقراری ارتباطات *VPN* به شرح جدول زیر است:

- *L۲TP/IPsec for mobile devices*
- *IPsec and OpenVPN*
- *Multi-WAN for failover*
- *Site-to-site and remote access VPN support*
- *Split tunneling*
- *SSL encryption*
- *Automatic or custom routing*
- *VPN client for multiple operating systems*

آدرس
تهران، خیابان آزادی، خیابان حبیب زادگان، پلاک ۳۶، طبقه ۲
یزد، خیابان مطهری، مرکز فناوری اقبال، واحد ۲۲۵
کدپستی
۱۴۵۸۷۷۷۱۵۴
۸۹۱۷۶۹۷۹۹۸
تلفن
۰۲۱۶۶۱۹۸۶۸۰
۰۳۵۳۷۲۶۵۳۴۳
فکس
۰۲۱۶۶۱۹۸۶۷۸
۰۳۵۳۷۲۴۵۰۸۷
پویش داده نوین
PDNSOFT.COM | INFO@PDNSOFT.COM

۴.۱.۴ عمل‌کرد *Proxy* سرور و فیلترینگ محتوا

با استفاده از سامانه *pfsense* میتوان به دسترسی کاربران به برخی وبسایت‌ها و سرویسهای اینترنـــتی را مانیتور و محدود کرد. قابلیت‌های این بخش نیز در جدول زیر قرار داده شده است:

- *HTTP and HTTPS proxy*
- *Non Transparent or Transparent caching proxy*
- *Domain/URL filtering*
- *HTTPS URL and content screening*
- *Website access reporting*
- *Domain Name blacklisting (DNSBL)*
- *Usage reporting for daily, monthly, etc.*

آدرس
تهران، خیابان آزادی، خیابان حبیب زادگان، پلاک ۳۶، طبقه ۲
یزد، خیابان مطهری، مرکز فناوری اقبال، واحد ۲۲۵
کدپستی
۱۴۵۸۷۷۷۱۵۴
۸۹۱۷۶۹۷۹۹۸
تلفن
۰۲۱۶۶۱۹۸۶۸۰
۰۳۵۳۷۲۶۵۳۴۳
فکس
۰۲۱۶۶۱۹۸۶۷۸
۰۳۵۳۷۲۴۵۰۸۷
پویش داده نوین
PDNSOFT.COM | INFO@PDNSOFT.COM

۲.۴ سامانه *Network Access Control*

NAC یکی از بهترین نرم افزاره برای کنترل دسترسی نودهای شبکه است. به کمک این نرم‌افزار، تمامی کاربران برای ورود به شبکه و دریافت *VLAN* مربوطه ابتدا تأیید هویت می‌شوند. تأیید هویت نودها به کمک یوزر و پسورد شخصی (*dot۱x*)، یوزر و پسورد کاربر در اکتیودایرکتوری، مک آدرس کاربر و غیره امکان‌پذیر است.

۱.۲.۴ کاربردهای سامانه *Network Access Control*:

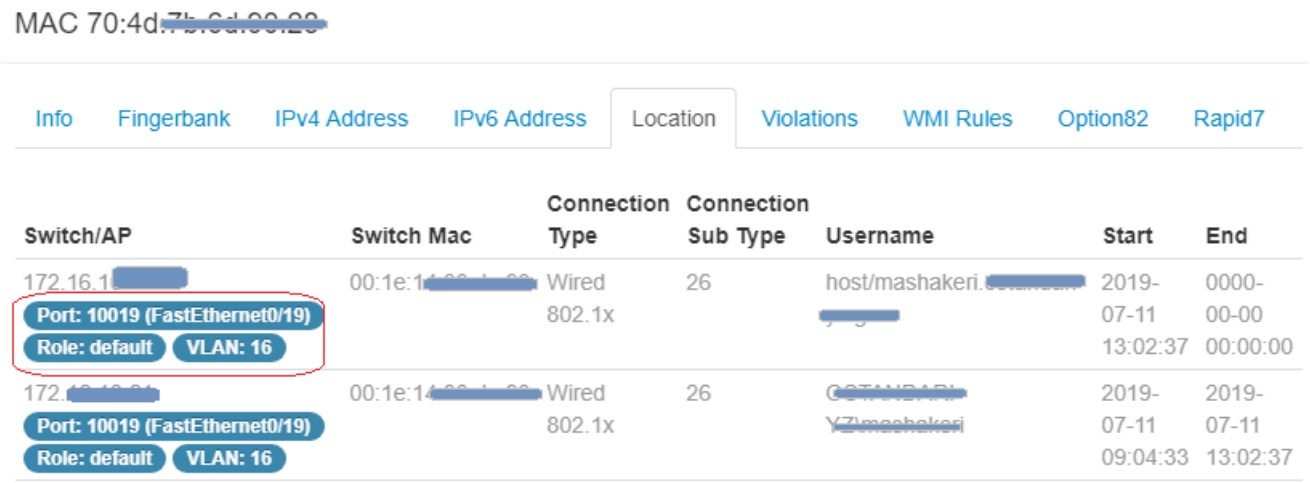
برای تأمین امنیت شبکه‌ها در سازمانهای بزرگ، شبکه به چندین *vlan* تقسیم شده و کاربران بر طبق سیاست‌های سازمان در *vlan* مربوطه قرار میگیرند. در عین حال، مدیریت این vlan ها برای مدیر شبکه کاری زمان بر بوده و در برخی موارد دشوار میگردد. برای مثال، پیدا کردن دقیق شماره پورت سوئیچی که کاربر، رایانه خود را به آن متصل نموده در برخی موارد چالش برانگیز بوده و تنظیم پورت شبکه و اختصاص vlan در محیط کامند لاین (command line) نیز نیاز به دانش کانفیگ تجهیزات دارد.

از طرفی، از لحاظ امنیتی لازم است تا تمامی کسانی که قصد ورود به شبکه داخلی سازمان را دارند شناسایی و تأیید هویت شده و از ورود افراد و دستگاههای ناشناس به شبکه جلوگیری گردد. مجوعه فعالیت‌های ذکر شده بخشی از وظایف یک سامانه کنترل دسترسی شبکه (Network Access Control) است.

آدرس
تهران، خیابان آزادی، خیابان حبیب زادگان، پلاک ۳۶، طبقه ۲
یزد، خیابان مطهری، مرکز فناوری اقبال، واحد ۲۲۵
کدپستی
۱۴۵۸۸۸۷۱۵۴
۸۹۱۷۶۹۷۹۹۸
تلفن
۰۲۱۶۶۱۹۸۶۸۰
۰۳۵۳۷۲۶۵۳۴۳
فکس
۰۲۱۶۶۱۹۸۶۷۸
۰۳۵۳۷۲۴۵۰۸۷
پویش داده نوین
PDNSOFT.COM | INFO@PDNSOFT.COM

۲.۲.۴ نحوه کار سامانه *Network Access Control*:

NAC قادر است تا به تجهیزات زیرساختی شبکه مانند روتر و سوئیچها متصل شده و آن‌ها را کنترل کند. نرم‌افزار NAC با اتصلال به سوئیچ از طریق پروتکل SNMP میتواند اطلاعات کاربری که به آن متصل شده، از جمله شماره پورت، آدرس سوئیچ، مک آدرس کاربر، یوزر و پسورد کاربر، vlan و سایر اطلاعات آن را دریافت کرده و نمایش دهد. در تصویر زیر برخی از این اطلاعات برای یک کاربر نشان داده شده است.



تصویر ۴: نمایش اطلاعات یک کاربر شبکه

در نرم‌افزار *NAC*، کاربران بر اساس یوزر و پسوردشان (مطابق با اکتیودایرکتوری و یا دیتابیس لوکال) و همچنین بر اساس مک آدرس دسته بندی شده و مدیریت می شوند. کاربر به محض اتصال به شبکه باید اطلاعات شخصی مانند نام کاربری و رمز عبور خود را وارد کرده تا بتواند به صورت خودکار در سیستم *NAC*

آدرس: تهران، خیابان آزادی، خیابان حبیب زادگان، پلاک ۳۶، طبقه ۲
یزد، خیابان مطهری، مرکز فناوری اقبال، واحد ۲۲۵
کدپستی: ۱۴۵۸۷۷۷۱۵۴ ۸۹۱۷۶۹۷۹۹۸
تلفن: ۰۲۱۶۶۱۹۸۶۸۰ ۰۳۵۳۷۲۶۵۳۴۳
فکس: ۰۲۱۶۶۱۹۸۶۷۸ ۰۳۵۳۷۲۴۵۰۸۷
پویش داده نوین
PDNSOFT.COM | INFO@PDNSOFT.COM

ثبت نام کرده و در *vlan* مربوطه قرار بگیرد. فرایند تغییر *vlan* کاربر به صورت خودکار توسط *NAC* انجام می‌شود و نیازی نیست که مدیر شبکه به صورت دستی تنظیمی برای سوئیچ و پورت کاربر انجام دهد. همچنین تمامی فعالیت‌های کاربران در سیستم ثبت شده و قابل پیگیری است. برای مثال تعداد مک آدرس‌هایی که یک کاربر با آن به شبکه وارد شده، سابقه *vlan* ها، زمان اولین ورود در سرور ثبت و ذخیره میشود.

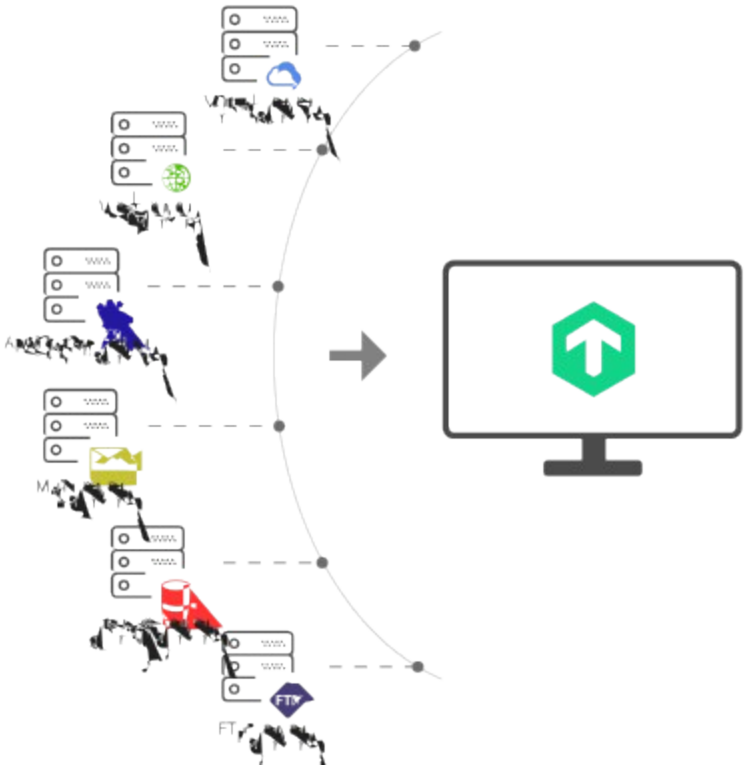
تغییر *vlan* یک کاربرد به راحتی و در محیط گرافیکی نرم‌افزار امکان‌پذیر است و میتوان با نوشتن قوانین مخصوص برای هر گروه (گروه مدیران شبکه، گروه کارکنان،...) و یا قوانین مختص به هر سوئیچ (سوئیچ سالن شماره یک با *vlan* شماره ۱ و ...) و یا هر ترکیب استاندارد دیگر فرایند اختصاص *vlan* ها را به صورت خودکار برنامه‌ریزی کرد. همچنین سامانه *NAC* به خوبی از تلفن‌های *VoIP* پشتیبانی کرده و با آن یکپارچه می‌شود و میتواند به صورت خودکار *vlan* آن را تخصیص دهد. در صورتی که شخص غیر مجازی با مک آدرس تأیید نشده و یا بدون داشتن یوزر و پسورد تلاش کند دستگاهی را وارد شبکه کند، سامانه با آن مقابله کرده و گزارش آن را به مدیر شبکه خواهد داد.

به طور کلی سامانه *NAC* میتواند امنیت شبکه‌های سازمانی را به طرز چشمگیری افزایش داده و مدیریت آن را برای کارشناسان و مدیران شبکه ساده‌تر نماید.

آدرس
تهران، خیابان آزادی، خیابان حبیب زادگان، پلاک ۳۶، طبقه ۲
یزد، خیابان مطهری، مرکز فناوری اقبال، واحد ۲۲۵
کدپستی
۱۴۵۸۸۸۷۱۵۴
۸۹۱۷۶۹۷۹۹۸
تلفن
۰۲۱۶۶۱۹۸۶۸۰
۰۳۵۳۷۲۶۵۳۴۳
فکس
۰۲۱۶۶۱۹۸۶۷۸
۰۳۵۳۷۲۴۵۰۸۷
پویش داده نوین
PDNSOFT.COM | INFO@PDNSOFT.COM

۳.۴ قابلیت‌های سامانه مانیتورینگ:

سامانه مانیتورینگ متن باز شرکت پویش داده نوین یک راهکار جامع برای پایش وضعیت سرورها، نرم‌افزارها و شبکه‌ها است.این سامانه مجهز به بیش از ۱۷۰۰ پلاگین هوشمند برای مانیتورینگ انواع سخت‌افزار و نرم‌افزار میباشد. همچنین این سامانه با ارائه گزارش‌های لحظه‌ای و همچنین ترسیم نمودارهای بصری از سوابق سرویسها، مدیران فناوری اطلاعات را قادر می‌سازد تا در کسری از ثانیه کوچکترین اختلال موجود در تمامی سرویسهای تحت مدیریت خود آگاه شده و نسبت به رفع آن اقدام کنند. اطلاع رسانی اختلالات بحرانی در سامانه مانیتورینگ به روش‌های مختلفی از جمله ارسال پیامک، ارسال ایمیل و به صدا درآوردن آژیر خطر انجام میپذیرد.



آدرس
تهران، خیابان آزادی، خیابان حبیب زادگان، پلاک ۳۶، طبقه ۲
یزد، خیابان مطهری، مرکز فناوری اقبال، واحد ۲۲۵
کدپستی
۱۴۵۸۷۷۷۱۵۴
۸۹۱۷۶۹۷۹۹۸
تلفن
۰۲۱۶۶۱۹۸۶۸۰
۰۳۵۳۷۲۶۵۳۴۳
فکس
۰۲۱۶۶۱۹۸۶۷۸
۰۳۵۳۷۲۴۵۰۸۷
پویش داده نوین
PDNSOFT.COM | INFO@PDNSOFT.COM

یکی از اهداف استفاده از سامانه مانیتورینگ، مشخص کردن میزان نیاز سرویسها و نرم‌افزارها به منابع سخت‌افزاری است. برای مثال، در صورتی که یک سرور دارای دیتابیس، دارای مشکل کند شدن در ساعات اداری باشد، سامانه مانیتورینگ میتواند وضعیت استفاده از منابع سرور را گزارش کرده تا مشخص شود سرور مورد نظر به چه سخت‌افزار بالاتری نیاز دارد. با استفاده از نمودارهای *RAM usage*، *CPU usage* و *Disk IO* میتوان مقدار مورد نیاز این سرور به منابع سخت‌افزاری را به دقت مشخص نمود تا از هدررفت منابع و یا کاهش بازدهی سرویس جلوگیری شود.

با رصد مستمر نمودارها و تحلیل داده‌های ارائه شده توسط سرور مانیتورینگ، مدیر شبکه قادر است اطلاعات بسیار مفیدی را درباره وضعیت سرورها و شبکه بدست آورد. برای مثال در صورتی که مدیر شبکه متوجه شود که پس از اتمام ساعت اداری تا صبح روز بعد سروری به طور مستمر داری ۱۰۰% *CPU Usage* و میزان آپلود غیر معقول است میتواند حدس بزند که سرورش به ماینر ارز دیجیتالی گرفتار شده و در حال استخراج ارز است و باید موضوع را بررسی کند. همچنین افزایش ناگهانی میزان *CPU* و *disk usage* میتواند زنگ خطری برای شروع رمزنگاری یک باج افزار قلمداد شود. اطلاعات جامع ارائه شده توسط سرور مانیتورینگ در کنار هوشمندی مدیر *IT* میتواند از بروز چنین بحران‌هایی جلوگیری کند.

در ادامه با قابلیتهای این سامانه آشنا خواهیم شد.

۱.۳.۴ رابط تحت وب زیبا برای مدیریت سامانه

وجود رابط کاربری زیبا و مفهوم، لازمه‌ای اصلی یک سرویس مانیتورینگ است. این سامانه مانیتورینگ با بهره گیری از رابط کاربری تحت وب زیبا، میتواند کلیه اطلاعات دریافتی از وضعیت هاست ها و سرویسها را به مدیر سیستم اطلاع دهد. این ربط کاربری شامل اطلاعات وضعیت هاست‌ها، سرویسها وشبکه‌ها، دما، سرعت فن، وضعیت هارد دیسک و رم *cpu usage*، درصد اشغال شدن پهنای باند شبکه،

آدرس
تهران، خیابان آزادی، خیابان حبیب زادگان، پلاک ۳۶، طبقه ۲
یزد، خیابان مطهری، مرکز فناوری اقبال، واحد ۲۲۵
کدپستی
۱۴۵۸۸۷۱۵۴
۸۹۱۷۶۹۷۹۹۸
تلفن
۰۲۱۶۶۱۹۸۶۸۰
۰۳۵۳۷۲۶۵۳۴۳
فکس
۰۲۱۶۶۱۹۸۶۷۸
۰۳۵۳۷۲۴۵۰۸۷
پویش داده نوین
PDNSOFT.COM | INFO@PDNSOFT.COM

نمودار وضعیت پایداری سرویس در طول زمان و نقشه گرافیکی است.

در تصویر زیر برخی از اعلانات سوئیچ، سرور و دیتابیس را ملاحظه میکنید. این اعلانات به دسته‌های *Critical* و *Warning* تقسیم می‌شوند و قابل تنظیم هستند.

تصویر ۵: نمای داشبود سامانه مانیتورینگ

در تصویر بعدی، رخدادهای چهار ساعت گذشته به نمایش گذاشته شده است:

آدرس
تهران، خیابان آزادی، خیابان حبیب زادگان، پلاک ۳۶، طبقه ۲
یزد، خیابان مطهری، مرکز فناوری اقبال، واحد ۲۲۵
کدپستی
۱۴۵۸۷۷۷۱۰۴
۸۹۱۷۶۹۷۹۹۸
تلفن
۰۲۱۷۷۱۹۸۶۸۰
۰۳۵۳۷۲۶۰۳۴۳
فکس
۰۲۱۷۷۱۹۸۶۷۸
۰۳۵۳۷۲۴۵۰۸۷
پویش داده نوین
PDNSOFT.COM | INFO@PDNSOFT.COM

EVENTS OF RECENT 4 HOURS

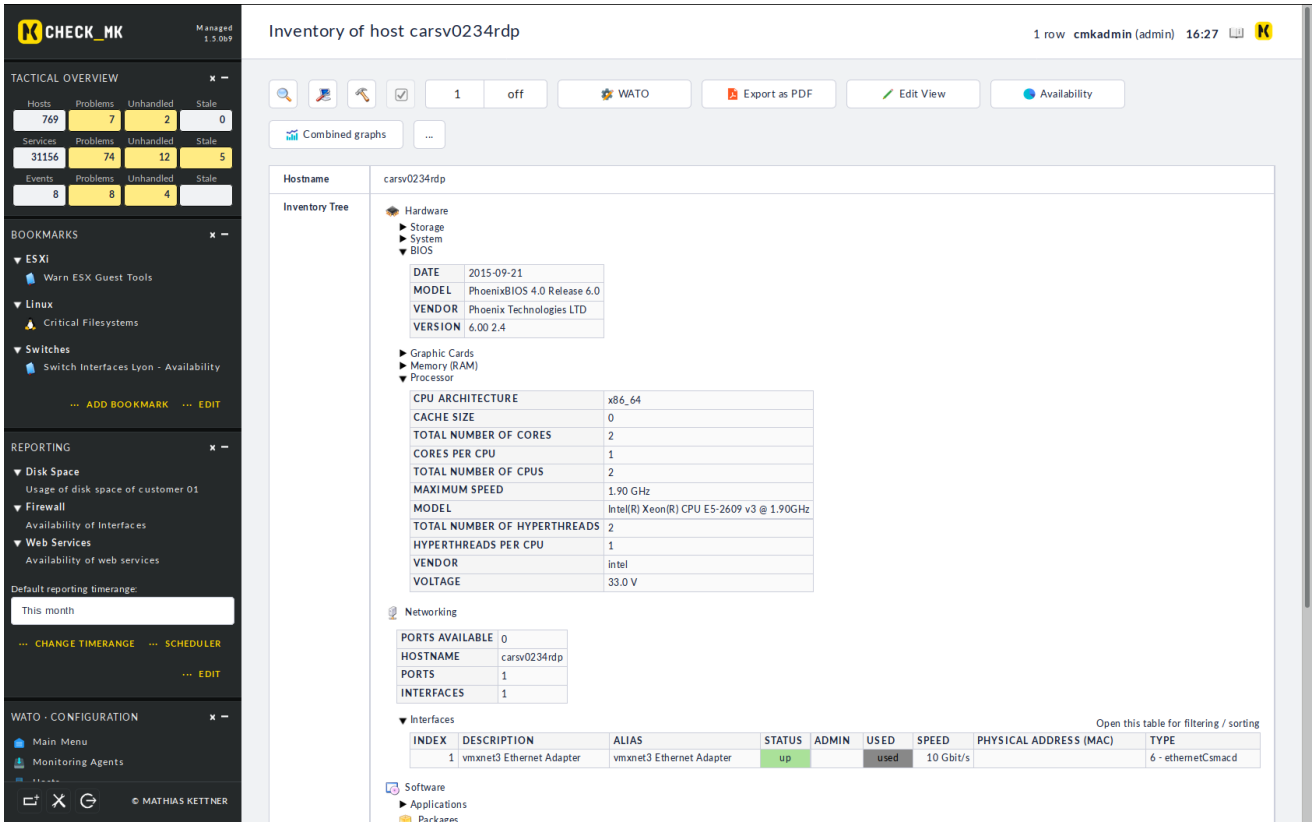
	41 m	Sara-New	MSSQL Connections MSSQLSERVER DBSara8_M1	WARN - Connections: 20 (warn/crit at 20/50)
	41 m	Sara-New	MSSQL Connections MSSQLSERVER DBSara8_M1	WARN - Connections: 20 (warn/crit at 20/50)
	41 m	SAN2-MSA2040	Temperature Power Supply Enclosure 1 Right	OK - 39.0 °C
	41 m	SAN2-MSA2040	Temperature Power Supply Enclosure 1 Left	OK - 39.0 °C
	41 m	server	Check_MK	OK - [agent] Version: 1.2.8p16, OS: windows, execution time 10.8 sec
	42 m	server	Check_MK	(Service Check Timed Out)
	44 m	SAN2-MSA2040	Temperature Power Supply Enclosure 1 Right	WARN - 40.0 °C (warn/crit at 40/45 °C)

تصویر ۶: رخدادهای چهار ساعت گذشته

آدرس
تهران، خیابان آزادی، خیابان حبیب زادگان، پلاک ۳۶، طبقه ۲
یزد، خیابان مطهری، مرکز فناوری اقبال، واحد ۲۲۵
کدپستی
۱۴۵۸۷۷۷۱۰۴
۸۹۱۷۶۹۷۹۹۸
تلفن
۰۲۱۶۶۱۹۸۶۸۰
۰۳۵۳۷۲۶۵۳۴۳
فکس
۰۲۱۶۶۱۹۸۶۷۸
۰۳۵۳۷۲۴۵۰۸۷
پویش داده نوین
PDNSOFT.COM | INFO@PDNSOFT.COM

۲.۳.۴ مانیتورینگ دارایی‌های سخت افزاری و نرم افزاری(Inventory)

سامانه مانیتورینگ قادر است تا با استفاده از agent خود inventory تجهیزات، شامل مقدار و مدل cpu، مقدار RAM، هارددیسک، مشخصات سیستم عامل و نرم افزارهای نصب شده را نیز به نمایش گذاشته و گزارش دهد:

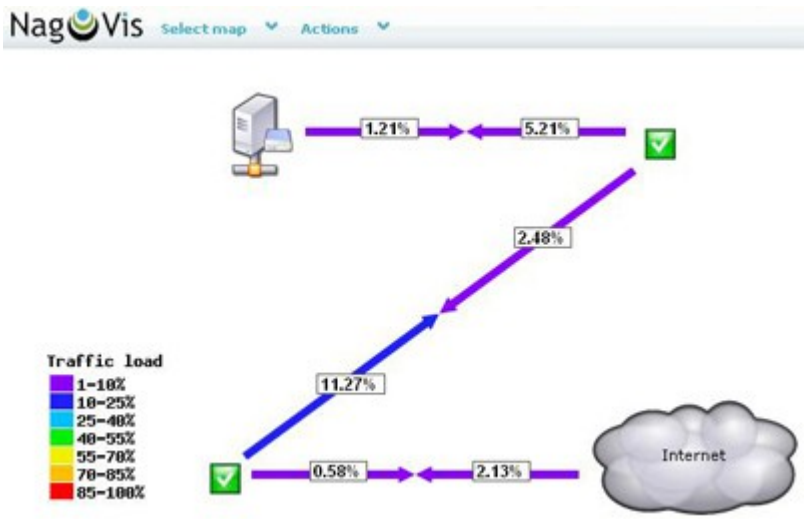


تصویر ۷: مانیتورینگ سخت افزاری و نرم افزاری

آدرس
تهران، خیابان آزادی، خیابان حبیب زادگان، پلاک ۳۶، طبقه ۲
یزد، خیابان مطهری، مرکز فناوری اقبال، واحد ۲۲۵
کدپستی
۱۴۵۸۸۷۱۵۴
۸۹۱۷۶۹۷۹۹۸
تلفن
۰۲۱۷۷۱۹۸۶۸۰
۰۳۵۳۷۲۶۰۳۴۳
فکس
۰۲۱۷۷۱۹۸۶۷۸
۰۳۵۳۷۲۴۰۸۷
پویش داده نوین
PDNSOFT.COM | INFO@PDNSOFT.COM

۳.۳.۴ ترسیم نقشه:

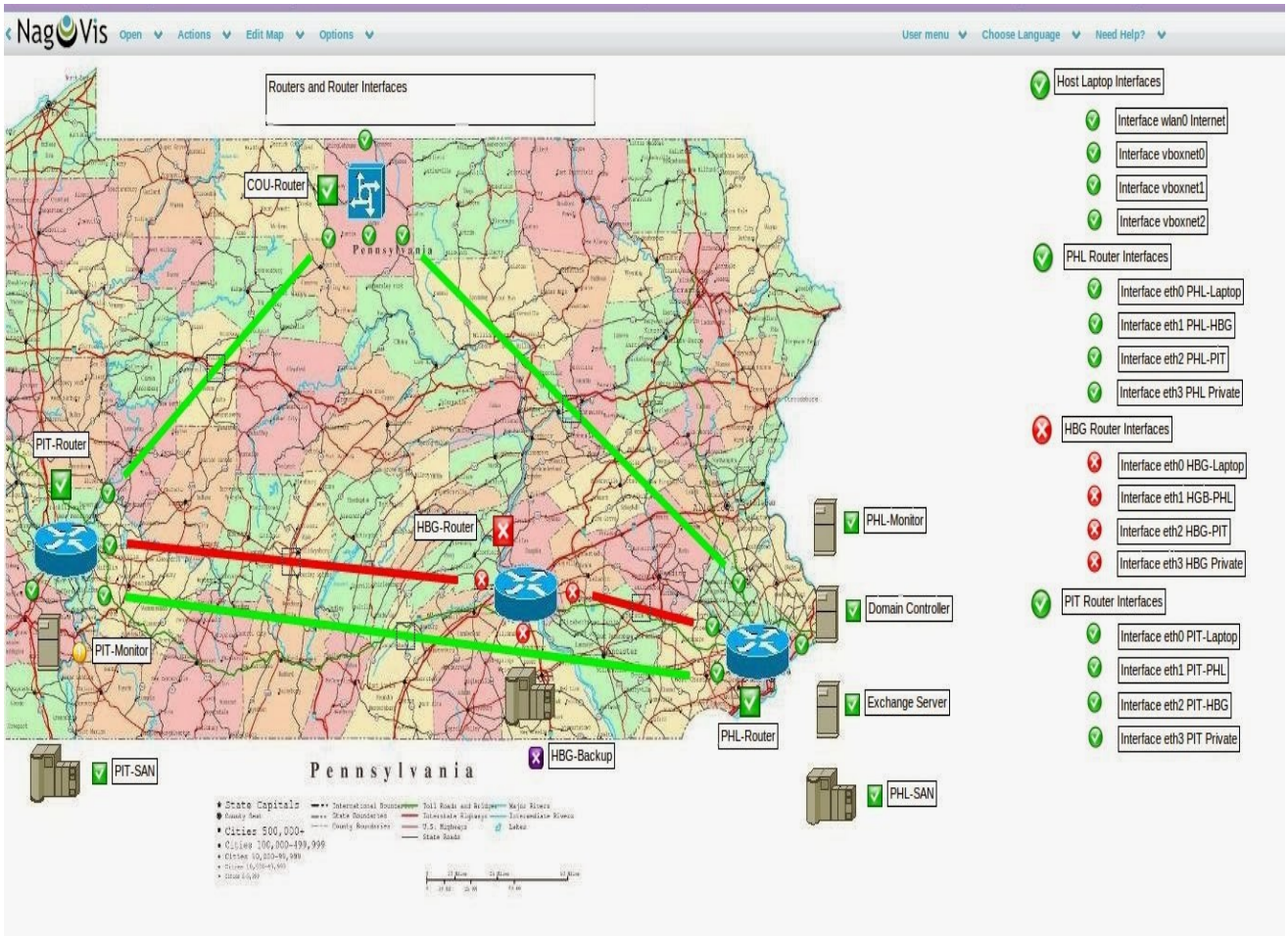
یکی ازقابلیت های مهم سامانه مانیتورینگ، امکان ترسیم نقشه و گراف اتصالات و تجهیزات شبکه و سرورها با استفاده از ماژول nagvis و نمایش اطلاعات سرویسها بر روی آن است. این نقشه‌های گرافیکی به فهم ساده‌تر مفاهیم و رخدادها کمک شایانی میکند. به تصاویر زیر که نمونه‌ای نقشه های رسم شده در ماژول nagvis نرم‌افزار مانیتورینگ است توجه کنید.



تصویر ۸: نمایش نقشه گرافیکی

انواع نمایش‌های گرافیکی:

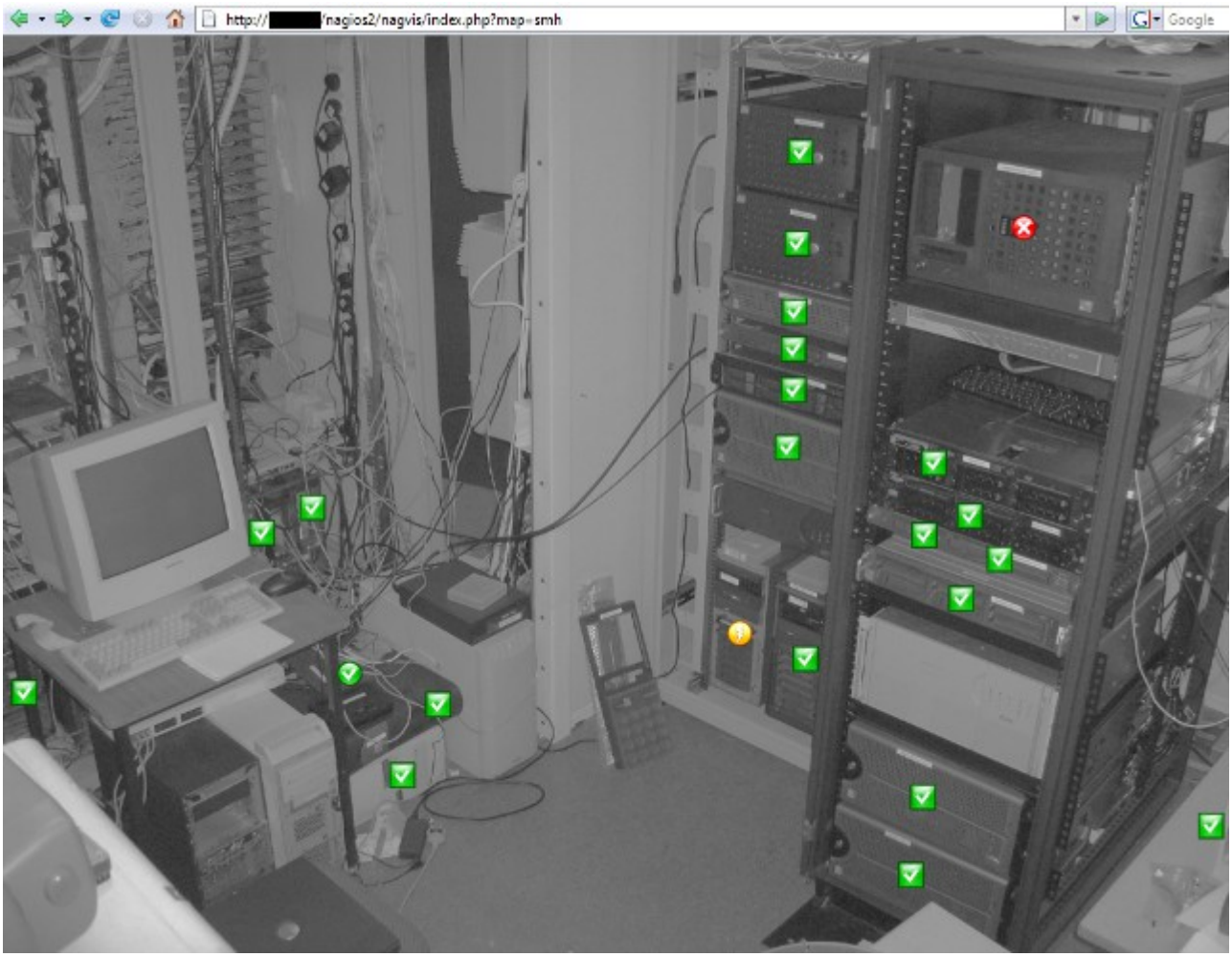
آدرس
تهران، خیابان آزادی، خیابان حبیب زادگان، پلاک ۳۶، طبقه ۲
یزد، خیابان مطهری، مرکز فناوری اقبال، واحد ۲۲۵
کدپستی
۱۴۵۸۸۸۷۱۵۴
۸۹۱۷۶۹۷۹۹۸
تلفن
۰۲۱۶۶۱۹۸۶۸۰
۰۳۵۳۷۲۶۵۳۴۳
فکس
۰۲۱۶۶۱۹۸۶۷۸
۰۳۵۳۷۲۴۵۰۸۷
پویش داده نوین
PDNSOFT.COM | INFO@PDNSOFT.COM



تصویر ۹: ترسیم نقشه برای تجهیزات شبکه

آدرس
تهران، خیابان آزادی، خیابان حبیب زادگان، پلاک ۳۶، طبقه ۲
یزد، خیابان مطهری، مرکز فناوری اقبال، واحد ۲۲۵
کدپستی
۱۴۵۸۷۷۷۱۰۴
۸۹۱۷۶۹۷۹۹۸
تلفن
۰۲۱۶۶۱۹۸۶۸۰
۰۳۵۳۷۲۶۵۳۴۳
فکس
۰۲۱۶۶۱۹۸۶۷۸
۰۳۵۳۷۲۴۵۰۸۷
پویش داده نوین
PDNSOFT.COM | INFO@PDNSOFT.COM

انتخاب تصاویر دلخواه به عنوان پس زمینه نقشه و قرار دادن اعلان ها روی تصویر:



تصویر ۱۰: امکان انتخاب تصاویر دلخواه برای نقشه های *nagvis*

آدرس
تهران، خیابان آزادی، خیابان حبیب زادگان، پلاک ۳۶، طبقه ۲
یزد، خیابان مطهری، مرکز فناوری اقبال، واحد ۲۲۵
کدپستی
۱۴۵۸۷۷۷۱۵۴
۸۹۱۷۶۹۷۹۹۸
تلفن
۰۲۱۶۶۱۹۸۶۸۰
۰۳۵۳۷۲۶۵۳۴۳
فکس
۰۲۱۶۶۱۹۸۶۷۸
۰۳۵۳۷۲۴۵۰۸۷
پویش داده نوین
PDNSOFT.COM | INFO@PDNSOFT.COM

۴.۳.۴ مانیتورینگ اپلیکشن ها:

تشخیص صحیح خطا در اجزا یک اپلیکیش یکی از مهم‌ترین بخش‌های پشتیبانی برنامه‌ها و سرویس‌های شبکه ای میباشد. این سامانه این قابلیت را دارد که با ارائه داده‌های صحیح از جزئیات برنامه مانند تعداد کانکش های باز – حجم دیتابیس ها و ... به مدیر سیستم برای حل مشکلات سرویس کمک کند.

آدرس
تهران، خیابان آزادی، خیابان حبیب زادگان، پلاک ۳۶، طبقه ۲
یزد، خیابان مطهری، مرکز فناوری اقبال، واحد ۲۲۵
کدپستی
۱۴۵۸۷۷۷۱۵۴
۸۹۱۷۶۹۷۹۹۸
تلفن
۰۲۱۶۶۱۹۸۶۸۰
۰۳۵۳۷۲۶۵۳۴۳
فکس
۰۲۱۶۶۱۹۸۶۷۸
۰۳۵۳۷۲۴۵۰۸۷
پویش داده نوین
PDNSOFT.COM | INFO@PDNSOFT.COM

از مهم‌ترین قابلیت‌های سامانه مانیتورینگ در این قسمت به شرح زیر میباشد:

۱. پشتیبانی از انواع وب اپلیکیش ها مانند *Apache, nginx, HAProxy*

۲. مانیتورینگ *Middleware* ها مانند *JBoss, Oracle WebLogic, Apache Tomcat, IBM WebSphere*

۵.۳.۴ مانیتورینگ شبکه

این بخش از سامانه به مانیتورینگ تجهیزات شبکه میپردازد. مدیر شبکه میتوان با انواع داده‌های دریافتی توسط سامانه به رفع عیب شبکه خود اقدام کند.

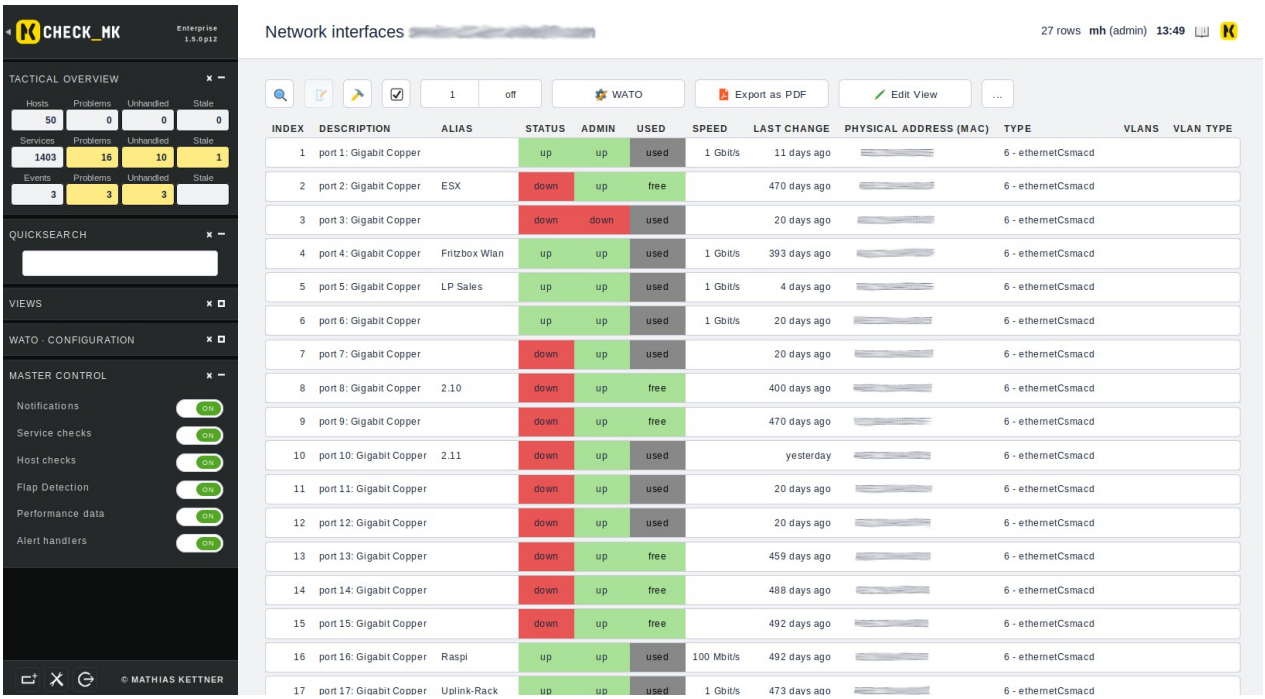
برخی قابلیتهای

۳. مانیتورینگ روترها و سوئیچ ها شامل : وضعیت /سرعت /خطا/ پهنای باند هر پورت . نمایش وضعیت *CPU* و دما و ...

۴. پشتیبانی از برندهای معروف شبکه شامل : *Cisco, Brocade, Dell, Enterasys, Extreme Networks, Huawei, Intel, Juniper, TP-Link*

۵. پشتیبانی از تجهیزات وایرلس شامل نمایش وضعیت *access points* و اندازه سیگنال و ..

آدرس
تهران، خیابان آزادی، خیابان حبیب زادگان، پلاک ۳۶، طبقه ۲
یزد، خیابان مطهری، مرکز فناوری اقبال، واحد ۲۲۵
کدپستی
۱۴۵۸۷۷۷۱۵۴
۸۹۱۷۶۹۷۹۹۸
تلفن
۰۲۱۶۶۱۹۸۶۸۰
۰۳۵۳۷۲۶۵۳۴۳
فکس
۰۲۱۶۶۱۹۸۶۷۸
۰۳۵۳۷۲۴۵۰۸۷
پویش داده نوین
PDNSOFT.COM | INFO@PDNSOFT.COM

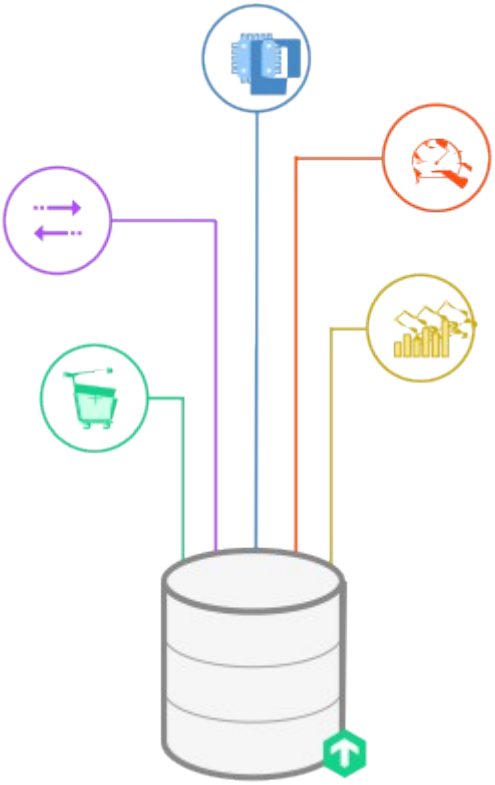


تصویر ۱۱: نمایش وضعیت پورتهای سوئیچ

۶.۳.۴ مانیتورینگ دیتابیس

این سامانه مجموعه‌ای کامل از انواع دیتابیس سرورها را پشتیبانی میکند. مدیر دیتابیس میتواند بـا داده‌هـایی که این سامانه در اختیار او قرار میدهد کنترل کاملی روی سرویس دهی دیتابیس ها و نیز سامانه های وابسته بـه دیتابیس داشته باشد.

آدرس
تهران، خیابان آزادی، خیابان حبیب زادگان، پلاک ۳۶، طبقه ۲
یزد، خیابان مطهری، مرکز فناوری اقبال، واحد ۲۲۵
کدپستی
۱۴۵۸۷۷۱۵۴
۸۹۱۷۶۹۷۹۹۸
تلفن
۰۲۱۶۶۱۹۸۶۸۰
۰۳۵۳۷۲۶۵۳۴۳
فکس
۰۲۱۶۶۱۹۸۶۷۸
۰۳۵۳۷۲۴۵۰۸۷
پویش داده نوین
PDNSOFT.COM | INFO@PDNSOFT.COM



برخی از قابلیت‌های این سامانه در حوزه مانیتورینگ دیتابیس ها به شرح زیر میباشد:

۱. پشتیبانی از انواع دیتابیس ها روی سیستم عامل های مختلف شامل : *Linux, Solaris, AIX, HP-UX, Windows*

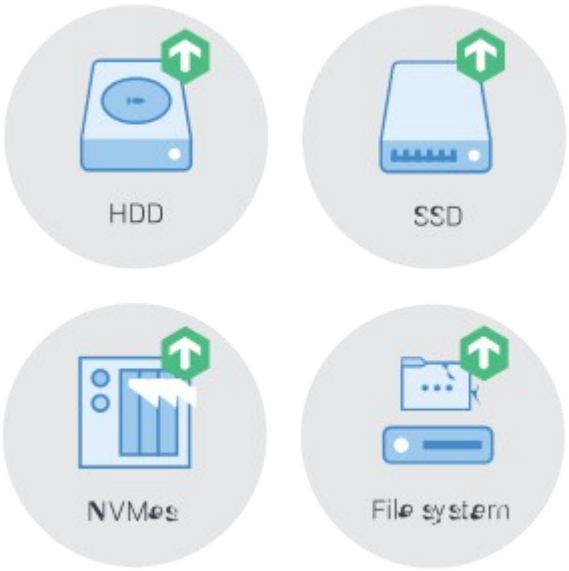
۲. پشتیبانی از دیتابیس سرورها مختلف شامل : *Oracle. MSSQL- MySQL/MariaDB- PostgreSQL* و ...

۳. نمایش جزئیات مربوط به دیتابیس سرور *Mssql* شامل : *Locks per batch and locks per second- Cache hit ratio-Transactions per second* – حـجم دیتابیس- وـلاگ هـا

آدرس
تهران، خیابان آزادی، خیابان حبیب زادگان، پلاک ۳۶، طبقه ۲
یزد، خیابان مطهری، مرکز فناوری اقبال، واحد ۲۲۵
کدپستی
۱۴۵۸۷۷۷۱۵۴
۸۹۱۷۶۹۷۹۹۸
تلفن
۰۲۱۶۶۱۹۸۶۸۰
۰۳۵۳۷۲۶۵۳۴۳
فکس
۰۲۱۶۶۱۹۸۶۷۸
۰۳۵۳۷۲۴۵۰۸۷
پویش داده نوین
PDNSOFT.COM | INFO@PDNSOFT.COM

۷.۳.۴ مانیتورینگ *storage* ها :

یکی از اصلی‌ترین بخش‌های دیتاسنتر ها محل ذخیره سازی داده‌ها میباشد. معمولاً برای ذخیره سازی داده‌ها از انواع *SAN* یا *NAS* استفاده میشود.



برخی از قابلیت‌های سامانه برای مانیتورینگ *Storage* ها به شرح زیر میباشد:

۱. پشتیبانی از انواع برند های معروف تجهیزات ذخیره سازی اطلاعات شامل : *QNAP- NetApp – HP* و ...

۲. پشتیبانی از انواع فایل سیستم‌های تحت شبکه شامل *NFS- Ceph – GFS* و ...

۳. نمایش وضعیت هاردها

آدرس
تهران، خیابان آزادی، خیابان حبیب زادگان، پلاک ۳۶، طبقه ۲
یزد، خیابان مطهری، مرکز فناوری اقبال، واحد ۲۲۵
کدپستی
۱۴۵۸۷۷۷۱۵۴
۸۹۱۷۶۹۷۹۹۸
تلفن
۰۲۱۶۶۱۹۸۶۸۰
۰۳۵۳۷۲۶۵۳۴۳
فکس
۰۲۱۶۶۱۹۸۶۷۸
۰۳۵۳۷۲۴۵۰۸۷
پویش داده نوین
PDNSOFT.COM | INFO@PDNSOFT.COM

۸.۳.۴ دیگر قابلیتهای سامانه مانیتورینگ :

۱. مانیتور و ذخیره لاگ ها از طریق *syslog* یا *SNMP traps*
۲. قابلیت ارسال *event* ها برای تولید *notifications*
۳. قابلیت شخصی سازی گسترده برای آستانه هشدارها و رخدادها
۴. قابلیت رسم گراف های *interactive* بر اساس تکنولوژی *HTML۵*
۵. قابلیت مقایسه چند گراف در کنار هم
۱. ذخیره گراف ها روی دیسک با حداقل فضای ذخیره سازی
۲. قابلیت سفارشی سازی داشبورد برای مشاهده موارد مورد نیاز
۳. قابلیت سفارسی سازی داشبورد براساس کاربران مختلف
۴. قابلیت ایجاد بوک مارک جهت دسترسی سریع به قسمت‌های مختلف سامانه با یک کلیک!
۵. قابلیت ایجاد کاربران با سطوح دسترسی مختلف
۶. جمع آوری لاگ از هاست‌های مانیتور شده و عمل‌کردی مشابه با لاگ سرور.
۷. ساده بودن رابط کاربری و توسعه نرم‌افزار در شبکه
۸. دارای *Agent* های مخصوص برای سیستم عامل ویندوز – لینوکس– و دیگر سیستم عامل ها
۹. سرعت مناسب در توسعه قابلیتهای محصول
۱۰. قابلیت مانیتورینگ بدون *Agent* از طریق پروتکل *SNMP* یا اتصال مستقیم به پورت‌های سرویس ها شامل *FTP, LDAP, IMAP* و ...
۱۱. قابلیت اجرای *API-Based* چک ها با استفاده از *HTTP/XML, SSH or TELNET*

آدرس
تهران، خیابان آزادی، خیابان حبیب زادگان، پلاک ۳۶، طبقه ۲
یزد، خیابان مطهری، مرکز فناوری اقبال، واحد ۲۲۵
کدپستی
۱۴۵۸۸۸۷۱۵۴
۸۹۱۷۶۹۷۹۹۸
تلفن
۰۲۱۶۶۱۹۸۶۸۰
۰۳۵۳۷۲۶۵۳۴۳
فکس
۰۲۱۶۶۱۹۸۶۷۸
۰۳۵۳۷۲۴۵۰۸۷
پویش داده نوین
PDNSOFT.COM | INFO@PDNSOFT.COM

۴.۴ سامانه لاگ سرور

بهترین راه برای مشاهده و ریشه‌یابی انواع خطاها، رویدادها و خرابی‌ها در یک سیستم، بررسی لاگ‌ها (گزارشهای) آن است. هر سیستم رایانه‌ای یک ساختار ویژه و جداگانه‌ای برای تولید و ذخیره‌سازی لاگ‌های خود داشته و به طور معمول لاگ‌ها را در حافظه‌ی داخلی خود ذخیره کرده و برای مدت محدودی نگهداری می‌کند.

زمانی که تعداد سیستم‌های رایانه‌ای، دستگاه‌ها و تجهیزات در یک مجموعه بیشتر می‌شود، مدیریت و بررسی لاگ‌ها در مجموعه زمان‌بر و گاهی دشوار می‌گردد. برای بررسی لاگ‌ها باید به سیستم‌های متعدد لاگین کرده و با تنوع ساختارها، سیستم‌عامل‌ها و روش‌های ذخیره سازی و پالایش لاگ رو به رو خواهیم شد. از این رو، وجود یک سامانه جامع و یکپارچه برای جمع‌آوری، ذخیره‌سازی و جستجوی پیشرفته در میان لاگ‌های تولید شده توسط دستگاه‌های مختلف امری ضروری به نظر می‌رسد.

نرم‌افزار *graylog* یک سامانه مرکزی برای جمع‌آوری، ذخیره سازی و مدیریت لاگ در سازمان‌ها است. رابط کاربری تحت وب آن می‌تواند به سادگی و بر اساس نیاز شما، در میان میلیون‌ها لاگ از میان دستگاه‌های متخلف جستجو کرده و در داشبوردی زیبا به صورت نمودار و چارت، اطلاعات مورد نظر شما را نمایش دهد.

۱.۴.۴ ویژگی‌های سامانه لاگ سرور:

جمع‌آوری لاگ:

نرم‌افزار *graylog* می‌تواند هر نوع لاگ با هر ساختار استانداردی را دریافت و ذخیره سازی کند. پس از جمع‌آوری، تمامی این لاگ‌ها در *indice* های *graylog* با فرمتی خاص ذخیره شده و قابل جستجو می‌گردد. این سامانه، میتواند از طریق پروتکل‌های استاندارد زیر لاگ‌ها را دریافت کند:

آدرس
تهران، خیابان آزادی، خیابان حبیب زادگان، پلاک ۳۶، طبقه ۲
یزد، خیابان مطهری، مرکز فناوری اقبال، واحد ۲۲۵
کدپستی
۱۴۵۸۸۷۱۵۴
۸۹۱۷۶۹۷۹۹۸
تلفن
۰۲۱۶۶۱۹۸۶۸۰
۰۳۵۳۷۲۶۵۳۴۳
فکس
۰۲۱۶۶۱۹۸۶۷۸
۰۳۵۳۷۲۴۵۰۸۷
پویش داده نوین
PDNSOFT.COM | INFO@PDNSOFT.COM

- Syslog (TCP, UDP, AMQP, Kafka)
- GELF(TCP, UDP, AMQP, Kafka, HTTP)
- AWS - AWS Logs, FlowLogs, CloudTrail
- Beats/Logstash
- CEF (TCP, UDP, AMQP, Kafka)
- JSON Path from HTTP API
- Netflow (UDP)
- Plain/Raw Text (TCP, UDP, AMQP, Kafka)

برای نمونه، روتر و سوییچ‌های میکروتیک و سیسکو، فایروال *pfsense* و کلیه سرورهای لینوکسی از طریق پروتکل *syslog UDP* و سرورهای ویندوزی از طریق *GELF UDP* لاگ‌های خود را برای لاگ‌سرور ارسال می‌کنند.

دسته‌بندی لاگ‌ها:

لاگ‌های خامی که از طریق دستگاههای مختلف برای لاگ سرور ارسال می‌شوند برای آنکه برای انسان مفهوم باشد باید دسته‌بندی و مرتب شده و گاهی لازم است تا اطلاعات فیلدهای مختلف را از درون لاگ‌ها استخراج کرد. لاگ سرور با استفاده از *extractor*های مختلفی که به صورت پیشفرض روی پروتکل‌های *syslog* و *GELF* اعمال می‌کند، میتواند اطلاعات مهم درون یک لاگ‌مسیج را استخراج کرده و در فیلدهای مناسب نمایش دهد. برای نمونه به تصویر زیر که اطلاعات استخراج شده ازیک لاگ دریافت شده از یک سرور ویندوزی است دقت کنید:

آدرس
تهران، خیابان آزادی، خیابان حبیب زادگان، پلاک ۳۶، طبقه ۲
یزد، خیابان مطهری، مرکز فناوری اقبال، واحد ۲۲۵
کدپستی
۱۴۵۸۷۷۷۱۵۴
۸۹۱۷۶۹۷۹۹۸
تلفن
۰۲۱۶۶۱۹۸۶۸۰
۰۳۵۳۷۲۶۵۳۴۳
فکس
۰۲۱۶۶۱۹۸۶۷۸
۰۳۵۳۷۲۴۵۰۸۷
پویش داده نوین
PDNSOFT.COM | INFO@PDNSOFT.COM

Channel
DNS Server

EventID
7062

EventReceivedTime
2019-07-14 14:09:43

EventType
WARNING

Keywords
36028797018963970

OpcodeValue
0

ProcessID
0

ProviderGuid
{71A551F5-C893-4849-886B-B5EC8502641E}

RecordNumber
167904258

Severity
WARNING

SeverityValue
3

SourceModuleName
eventlog

SourceModuleType
im_msvistalog

SourceName
Microsoft-Windows-DNS-Server-Service

Task
0

تصویر ۱۲: لاگ استخراج و دسته‌بندی شده از یک سرور ویندوزی

این اطلاعات به صورت خودکار توسط لاگ سرور از متن لاگ استخراج و دسته‌بندی شده است.

آدرس
تهران، خیابان آزادی، خیابان حبیب زادگان، پلاک ۳۶، طبقه ۲
یزد، خیابان مطهری، مرکز فناوری اقبال، واحد ۲۲۵
کدپستی
۱۴۵۸۸۷۱۵۴
۸۹۱۷۶۹۷۹۹۸
تلفن
۰۲۱۶۶۱۹۸۶۸۰
۰۳۵۳۷۲۶۵۳۴۳
فکس
۰۲۱۶۶۱۹۸۶۷۸
۰۳۵۳۷۲۴۵۰۸۷
پویش داده نوین
PDNSOFT.COM | INFO@PDNSOFT.COM

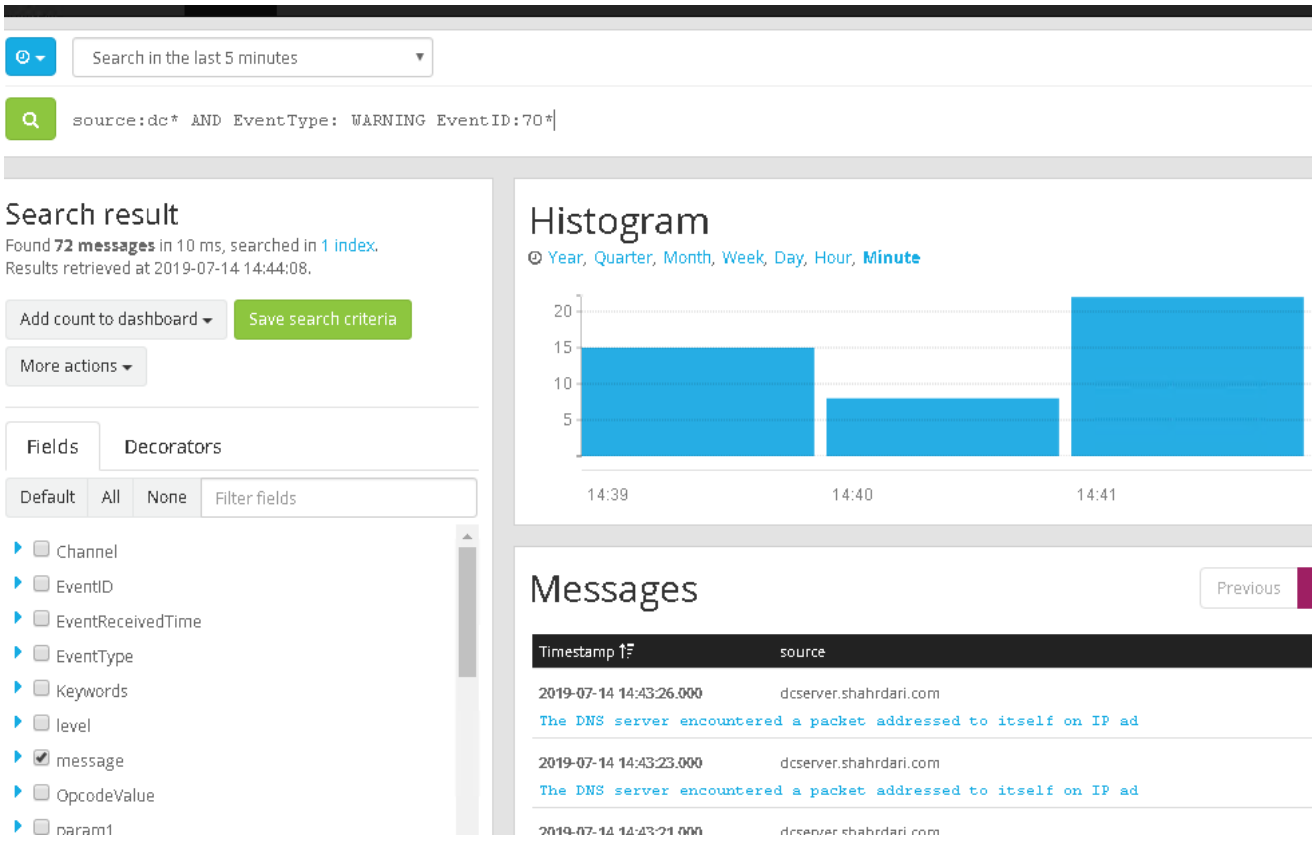
در صورتی که لاگ سرور نتواند فیلدهای پیام را تشخیص داده و دسته‌بندی کند، قابلیت ساخت *extractor* دلخواه برای استخراج فیلدهای مهم از متن یک پیام غیر استاندارد نیز در لاگ سرور وجود دارد. همچنین موتور جستجوی لاگ سرور قادر است تا در میان پیام‌هایی که فیلدهای آن مشخص نشده نیز جستجوی خود را انجام داده و اطلاعات مورد نیاز شما را نمایش دهد.

آنالیز لاگ:

لاگ سرور امکانات مناسبی را برای آنالیز لاگ در اختیار کارشناسان قرار می‌دهد.

۱. **موتور جستجوگر بسیار قوی:** این موتور جستجوی لاگ سرور کارشناسان را قادر میسازد تا اطلاعات مورد نظر خود را با سرعت و دقت بسیار بالا از میان میلیون‌ها لاگ موجود در سرور پیدا کنند. این موتور جستجو از *syntax* های استاندارد *elasticsearch* استفاده کرده و قابلیت انطباق پذیری بسیاری دارد. برای نمونه به تصویر زیر توجه کنید. در این تصویر کاربر درخواست کرده تا لاگ‌هایی که فیلد *source* آن با حروف *dc* شروع شده و فیلد *EventType* آن دارای مقدار *WARNING* بوده و فیلد *EventID* آن با مقدار ۷۰ شروع می‌شود و در ۵ دقیقه اخیر اتفاق افتاده است را نشان دهد:

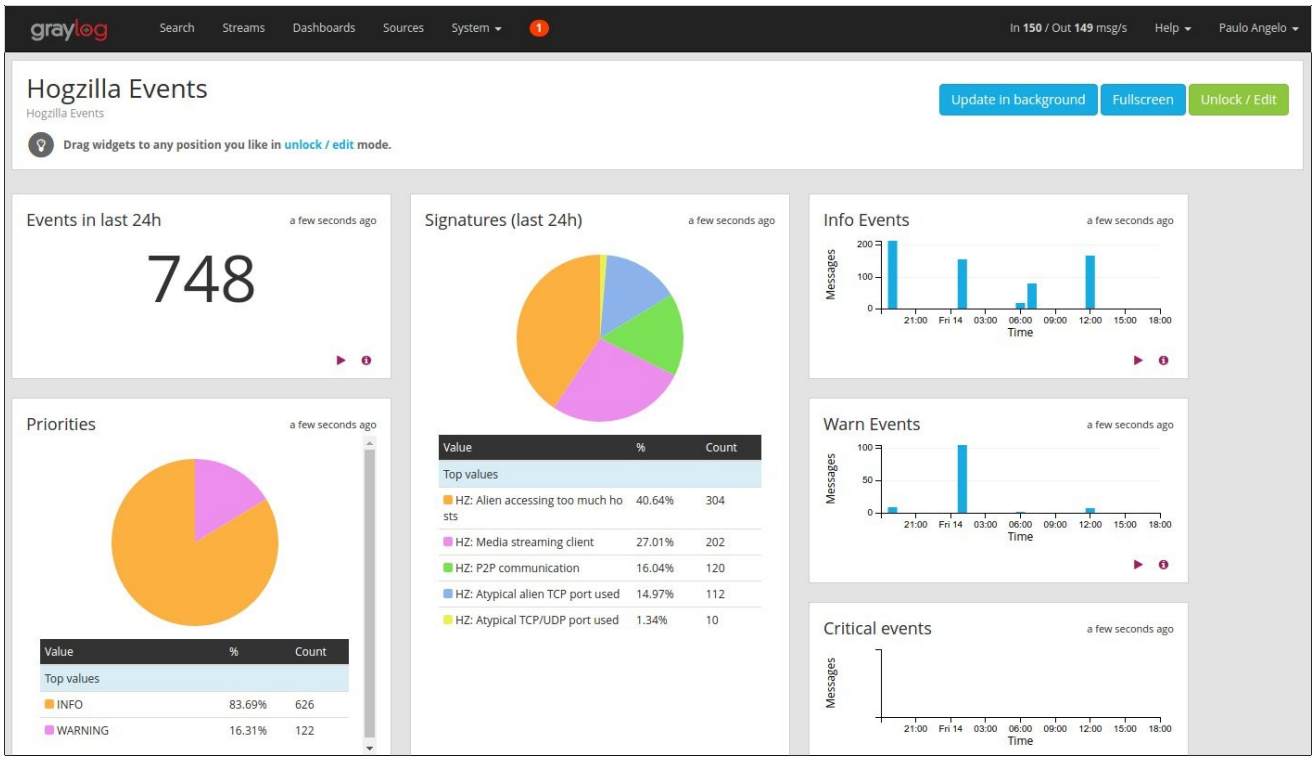
آدرس
تهران، خیابان آزادی، خیابان حبیب زادگان، پلاک ۳۶، طبقه ۲
یزد، خیابان مطهری، مرکز فناوری اقبال، واحد ۲۲۵
کدپستی
۱۴۵۸۸۸۷۱۵۴
۸۹۱۷۶۹۷۹۹۸
تلفن
۰۲۱۶۶۱۹۸۶۸۰
۰۳۵۳۷۲۶۵۳۴۳
فکس
۰۲۱۶۶۱۹۸۶۷۸
۰۳۵۳۷۲۴۵۰۸۷
پویش داده نوین
PDNSOFT.COM | INFO@PDNSOFT.COM



تصویر ۱۳: نمونه ای از سرچ لاگ توسط موتور جستجوی لاگ سرور

۲. **داشبورد سفارشی:** در لاگ سرور امکان ایجاد یک داشبورد سفارشی برای کاربران وجود دارد. برای مثال میتوان تعداد لاگ‌هایی در یک زمان مشخص دارای عبارت مورد نظر بوده را در یک داشبورد به نمایش گذاشت. کاربر میتواند بر حسب نیاز خود داشبورد مورد نیاز خود را ساخته و لاگ‌های مورد نظر خود را توسط آن را مدیریت کند.

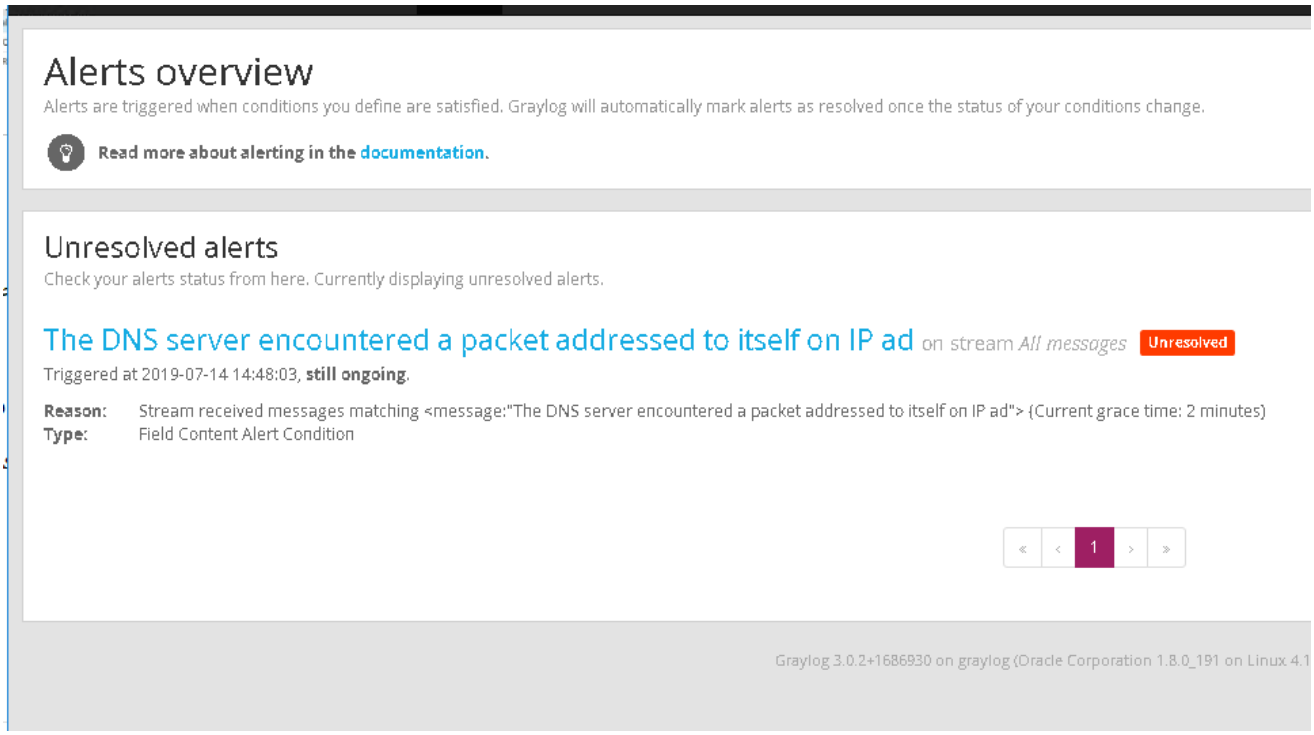
آدرس
تهران، خیابان آزادی، خیابان حبیب زادگان، پلاک ۳۶، طبقه ۲
یزد، خیابان مطهری، مرکز فناوری اقبال، واحد ۲۲۵
کدپستی
۱۴۵۸۸۸۷۱۵۴
۸۹۱۷۶۹۷۹۹۸
تلفن
۰۲۱۶۶۱۹۸۶۸۰
۰۳۵۳۷۲۶۵۳۴۳
فکس
۰۲۱۶۶۱۹۸۶۷۸
۰۳۵۳۷۲۴۵۰۸۷
پویش داده نوین
PDNSOFT.COM | INFO@PDNSOFT.COM



تصویر ۱۴: داشبورد سفارشی لاگ سرور

۳. **ایجاد یک هشدار *alert*** : لاگ سرور میتواند با ساخت یک هشدار، در صورت بروز یک خطا در سیستم، مدیر را مطلع کند. این هشدار از طریق ساختن قوانین و شرایط مورد نظر به سادگی قابل ایجاد است. برای مثال در تصویر زیر، لاگ سرور طوری برنامه‌ریزی شده تا در صورت وجود عبارت *The DNS server encountered a packet addressed to itself* در لاگ *DNS server* یک هشدار تولید کند.

آدرس
تهران، خیابان آزادی، خیابان حبیب زادگان، پلاک ۳۶، طبقه ۲
یزد، خیابان مطهری، مرکز فناوری اقبال، واحد ۲۲۵
کدپستی
۱۴۵۸۷۷۷۱۵۴
۸۹۱۷۶۹۷۹۹۸
تلفن
۰۲۱۶۶۱۹۸۶۸۰
۰۳۵۳۷۲۶۵۳۴۳
فکس
۰۲۱۶۶۱۹۸۶۷۸
۰۳۵۳۷۲۴۵۰۸۷
پویش داده نوین
PDNSOFT.COM | INFO@PDNSOFT.COM



تصویر ۱۵: تولید هشدار در صورت وجود یک عبارت خاص در متن لاگ

ابزارهای یادشده می‌تواند به خوبی کارشناسان مربوطه را در آنالیز بهینه لاگ و استخراج اطلاعات حیاتی موجـــود در آن‌ها یاری کند.

آدرس
تهران، خیابان آزادی، خیابان حبیب زادگان، پلاک ۳۶، طبقه ۲
یزد، خیابان مطهری، مرکز فناوری اقبال، واحد ۲۲۵
کدپستی
۱۴۵۸۸۷۱۵۴
۸۹۱۷۶۹۷۹۹۸
تلفن
۰۲۱۷۷۱۹۸۶۸۰
۰۳۵۳۷۲۶۵۳۴۳
فکس
۰۲۱۷۷۱۹۸۶۷۸
۰۳۵۳۷۲۴۵۰۸۷
پویش داده نوین
PDNSOFT.COM | INFO@PDNSOFT.COM

۲.۴.۴ وجود لاگ سرور چه کمکی به سازمانها می‌کند؟

یک سامانه لاگ سرور کارکردهای زیر را برای سازمان خواهد داشت:

۱. **شناسایی پیامدها:**

هر رخدادی در یک سیستم رایانه‌ای با تولید یک لاگ همراه است. با بررسی دقیق لاگ‌های تولید شده توسط دستگاههای مختلف، میتوان هر رخدادی از جمله لاگین به یک سرور، حمله بر روی فایروال، درخواست‌های *DNS* و حتی وارد کردن یک دستگاه *USB* به یک سرور را ثبت و بررسی کرد. بررسی رخدادهای مهم در سیستم، کمک شایانی به تأمین امنیت و پایداری سیستمها خواهد کرد.

۲. **پاسخ مناسب به پیامدها:**

پس از شناسایی یک رخداد یا یک هشدار که در لحظه توسط لاگ سرور تولید می‌شود، مدیر سیستم قادر خواهد بود تا به سرعت نسبت به آن رخداد، واکنش مناسب را انجام دهد. همچنین در صورتی که مدیر سیستم از آن رخداد در آن لحظه باخبر نشود، میتواند با جستجو در لاگ‌هایی که برای مدت طولانی‌تری در سرور ذخیره شده نسبت به رفع مشکل اقدام کند.

آدرس
تهران، خیابان آزادی، خیابان حبیب زادگان، پلاک ۳۶، طبقه ۲
یزد، خیابان مطهری، مرکز فناوری اقبال، واحد ۲۲۵
کدپستی
۱۴۵۸۸۸۷۱۵۴
۸۹۱۷۶۹۷۹۹۸
تلفن
۰۲۱۶۶۱۹۸۶۸۰
۰۳۵۳۷۲۶۵۳۴۳
فکس
۰۲۱۶۶۱۹۸۶۷۸
۰۳۵۳۷۲۴۵۰۸۷
پویش داده نوین
PDNSOFT.COM | INFO@PDNSOFT.COM

۵.٤ سامانه جامع پشتیبان‌گیری / ***Backup***

از آنجایی که هیچ یک از راهکارهای امنیتی نمی‌تواند به طور قطع امنیت و سلامت اطلاعات یک سازمان را تضمین کند، نیاز به تهیه نسخه‌های پشتیبان و یا بکاپ یک امر بدیهی به نظر میرسد. نسخه‌های پشتیبان می‌توانند در صورت بروز حادثه‌های سخت‌افزاری مانند سوختن هارددیسک و یا کارت *RAID* نیز به کمک سازمان‌ها بیایند.

سامانه جامع بکاپ دارای سه ویژگی مهم زیر است:

۱.۵.۴ بکاپ‌گیری خودکار:

هنگامی که تعداد سرورها و خدمات سازمان زیاد باشد، تهیه بکاپ منظم از یک به یک سرورها کاری زمامبر و دشوار بوده و در اغلب سازمان‌ها به دلیل زمانبر بودن به صورت منظم انجام نمیگیرد. لذا وجود یک سامانه جامع که به طور خودکار از تمامی سرورها و اطلاعات مهم سازمانی بکاپ تهیه کند امری ضروری به نظر می‌رسد.

سامانه جامع بکاپ می‌تواند پس از راه‌اندازی کامل، به صورت خودکار از تمامی مسیرها و سیستم‌عامل‌های مهم شما به صورت منظم یک نسخه پشتیبان تهیه کرده و به صورت خودکار به سرور و هارد دیسک خود منتقل کند.

۲.۵.۴ داشبورد مدیریت وضعیت بکاپ‌ها:

سامانه جامع بکاپ دارای یک داشبورد مدیریتی تحت وب بوده که میتواند آخرین وضعیت بکاپ‌های تهیه شده از تمامی سرورها را در یک تصویر و به صورت خلاصه نمایش دهد. با استفاده از این داشبورد، مدیر سیستم می‌تواند در کوتاه‌ترین زمان ممکن از وضعیت سلامت بکاپ‌های تمامی سرورهای خود اطمینان حاصل کند.

آدرس
تهران، خیابان آزادی، خیابان حبیب زادگان، پلاک ۳۶، طبقه ۲
یزد، خیابان مطهری، مرکز فناوری اقبال، واحد ۲۲۵
کدپستی
۱٤٥٨٨٧١٥٤
۸۹۱۷٦۹۷۹۹۸
تلفن
۰۲۱٦٦۱۹۸٦۸۰
۰۳٥۳۷۲٦٥۳٤۳
فکس
۰۲۱٦٦۱۹۸٦۷۸
۰۳٥۳۷۲٤٥۰۸۷
پویش داده نوین
PDNSOFT.COM | INFO@PDNSOFT.COM

۳.۵.۴ عدم استفاده از پروتکل‌های *share* و استاندارد برای تهیه و انتقال بکاپ

عدم وابستگی سامانه جامع بکاپ به پروتکل‌های *share* استاندارد، باعث می‌شود تا مدیر سیستم بتواند ویژگی *share* را در سرورهای خود غیر فعال کرده و از انتشار ویروس‌ها، باج‌افزارها و سایر مخاطرات امنیتی در شبکه خود جلوگیری کند. سامانه جامع بکاپ با استفاده از *agent* و پروتکل مخصوصی که روی سرورها نصب می‌کند، اقدام به تهیه و انتقال بکاپ نموده و این روش نگرانی‌های امنیتی را به کلی از بین می‌برد.

۴.۵.۴ سرور لینوکسی

سامانه جامع بکاپ بر روی یک سرور لینوکسی قرار داشته و میتواند از تمامی سرورهای ویندوزی و لینوکسی با تمامی نسخه‌ها بکاپ تهیه کند. نصب سرور اصلی سامانه جامع بر روی یک سرور لینوکسی باعث می‌شود فایل‌های بکاپ شما از ویروس‌ها و باج‌افزارها در امان باشند.

۵.۵.۴ تهیه بکاپ از فایل، فولدر، دیتابیس و سیستم‌عامل همگی در کنار هم

سامانه جامع می‌تواند بر اساس نوع برنامه‌ریزی، از یک فایل و یا فولدر یک نسخه پشتیبان تهیه کند. با ترکیب این سامانه با سایر روش‌های بکاپ‌گیری، تهیه بکاپ از هر نرم‌افزار و یا سیستم‌عاملی امکان‌پذیر خواهد بود. برای مثال کافیست نرم‌افزار دلخواه شما در فولدری در درایو *D* از دیتای خود یک نسخه بکاپ تهیه کند. سپس سامانه جامع تمامی محتویات آن فولدر را به سرور بکاپ منتقل کرده و نگهداری خواهد کرد. تهیه بکاپ از ایمیج‌های ویندوز نیز به همین صورت امکان‌پذیر است. کافیست تا بکاپ اتوماتیک ویندوز و یا نرم‌افزارهای جانبی مانند *SnapShot Drive* به نحوی تنظیم شود تا یک ایمیج کامل از سیستم‌عامل، نرم‌افزارها و سرویس‌های خود تهیه کند تا نرم‌افزارجامع آن را به سرور بکاپ منتقل کرده و نگهداری کند. تهیه بکاپ از سیستم‌عامل به این روش و با استفاده از سامانه جامع، بدون نیاز به خاموشی رایانه و قطعی سرویس‌ها انجام میگیرد.

آدرس
تهران، خیابان آزادی، خیابان حبیب زادگان، پلاک ۳۶، طبقه ۲
یزد، خیابان مطهری، مرکز فناوری اقبال، واحد ۲۲۵
کدپستی
۱۴۵۸۸۸۷۱۵۴
۸۹۱۷۶۹۷۹۹۸
تلفن
۰۲۱۶۶۱۹۸۶۸۰
۰۳۵۳۷۲۶۵۳۴۳
فکس
۰۲۱۶۶۱۹۸۶۷۸
۰۳۵۳۷۲۴۵۰۸۷
پویش داده نوین
PDNSOFT.COM | INFO@PDNSOFT.COM