ایمن دیده‌بان شبکه
(ایده‌نت)

واحد تحقیق و توسعه

R&D

واحد تحقیق وتوسعه از حضور نیروهایی خلاق و توانمند بهره می‌برد و در پی آن است که به یاری آنان راه به چشم‌اندازهای تازه‌ای بگشاید. این واحد علاوه بر آماده‌سازی نرم‌افزارهای مختلف، خدمات گوناگونی نیز ارائه می‌کند. خدماتی مانند: اجرای پسیو، مجازی‌سازی، نصب انواع فایروال، اجرای استراتژی پشتیبان‌گیری و ...

فهرست

آشنایی با واحد تحقیق و توسعه ایمن دیده‌بان شبکه

شرکت ایمن دیده‌بان شبکه با سابقه‌ای فراوان در زمینه سخت‌افزار، اینک در حوزه تولید نرم‌افزار نیز به کار و فعالیت می‌پردازد. واحد نرم‌افزار شرکت از حضور نیروهایی خلاق و توانمند بهره می‌برد و در پی آن است که به یاری آنان راه به چشم‌اندازهای تازه‌ای بگشاید. هدف اصلی ایده‌نت ساخت و ارائه برنامه‌های باکیفیت است و می‌خواهد وقتی کاربران از این برنامه‌ها استفاده می‌کنند تجربه کاربری متفاوتی داشته باشند و از نحوه پشتیبانی شرکت راضی باشند.

طراحی و برنامه‌نویسی پروژه‌های سفارشی

نیازهـای افـراد و شـرکت‌ها بـه نرم‌افزارهـا و سـامانه‌های نرم‌افـزاری بسـیار گسـترده‌تر و متنوع‌تـر از دیگـر شاخه‌هاسـت. هرجـا کـه فراینـدی در جریـان باشـد نرم‌افـزار می‌توانـد بـرای توسـعه و بهبـود آن فراینـد، وارد میـدان شـود. در ایـن میـان ایده‌نـت می‌توانـد هـر نـوع برنامـه‌ای را بـر اسـاس نیـاز و درخواسـت مشـتریان آمـاده کنـد: چـه بـرای توسـعه کسـب و کار خـود یـک وبسـایت بـا طرحـی نـو بخواهیـد، چـه بـرای ارتبـاط بـا مشـتریان خـود یـا مدیریـت فراینـد فـروش و بازرگانـی خـود برنامه‌هـای اختصاصـی بخواهیـد واحـد نرم‌افـزار ایده‌نـت چنیـن نرم‌افـزاری را بـرای شـما فراهـم خواهـد سـاخت.

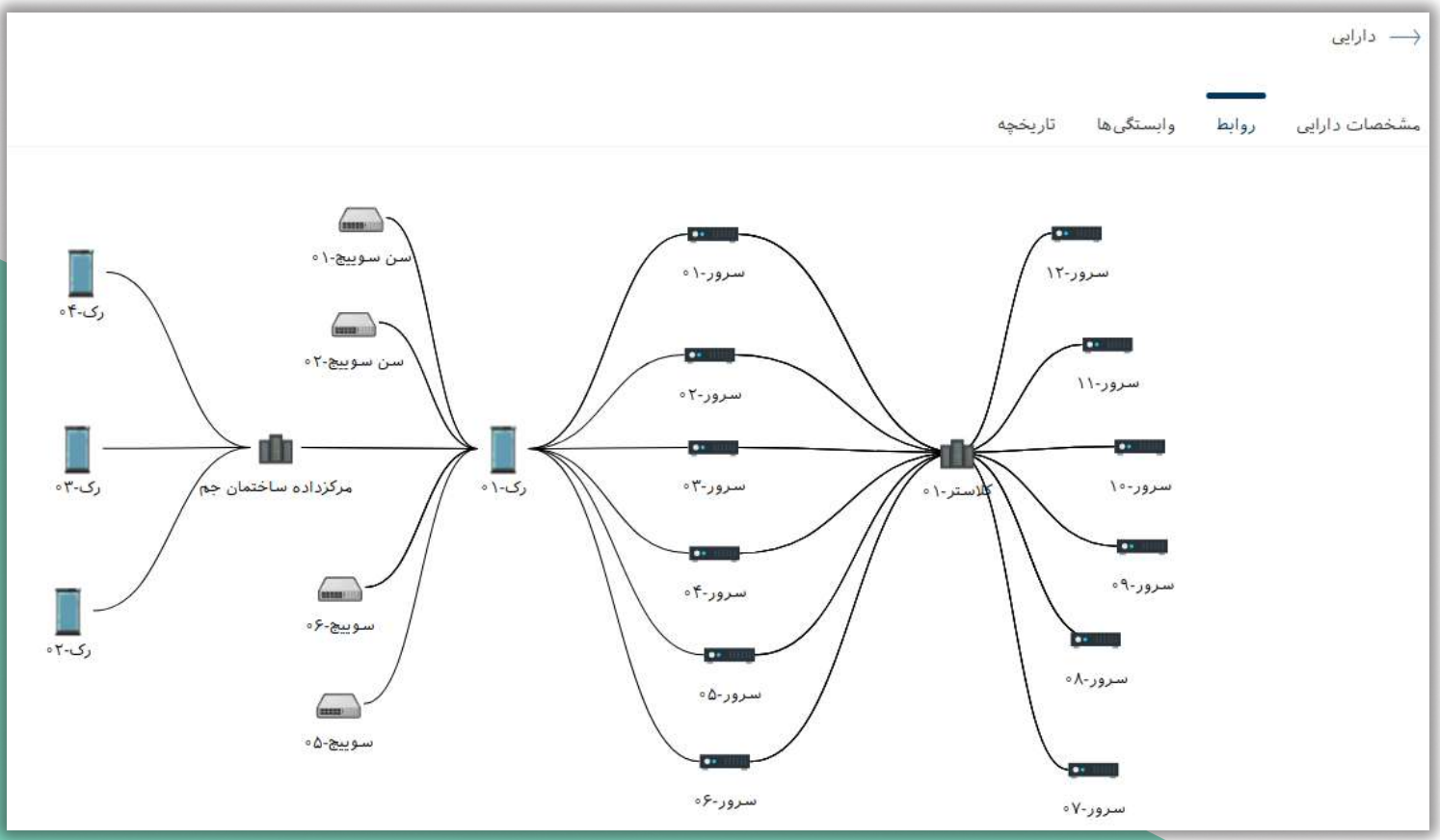
پروژه‌ها

نرم‌افزارهـای اینفونـت و CRM ایده‌نـت، از جملـه برنامه‌هایـی هسـتند کـه در بخـش نرم‌افـزار شـرکت تهیـه شـده‌اند. ایـن برنامه‌هـا پـس از مطالعـه و پژوهـش فـراوان سـاخته شـده‌اند و می‌تـوان گفـت نمونه‌هایـی بومـی و قابـل رقابـت بـا نسـخه‌های خارجـی هسـتند. نرم‌افـزار اینفونـت نوعـی برنامـه CMDB اسـت کـه مطابـق چهارچـوب ITIL4 فراهـم شـده و بـرای مدیریـت بهینـه تجهیـزات و خدمـات بخـش فنـاوری اطلاعـات بـه کار مـی‌رود. ایـن برنامـه می‌توانـد بـه صـورت خـودکار تمامـی ایـن گونـه سـخت‌افزارها و نرم‌افزارهـا را شناسـایی کنـد و در پایـگاه داده‌ای همگـی آن‌هـا را ثبـت و ضبـط نمایـد.

هـدف CMDB آن اسـت کـه اطلاعاتـی را در اختیـار سـازمان بگـذارد کـه بـه یـاری آن‌هـا در کسـب و کار خویـش تصمیم‌هـای مناسـب‌تری بگیـرد و فرایندهـای کارامدتـری را بـرای مدیریـت فنـاوری اطلاعـات مسـتقر نمایـد. اگـر تمامـی اطلاعـات مربـوط بـه پیکربنـدی تجهیـزات یکجـا ثبـت و ضبـط شـود رهبـران سـازمان می‌تواننـد بهتـر اجـزای حیاتـی سیسـتم را شناسـایی کننـد و بـه روابـط میـان آن‌هـا پـی ببرنـد.

در نهایت شما با نرم‌افزار اینفونت می‌توانید:

- رخدادها و درخواست‌ها را به آسانی مدیریت کنید.
- سخت‌افزارها و نرم‌افزارها را به صورت خودکار شناسایی و ثبت کنید.
- تاثیر هر تغییری را بر کسب و کار و سازمان خویش پیش‌بینی کنید.
- مشکلات را مدیریت کنید یعنی علت اصلی رخدادهای تکراری را دریابید و آن را برطرف سازید.



استراتژی پشتیبان‌گیری

روزانه تعداد زیادی فایل بر روی رایانه، سرور و دیگر ذخیره‌سازها قرار می‌گیرد همچنین با اتصال دائمی به شبکه اینترنت هر لحظه با خطراتی مثل هجوم ویروس‌ها و دیگر حملات مواجه هستیم.

برای اینکه اطلاعات حیاتی را در چنین شرایطی از دست ندهیم بهتر است که یک استراتژی برای پشتیبان‌گیری از اطلاعات داشته باشیم.

به طور قطع استراتژی‌ای وجود ندارد که بتواند در تمامی شرایط ممکن از اطلاعات شما محافظت کند ولی استراتژی ۱-۲-۳ بهترین راه برای پشتیبانی‌گیری از اطلاعات است که مهندسان فناوری اطلاعات استفاده از آن را توصیه می‌کنند. شرکت ایمن دیده‌بان شبکه نیز می‌تواند با بهره‌گیری از متخصصانی توانمند بهترین استراتژی‌های پشتیبان‌گیری را به شما ارائه نماید و راه‌حل مناسب را برای سازمان شما پیاده‌سازی کند.

این استراتژی بیشتر مناسب رایانه‌های خانگی و شرکت‌های کوچک و متوسط است که به طور حتم روشی بهتر از عذرخواهی کردن برای از دست رفتن اطلاعات است.

در ادامه نگاهی دقیق‌تر به نحوه عملکرد استراتژی ۳-۲-۱ خواهیم کرد.

۳ داشتن نسخه از اطلاعات

اولین اصل این استراتژی نگه داشتن ۳ نسخه از اطلاعات است؛ شما باید علاوه بر داشتن فایل اصلی اطلاعات، دو نسخه رونوشت نیز تهیه کنید. برای مثال اگر فایلی به نام ((آ)) دارید دو نسخه «پشتیبان ۱-آ» و «پشتیبان ۲-آ» را نیز داشته باشید.

به طور یقین احتمال از دست دادن اطلاعاتی که در چند جا ذخیره شده‌اند کمتر از احتمال از دست دادن اطلاعاتی است که در یک‌جا ذخیره شده‌است.

---

۲ قراردادن نسخه‌ها در دستگاه متفاوت

اگر ۳ نسخه از اطلاعات خود را در یک مکان قرار دهید با از دست رفتن یک نسخه بقیه را نیز از دست می‌دهید به همین منظور توصیه می‌شود که دو نسخه از اطلاعات خود را در دو نوع مختلف از ذخیره‌سازها قراردهید؛ مثلاً یک نسخه را در USB فلش‌ها و دیگری در هاردهای اکسترنال HDD یا SDD. این عمل خطر از دست دادن اطلاعات را بسیار کاهش می‌دهد چرا که اگر یکی از نسخه‌ها از دست رفت نسخه دیگری در دسترس هست.

---

۱ داشتن نسخه از اطلاعات در خارج از سیستم یا شبکه

نگه‌داری اطلاعات در یک ذخیره‌ساز خارجی بسیار تاثیرگذار است ولی درایوهای سخت‌افزاری نیز ممکن است دچار مشکل شوند و از کار بیفتند بنابراین انتقال نسخه سوم به فضای ابری یا NAS گزینه مناسب‌تری است.

درایوهای فیزیکی ممکن است بر اثر خطای انسانی، سیل، زلزله یا سرقت آسیب ببینند اما چنین اتفاقاتی در فضای ذخیره‌سازی ابری به سختی رخ می دهند.

پیاده‌سازی راهکارهای مجازی‌سازی

در سال‌های اخیر، مجازی‌سازی به عنوان یکی از راهکارهای پیشرفته و نوین در حوزه فناوری اطلاعات مطرح گردیده و فرصت‌های جدیدی نظیر رایانش ابری را فراهم نموده است. در این راستا، مجازی سازی به خاطر قابلیت اطمینان، دسترس‌پذیری، امنیت و کارایی در حوزه‌های گوناگون سخت افزاری و نرم افزاری به‌کار می‌رود.

شرکت ایمن دیده بان شبکه، تجربه‌ای فراوان در زمینه مشاوره، طراحی، پیاده سازی و پشتیبانی، بهینه سازی و آموزش زیر ساخت مجازی دارد. این شرکت بر پایه دانش و تخصص کارشناسان خود، به‌عنوان یکی از شرکت های دانش‌محور در زمینه ارائه و توسعه راهکارهای نوین فناوری ذخیره‌سازی و پردازش اطلاعات، فراهم‌سازی امنیت داده و محافظت از آن در مراکز داده پشتیبان، فعالیت دارد. فهرست زیر نمونه‌ای از توانمندی‌ها و تجربه تیم تخصصی و مشاوران این شرکت است که همواره خود را با بروزرسانی‌های فناوری همگام و هماهنگ ساخته‌اند:

- انجام پروژه‌های شناخت، تحلیل و طراحی در حوزه مجازی‌سازی با بهره‌گیری از راهکارهای VMware
- مشاوره، طراحی، راه اندازی و پشتیبانی اکوسیستم محصولات VMware vSphere
- طراحی، پیاده‌سازی، بهینه‌سازی و آزمون‌های عملکردی دقیق استفاده از راهکار ذخیره‌سازی مبتنی بر NAS به جای SAN در زیرساخت مجازی سازی کسب و کارهای کوچک و متوسط با بودجه اقتصادی
- مهاجرت از محیط فیزیکی یا مجازی کنونی به محیط مجازی با ایجاد حداقل اختلال برای سرویس‌های موجود
- طراحی و پیاده سازی راهکارهای مانیتورینگ اختصاصی تجهیزات مجازی‌سازی
- ارائه راهکارهای بهینه پشتیبان‌گیری از محیط‌های مجازی
- مشاوره، طراحی، راه‌اندازی و پشتیبانی VMware NSX برای محافظت و مدیریت شبکه
- ارائه راهکارهای Disaster Recovery با استفاده از راه حل VMware SRM
- مشاوره، نصب و راه‌اندازی راه حل‌های VDI و مجازی‌سازی دسکتاپ (Desktop Virtualization) با استفاده از VMware Horizon View
- مشاوره، طراحی، راه‌اندازی و پشتیبانی Failover Cluster، High Availability و Load Balancing برای سرویس‌ها و سرورهای حیاتی شبکه

مرکز داده کانتینری

امروزه چنین احساس می‌شود که شرکت‌ها و سازمان‌ها به مراکز داده استاندارد بیش از هر زمانی نیاز دارند. از آنجا که مراکز داده سنتی معایب و مشکلاتی مانند زمان ساخت و بهره‌برداری طولانی و مصرف انرژی بالا را داشته و نیاز به صرف هزینه فراوانی نیز دارند، با گسترش شتابان کسب و کارهای آنلاین، زیرساخت‌های این حوزه نیز با چالش‌هایی بسیار جدی روبرو خواهند شد.

شرکت ایمن دیده‌بان شبکه با در نظر داشتن چنین دورنمایی، پروژه مراکز داده کانتینری را با بهره‌گیری از نوین‌ترین فناوری‌ها از اواخر سال ۱۳۹۴ آغاز نموده است و در این راه مدل‌های گوناگونی از این گونه مراکز که داری منبع تغذیه‌ای یکپارچه، سیستم توزیع برق، سیستم خنک‌کننده، رک، امکانات فرونشاندن حریق و دیگر تجهیزات ایمنی هستند را در کانتینرهای استاندارد مهیا و عرضه کرده است.

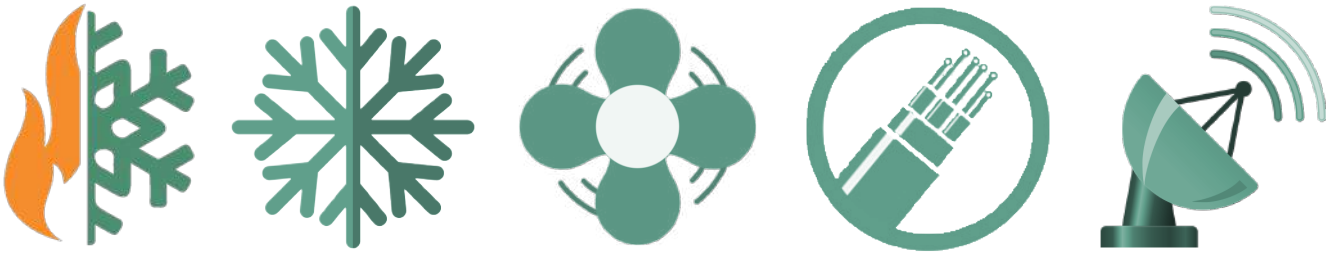
ویژگی‌ها

مراکز داده کانتینری ماژولار در ابعاد ۱۰،۲۰،۴۰ فوت قابل عرضه هستند که تراکم بالا، توسعه‌پذیری، انعطاف‌پذیری، بازدهی بالای انرژی، کابل کشی شبکه و سیستم برق‌رسانی عایق‌های امواج الکترومغناطیسی و بازدهی مناسب سیستم‌های سرمایشی تنها پاره‌ای از امکانات و امتیازات آن‌هاست و افزون بر آن به دلیل امکان جابجایی و حمل با تجهیزات کامل، گزینه‌ای مناسب برای زمان بحران به عنوان مراکز داده پشتیبان به شمار می‌آیند.

این قبیل مراکز به خاطر بهره جستن از شبکه زیرساخت‌های مدرن و پیشرفته در حوزه برق و داده موجب کاهش ۷۰ درصدی کابل کشی و ۲۵ درصدی هزینه‌های عملیاتی و نگهداری می‌گردند و به همین دلیل در محیط های گوناگون از قبیل شرکت‌ها، سازمان‌ها و وزارت‌خانه‌ها با اهداف متفاوت و متنوع قابل بهره‌برداری‌اند. از سوی دیگر هر یک امکان جاگذاری ۱۱۵۲۰ هسته پردازشی یا ۳۶ پتا بایت فضای ذخیره‌سازی در هر کانتیر را دارند که این ویژگی آن‌ها را به عنوان سامانه‌ای ایده‌آل و جایگزینی مطمئن برای مراکز سنتی بدل نموده است.

مزایا

- مجهز به راهرو گرم و راهرو سرد
- سرعت گردش بالای هوای داخل
- افزایش بازده سیستم سرمایشی به حدود ۴۰٪
- تنوع درگاه‌های ارتباطی
- ارتباط فیبرنوری از ۸ هسته به بالا
- ارتباط ماهواره ای
- ارتباط رادیویی (Wi-Fi , WiMAX , HF , Tetra)



کاربردها

- بهترین انتخاب برای موقعیت های بحرانی
- گزینه مناسب به عنوان پشتیبان مراکز داده موجود در سازمان ها
- جایگزین مطلوب برای مراکز داده سنتی به خاطر توسعه‌پذیری و هزینه نگهداری اندک
- مناسب برای پروژه‌های پدافند غیر عامل به دلیل داشتن عایق های ضدآب و گرد و خاک
- گزینه‌ای ایده‌آل برای سازمان‌ها و ارگان‌هایی که جابجایی سریع و یکباره مرکز داده را مدنظر دارند.

واحد شبکه

خدمات پسیو شبکه یکی از مهمترین و اساسی‌ترین عملیات زیر ساخت شبکه است که اجرای صحیح و رعایت استانداردهای کابل کشی ساخت‌یافته در آن اهمیت بسیار بالایی دارد. اجرای صحیح و اصولی چنین عملیاتی می تواند باعث جلوگیری از هدر رفتن و افت سرعت در شبکه شود و تاثیر به سزایی نیز در زیبایی محل استقرار تجهیزات داشته باشد.

اجرای درست و دقیق زیرساخت شبکه به دانش و تخصص و تجربه فراوانی نیاز دارد. تیم اجرایی شرکت ایمن دیده‌بان شبکه با تکیه بر توان و تخصص خود و بیش از بیست سال تجربه اجرای پروژه‌های بزرگ و کوچک در محیط‌های عملیاتی گوناگون، آمادگی و دانش کافی را برای اجرای عملیات کابل‌کشی ساخت‌یافته شبکه با کابل فیبرنوری، مسی، برق و ... در اختیار دارند.

نصب و راه‌اندازی دکل

یکی دیگر از خدمات شرکت ایمن دیده‌بان شبکه طراحی ، تهیه، نصب و راه‌اندازی دکل‌های مختلف(خود ایستا، مهاری و....) با کاربردهای متفاوت(مخابراتی، نظارتی، روشنایی و ...) و ارتفاع مورد نیاز است. این دکل‌ها بر اساس نوع کاربرد و محل نصب نیر متفاوت هستند. البته دیگر نکته مهم درباره این دکل‌ها، انجام و اجرای زیرسازی و فونداسیون مناسب و اصولی برای آن‌ها است به گونه‌ای که در شرایط مختلف آب و هوایی و درطول زمان مشکلی برای آن‌ها پیش نیاید. در این میان بازدید دوره‌ای و پشتیبانی و نگهداری نیز اهمیت حیاتی دارد.

انجام تست‌های مختلف مربوط به کابل فیبر نوری

یکی دیگر از مراحل ارائه خدمات پسیو، انجام تست‌های اصولی و مناسب برروی کابل‌های نصب شده و اتصالات آن‌ها است که این امر نیاز به تجهیزات مناسب و تخصص و تجربه کافی در این حوزه دارد. این تست‌ها میزان افت و یا درستی اتصالات و صحت عملکرد تجهیزات نصب شده پسیو را نشان می‌دهد و برای انجام آن‌ها نیاز به تسترهای مختلف با قابلیت‌های متفاوت است.

نصب و آرایش رک‌های ایستاده و دیواری

یکی دیگر از خدمات ایده‌نت در حوزه خدمات پسیو، تهیه و نصب و آرایش رک‌های مختلف در سایزهای متفاوت با توجه به نیاز و شرایط محیطی کارفرماست. آرایش درست رک می‌تواند هم به زیبایی محیط کار و هم به سادگی کنترل کابل‌ها و اتصالات کمک کند و همچنین در سرویس‌های دوره ای در افزایش سرعت انجام کار بسیار موثر باشد. البته انتخاب رک مناسب و تجهیزات مناسب برای آرایش مانند Cable Management و Blank Panel و ... خود از اهمیت بالایی برخوردار است.

نصب و طراحی شبکه‌های برق اضطراری و UPS

برق اضطراری خود به تنهایی نیاز به دانش علمی و فنی جداگانه‌ای دارد و از اهمیتی حیاتی نسبت به سایر تجهیزات برخوردار است. انتخاب نامناسب تجهیزات و کابل‌های ارتباطی برق و همچنین تابلوهای مرکزی و توزیع برق اضطراری و اصلی می‌تواند عامل اصلی قطع برق و بروز خرابی در تجهیزات و حتی در برخی از موارد بروز آتش‌سوزی شود . UPS و کابل و تابلوها باید حتما بر اساس میزان بار تجهیزات و پس از بررسی‌های علمی و دقیق و با نگاهی به آینده انتخاب و تهیه و اجرا شوند. متخصصان شرکت ایده‌نت آماده هستند تا در این زمینه و در قالب خدمات پسیو خدمات لازم را ارائه نمایند.

نصب پچ پنل‌های مختلف اعم از مخابراتی، فیبر نوری و شبکه

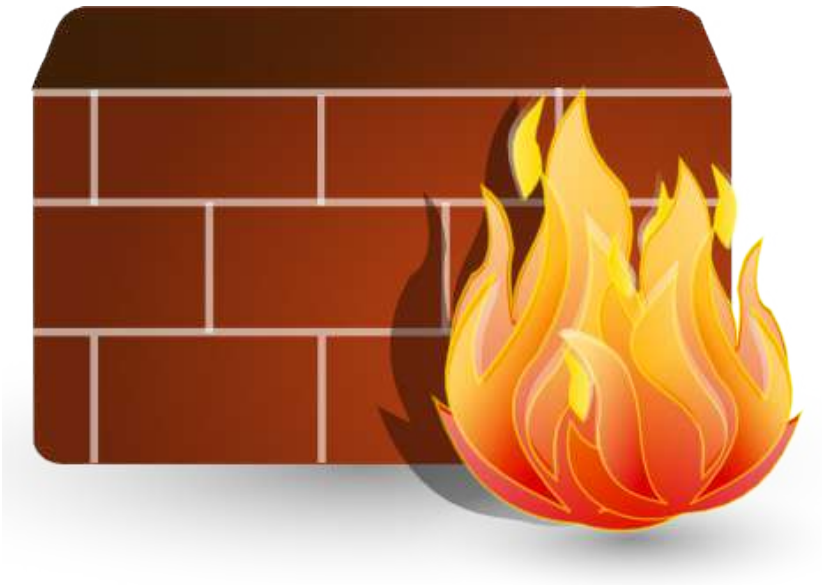
پـچ پنـل بـه عنـوان رابطـی بیـن کابل‌هـای مسـیر و دسـتگاه‌های کنترل‌کننـده در ابتـدا و انتهـای مسـیر درداخـل رک‌هـا نصـب مـی شـود. در ایـن نقـاط، کیفیـت پـچ پنـل و پانـچ درسـت و اصولـی آن بسـیار اهمیـت دارد . پانـچ نادرسـت و یـا کیفیـت نامناسـب پـچ پنـل می‌توانـد باعـث افـت شـدید سـرعت در شـبکه‌های رایانـه‌ای و یـا قطـع و وصـل صـدا در پـچ پنل‌هـای مخابراتـی و ... شـود. نصـب صحیـح و مرتـب پـچ پنـل نیـاز بـه دقـت بالایـی دارد، کاری زمان‌بـر اسـت و بایـد بـر اسـاس شـماره‌های از پیـش مشخص‌شـده انجـام شـود.

فایروال

به نرم‌افزار یا سخت‌افزاری که بر ترافیک رد و بدل شده در شبکه را نظارت می‌کند، فایروال یا دیواره آتش (Firewall) می‌گویند؛ فایروال در حقیقت یک ابزار امنیتی است که می‌تواند یک برنامه‌ی نرم‌افزاری یا یک دستگاه اختصاصی شبکه باشد.

شرکت ایمن دیده‌بان شبکه با سال‌ها تجربه در زمینه فایروال‌ها و بهره‌گیری از تیمی باتجربه و متخصص، در این زمینه فعالیت می نماید و آماده ارائه خدمات به شرکت‌های مختلف است.

هدف از ایجاد فایروال



فایروال در حقیقت فیلتری است که داده‌ها باید از آن عبور کنند. هدف اصلی آن نیز جداسازی یک داده‌ی امن از ناحیه‌ی ناامن و کنترل ارتباط‌های بین این دو است. فایروال یکی از مهم‌ترین لایه‌های امنیتی شبکه‌های رایانه‌ای است و اگر از آن‌ها استفاده نکنید، هکرها به‌راحتی وارد شبکه یا رایانه شخصی شما می‌شوند و بدون هیچ محدودیتی خراب‌کاری‌های خود را انجام می‌دهند.

فایروال می‌تواند کارهای دیگری نیز انجام دهد اما بیشتر مسئول نظارت بر ارتباط‌های ورودی و خروجی از یک دستگاه به شبکه است.

به طور معمول فایروال‌ها این کارها را انجام می‌دهند:

- از منابع محافظت می‌کنند.
- اجازه‌ی دسترسی مجاز را می‌دهند.
- نقش یک میانجی را ایفا می‌کنند.
- ترافیک شبکه را مدیریت و کنترل می‌کنند.
- رخدادها را ذخیره می‌کنند و درباره آن‌ها گزارش می‌دهند.

در زمانه‌ی اینترنت پرسرعت، رایانه شما به‌صورت الکترونیکی به شبکه‌ای گسترده متصل می‌شود که همین سرعت بالا باعث آسیب‌پذیرتر شدن اتصال می‌شود، مگر این که یک فایروال شخصی داشته باشید و بتوانید از اطلاعات خود محافظت کنید. در واقع اتصال به اینترنت پرسرعت را می‌توان به خارج شدن از خانه و نبستن در تشبیه کرد.

انواع فایروال‌ها

فایروال‌ها انواع مختلفی دارند که در ادامه به آن‌ها اشاره خواهیم‌کرد، اما معمولا دریکی از دودسته‌ی فایروال‌های مبتنی بر میزبان و فایروال‌های مبتنی بر شبکه قرار می‌گیرند.
فایروال‌های مبتنی بر میزبان بر روی سرورهای شخصی نصب می‌شوند و بر سیگنال‌های ورودی و خروجی نظارت می‌کنند.
فایروال‌های مبتنی بر شبکه می‌توانند در زیرساخت‌های ابری ساخته شوند، یا می‌توانند سرویس فایروال مجازی باشند.

فایروال‌های فیلتر بسته‌ها (Packet-filtering)

اساس کار این فایروال در بررسی بسته‌ها به‌صورت جداگانه است. هنگامی که یک بسته از این فایروال عبور می‌کند، آدرس منبع و مقصد آن و همچنین پروتکل و شماره پورت مقصد آن بررسی می‌شود. چنانچه این بسته نتواند قوانین فایروال را رعایت کند، قطع می‌شود و به مقصد نمی‌رسد.

فایروال های بازرسی قانونی (Stateful inspection)

فایروال‌های بازرسی قانونی به فایروال‌های فیلتر دینامیک بسته‌ها (dynamic packet-filtering) نیز معروف هستند. این فایروال دارای جدولی است که مسیر تمام ارتباط‌ها را باز نگه می‌دارد. هنگامی‌که یک بسته‌ی جدید می‌آید، فایروال اطلاعات موجود در سربرگ (header) بسته را با جدول خود مقایسه می‌کند و تشخیص می‌دهد که آیا این ارتباط قابل برقراری است یا خیر؟ چنانچه اطلاعات بسته با ارتباط فعلی مطابقت داشته باشد، بسته اجازه‌ی عبور را خواهد داشت. در غیر این صورت بسته مطابق قوانین تنظیم شده برای ارتباط جدید ارزیابی خواهد شد.

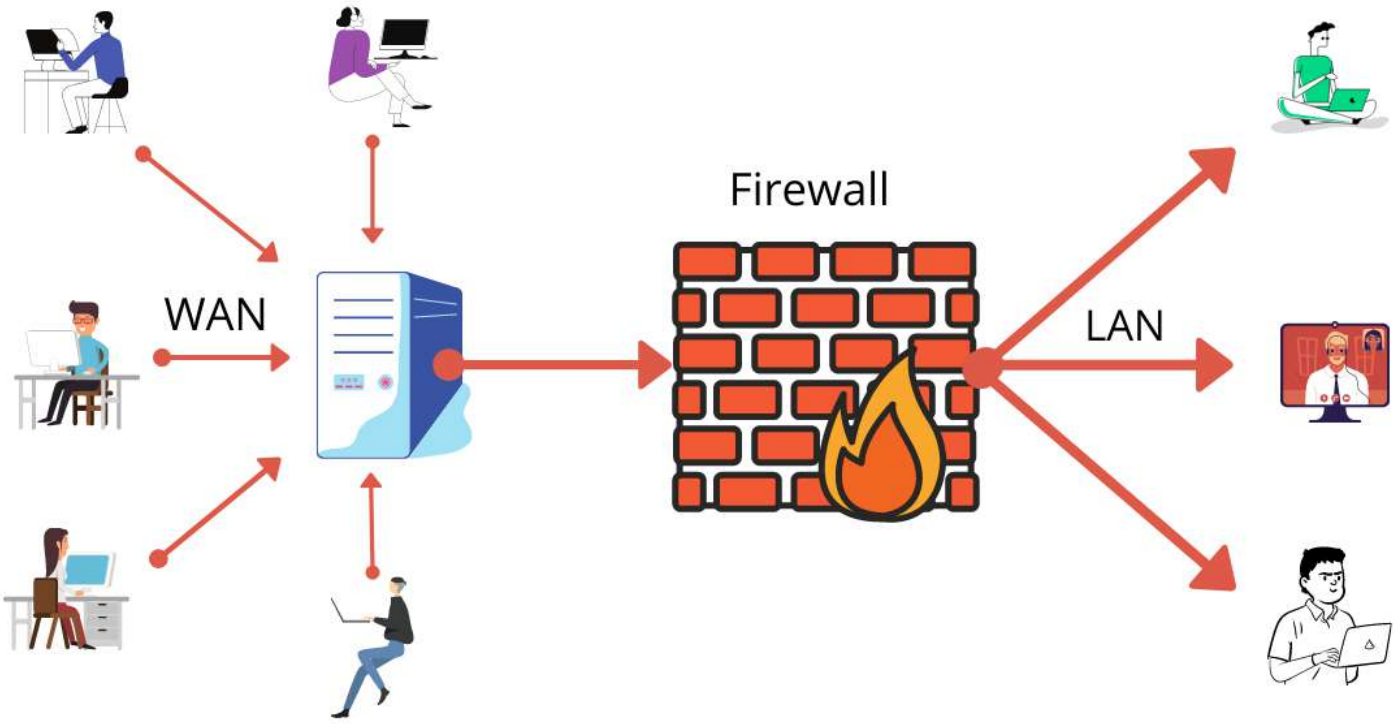
این فایروال‌ها ارتباط‌ها را در دوره‌های زمانی مختلف رصد می‌کنند و بسته‌های ورودی و خروجی را مورد بررسی قرار می‌دهند. تمامی بسته‌های ورودی و خروجی ردیابی می‌شوند و تنها بسته‌هایی که واکنش مناسبی نسبت به قوانین فایروال دارند مجاز به عبور خواهند بود. اگرچه فایروال‌های Stateful inspection بسیار مؤثرند، اما گاهی اوقات در برابر حملات (DoS) آسیب‌پذیر هستند.

فایروال های لایه کاربری و پروکسی (Application Layer and Proxy)

هم اکنون حمله به وب سرورها روزبه‌روز در حال افزایش است. به همین دلیل برای محافظت از شبکه در برابر چنین حملاتی، نیاز به یک فایروال قدرتمند به‌شدت احساس می‌شود. قرار دادن فایروال در پروکسی سرور، کار را برای مهاجمین سخت‌تر خواهد کرد و آن‌ها نمی‌توانند به‌راحتی بفهمند که شبکه در چه مکانی قرار دارد.
رمز موفقیت فایروال‌های لایه کاربری، توانایی آن‌ها در بلاک کردن محتوای خاص مانند malware ها و وب‌سایت‌های خاص و همچنین تشخیص مضر بودن پروتکل‌هایی مانند FTP، HTTP و DNS است.
ازآنجایی‌که این نوع فایروال‌ها بر اساس محتوای انتقالی کار می‌کنند، به مهندسان امنیتی امکان نظارت دقیق‌تری را بر روی ترافیک شبکه می‌دهند و قوانین را برای تایید یا رد درخواست اعمال می‌کنند.

فایروال های نرم افزاری

فایروال‌های نرم‌افزاری (Software Firewall) را فایروال‌های شخصی نیز می‌نامند. این فایروال‌ها برای راه‌اندازی در یک رایانه طراحی شده‌اند و معمولاً در خانه یا رایانه‌های اداری کوچک مورد استفاده قرار می‌گیرند که مدت زمان زیادی به اینترنت متصل هستند. فایروال نرم‌افزاری از دسترسی ناخواسته به یک رایانه در شبکه از طریق شناسایی و جلوگیری از برقراری ارتباط بر روی درگاه‌های پر خطر جلوگیری می‌کند.
بیشتر فایروال‌های شخصی دارای تنظیماتی هستند تا بتوانید به‌راحتی سیاست‌های امنیتی را متناسب با نیاز خودتان اجرا کنید.



pfSense؛ رایگان با امکانات یک فایروال تجاری سطح‌بالا

pfSense یک فایروال و مسیریاب (روتر) متن باز و رایگان مبتنی بر FreeBSD است که یک رابط کاربری وب به آسانی می‌تواند آن را مدیریت کند. این فایروال قدرتمند امکاناتی را ارائه می‌دهد که آن را در جایگاه رقابت با گزینه‌های تجاری مطرح و گران قرار داده است و به همین دلیل میان کاربران از محبوبیت فراوانی برخوردار است.

نگاهی به تاریخچه *pfSense*

پروژه pfSense سال ۲۰۰۴ به عنوان شاخه‌ای از پروژه فایروال monowall آغاز به کار کرد و سال ۲۰۰۶ برای نخستین بار به صورت عمومی عرضه شد. نام این نرم‌افزار از آنجا آمده که از PF به معنای ابزار فیلترینگ بسته‌ها (Packet-filtering) بهره می‌برد.مهم‌ترین تفاوت pfSense و monowall در این بود که pfSense به جای دستگاه‌های توکار (Embedded devices) برای رایانه‌های شخصی و سرورها طراحی شده بود؛ به همین دلیل نیز قابلیت‌ها و انعطاف بیشتری در اختیار کاربران قرار می‌داد.

قابلیت‌های مهم pfSense

pfSense علاوه بر اینکه یک پلتفرم بسیار قدرتمند فایروال و مسیریابی (روتینگ) است شامل فهرستی طولانی از قابلیت‌های گوناگون و مرتبط نیز می‌شود.

سامانه مدیریت بسته‌ها در pfSense توسعه‌پذیری بدون ایجاد آسیب‌های امنیتی را ممکن می‌سازد. به همین دلیل pfSense ابزاری بسیار نیرومند و انعطاف‌پذیر است که می‌توان آن را به سادگی برای مقاصد گوناگون مورد استفاده قرار داد: از یک روتر خانگی گرفته تا یک فایروال برای شرکتی بزرگ. نصب این فایروال آسان است و تعمیر و نگهداری‌اش نیز دشواری چندانی ندارد. همچنین رابط کاربری ساده‌ای دارد و قابلیت‌های یک محصول تجاری بسیار گران‌قیمت را رایگان در اختیار کاربران می‌گذارد، در نتیجه می‌توانید آن را به آسانی دریافت و بر روی هر سخت‌افزاری نصب کنید، مقیاس‌پذیری و انعطاف‌پذیری آن هم به همین خاطر است.

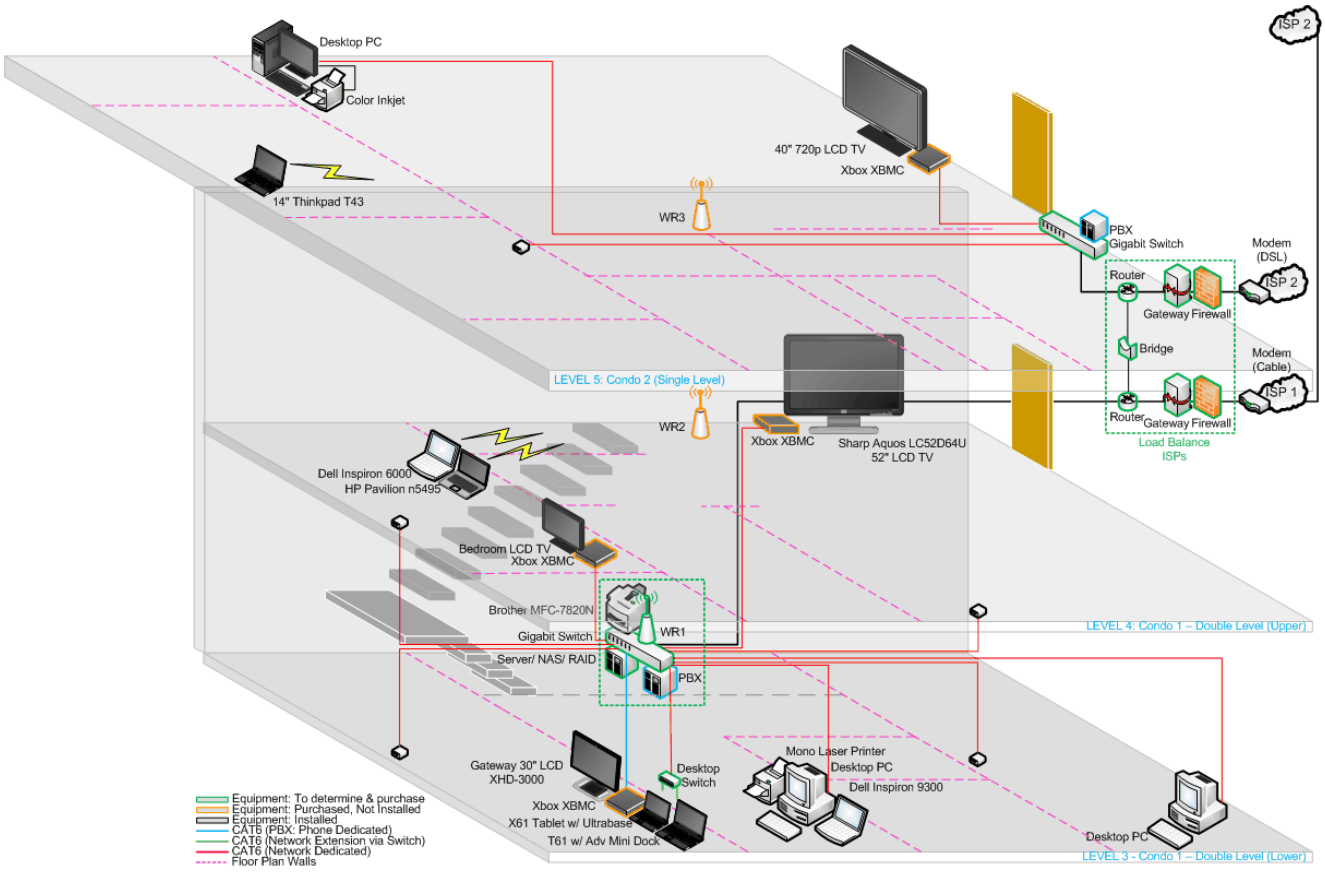
یک ویژگی مهم دیگر این نرم‌افزار توسعه‌پذیری بسیار بالای آن است. گروه‌های بسیاری بر روی این نرم‌افزار کار می‌کنند و تا کنون افزونه‌های گوناگونی برای آن تولید کرده‌اند که تقریبا بیشتر آن‌ها به شکل رایگان در دسترس کاربران قرار می‌گیرند.

pfSense علاوه بر ویژگی‌های اساسی یک فایروال، ویژگی‌ها و امکانات دیگری نیز دارد که شامل شکل‌دهی به ترافیک، امکان تنظیم به شکل VPN Router، قابل استفاده به عنوان سرور DNS یا DHCP، قابل استفاده به عنوان برگردان نشانی شبکه (NAT)، اتصال از راه دور، عیب‌یابی، گزارش‌دهی، ایفای نقش روتر LAN یا WAN، ایفای نقش به عنوان یک Wireless hotspot و بسیاری امکانات دیگر می‌شود.

برای استقرار و استفاده از نرم‌افزار pfSense بهره بردن از دانش FreeBSD ضرورتی ندارد. در واقع اکثر کاربران pfSense هرگز از FreeBSD خارج از این نرم‌افزار استفاده نکرده‌اند.

در نهایت pfSense پروژه‌ای محبوب است که از زمان معرفی تا کنون میلیون‌ها بار دانلود شده و در حال حاضر صدها هزار کاربر فعال دارد. استفاده از این نرم‌افزار در موقعیت‌های گوناگون سودمندی‌اش را به اثبات رسانده است؛ از امنیت رایانه‌های شبکه‌های کوچک خانگی گرفته تا هزاران دستگاه در شبکه‌های بزرگ شرکت‌ها، دانشگاه‌ها و سازمان‌ها، این فایروال همه جا از خود ویژگی‌های قابل اتکا و بسیار موثری نشان داده است.

متخصصان و نیروهای فنی ایمن دیده‌بان شبکه می‌توانند این نرم‌افزار را برای شما نصب و راه‌اندازی نمایند و آموزش‌های لازم برای استفاده از آن را نیز به شما ارائه کنند.



زبیکس؛ راه‌حل طلایی پایش زیرساخت فناوری اطلاعات سازمان‌ها

زبیکس یک نرم‌افزار مانیتورینگ متن‌باز مناسب برای کسب‌وکارهای بزرگ و کوچک است. این نرم‌افزار پارامترهای متعدد یک شبکه، سلامت و یکپارچگی سرورها، ماشین‌های مجازی، اپلیکیشن‌ها، سرویس‌ها، پایگاه‌های داده، وبسایت‌ها، فضای ابری و ... را به صورت مستمر پایش می‌کند.

زبیکس از یک سازوکار اطلاع‌رسانی منعطف بهره می‌برد که به کاربران امکان می‌دهد هنگام هر رخدادی هشداری را در قالب‌های مختلف از جمله ایمیل دریافت کنند. این شیوه به کاربران امکان می‌دهد تا واکنش سریعی در برابر همه مشکلات سرور از خود نشان دهند. همچنین زبیکس بهترین شیوه‌های گزارش‌دهی و قابلیت‌های بصری‌سازی داده‌ها را براساس داده‌های ذخیره‌شده در اختیار کاربران قرار می‌دهد. این ویژگی هم زبیکس را به گزینه‌ای ایده‌آل برای برنامه‌ریزی ظرفیت (Capacity planning) تبدیل می‌کند.

تمام گزارش‌ها و آمار مربوط به زبیکس و همچنین تمام پارامترهای مربوط به پیکربندی و تنظیم آن، از طریق یک فرانت‌اند مبتنی بر وب در دسترس است؛ چنین ویژگی‌ای تضمین می‌کند که وضعیت شبکه شما و سلامت سرورهایتان از هر مکانی قابل ارزیابی باشد. در واقع اگر زبیکس به درستی و با دقت تنظیم شود می‌تواند نقشی بسیار حیاتی در پایش زیرساخت فناوری اطلاعات سازمان ایفا کند. این موضوع چه برای سازمان‌های کوچک با فقط چند سرور و چه شرکت‌های بزرگ با تعداد بسیار زیادی سرور به یک اندازه درست است.

در این میان باید به این موضوع هم اشاره کنیم که نرم‌افزار زبیکس رایگان است. زبیکس تحت نسخه GPL 2 نوشته و منتشر شده است؛ این بدین معناست که کد منبع آن به شکل رایگان منتشر شده و برای عموم در دسترس است. همچنین شرکت زبیکس و شریکانش از آن در سراسر جهان پشتیبانی تجاری می‌کنند.

ویژگی‌های کلیدی زبیکس

بکارگیری آسان

زبیکس ویژگی‌هایی دارد که استفاده از آن را ساده و در کمترین زمان، امکان‌پذیر می‌سازد. نصب ساده و سریع طی چند دقیقه، ارائه قالب‌ها برای اغلب پلتفرم‌های محبوب، امکان ساخت قالب‌های سفارشی‌سازی‌شده، امکان استفاده از صدها قالب آماده که انجمن‌های زبیکس قبلا آن‌ها را ساخته‌اند و پایش هزاران دستگاه مشابه با بهره‌بردن از تنظیمات این قالب‌ها بخشی از این ویژگی‌ها به شمار می‌آیند.

بصری‌سازی و گزارش‌دهی

رابط وب روش‌های گوناگونی برای ارائه یک نمای بصری از محیط زیرساخت فناوری اطلاعات شرکت دارد؛ برای مثال می‌توان به داشبوردهای مبتنی بر ویجت، نمودارها، نقشه‌های شبکه، اسلایدها و گزارش‌های تعاملی اشاره کرد.

عیب‌یابی

تعیین آستانه‌های هوشمند، شرایط ایده‌آلی را برای عیب‌یابی به کمک زبیکس ایجاد می‌کند. دیگر امکانات زبیکس در این حوزه عبارتند از: تشخیص خودکار حالت‌های گوناگون بروز مشکل در جریان ورودی به شکلی که نیاز به بررسی مداوم معیارهای ورودی نباشد، تشخیص ناهنجاری‌ها، تحلیل دلیل ریشه‌ای مشکلات، پیش‌بینی روندها در کنار امکان تعیین آستانه‌های هوشمند به طرزی بسیار انعطاف‌پذیر و تعیین سطوح مختلف بحرانی‌بودن مشکل.

اطلاع‌رسانی و اصلاح

با زبیکس آگاهی از هر مشکل به نوعی تضمین شده است. این نرم‌افزار افراد مسئول را از راه‌ها و روش‌های مختلف در مورد رخدادهای گوناگون آگاه می‌سازد. امکاناتی چون ارسال پیام، رفع مشکل به شکل خودکار و همچنین سفارشی‌سازی پیام‌ها تنها بخشی از این امکانات و راه‌ها هستند.

امنیت و اعتبار

زبیکس حفاظت از داده‌ها را در تمام سطوح ممکن می‌سازد. از جمله ویژگی‌های امنیتی این نرم‌افزار می‌توان به رمزگذاری قوی میان همه اجزای آن، چند روش متفاوت احراز هویت و صدور اجازه دسترسی به گونه‌ای انعطاف‌پذیر اشاره کرد.

خدمات سانیار

این روزها خدمات HP Care Pack در ایران به صورت مستقیم قابل ارائه نیست و از سویی بیش از ۹۰ درصد از سرورهای مورد استفاده در کشورمان از محصولات این شرکت به شمار می‌آیند، به همین خاطر شرکت ایمن دیده‌بان شبکه اقدام به طراحی و ارائه خدمات HP Care Pack در ایران نموده و با در اختیار داشتن متخصصان با تجربه در این رشته، بسته‌های خدمات پشتیبانی و نگهداری با نام تجاری سانیار را برای عرضه آماده کرده است.

سانیار که در لغت به معنای نگهبان است، همانند خدمات شرکت HP دارای تنوع مناسبی است و متناسب با شرکت‌ها و محصولات موجود در ایران طراحی شده است. سانیار مانند بیمه‌ای برای حداکثر آسودگی خاطر از فعال ماندن تجهیزات حساس HP Server & Storage طراحی شده و الویت این سرویس حذف هرگونه مشکل در تجهیزات و یا به حداقل رساندن زمان حل مشکل است.

مراحل سانیار

۱. در مرحله اول، کارشناس شرکت ایده‌نت برای بازدید سرورها، به شرکت مورد نظر مراجعه و فرم‌های ارزیابی سخت‌افزاری را پر می‌کند. این مرحله، هیچ بار مالی برای شرکت متقاضی در بر نخواهد داشت.

۲. در مرحله دوم، اعضای تیم سانیار با بررسی فرم‌ها، شرایط موجود را جهت ارائه خدمات بررسی می‌کنند.

۳. در مرحله سوم، نوع طرح متناسب با شرایط آن شرکت انتخاب می‌شود.

۴. در مرحله چهارم پیشنهاد سانیار که حاوی توضیحات طرح انتخاب شده، تعهدات شرکت ایده‌نت و هزینه‌های محاسبه شده است، آماده و ارسال می‌گردد.

۵. شرکت متقاضی پس از مطالعه پیشنهاد و رفع ابهامات احتمالی با مشورت با کارشناسان شرکت ایده نت، توافق نهایی خود را اعلام می‌کند.

۶. قرارداد سانیار آماده و برای امضای نهایی ارسال می‌گردد.

انتخاب بهترین طرح خدماتی سانیار

این سرویس دارای سه طرح از پیش تعیین‌شده و یک طرح ویژه و سفارشی است.

طرح نقره‌ای

این سطح از پشتیبانی برای شرکت‌ها و سازمان‌هایی طراحی شده که در محدوده زمانی بیشتری فعالیت می‌کنند. در طرح نقره‌ای خدمات پشتیبانی برای ۱۲ ساعت در ۵ روز هفته (شنبه تا چهارشنبه)، در نظر گرفته شده است. در این طرح، سانیار متعهد می‌شود حداکثر تا ۴ ساعت پس از تماس شرکت تحت پشتیبانی به محل مراجعه و اقدام به رفع مشکل نماید. شرکت‌های تحت پوشش این طرح می توانند هر سال ۴ بار، در صورت بروز حوادث تحت قرارداد با گروه سانیار تماس بگیرند. همچنین به صورت پیش‌فرض، این طرح شامل ۲بار مراجعه کارشناسان سانیار جهت بروزرسانی Firmware سرورها و عملیات PM **Preventive Maintenance** است.

طرح برنزی

طرح برنزی برای شرکت‌ها و سازمان‌هایی آماده شده که در ساعت‌های کاری مرسوم فعالیت می‌کنند. در این طرح خدمات پشتیبانی برای ۹ ساعت در ۵ روز هفته (شنبه تا چهارشنبه)، در نظر گرفته شده است. در طرح برنزی سانیار متعهد می‌شود حداکثر تا ۴ ساعت پس از تماس شرکت تحت پشتیبانی، به محل مراجعه و اقدام به رفع مشکل نماید. شرکت‌های تحت پوشش این طرح می‌توانند هر سال ۳ بار، در صورت بروز حوادث تحت قرارداد با گروه سانیار تماس بگیرند. همچنین به صورت پیش‌فرض، این طرح شامل ۲بار مراجعه کارشناسان سانیار جهت بروزرسانی Firmware سرورها و عملیات PM **Preventive Maintenance** است.

طرح طلایی

این طرح برای شرکت‌ها و سازمان‌هایی با فعالیت‌های حساس و شبانه‌روزی در نظر گرفته شده است. در این طرح، سانیار به صورت شبانه روزی (۷x۲۴) و با زمان پاسخگویی ۲ ساعت پس از اولین تماس، آماده ارائه خدمات است. همچنین این طرح، شامل ۵ بار تماس در سال و ۲ بار مراجعه کارشناسان سانیار جهت بروزرسانیFirmware سرورها و عملیات PM **Preventive Maintenance** است. ویژگی اصلی این طرح، ارسال سرور جایگزین در صورت طولانی‌شدن زمان رفع مشکل و یا انتقال سرور به خارج از شرکت تحت قرارداد در موارد خاص است.

طرح پلاتینیوم

طرح پلاتینیوم یک طرح ویژه است که برای شرکت‌ها و سازمان‌های بسیار بزرگ طراحی شده است. در این طرح شرایط خاص متقاضی پس از بررسی کامل در نظر گرفته می‌شود و پیشنهاد ویژه‌ای برای آن شرایط، آماده و ارائه می‌شود.

سابقه
بیش از دو دهه تجربه در زمینه تامین سرور و تجهیزات شبکه

تیم‌فنی
بهره‌گیری از تیم فنی ماهر و آشنا با فناوری دانش نوین

پشتیبانی
ارائه خدمات پشتیبانی در کوتاه‌ترین زمان با بالاترین کیفیت

آموزش
برگزاری دوره‌های آموزشی درحوزه فناوری اطلاعات

مشاوره
مشاوره در انتخاب سخت‌افزار مناسب و راه‌اندازی آن

فناوری زیرساخت
طراحی و راه‌اندازی مرکز داده سنتی و کانتینری

نرم‌افزار
تولید نرم‌افزار اختصاصی و تهیه برنامه‌های سفارشی

خدمات فنی
ارائه سانیار، نسخه بومی HPE Care Pack

تهران، خیابان مطهری، خیابان فجر، پلاک۳۴، واحد۸

۸۸۴۹۳۰۸۹

۰۲۱-۸۸۴۹۳۱۰۷-۱۰

idehnet

info@idehnetco.com

www.idehnetco.com