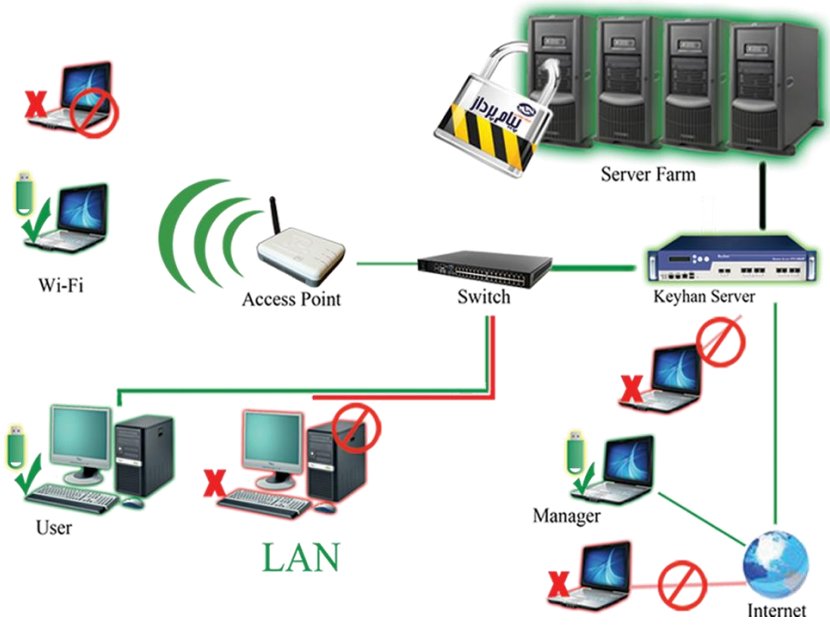
# کیهان

## سامانه امن ساز زیرساخت شبکه

کیهان سامانه‌ای برای امن‌سازی شبکه است که سرویس‌های امنیتی مختلف از قبیل احراز اصالت چند عاملی کاربران، کنترل دسترسی، محرمانگی و صحت اطلاعات مبادله شده، تحلیل ترافیک و قابلیت دسترسی بالا را به صورت شفاف ارایه می‌کند. در این سامانه، سرور کیهان به عنوان دروازه ورودی، جهت کنترل دسترسی به سرورهای حیاتی سازمان ایفای نقش می‌نماید.

از آنجا که کلیه بسته‌های مبادله شده با سرورهای تحت حفاظت، پس از نظارت سرور کیهان اجازه ورود به این شبکه را می‌یابند، این سرور می‌تواند نقش نظارتی و کنترلی ویژه‌ای را برای دسترسی های کاربران در کنار سایر سرویس‌های اصلی اعم از محرمانگی، صحت و احراز اصالت دو عاملی ایفا نماید. این سامانه با پروتکل‌ها، الگوریتم‌ها و توکن‌های امنیتی بومی خود می‌تواند کمک شایانی به پیاده‌سازی استانداردهای امنیتی مطرح نظیر ISO 27001 در سازمانها نماید.






آدرس: تهران، خیابان شریعتی، بالاتر از پل سیدخندان، خیابان شهید مجتبایی، کوچه دایانا، ابتدای کوچه بروجردی، پلاک ۴۴، واحد ۱۰
تلفکس: ۰۲۱-۲۲۸۸۶۶۳۰ کد پستی: ۱۵۴۳۸-۴۳۴۱۴

## مزایای استفاده از سامانه کیهان

- شناسایی و احراز هویت چند عاملی کاربران
- تامین محرمانگی ترافیک شبکه ارتباطی
- تامین صحت ترافیک شبکه ارتباطی
- مولفه های بومی امنیتی (پروتکل، الگوریتم،توکن)
- کنترل دسترسی به منابع حساس شبکه
- تعیین خط مشی استفاده از خدمات شبکه
- ارایه سرویسهای امنیتی بصورت شفاف
- دسترس پذیری بالا
- کنترل اتصال به شبکه
- تفکیک در شبکه‌ها
- انقضای مهلت نشست
- محدود ساختن زمان ارتباط
- کنترل دسترسی به اطلاعات
- جداسازی سیستم‌های حساس کار از راه دور

## ویژگیهای کیهان

### امکان بکارگیری کیهان کلاینت در سکوهای مختلف

- ویندوز
- لینوکس
- اندروید

### احراز اصالت کاربران

- حمایت از پروتکل احراز اصالت اختصاصی شده
- احراز اصالت دوسویه (کاربر برای سرور و سرور برای کاربر)
- حمایت از تکنیکهای احراز اصالت چند عاملی کاربران (*MFA*)
- احراز اصالت مبتنی بر توکن امنیتی سخت افزاری
- احراز اصالت مبتنی بر توکن مجازی
- احراز اصالت بر اساس ارسال *OTP* از طریق *SMS*
- احراز اصالت کاربر بر اساس اثر انگشت (در نسخه اندروید)



آدرس: تهران، خیابان شریعتی، بالاتر از پل سیدخندان، خیابان شهید مجتبایی، کوچه دایانا، ابتدای کوچه بروجردی، پلاک ۴۴، واحد۱۰
تلفکس: ۰۲۱-۲۲۸۸۶۶۳۰ کد پستی: ۱۵۴۳۸-۴۳۴۱۴

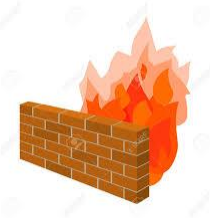
## کنترل دسترسی کاربران

- کنترل دسترسی کاربران و جلوگیری از نفوذ به شبکه سرورهای تحت حفاظت
- امکان تعریف سیاست در سطح گروه و کاربر
- تعریف سیاستهای دسترسی بر اساس *5-Tuples*
- سیاستهای دسترسی پویا و دینامیک

## شبکه اختصاصی مجازی


- محرمانگی و صحت داده‌ها مبتنی بر یک پروتکل تونلینگ اختصاصی در لایه شبکه
- استفاده از الگوریتم‌های رمز و صحت استاندارد و بومی (قابل سفارش توسط مشتری)
- امنیت پروتکل‌های تونلینگ و احراز اصالت با الگوریتم‌های رمز با طول کلید ۲۵۶ بیت
- امکان تعریف LAN های مجازی امن به صورت متمرکز و توزیع شده

## دیواره آتش



- جلوگیری از نفوذ به شبکه سرورهای تحت حفاظت
- کنترل ترافیک عبوری به شبکه تحت حفاظت

## چک سلامتی سیستم کاربر قبل از دسترسی به سرورهای سازمان


- قابلیت تنظیم سیاستهای امنیتی سازمان برای سیستم کاربر قبل از دسترسی به سرورها
- بررسی وضعیت سیستم عامل(نوع و نسخه، تاریخ آخرین بروزرسانی، مجازی/واقعی)
- بررسی وضعیت آنتی ویروس (فعال/غیر فعال، بروز بودن)
- بررسی کاربر (ادمین بودن، عضو دامین بودن)
- بررسی پردازه های سیستم (اجرا یا عدم اجرا سرویس‌ها، برنامه‌های کاربردی یا پروسه‌ها)
- بررسی وضعیت فایروال سیستم کاربر (فعال/غیر فعال بودن)
- بررسی بسته/باز بودن پورتهای *TCP/UDP*
- بررسی وجود یا عدم وجود فایل/فولدر خاص روی سیستم کاربر



آدرس: تهران، خیابان شریعتی، بالاتر از پل سیدخندان، خیابان شهید مجتبایی، کوچه دایانا، ابتدای کوچه بروجردی، پلاک ۴۴، واحد۱۰
تلفکس: ۰۲۱-۲۲۸۸۶۶۳۰ کد پستی: ۱۵۴۳۸-۴۳۴۱۴

## مدیریت از راه دور سیستم کاربران

- امکان اعمال فرمانهای مدیریتی توسط کیهان بر روی سیستم کاربران
- کنترل از راه دور (باز یا بستن کنترل از راه دور سیستم)
- دانلود / آپلود فایل از مسیر مشخص
- حذف، خواندن و نوشتن مقداری در رجیستری

## دسترس پذیری بالا


- قابلیت دسترسی بالا و مقاومت در برابر خرابی
- امکان توزیع بار بر روی چند سرور کیهان
- امکان همگام‌سازی خودکار ما بین سرورهای افزونه کیهان

## تعامل با سامانه های مدیریت رخداد و حوادث امنیتی


- امکان ارسال رخدادهای مربوط به کاربران برای سامانه های *SIEM* (نظیر راوین)
- امکان دستورپذیری از سامانه *SIEM* در راستای قطع فعالیت کاربر
- ارایه گزارشات متنوع تحلیل ترافیک کاربران

## ویژگیهای شبکه ای

- عملکرد شفاف سیستم از دید کاربردها و سرویس‌دهنده‌ها
- پشتیبانی از *NAT* و *DNAT*
- سربار کم ترافیکی نسبت به سایر پروتکل‌های امنیتی مشابه نظیر *IPsec*
- امکان فشرده سازی بسته‌ها
- امکان دستورپذیری از سایر سامانه های امنیتی سازمان مانند *SIEM* در راستای قطع فعالیت کاربر و یا گزارشات متنوع



آدرس: تهران، خیابان شریعتی، بالاتر از پل سیدخندان، خیابان شهید مجتبایی، کوچه دایانا، ابتدای کوچه بروجردی، پلاک ۴۴، واحد۱۰
تلفکس: ۰۲۱-۲۲۸۸۶۶۳۰ کد پستی: ۱۵۴۳۸-۴۳۴۱۴

## مدیریت کاربران

- امکان گروهبندی کاربران
- امکان تعیین زمان کار، تاریخ و ساعت انقضا برای کاربران
- امکان محدود کردن کاربر برای کار بر روی کامپیوتر خاص و یا بازه‌ای از *IP*ها
- امکان تفویض اختیارات مدیر در سامانه به مدیران میانی

## مدیریت سیاستها

- امکان تعریف سیاست‌های امنیتی و قوانین کنترل دسترسی برای هر کاربر
- امکان تعریف سیاست‌های امنیتی و قوانین کنترل دسترسی برای گروههای کاربران
- امکان گروه‌بندی سیاست‌های امنیتی


## مدیریت رخدادها

- رویدادنگاری از ورود و خروج کاربران
- رویدادنگاری از تراکنش‌های انجام گرفته توسط مدیران سیستم
- امکان ارسال رویدادها به سیستم رویدادنگاری *Syslog Server* و مانیتورینگ سیستم (*SNMP*)


## بروزرسانی خودکار

- امکان به‌روز رسانی خودکار نرم‌افزار کاربری

## گزارشات تحلیلی از رویدادهای اتصالی و دسترسی‌های کاربران

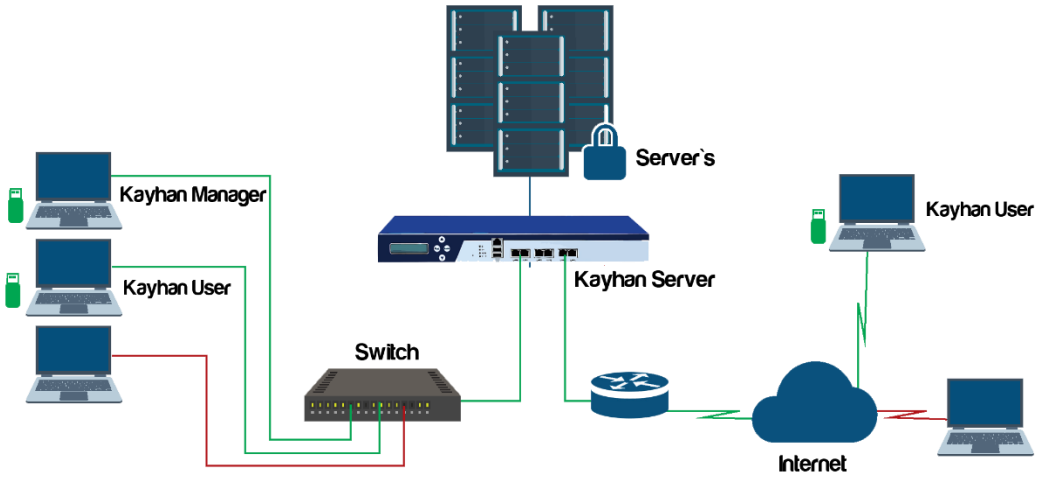
- گزارش از میزان دسترسی کاربران به سرورهای تحت حفاظت با ریزدانگی دقیقه، ساعت و روز با امکان فیلترگذاری بر روی کاربران
- گزارش از دسترسی به سرورهای تحت حفاظت کیهان توسط کاربران با ریزدانگی دقیقه، ساعت و روز
- گزارش از ۱۰ کاربری که بیشترین ترافیک را مبادله کرده‌اند (*Top 10 users*)



آدرس: تهران، خیابان شریعتی، بالاتر از پل سیدخندان، خیابان شهید مجتبایی، کوچه دایانا، ابتدای کوچه بروجردی، پلاک ۴۴، واحد۱۰
تلفکس: ۰۲۱-۲۲۸۸۶۶۳۰ کد پستی: ۱۵۴۳۸-۴۳۴۱۴

- گزارش از ۱۰ سروری که بیشترین ترافیک با آنها مبادله شده (*Top 10 servers*)
- گزارش از میزان کل پهنای باند مصرفی سیستم
- گزارش از پروتکل‌ها و پورت‌های پر استفاده سیستم
- امکان *Export* کلیه نمودارها و جداول مشاهده شده

## کاربردهای کیهان




کیهان در کاربردهای مختلفی مورد استفاده قرار میگیرد. متداولترین این کاربردها عبارتست از :

- ارتباط امن با سرورهای سازمان توسط کاربران راه دور (فرایند دورکاری امن)
- برقراری ارتباط امن بین کامپیوترها در دفاتر نمایندگی یک سازمان و سرورهای ساختمان مرکزی
- امن‌سازی کاربردهای تحت شبکه سازمان از قبیل اتوماسیون اداری
- امن‌سازی ارتباط *Remote Desktop* مشتریان با سرورهای اختصاصی خود در مراکز داده
- امکان ایجاد یک شبکه مجازی ایزوله و امن (*VLAN*) برای بخش‌های حساس سازمان مثل حراست
- امن‌سازی ارتباط بین کامپیوترهای کاربران با مدیریت متمرکز و یا با مدیریت توزیع شده
- تأمین امنیت بستر شبکه‌های بی‌سیم



آدرس: تهران، خیابان شریعتی، بالاتر از پل سیدخندان، خیابان شهید مجتبایی، کوچه دایانا، ابتدای کوچه بروجردی، پلاک ۴۴، واحد۱۰
تلفکس: ۰۲۱-۲۲۸۸۶۶۳۰ کد پستی: ۱۵۴۳۸-۴۳۴۱۴

# اجزای سامانه کیهان

## سامانه سرور کیهان

کیهان در مدلهای مختلف با ویژگیهای سخت افزاری مجزا و نرخهای گذردهی متفاوت ارایه میشود

## نرم افزار کلاینت کیهان

نرم افزار کلاینت کیهان بر سکوهای مختلف ویندوز، لینوکس و اندروید قابل نصب و استفاده میباشد

## نرم افزار مدیریت کیهان

بمنظور مدیریت کاربران و تعریف سیاستهای مختلف امنیتی و تنظیمات شبکه ای و سیستمی استفاده میشود

## سامانه تحلیل ترافیک کیهان


این سامانه بمنظور مدیریت رویداد و تحلیل ترافیک شبکه تحت حفاظت کیهان استفاده میشود



آدرس: تهران، خیابان شریعتی، بالاتر از پل سیدخندان، خیابان شهید مجتبایی، کوچه دایانا، ابتدای کوچه بروجردی، پلاک ۴۴، واحد۱۰
تلفکس: ۰۲۱-۲۲۸۸۶۶۳۰ کد پستی: ۱۵۴۳۸-۴۳۴۱۴