معرفی سیستم امن‌سازی شبکه کیهان

اصغر نعمتی

مدیرخدمات پس از فروش شرکت پیام پرداز

nemati@payampardaz.net

دیماه ۱۳۸۸

نیازهای امنیتی در کاربردهای تحت شبکه

- محرمانگی
  - ✓ عدم امکان دسترسی به محتوای اطلاعات مبادله شده (Sniffing)
- صحت
  - ✓ عدم امکان تغییر یا دستکاری اطلاعات مبادله شده (Spoofing, Modification)
- عدم اطمینان به سرویس‌های امنیتی موجود در سیستم عامل برای کاربردهای حساس
  - ✓ IPSec
  - ✓ SSL

نیازهای امنیتی در کاربردهای تحت شبکه

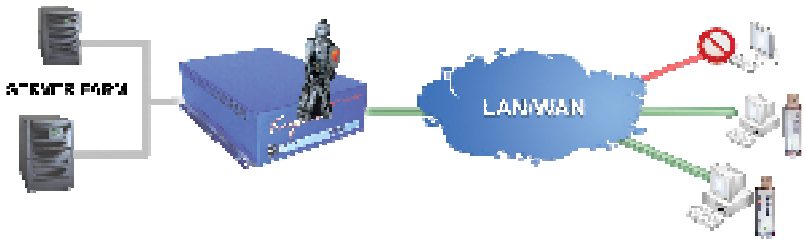
- احراز اصالت کاربران
  - ✓ برطرف کردن ضعف روشهای یک عاملی (مبتنی بر نام کاربر و کلمه عبور)
    - کاربران در انتخاب کلمه عبور ، موارد امنیتی را رعایت نمی‌کنند.
    - کاربران در حفظ کلمه عبور دقت نمی‌کنند.
    - کلمه عبور کاربر (و حتی مدیر شبکه) ممکن است لو برود
- کنترل دسترسی کاربران
  - ✓ کاربران سطوح دسترسی و اهمیت متفاوتی دارند.
    - دسترسی به سرورها
    - دسترسی به برنامه‌های کاربردی

سایر نیازها

- عدم بهره‌مندی عموم از دانش امنیت
  - ✓ پیکربندی سرورها برای ایجاد امنیت پیچیده است.
  - ✓ پیکربندی کامپیوترهای کاربران برای ایجاد امنیت کاری دشوار است و کاربران ممکن است اطلاعات کافی در این زمینه نداشته باشند.
- تغییرات شبکه
  - ✓ شبکه کاربران مداوم تغییر می‌کند.
  - ✓ کاربران ممکن است از هر جایی بخواهند با شبکه کار کنند
- مدیریت متمرکز
  - ✓ در امن‌سازی یک شبکه، مدیریت متمرکز کلیه کاربران مهم است.

یک راه حل برای رفع کلیه نیازهای فوق

سیستم کیهان



سرویس‌های امنیتی کیهان

- احراز اصالت
  - ✓ دوسویه
  - ✓ دوعاملی
- کنترل دسترسی کاربر
- جلوگیری از نفوذ به شبکه تحت حفاظت
  - ✓ فایروال قوی
- محرمانگی و صحت اطلاعات مبادله شده
  - ✓ با ایجاد تونل امنیتی در لایه IP (سرویس VPN)

اجزای سیستم کیهان

- دستگاه سرویس دهنده کیهان
- نرم‌افزار کاربر
- نرم‌افزار مدیریت
- ماژول سخت‌افزاری کیا
  - ✓ کیای کاربر
  - ✓ کیای مدیر
  - ✓ کیای سرور

www.payampardaz.net

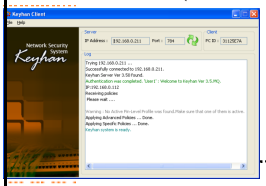
دستگاه Keyhan Server

- نرم‌افزار سرور کیهان بر روی یک کامپیوتر صنعتی
- پایگاه داده امن حاوی اطلاعات کاربران، سیاستهای امنیتی و ...
- قرارگیری در نقطه ورودی شبکه تحت حفاظت
- فرایندهای امنیتی
  - ✓ فایروال
  - ✓ احراز اصالت کاربران
  - ✓ کنترل دسترسی کاربران
  - ✓ VPN
    - یک طرف تونل امنیتی (رمزنگاری و درهم‌سازی داده‌های مبادله شده)

www.payampardaz.net

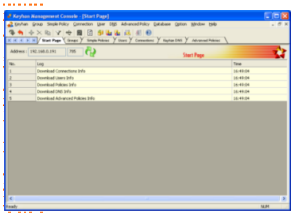
نرم‌افزار کاربر (Keyhan Client)

- پروتکل احراز اصالت و توافق کلید با دستگاه Keyhan Server
  - ✓ دوعاملی
    - ماژول کیای کاربر
    - PIN دریافتی از کاربر
  - ✓ دوسویه
- دریافت سیاست‌های امنیتی تعریف شده برای کاربر از دستگاه Keyhan Server و اعمال آنها
- سرویس VPN
  - ✓ طرف دیگر تونل امنیتی (رمزنگاری و درهم‌سازی داده‌های مبادله شده)



نرم‌افزار مدیریت (Management Software)

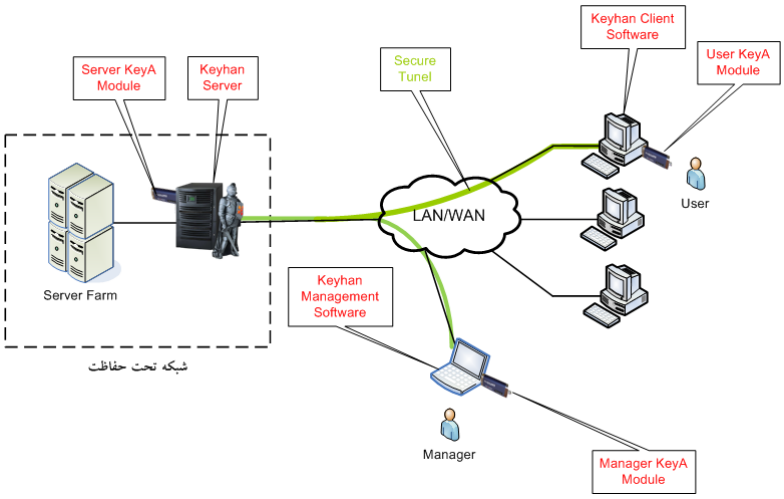
- احراز اصالت مدیر
  - ✓ به وسیله ماژول کیای مدیر
- ارتباط امن و حفاظت شده با دستگاه Keyhan Server
- تعریف و تنظیم سیستم
  - ✓ گروه‌ها
  - ✓ سیاست‌های امنیتی
  - ✓ کاربران
- برنامه‌ریزی ماژولهای کاربران



ماژول امنیت کیا

- کیای سرور
  - ✓ کلید رمز پایگاه داده
  - ✓ کلید احراز اصالت مدیر
- کیای مدیر
  - ✓ کلید احراز اصالت مدیر
  - ✓ کلید رمز پایگاه داده
  - ✓ آدرس IP دستگاه Keyhan Server
- کیای کاربر
  - ✓ ID کاربر
  - ✓ کلید احراز اصالت کاربر
  - ✓ آدرس IP دستگاه Keyhan Server

معماری امن‌سازی ارتباط Client-Server



ویژگیهای کاربری

- ✓ سادگی نصب و راه‌اندازی
- ✓ شفافیت عملکرد
  - عدم نیاز به تغییر در کاربردهای شبکه
- ✓ سادگی کار کاربران و عدم نیاز به آموزش‌های خاص
- ✓ قابلیت جابجایی کاربران در شبکه
- ✓ امکان محدود کردن کاربر برای کار بر روی یک کامپیوتر خاص یا یک دامنه خاص

ویژگیهای مدیریتی

- ✓ مدیریت متمرکز کاربران
- ✓ امکان تعریف کلیه کلیدهای امنیتی سیستم توسط مدیر
- ✓ امکان مشاهده رویدادهای مربوط به ورود و خروج کاربران
- ✓ امکان تعریف نام برای سرورهای تحت حفاظت بجای آدرس IP (DNS داخلی)
- ✓ اجرای برنامه مدیریت از هر نقطه شبکه

ویژگیهای شبکه‌ای

- ✓ پشتیبانی از NAT و PAT
  - ✓ قرارگیری کاربر در داخل NAT
  - ✓ قرارگیری سرور پشت PAT
- ✓ امکان تعریف LANهای مجازی امن به صورت متمرکز و توزیع شده
- ✓ قابلیت دسترسی بالا و مقاومت در برابر خرابی با امکان توزیع بار بر روی چند سرور کیهان
- ✓ امکان استفاده از آدرس مجازی برای سرورها و سرور کیهان برای حفاظت بیشتر
- ✓ ارائه سرویس ورود یک باره (Single Sign On)

برتری‌های کیهان نسبت به VPN Clientها

- ✓ امنیت بالاتر
- ✓ امکان تعریف سیاست‌های امنیتی مجزا برای کاربران
- ✓ سربار کمتر بسته‌ها در شبکه (سرعت بیشتر)
- ✓ عبور از NAT وPAT
- ✓ امکان ارتباط امن بین کامپیوترهای کاربران (با مدیریت متمرکز یا توزیع شده)
- ✓ امکان تخصیص IP مجازی اختصاصی برای هر کاربر (ارایه سرویس SSO)
- ✓ تکنولوژی بومی
- ✓ امکان اختصاصی سازی با استفاده از الگوریتم های سفارشی

موارد استفاده وسیع از کیهان

- امن‌سازی ارتباط دفاتر خدمات ارتباطی با مرکز شبکه شرکت ارتباطات سیار
- امن‌سازی ارتباط شعب و ادارات بیمه البرز
- امن‌سازی ارتباط دفاتر پلیس +۱۰
- امن‌سازی سرویس استعلام سازمان ثبت احوال کشور

www.payampardaz.net