

روش نوین و امن جداسازی اینترنت از شبکه داخلی

موضوع جداسازی شبکه اینترنت از شبکه داخلی (اینترنت) از جمله موضوعات امنیت اطلاعات می باشد که در دهه اخیر مورد توجه سازمان ها و نهادهای نیازمند به ضریب امنیت بالا قرار گرفته است. پس از حمله ویروس STUXNET به صنایع و مراکز کنترلی به ویژه نیروگاه ها ضرورت ایزوله کردن رایانه ها از فضای عمومی اینترنت بیش از پیش در دستور کار سازمان ها و در رأس آنها مدیران فناوری اطلاعات کشور قرار گرفت. لیکن به دلایلی مانند عدم وجود یک استراتژی یکپارچه و همچنین هزینه های مضاعف راه اندازی و پشتیبانی شبکه های ایزوله موازی و یا استفاده از نرم افزارهای مجازی سازی غیر امن خارجی، دستیابی به این مهم محقق نگردیده است. تا اینکه کشف ویروس (بد افزار) FLAME پس از دو سال فعالیت پنهان در شبکه عملیاتی وزارت خانه ها هشدار جدی محسوب شد و وجود ضعف در تأمین امنیت فضای سایبری کشور را بیش از پیش نمایان ساخت.

در حال حاضر با توجه به نیاز ملی و بخشنامه های اجرایی تنها راه حفظ امنیت اطلاعات در برابر تهدیدهای اینترنتی، جداسازی شبکه امن داخلی سازمان ها به صورت کاملاً فیزیکی از فضای اینترنت می باشد. کارت امن افزار اینترنت بدون نیاز به خرید رایانه های جدید و نیز کابل کشی مجدد شبکه، دسترسی به هر دو محیط داخلی و اینترنت را به صورت امن و ایزوله از یکدیگر بر روی یک رایانه فراهم می آورد. این کارت در قالب یک کارت PCIe به سیستم کاربر اضافه شده و نقش یک رایانه مستقل و ایزوله را ایفا می کند. بدین ترتیب کاربران یک سازمان در امنیت کامل به هر دو شبکه داخلی و اینترنت دسترسی خواهند داشت.

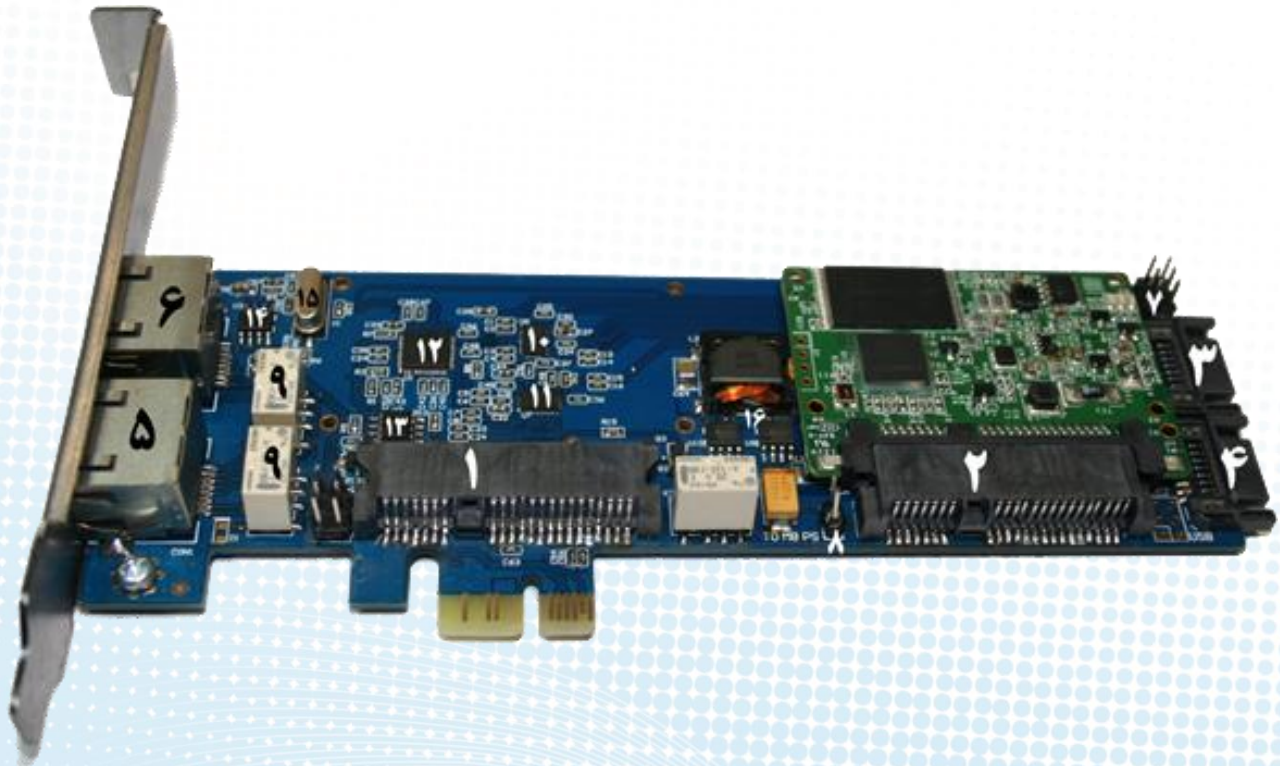
طراحی و تولید کارت امن افزار اینترنت ایرانی بوده و تمام معیارهای امنیتی در آن لحاظ شده است. این سخت افزار مشابه داخلی یا خارجی ندارد، همچنین دارای **گواهینامه تأییدیه بهره برداری از سازمان پدافند غیر عامل کشور** در زیر ساخت های سطوح ۱ تا ۴ (زیر ساخت های حساس) و **گواهینامه سطح بلوغ امنیتی از مرکز تحقیقات صنایع انفورماتیک** می باشد.

امن افزار اینترنت

امن افزار اینترنت از دو تجهیز اصلی تشکیل شده است:

۱،۱- کارت امن افزار PCIe نسخه ۱

این کارت بر روی برد اصلی Motherboard سیستم کاربران نصب می گردد و هر دو شبکه به صورت کابلی با مبدل کابل ایزوله شبکه به آن متصل می گردند. در این حالت هر دو شبکه در سرعت 100Gbps قابل استفاده خواهند بود.



۱،۲- کارت امن افزار PCIe نسخه ۲

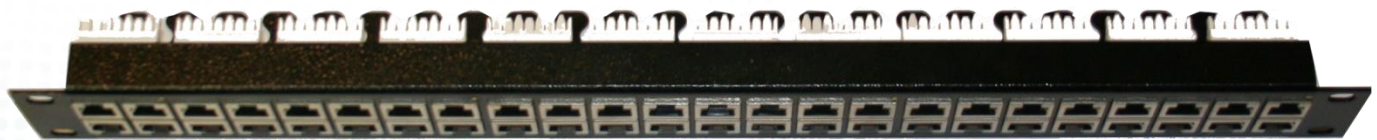
کارت امن افزار نسخه ۲ دارای قابلیت شبکه بی سیم برای یکی از شبکه ها می باشد. لذا در صورت بهره گیری از این قابلیت شبکه دیگر در سرعت 1Gbps قابل استفاده می باشد.



۲،۱- پنل ایزوله شبکه (جداسازی فیزیکی شبکه کارت نسخه ۱)

این پنل در ابعاد استاندارد طراحی شده و در رک شبکه دسترسی کاربران با Patch Panel های معمولی تعویض می گردد.

این پنل برای سایت های در حال ساخت و سایت هایی که امکان تعویض پنل امکانپذیر است پیشنهاد می گردد.



۲،۲- کابل ایزوله شبکه (جداسازی فیزیکی شبکه کارت نسخه ۱)

برای سایت هایی که تعویض پنل امکانپذیر نیست و یا کابل کشی شبکه دوم انجام شده است به جای استفاده از پنل ایزوله امکان بهره گیری از کابل شبکه ۲ به ۱ ایزوله نیز وجود دارد.

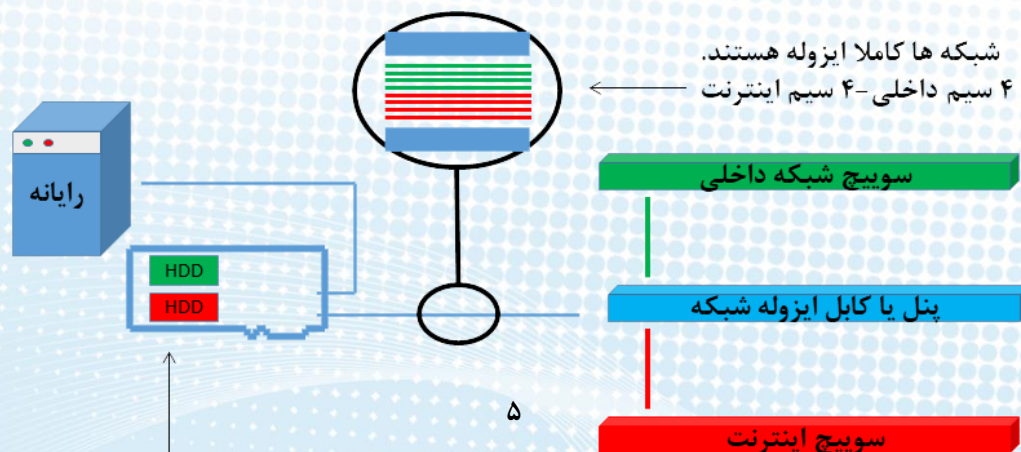


نحوه عملکرد کارت امن افزار اینترنت

پس از نصب کارت بر روی برد اصلی رایانه (Motherboard)، لازم است کابل دیتای هارددیسک رایانه به کارت متصل گردد. همچنین مطابق شکل زیر کابل شبکه منتهی به پنل ایزوله به جای اتصال به کارت شبکه رایانه به پورت شبکه اول این کارت و از پورت دوم توسط یک کابل شبکه کوتاه به کارت شبکه رایانه متصل می گردد.

هم اکنون رایانه کاربر به دو شبکه کاملاً ایزوله دسترسی دارد و همچنین مجهز به دو هارددیسک مستقل می باشد. در هر وضعیت؛ یک شبکه، یک هارددیسک و یک ماژول SSD به رایانه کاربر متصل می باشد و ارتباط شبکه، هارددیسک و ماژول SSD دوم به صورت فیزیکی از رایانه کاملاً قطع است.

کلید پاور کیس تعیین کننده وضعیت می باشد؛ بدین صورت که در هنگام روشن نمودن رایانه در صورتی که به صورت معمول فشرده شود، سیستم در وضعیت اول (شبکه داخلی) و در صورتی که ۲ بار متوالی فشرده شود، سیستم در وضعیت دوم (شبکه اینترنت) راه اندازی می شود. در هر بار راه اندازی، رایانه به صورت کامل خاموش و مجدد روشن می گردد؛ بنابراین اطلاعات و بد افزارهای احتمالی بار شده در حافظه (RAM) رایانه به صورت کامل پاک می شوند، بدین ترتیب هیچ نوع ارتباطی بین دو محیط وجود ندارد. نمایشگر LED کیس نیز نشان دهنده وضعیت فعال می باشد. (ثابت: شبکه داخلی / چشمک زن: شبکه اینترنت)



اطلاعات در دو هارددیسک کاملاً ایزوله ذخیره می گردند.

مشخصات

- ✓ ایجاد دو محیط (اطلاعات و شبکه) ۱۰۰٪ ایزوله به صورت کاملاً فیزیکی بر روی یک دستگاه
- ✓ عدم نیاز به نرم افزار جانبی
- ✓ عدم وابستگی به MAC و IP دستگاه
- ✓ استفاده از زیر ساخت موجود شبکه (استاندارد EIA/TIA 568B)
- ✓ قابلیت ترکیب با سایر روش های امنیت شبکه

مزایا

- ✓ عدم نیاز به کابل کشی مجدد شبکه (کاهش هزینه)
- ✓ عدم نیاز به رایانه دوم (کاهش هزینه)
- ✓ عدم امکان دسترسی غیرمجاز از طریق جابجایی کابل شبکه توسط کاربر
- ✓ عدم نشت اطلاعات هارددیسک داخلی در وضعیت اینترنت به دلیل مدیریت کابل Data هارددیسک به جای کابل Power
- ✓ عدم خرابی هارددیسک به دلیل مدیریت کابل Data هارددیسک به جای کابل Power
- ✓ تغییر وضعیت کار از اینترنت به اینترنت (شبکه داخلی) در کمتر از یک دقیقه
- ✓ استفاده از هارددیسک های سرعت بالا (SSD) بر روی برد جهت افزایش ۳ تا ۵ برابری سرعت سیستم عامل
- ✓ امکان مدیریت درگاه USB (بر اساس سفارش کاربر)
- ✓ امکان استفاده از ۴ عدد هارددیسک یا DVD-Drive علاوه بر درگاه های SATA بر روی Motherboard
- ✓ امکان غیر فعال سازی درایو لوح فشرده در حالت شبکه داخلی
- ✓ نصب و راه اندازی سریع و آسان
- ✓ هزینه پایین و مقرون به صرفه در مقایسه با سایر روشها

جداسازی شبکه اینترنت به صورت کاملاً فیزیکی + سرعت در تغییر وضعیت + هزینه مقرون به صرفه = امن افزار اینترنت

مزایای امن افزار اینترنت نسبت به ایزولاتور شبکه

- ۱- استفاده از درگاه PCIe
کارت امن افزار اینترنت به صورت مستقیم بر روی مادر برد رایانه نصب می گردد، لذا نیازمند کابل های اضافی ارتباطی نمی باشد. همچنین از سرعت و امنیت بالاتری برخوردار است.
- ۲- حذف پنل جلوی کیس
یکی از محدودیت های ایزولاتور شبکه، پنل تغییر وضعیت می باشد که به علت گوناگونی کیس ها نصب آن با مشکل مواجه می گردد. کارت امن افزار اینترنت از کلید پاور استفاده می نماید و نیازی به پنل ندارد.
- ۳- کنترل بر اطلاعات (Data Bus) به جای کنترل بر پاور هارددیسک ها
در کارت امن افزار اینترنت اطلاعات دو شبکه با کنترل بر گذرگاه اطلاعات ایزوله می گردند که بسیار امن تر از کنترل بر منبع تغذیه هارددیسک ها می باشد. همچنین یکی از دلایل خرابی در ایزولاتور شبکه و یا هارددیسک های متصل به آن قطع و وصل مکرر پاور سویچ و رله های به کار رفته در آن می باشد که این مشکل در کارت امن افزار اینترنت برطرف شده است.
- ۴- عدم نیاز به کابل کشی مجدد شبکه و استفاده از پنل ایزوله شبکه
ایزولاتور شبکه دارای دو ورودی کابل شبکه می باشد لیکن می بایست هر دو شبکه به صورت مستقل کابل کشی شوند. در صورت استفاده از پنل ایزوله شبکه که به همراه کارت امن افزار اینترنت ارائه می گردد نیازی به کابل کشی شبکه دوم نیست و توسط پنل ایزوله هر دو شبکه منتقل می گردند.
- ۵- عدم امکان جابجایی کابل شبکه توسط کاربر
کارت امن افزار اینترنت دارای یک ورودی کابل شبکه می باشد، لذا کاربر اختیاری در جابجایی کابل های شبکه ندارد.
- ۶- سرعت بسیار بالا هنگام سویچ بین شبکه ها
به علت استفاده از تکنولوژی SATA III و حافظه های SSD سرعت تغییر وضعیت (از شبکه داخلی به اینترنت) نسبت به ایزولاتور شبکه بسیار بالا و میانگین بین ۲۰ تا حداکثر ۶۰ ثانیه می باشد.
- ۷- پشتیبانی از ۴ هارددیسک یا درایو نوری SATA و SSD
کارت امن افزار اینترنت از ۲ هارددیسک SATA III و ۲ ماژول SSD پشتیبانی می نماید و ایزولاتور شبکه فقط از دو هارددیسک SATA.

گواهینامه ها

- گواهینامه ثبت اختراع
- گواهینامه سطح A بلوغ امنیتی مرکز صنایع انفورماتیک ایران
- گواهی نامه تأیید بهره برداری از سازمان پدافند غیر عامل
- گواهی نامه سازمان فناوری اطلاعات (افتا) - در مرحله آزمایشگاه



وزارت دفاع و پشتیبانی نیروهای مسلح



جمهوری اسلامی ایران



سازمان پدافند غیر عامل کشور

تاریخ صدور: ۹۷/۱۲/۱۰

تاریخ اعتبار: ۹۸/۱۲/۱۰

شماره تأییدیه: ۹۴۰۶-۰۷-۰۱

گواهی نامه تأیید بهره برداری از نیروهای مسلح

مدیر عامل محترم شرکت بهینه پرداز شکوفا

با استناد به ماده ۱۰ اساسنامه سازمان پدافند غیر عامل کشور و وظیفه ناشی از تبصره بند یکم از بخش ۴ مصوبه شماره ۱۲۷/۱۲۰/۴۰۰ مورخ ۹۲/۴/۵ کمیته دائمی پدافند غیر عامل کشور، صلاحیت بهره برداری از سامانه چراغ راهنما با نام تجاری امن افزار شرکت آن به شماره ثبت ۴۳۶۰۸۱ مورد تأیید می باشد.

لذا به آن شرکت اجازه داده می شود از تاریخ صدور مجوز به مدت یک سال از محصول خود در راستای ارتقاء امنیت، ایمنی و پایداری زیرساخت های حساس کشور با تأکید بر حضور نماینده قرارگاه پدافند سایبری کشور در زمان نصب و راه اندازی سامانه، بهره برداری نماید.

رییس سازمان پدافند غیر عامل کشور

رتیب پاسدار دکتر غلامرضا جلالی



