« **امنیت** »

تعریف

امنیت در شبکه های کامپیوتری مجموعه ای از روالها می باشد که دسترسی به اطلاعات را از نظر فیزیکی و سطح دسترسی به کامپیوترها و عبور داده ها در شبکه تعیین می نمایند. بدیهی است در صورتیکه که هر یک از عوامل گفته شده نادیده گرفته شوند می توانند منجر به بروز خسارات گردند. این خسارات می‌تواند شامل از بین رفتن اطلاعات و یا سرقت اطلاعات باشد. بنابراین در پیاده سازی سیستم ها بایستی حتماً نکات امنیتی در نظر گرفته شوند. در ادامه سعی می‌گردد تا امنیت در سطوح مختلف تعریف و نحوه بکارگیری آن گفته شود.

سطوح امنیتی

امنیت را می توان در چهار رده زیر دسته بندی نمود :

١- دسترسی فیزیکی

٢- امنیت Client ها و سرورها

٣- امنیت در شبکه های LAN

٤- امنیت در شبکه های متصل به اینترنت یا اینترنت ها

١- دسترسی فیزیکی

در صورتیکه سرور و یا workstation دارای اطلاعات محرمانه ای باشد و یا سرورهائی که به عنوان هسته شبکه انجام خدمات زیادی را انجام می دهند در نظر بگیریم دسترسی به این گونه دستگاهها بایستی محدود و مشخص باشد و فقط اشخاص معینی مجاز به این باشند که بتوانند به این کامپیوترها داشته باشند دسترسی و در صورتیکه اطلاعات خیلی مهم باشد حتماً بایستی مسئولین سیستم ها در این هنگام حضور داشته باشند (مثلاً در هنگام Update و نصب نرم‌افزارهائی بروی سیستم).

٢- امنیت Client ها و سرورها

در این محدوده علاوه با در نظر داشتن بند قبلی بایستی انواع خطراتی که ممکن است اطلاعات موجود بروی دستگاه را به مخاطره می اندازد را محافظت نمود. در این جا بایستی خطرات احتمالی را شناسائی

و از آنها جلوگیری نمود این خطرات در ٤ حالت زیر ممکن است رخ دهد :

۲-۱- SPY Ware : ارسال اطلاعات موجود بروی کامپیوتری دیگر

۲-۲- IP-Spoofing : ایجاد هویت جعلی در سطح IP

۲-۳- Port-Scanning : شناسائی درگاههای باز

۲-٤- Denial – of – Service (DOS)

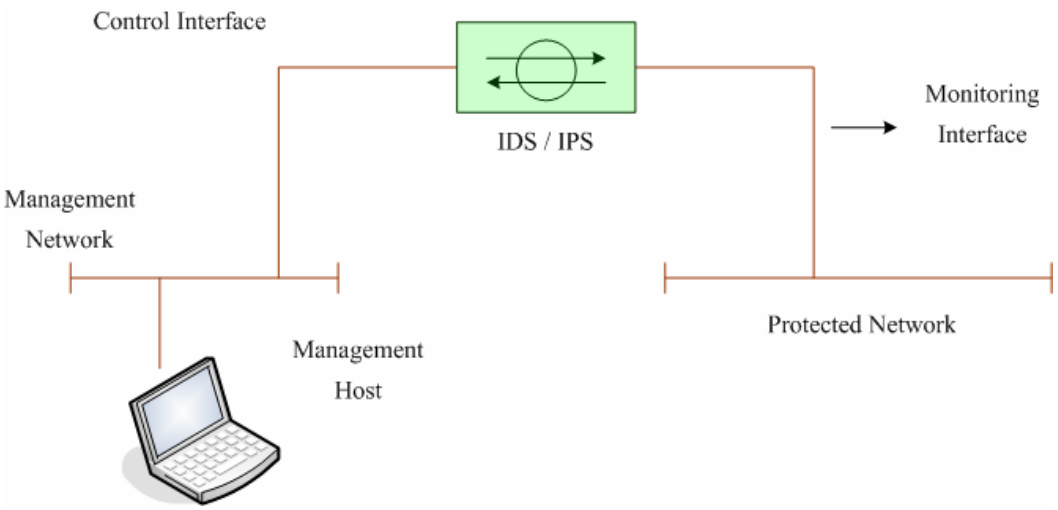
جهت جلوگیری از هر کدام از موارد فوق بایستی نرم افزارهای مناسب بروی سرور نصب باشد تا دستگاه از هر گونه تهدیدی در آن باشد. در این جا بایستی از نرم افزار Anti SPY ware برای جلوگیری از خطر SPY ware و HIDS با جلوگیری از نفوذ به سیستم و هم چنین از Firewall Client مناسب جهت دسترسی به پورت های مجاز استفاده نمود.

۳- امنیت در شبکه LAN

در شبکه های LAN می توان تمهیداتی را در نظر گرفت تا جلو خطرات احتمالی از سوی سایر سیستم‌ها را به یکدیگر به حداقل رساند. برای مثال استفاده از یک SPY ware که بروی سرور نصب می‌شود و Client ها را به صورت اتوماتیک به روز می رساند و یا استفاده از IDS ها و گونه جدیدتر آنها IPSها. در یک شبکه LAN می توان IPS یا IDS را بصورت سخت افزاری در دل شبکه قرارداد و با تنظیم آن از بسیاری از خطرات جلوگیری نمود.

در حالتی که IPS / IDS بکار گرفته می توان و دو سناریو را می توان در نظر گرفت.

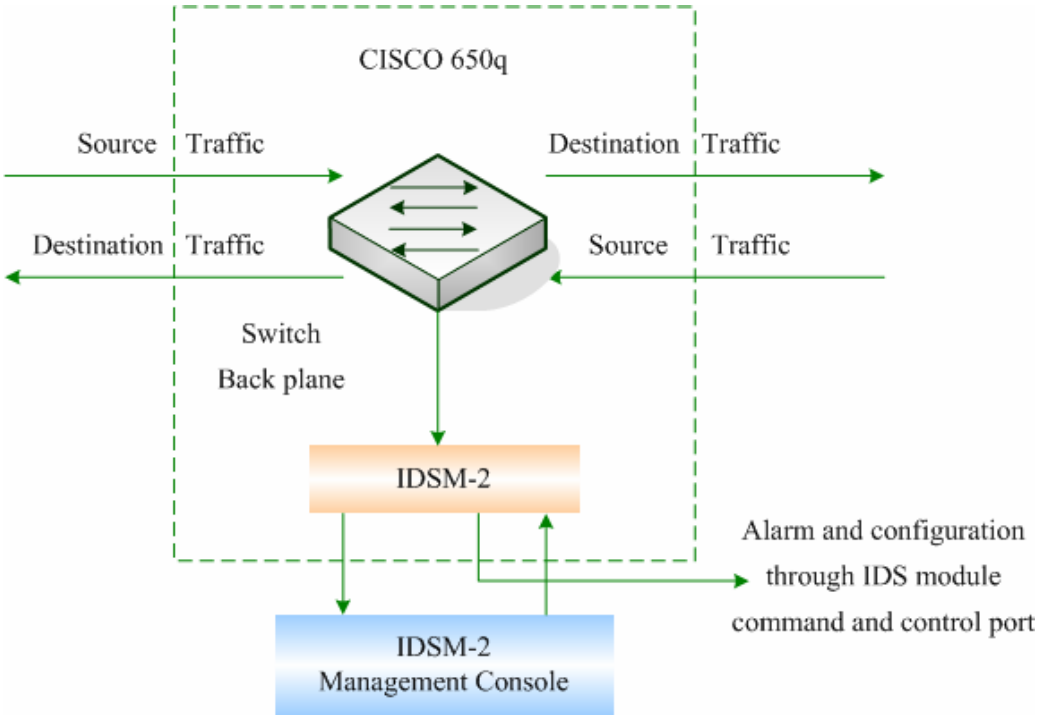
۳-۱- استفاده از Box (IDS) که به شکل زیر بکار گرفته می شود.



۳-۲- استفاده از یک ماجول سخت افزاری که در داخل سوئیچ Core و Distribution شبکه نصب می‌شود و تمامی Packet ها را چک می کنند که در صورت امکان بسیار روش مناسب می‌باشد.

نمونه این، جول، ماجول IDSM-2 می باشد که بعنوان یک ماجول در داخل یکی از اسلاتهای سوئیچ 650X سیسکو قابل بکارگیری می باشد.

در این حالت بلوک دیاگرام شکل زیر را خواهیم داشت :



در این حالت IDSM-2 چون به backplane متصل می باشد تمامی pattern ها را برای یافتن تطبیق از جدول signature های خود جستجو می کند که این جستجو شامل بخش Header و data می باشد. زیرا این جملات یا براساس Content و یا Context می تواند رخ دهد.

می توان IPS / IDS را طوری تنظیم نمود که در صورت وقوع حمله اقدام به ارسال هشدارهائی نماید و یا TCP-reset بفرستید و یا log ایجاد نماید و یا حتی اقدام به ایجاد یک دستور block بروی سایر دستگاهها نیز روترها و یا فایروالها بنماید.

٤- امنیت در اینترنت و اینترانت ها

علاوه بر تمامی نکات ذکر شده در بندهای قبلی جهت ایجاد یک محیط امن و مطمئن در یک شبکه که به شبکه های دیگری متصل می باشد نکات بسیار ظریف تر و دقیق تری نیز وجود دارد که بایستی بدقت بررسی و اجرا و همیشه زیر نظر باشند. در این جا سه مقوله مهم وجود دارد که بایستی حتماً و به دقت زیر نظر باشد :

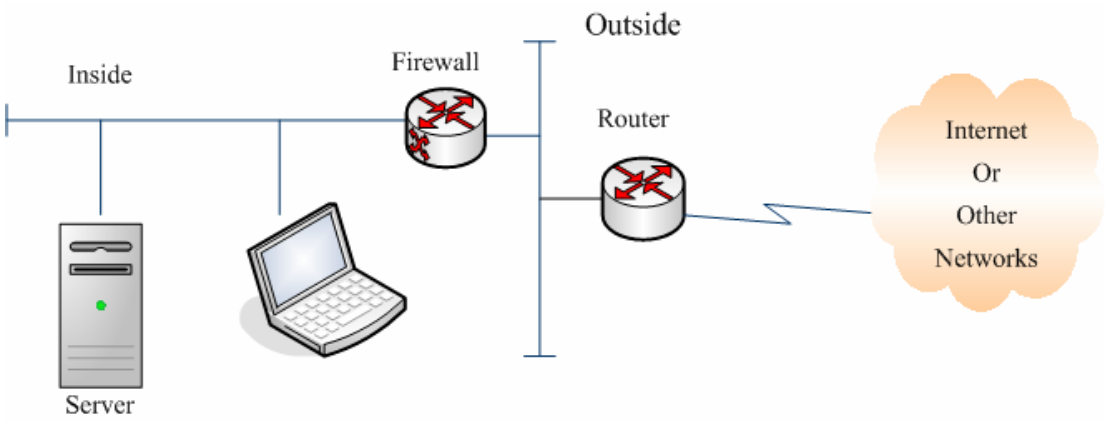
1- Monitoring
2- Firewall
3- IDS / IPS

٤-١- مانیتورینگ به معنای در اختیار داشتن تمامی Log هائی است که از طریق ابزارهائی نظیر فایروال و IDSها ، سرورهای وب، سرورهای Mail، سرورها و شبکه ایجاد می شوند. در اختیار داشتن نرم‌افزاری که قادر به تحلیل و ارائه گزارش های مطلوب از این Logها باشند توانائی مدیران شبکه را جهت بررسی و دسترسی به منابع داخل شبکه و همین طوراطلاعات ارسال شده به خارج از شبکه بسیار بهبود می بخشد.

٤-٢- فایروال

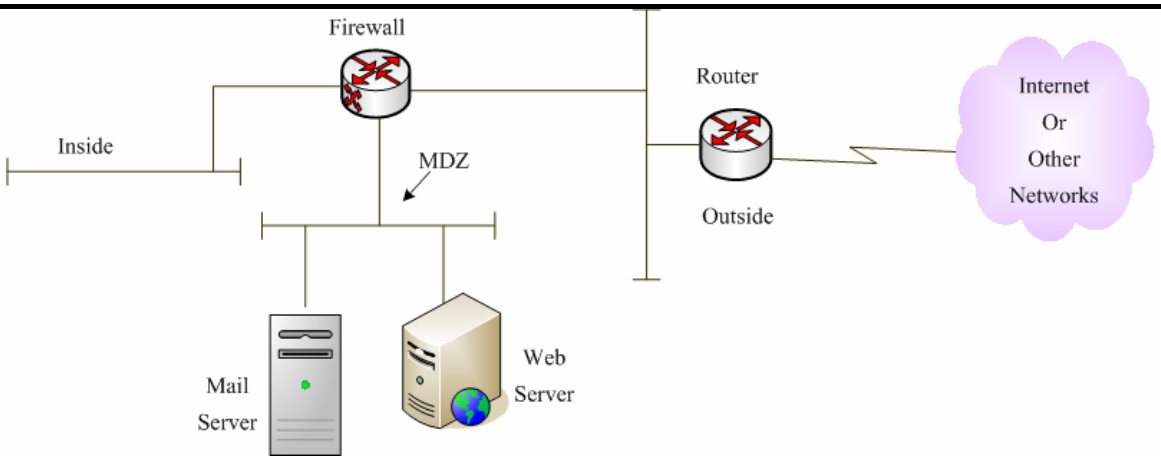
در هنگامی که شبکه بایستی به شبکه دیگری متصل باشد بخصوص اینکه اتصال از طریق مسیرهای ناشناخته باشد و یا کاربران شبکه مقابل تهدیدی جهت امنیت شبکه به حساب آیند در اینصورت دسترسی به منابع داخل شبکه و پورت های سرورهای مهم شبکه و پرتوکل های مورد نیاز بایستی بسیار دقیق انجام پذیرد و Log مربوط به فایروال نیز در جائی نگهداری و توسط ابزارهای مانیتورینگ بررسی گردند.

نحوه بکارگیری فایروال در شبکه بسیار مهم می باشد در ساده ترین حالت شکل زیر می باشد :



در این حالت همانطور که مشاهده میشود دسترسی از داخل به خارج امکان پذیر می باشد اما امکان تنظیم دسترسی به داخل بطور کامل در اختیار مدیر شبکه می باشد.

در شکل پیچیده تر امکان استفاده از DMZ به منظور ایجاد مناطق امن حفاظت شده نیز می باشد که به شکل زیر می باشد :



در صورت نیاز می توان از امکان VPN site-to-site استفاده نمود که در این حالت بیشترین حالت بیشترین امنیت عبور اطلاعات را داریم. ایجاد این VPN می تواند از طریق فایر والها و یا VPN-Concentrator ها انجام پذیرد.

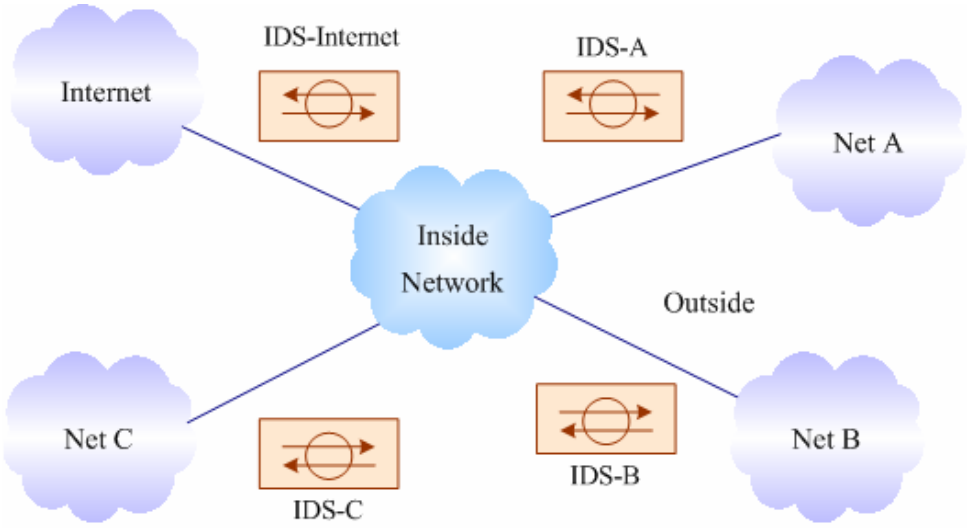
٤-٣- IDS / IP

این دستگاه در شبکه به عنوان تجهیزات شناسائی نفوذ بکار گرفته میشوند و با در نظر گرفتن این دستگاه محل مناسب آن در حالتی که شبکه به شبکه دیگری متصل می شود به دو صورت می‌باشد:

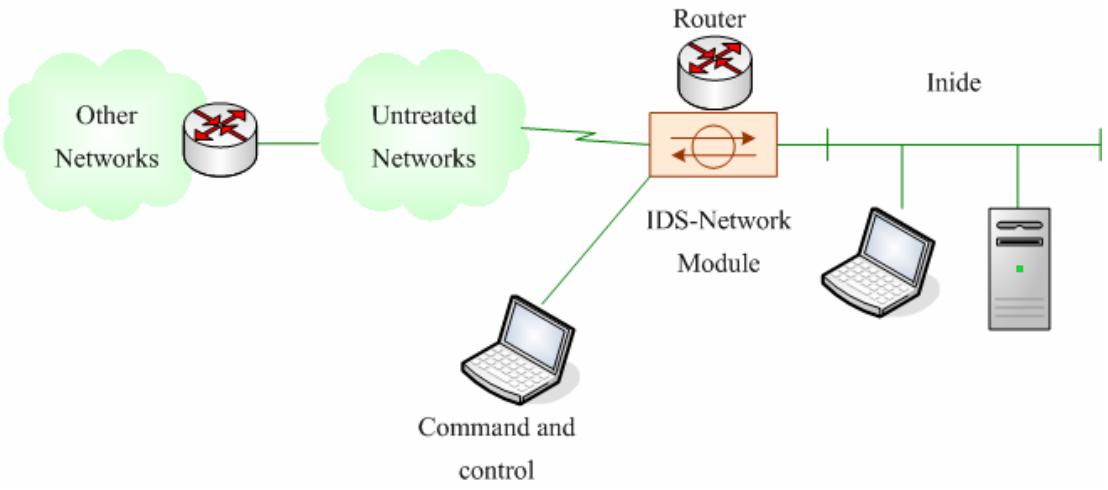
١- در حالتی که به عنوان یک قطعه مجزا بکار گرفته شود.

٢- در حالتی که بعنوان یک ماجول در روتر gateway شبکه بکار گرفته شود.

در حالت اول شبکه به شکل زیر می باشد :

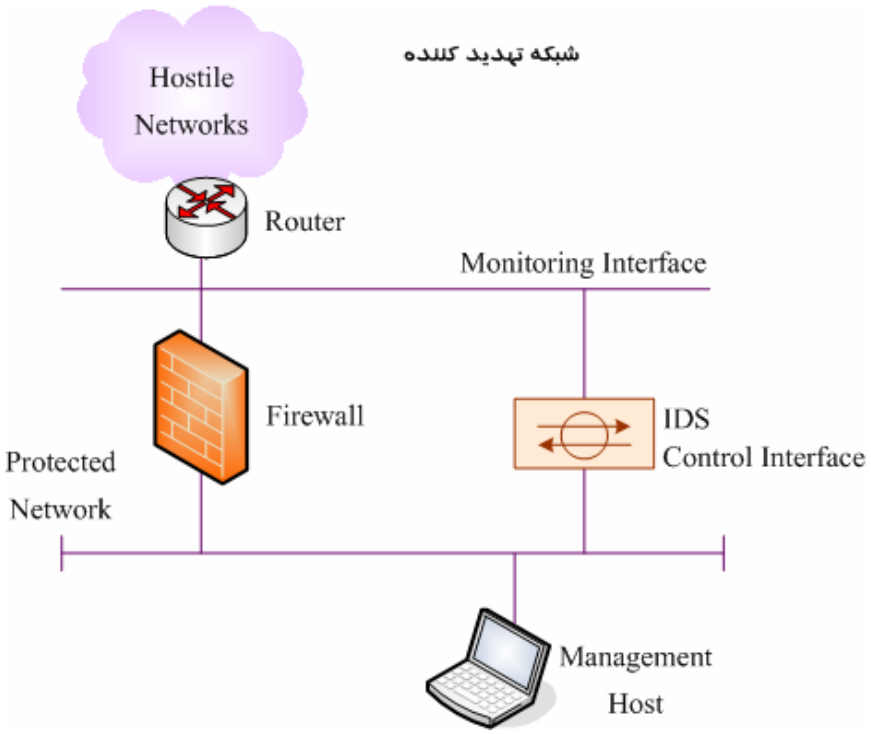


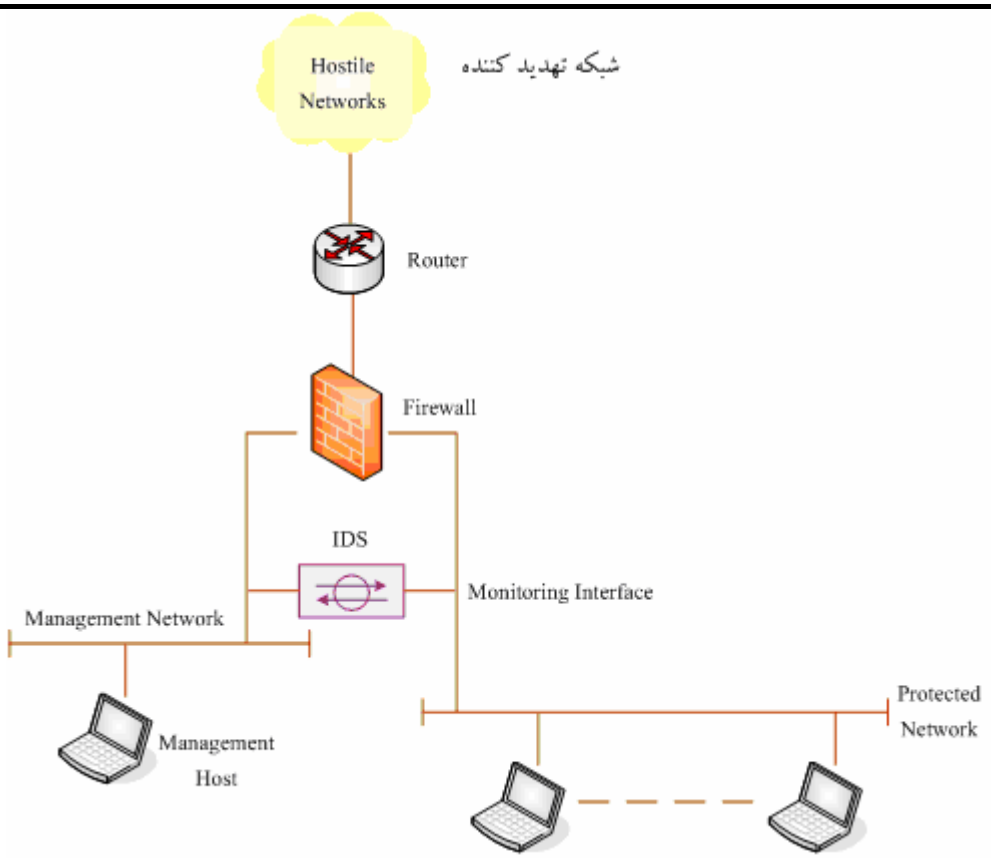
در حالتی که در روتر gateway بکار گرفته شود.



در اینجا other network سایر اداراتی می باشند که میخواهند از طریق یک شبکه نـامطمئن بـه شـبکه اصـلی وصل شوند. در اینجا چه Hacker در داخل و چه در خارج از شبکه باشد قابـل شناسـائی و امکـان بـه حـداقل رساندن ریسک می باشیم.

اما در حالت کلی در صورتیکه بخواهیم ترکیبی از فایروال و IDS / IPS را در شبکه بکار بگیریم بـه دو شـکل می توانیم آنها در شبکه قرار بدهیم که به شکل های زیر می باشد :





بکارگیری IDS در جلو و یا قبل از Firewall هر کدام مزایا و معایبی دارند.

در حالتی که IDS در جلوی فایروال گرفته شود اجازه میدهد تا IDS بتواند تمامی ترافیک ورودی و خروجی به شبکه را مانیتور کند. ولی در این دستگاه نمی تواند ترافیک داخلی شبکه را شناسائی نماید. و هکری که در داخل شبکه می باشد میتواند از نقایص امنیتی شبکه جهت آسیب به شبکه استفاده نماید.

در صورتیکه دستگاه IDS قبل از فایروال بکار گرفته شود امکان مانیتورینگ داخل شبکه فراهم می‌شود، اما دستگاه نمی تواند عدم تطبیق هایی که توسط فایروال پس زده شوند را مانتیور نماید.

در نهایت بایستی به این نکته مهم اشاره نمود که صرف به کارگرفتن تجهیزات نمی توان شبکه‌ای امن داشت بلکه امنیت شبکه مستلزم مانیتورینگ تمامی وقایع رخ داده در شبکه می باشد که بسیار سخت می باشد. بنابراین بایستی تمامی نکات گفته شده در مسائل امنیتی کنترل و تمامی نرم‌افزارها و Update های مورد نیاز آن بروز باشد و دسترسی به خود این دستگاه نیز بایستی تنظیم شده و فقط مدیران شبکه امکان اتصال و کاربا آن را داشته باشند.

در نهایت امنیت در شبکه نیازمند به تیم بسیار قوی و پرکار می باشد تا با کار و صرف زمان زیاد و تمامی شبکه را بررسی و محیطی امن را برای کاربران ایجاد نمایند.