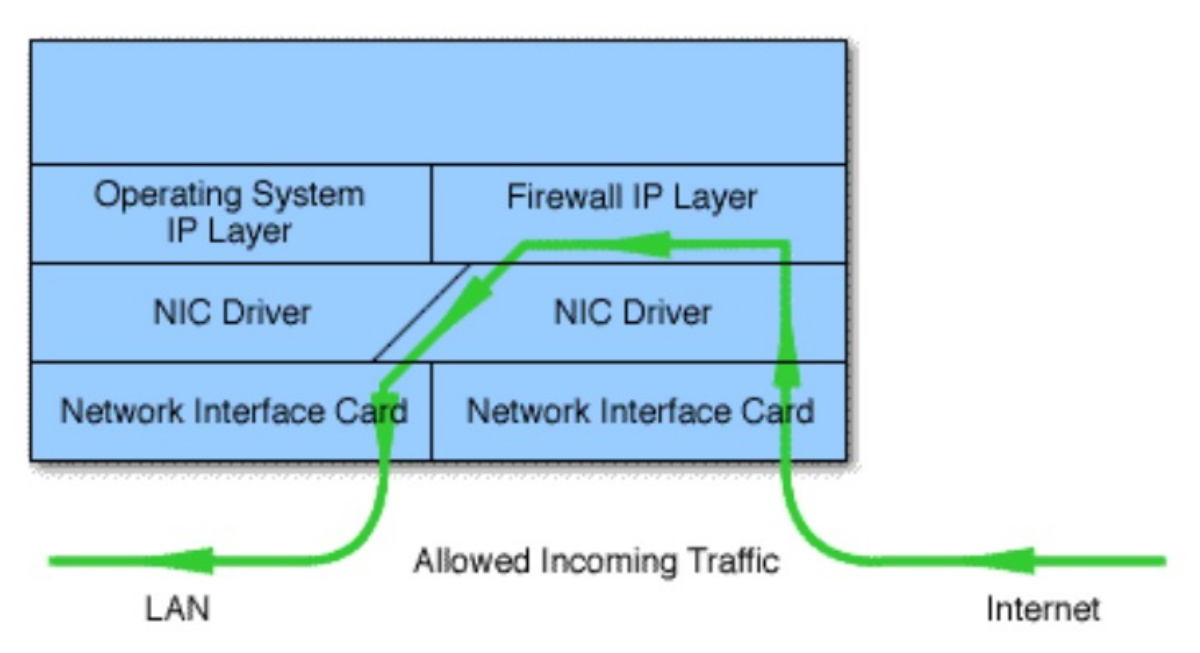
نمونه ایی از کتاب الکترونیکی آموزش

Forefront TMG 2010

مفهوم فایروال

➢ فایروال چیست؟

فایروال ها به ابزارها یا مکانیزمهایی گفته می شود که پکتهای ورودی و خروجی به شبکه را در لایه های مختلف، مورد بررسی قرار می دهند.



➢ فایروالها در دوسته طراحی شده اند:

- فایروالهای سخت افزاری
- فایروالهای نرم افزاری

➢ تفاوت بین فایروالهای نرم افزاری و فایروالهای سخت افزاری

✓ فایروالهای سخت افزاری :

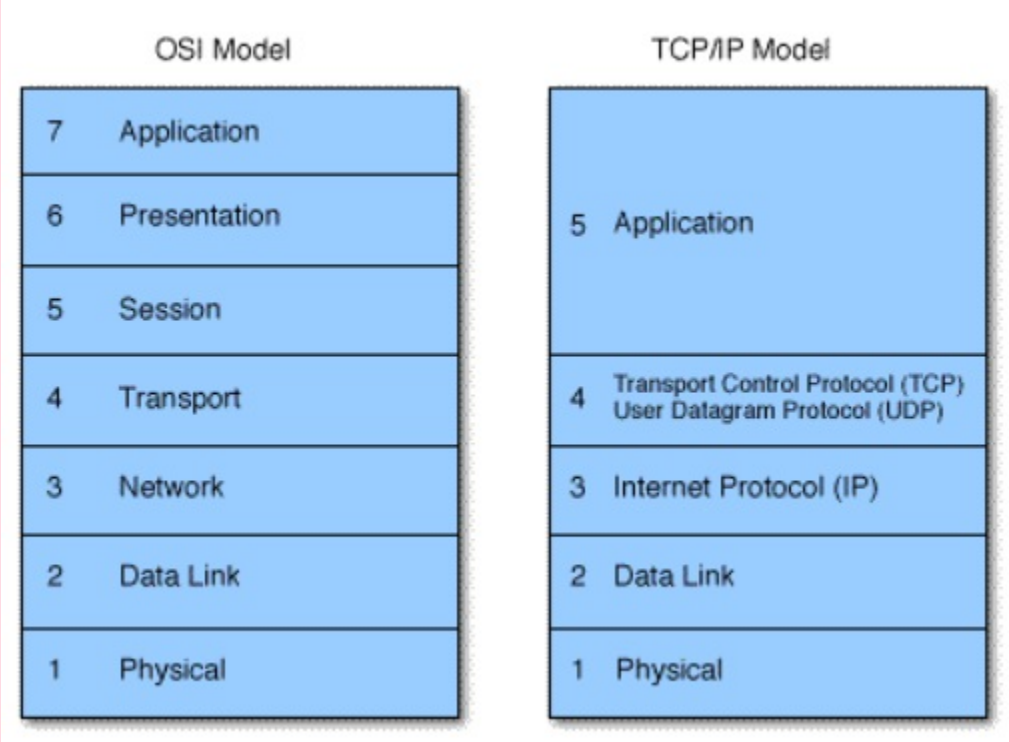
فایروالهای سخت افزاری به فایروالهایی گفته می شوند که شرکتهای سازنده آنها یک برنامه نرم افزاری را همراه با سخت افزار به خصوصی برای آنها، طراحی کرده و ارائه داده اند.

از جمله این فایروالها: فایروال سخت افزاری PIX بوده که نسخه Update شده آن، ASA می باشد و توسط شرکت سیسکو ارائه شده است، و یا میکروتیک که متعلق به شرکت میکروتیک می باشد.

✓ فایروالهای نرم افزاری:

فایروالهای نرم افزاری فایروالهایی هستند که طراحی آنها به صورت یک برنامه نرم افزاری و گرافیکی بوده و بر روی سیستم عاملها نصب می شوند و سخت افزار به خصوصی برای آنها طراحی نشده است. فایروالهای ارائه شده توسط مایکروسافت از این دسته می باشند. مانند ISA و نسخه جدیدترآن که TMG نامیده شده و قابلیتهای بسیار پر کاربردی به آن اضافه شده است.

به صورت کلی فایروالها در سه لایه کار می کنند:



✓ لایه Network :

که در مدل OSI، لایه شماره 3 بوده و در مدل TCP/IP نیز لایه Internet Protocol نامیده می شود و مسئولیت مسیریابی بسته های اطلاعاتی به مقصد را بر عهده دارد و می تواند مشخص کند که بسته از یک منبع قابل اعتماد بازگشته است یا خیر، اما توانایی تشخیص محتویات بسته و ارتباط سایر بسته ها با این بسته را ندارد.

✓ لایه Transport :

فایروالهایی که در لایه Transport، فعالیت می کنند، نسبت به لایه Network، اطلاعات بیشتری از بسته ها دارا بوده و قادر به بلاک کردن یا صدور اجازه دسترسی به درخواستها با توجه به معیارهای پیچیده تری را دارا می باشند.

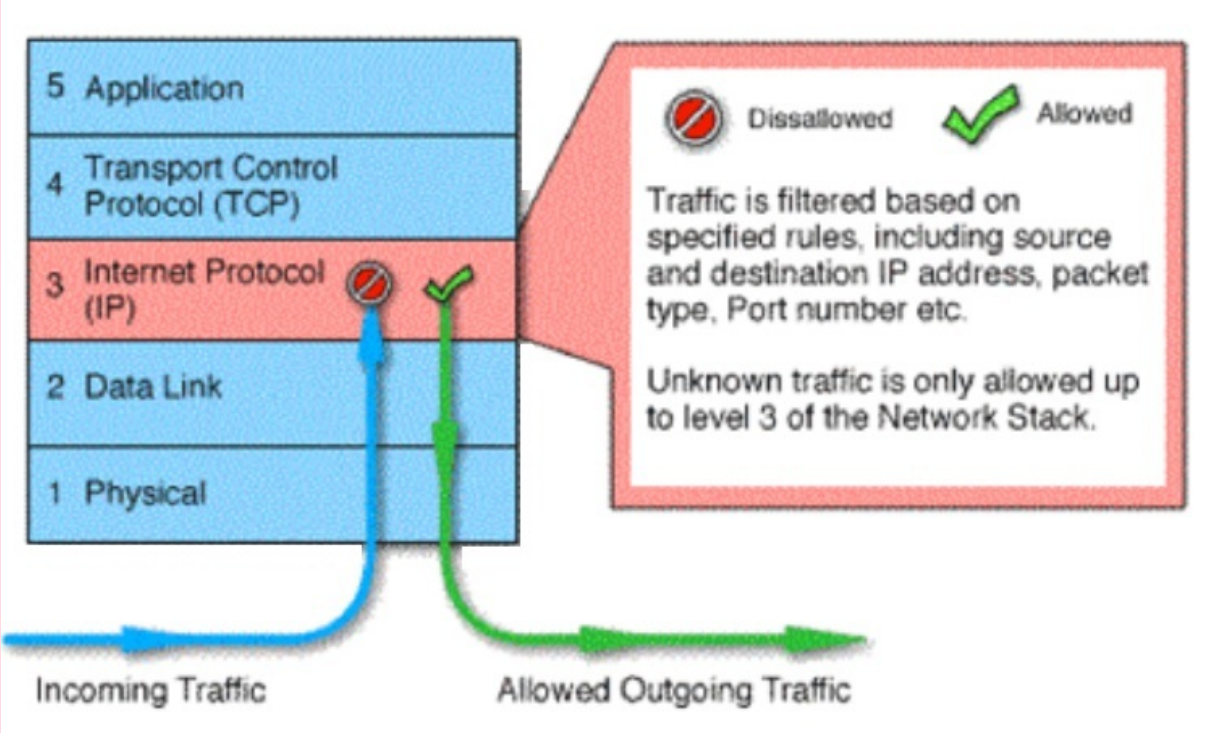
✓ **لایه Application :**

فایروالهایی که در این لایه فعالیت می کنند اطلاعات بسیار گسترده تری را از بسته های اطلاعاتی دارا بوده و توانایی کنترل بسته ها و دسترسی به آنها را با توجه به فاکتورها و مشخصه های کاملی از بسته ها در اختیار دارند.

فایروالهای مایکروسافت و سیسکو، بر اساس چهار نوع فیلترینگ، بسته ها را در لایه های مختلف بررسی می کنند:

- Packet Filtering
- Circuit Level Gateways
- Application Filtering
- stateful multilayer inspection firewalls

➢ Packet Filtering:



اولین نسل از معماری های فایروال که حدود سال 1985، به وجود آمد. این قابلیت معمولا توسط یک Router، به عنوان بخشی از یک فایروال اجرا می شود.

یک روتر با عملکرد معمولی، مشخص می کند که داده ها به کدام مسیر هدایت شوند و Router ای که در نقش packet

Filtering می باشد تعیین می کند که به داده ها اجازه Forward شدن داده شده و یا از Forward شدن آنها جلوگیری شود.

Packet Filtering می تواند در یکی از زیرمجموعه های زیر ایفای نقش کند:

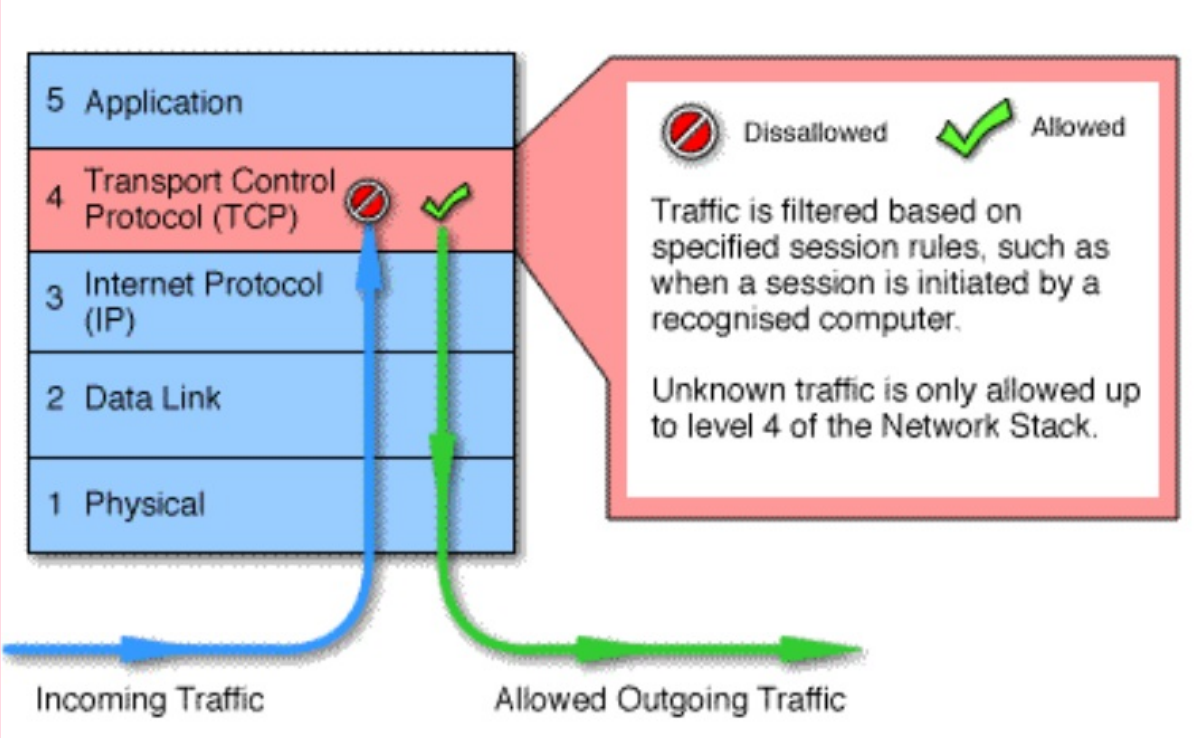
بسته ای که به کارت شبکه فیزیکی رسیده است، از چه IP آدرس مبدأ و مقصدی برخوردار می باشد، نوع انتقال آن از لایه Transport به چه صورت بوده است (TCP, UDP, ICMP) و یا شماره پورت مبدأ و مقصد آن در لایه Transport چه شماره پورتی می باشد.

☑ از جمله مزیتهای یک فایروال Packet Filtering، کم هزینه بودن و تأثیر گذاری اندک آن بر روی کارایی شبکه و عدم نیاز به پیکربندی کامپیوترهای کلاینتها می باشد.

☒ اما، Packet Filtering Firewall ها فایروالهای امنی در نظر گرفته نمی شوند زیرا هیچ درکی از عملکرد پروتکلهای لایه Application، نداشته و بنابراین نمی توانند در مورد محتوای بسته ها تصمیم گیری کنند و همین موضوع باعث می شود که نسبت به circuit level firewall ها که توانایی کنترل لایه Application را دارند از سطح امنیت پایین تری برخوردار باشند.

- یکی دیگر از معایب فایروالهای Packet Filtering، Stateless بودن آنها است به این معنی که نمی توانند حالت اتصال خود را حفظ کنند، و قابلیت ثبت Logg های اتصالات برقرار شده را دارا نمی باشند. همین امر قابلیت تشخیص Attack ها و آزمودن رولهایی که ترافیکها را Deny یا Access می کنند، بسیار مشکل ساخته و منجر به آسیب پذیر ساختن شبکه ها و یا پیکربندی نادرست می گردد.

➢ Circuit Level Gateways:



Circuit Level Gateway ها در لایه Transport از مدل OSI، و یا لایه TCP از مدل TCP/IP کار می کند. Circuit Level Gateway ها برای اتصالات TCP مورد استفاده می باشند و Handshaking بین بسته ها را برای اطمینان از صحت درخواستها مشاهده کرده و به صورت معمول اطلاعات زیر را ذخیره می کنند:

Unique session identifier حالت اتصال، (برای مثال، برقرار شدن Handshake ها یا خاتمه یافتن آن)، توالی اطلاعات، IP آدرسهای مبدأ و مقصد، و اینکه کدام Packet به کارت شبکه فیزیکی وارد شده یا از آن خارج شود،

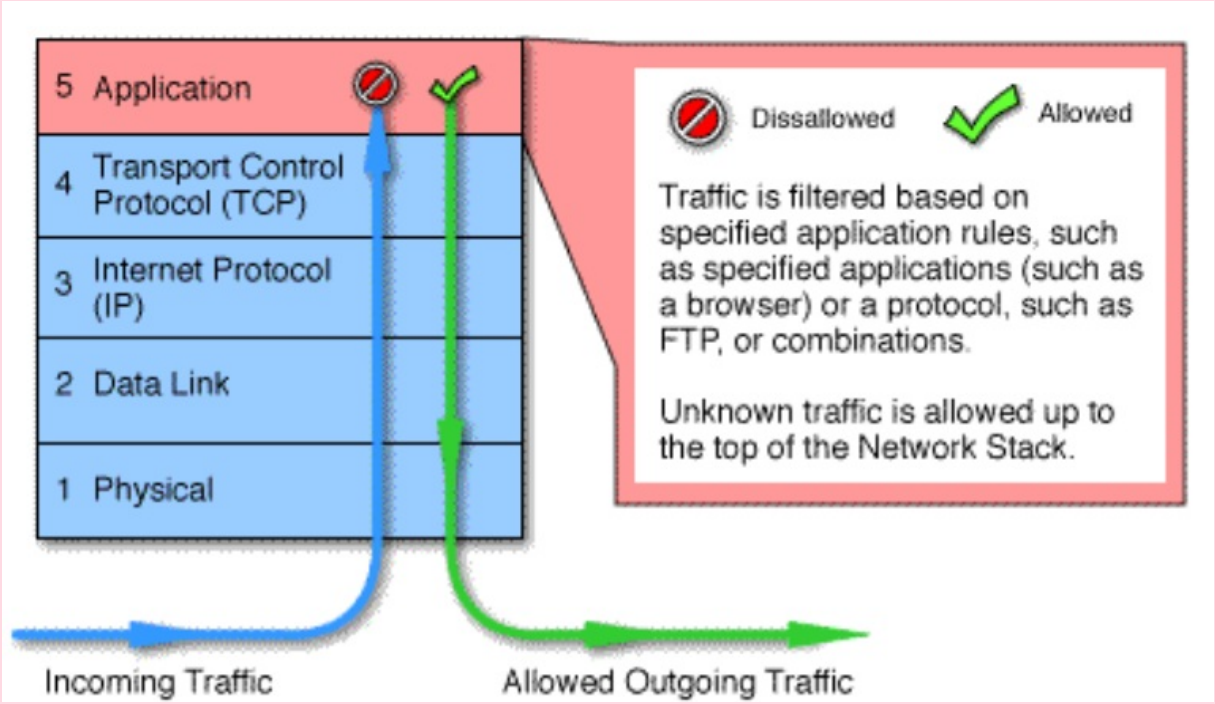
سپس فایروال بررسی می کند که آیا فرستنده اجازه ارسال اطلاعات به مقصد را دارا بوده و گیرنده نیز اجازه دریافت اطلاعات از فرستنده را دارا می باشد.

اگر این پروسه اتصال مورد قبول واقع شده باشد، تمامی Packet ها بدون تستهای امنیتی از طریق فایروال Rout می شوند.

☑ مزایای Circuit Level Gateway ها، این است که معمولا سریع تر از فایروالهای لایه Application هستند به این دلیل که ارزیابی های کمتری بر روی بسته های اطلاعاتی انجام می دهند و همچنین می توانند با بلاک نمودن اتصالات برقرار شده بین Host های اینترانت و منابع خاصی از اینترنت، از شبکه ها محافظت کنند.

☒ یکی از مهمترین معایب circuit level gateway ها عدم توانایی محدود نمودن دسترسی به پروتکلهای زیرمجموعه TCP و به همین ترتیب Packet Filtering و آزمودن رولهای دسترسی یا عدم دسترسی می باشد که باعث آسیب پذیری شبکه ها می گردد.

➢ Application Filtering:



این نوع فیلترینگ در لایه 7 از مدل OSI و در لایه 5 از مدل TCP/IP، عمل میکند. Application Level Gateway ها، پروکسی نیز نامیده شده و Software Application هایی با دو mode اصلی Proxy Server و Proxy client می باشند.

ابتدا درخواستهای اتصال کاربر یا شبکه مورد اعتمادی که قصد اتصال به سرویسی بر روی یک شبکه نا امن مانند اینترنت را دارند، به Proxy server روی فایروال هدایت می شوند.

پروکسی سرور به گونه ای وانمود می کند که یک سرور واقعی بر روی اینترنت می باشد و درخواستها را بر پایه مجموعه ای از رولها یا قوانین تعریف شده کنترل کرده و بر این اساس تصمیم می گیرد که آیا اجازه دسترسی به درخواستها داده شده یا آنها را بلاک کند.

اگر این درخواست مورد تأیید باشد، سرور این درخواست را به پروکسی کلاینت می فرستد که با سرور واقعی بر روی اینترنت تماس حاصل کند.

بعد از برقراری اتصال به اینترنت از طریق Proxy Client، این اتصال برای تحویل به کاربر از Proxy Server عبور داده می شوند.

این روش تضمین می کند که تمامی اتصالات ورودی با proxy client و تمامی اتصالات خروجی نیز با proxy server برقرار می شود. بنابراین بین شبکه های مطمئن و نامطمئن هیچ اتصال مستقیمی برقرار نمی شود.

☑ مهمترین مزیت application level gateway ها، تنظیم رولهایی مبتنی بر پروتکلهای High Level، نگهداری اطلاعات ارتباطات برقرار شده از طریق Firewall Server و توانایی نگهداری جزئیات فعالیت رکوردها می باشد.

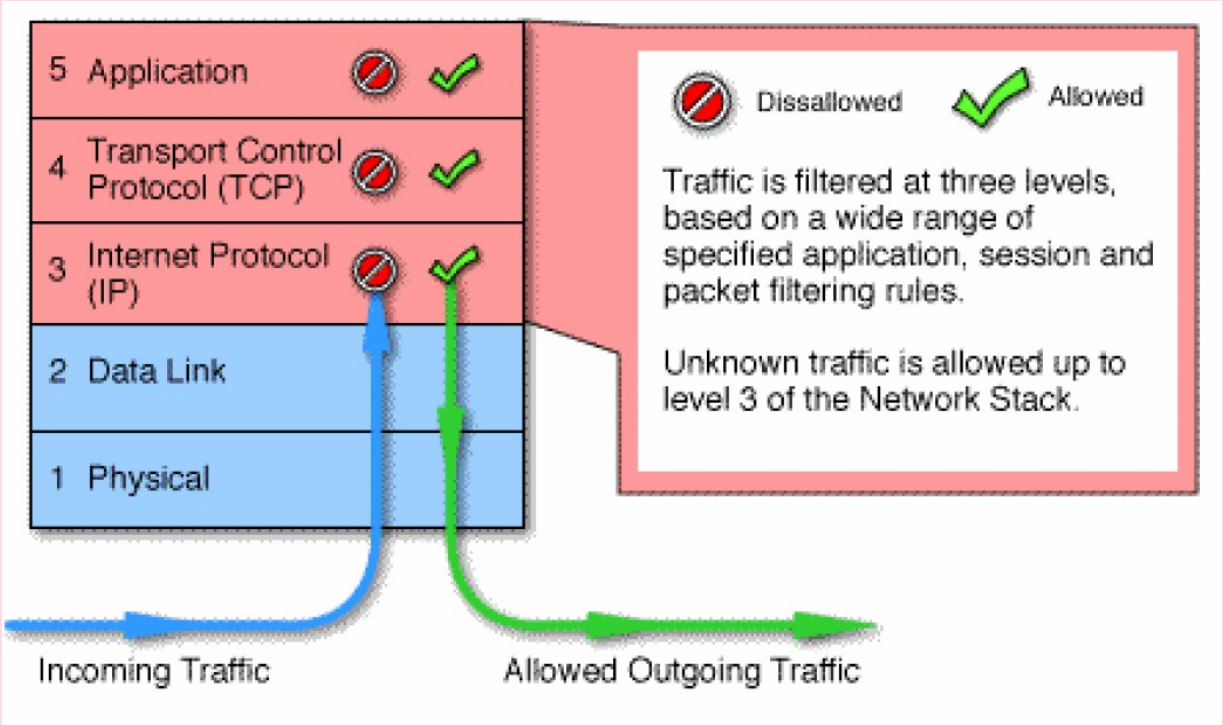
☒ و مهمترین معایب آن نیز، فیلترینگهای پیچیده و تصمیمات مرتبط با کنترل دسترسی هایی است که به منابع محاسباتی قابل توجهی نیاز دارند و می تواند باعث ایجاد افت performance و آسیب پذیری به سیستم عامل و بروز اشکالاتی در سطح برنامه های کاربردی شود.

❋ یکی از ویژگیهای TMG بهره مندی از این قابلیت می باشد، که میتوان با اعمال فیلترینگ بر روی مشخصه ها یا Signature های مورد استفاده Application ها و یا با

تعریف مشخصه های بسیاری از Worm ها یا ویروسها از بسیاری از حملاتی که در این لایه اتفاق می افتند جلوگیری نمود.

برای مثال، می خواهیم ارتباط Application ای مانند Yahoo Messenger را از داخل شبکه به خارج از شبکه بلاک کنیم. اگر بخواهیم پورت مورد استفاده توسط آن را ببندیم باز هم می توان با تغییر پورت، از آن استفاده کرد ولی با توجه به اینکه وقتی یک بسته اطلاعاتی به فایروال می رسد، اطلاعات مربوط به Header، Signature و محتویات آن بررسی می شوند، از طریق تنظیمات HTTP و ایجاد تغییر بر روی Signature ها یا مشخصه های ثابت Application که فقط مختص به همان Application می باشد، می توانیم از ترافیک آن در شبکه جلوگیری کنیم.

- stateful multilayer inspection firewalls



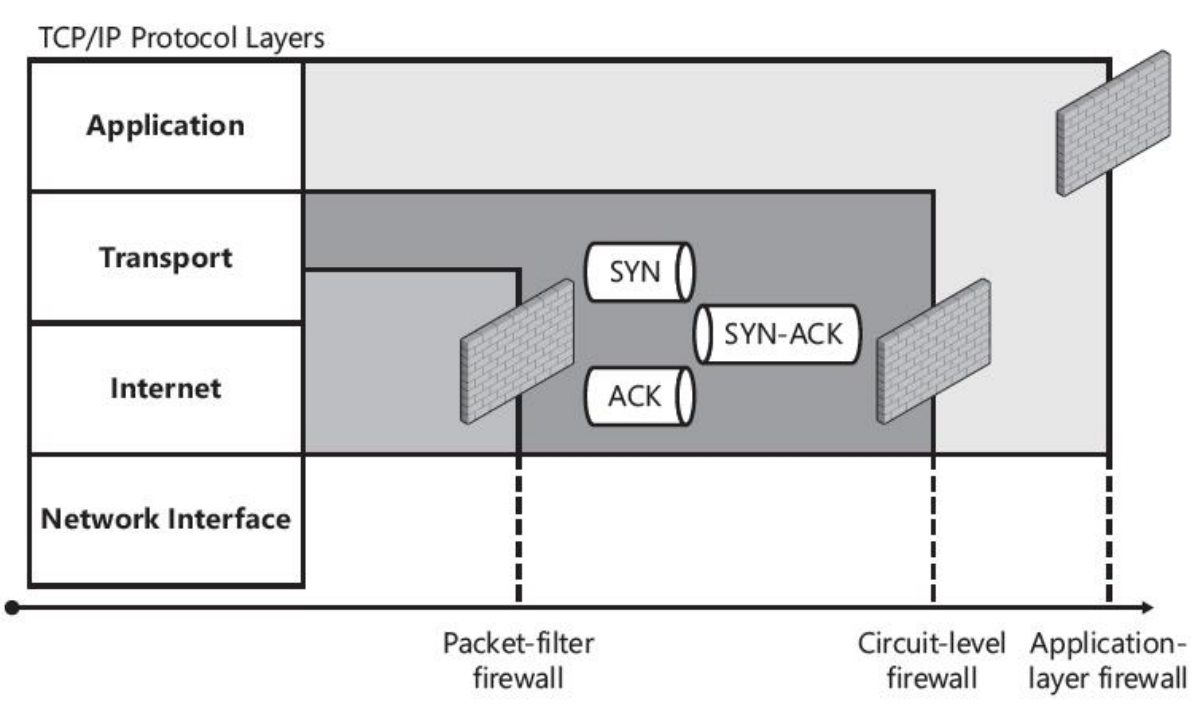
این نوع فایروال، بهترین سطح امنیتی را در بین 4 نوع فایروال، ارائه می دهد به این ترتیب که داده های مبادله شده در لایه Port را مانیتور کرده و بعد از تأیید عملکرد Protocol از نظر شماره پورت و Address مورد استفاده، آن درخواست را تأیید میکند.

برای مثالی در همین زمینه، اگر در طول Sesion برقرار شده با FTP، شماره پورت های مورد استفاده یا IP آدرس تغییر کرده باشد، فایروال اجازه ادامه این اتصال را نمی دهد.

- ☑ مزیت دیگر زمانی است که هریک از پورتهایی که در طول Session برقرار شده مورد استفاده بوده اند، بسته خواهند شد و این یکی از ویژگیهای Stateful inspection system ها است که می توانند به صورت داینامیک پورتهای مورد استفاده در هریک از Sesion های برقرار شده را باز کرده یا ببندند که با عملکرد Packet Filtering ساده که پورتها را در حالت باز شده یا بسته رها می کند، متفاوت می باشد.

☒ مهمترین معایب فایروالهای stateful multilayer inspection، هزینه بر بودن آنها به دلیل نیاز به خریداری Hardware یا Software اضافی است که با Network Device های معمولی قابل اجرا نمی باشد.

عملکرد سه نسل اصلی فایروالها در لایه TCP/IP



❋ TMG در نقش یک فایروال هر سه قابلیت:

- Packet Filtering
- Stateful Inspection
- Application Layer Filtering

را دارا می باشد.

انتخاب نوع فایروال مورد استفاده

در شبکه هایی که حجم بالایی از ترافیک در گذرگاه های شبکه در حال مبادله می باشند و بحث کارایی و امنیت از اهمیت بیشتری برخوردار است از فایروالهای سخت افزاری استفاده می شوند و در شبکه های کوچکتر یا متوسط، که ترافیک نرمال تری از گذرگاه های شبکه عبور می کنند، استفاده از فایروال نرم افزاری به دلیل صرف هزینه کمتر و پیکربندی ساده تر آن، راه کار مناسب تری می باشد.

فایروالهای نرم افزاری از سخت افزار سیستمی که، بر روی آن نصب شده اند استفاده می کنند.

ولی فایروالهای سخت افزاری به دلیل استفاده از منابع سخت افزاری منحصر به خود مانند CPU و RAM، نقش بسیار مهمی را در بالا بردن سرعت عملکرد ایفا نموده و به دلیل ماهیت سخت افزاری بودنشان بسیاری از آسیب پذیریها در آنها کاهش یافته است.

در مجموع با توجه به ابعاد و نوع شبکه مورد استفاده، و در جایی که داشتن کارایی بهتر و امنیت بالاتر در درجه اول اهمیت قرار می گیرند، توصیه می شود ترکیبی از فایروالهای نرم افزاری و سخت افزاری را در شبکه خود استفاده کنید.

این مبحث قسمتی از مطالب مختص به کتاب الکترونیکی آموزش TMG 2010 که توسط گروه آموزشی فرزان تولید شده است، می باشد.

WWW.Modir-Shabake.com