بسم الله الرّحمن الرّحيم

Firewall

دیوار آتش (Firewall)

چگونه از یک شبکه و خودمان محافظت کنیم؟

شما می‌توانید یک ساختمان با دیوارهای محکم و حصارهایی به منظور متوقف کردن دشمن از ورود به ساختمان‌تان بسازید امّا یک در کوچک و محافظت شده برای ورود دوستان خود به ساختمان تعبیه کنید.

مدت‌های طولانی این استراتژی برای یک closed network استفاده می‌شد. در آن زمان هیچ اتصال خارجی‌ای وجود نداشت و اینترنتی هم وجود نداشت. همه چیز خوب بود تا وقتی‌که اینترنت و تجارت الکترونیک ظهور کرد.

با ورود اینترنت، تجارت الکترونیک و رشد کاربردهای وابسته به آنها، closed network دیگر نمی‌توانست بسته بماند و شبکه‌های خصوصی به اینترنت عمومی وصل شدند.

دیوار آتش (Firewall)

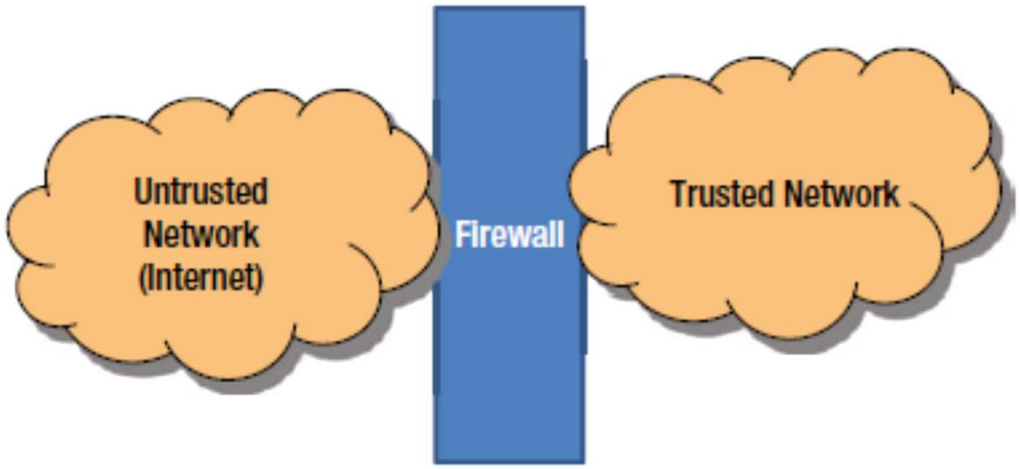
دستگاه‌های امنیتی مختلفی مثل Firewallها، Intrusion Detection Systemها، دستگاه‌های authentication and access control و VPNها پیاده‌سازی شدند. برای درک بهتر این دستگاه‌ها جدول زیر یک قیاس انجام داده است.

No	Description	Security Devices
1	دربان، قفل و کلید	Firewall
2	پاسپورت و ویزا	Access cards, Biometrics
3	نظارت	Intrusion Detection System/ Intrusion Prevention system
4	بدرقه کردن مهمانان تا آزمایشگاه شما	Virtual Private Network (VPN)
5	نگهبان‌ها، سگ‌های نگهبان	Intrusion Detection System/ Intrusion Prevention system

دیوار آتش (Firewall)

واژه‌ی فایروال در **دنیای واقعی** به معنی **یک دیوار ساخته شده برای محافظت در مقابل آتش و کند کردن سرایت آتش به داخل ساختمان است.** این مفهوم در شبکه نیز همین‌طور تعریف می‌شود.

یک فایروال **شبکه** قصد دارد **دسترسی کاربران غیرمجاز به شبکه و سرویس‌های شبکه‌های خارجی دیگر را متوقف کند.** رایج‌ترین آرایش فایروال بین شبکه‌ی مطمئن یک سازمان و شبکه‌ی نامطمئن، اینترنت، است (شکل زیر).



وظایف اصلی دیوار آتش (Firewall)

یک فایروال در دنیای شبکه ترافیک‌های ورودی به شبکه را بازرسی می‌کند و بر اساس قوانینی که توسط شبکه و منابعش تعریف می‌شود این ترافیک را از دیوار عبور می‌دهد.

فایروال مثل یک **نگهبان امنیتی** عمل می‌کند که معمولاً درکنار در اصلی نشسته است و هویت شما را چک می‌کند و در صورت تائید هویت به شما اجازه ورود می‌دهد.

فایروال سه وظیفه‌ی اصلی دارد (بسته به نوع فایروال):

۱- Packet Filtering:

فایروال بسته‌های IP را فیلتر می‌کند. سرآیند IP تمام بسته‌هایی که به فایروال شبکه وارد می‌شوند یا از آن خارج می‌شوند، بازرسی می‌شود. فایروال تصمیم واضحی برای هر بسته‌ای که وارد می‌شود اتخاذ می‌کند که آیا به بسته اجازه ورود داده شود یا نه؟

وظایف اصلی دیوار آتش (Firewall)

۲- Stateful Packet Filtering

در اینجا فیلتر کردن بسته‌ها فراتر از فیلتر کردن عادی بسته‌ها است. در این نوع فیلترینگ، **حالت (state) جریان‌های اتصالی برای تمام بسته‌ها در دو جهت نگهداری می‌شود. همچنین تمامی آدرس‌های IP که اخیراً در اتصالات در هر لحظه از زمان استفاده شده‌اند نیز نگهداری می‌شود.**

۳- Application Level Gateway (Proxy)

فایروال همچنین توانایی **بررسی کردن پروتکل‌های لایه‌ی کاربرد** را دارد. این کار مستلزم این است که فایروال برخی پروتکل‌های لایه‌ی کاربرد را درک کند.

Packet Filtering

یک فیلتر بسته، بسته‌هایی که به شبکه وارد یا خارج می‌شوند را فیلتر می‌کند. فایروال هر بسته‌ی IP را بازرسی می‌کند و تصمیم می‌گیرد. هر بسته با مجموعه‌ای از قانون‌های فیلتر مقایسه می‌شود و بر اساس هر مطابقتی بسته **مجاز، رد یا دور انداخته** می‌شود. فیلترینگ بسته بر روی لایه‌ی انتقال و کاربرد مدل مرجع OSI یا TCP و لایه‌ی IP مجموعه پروتکل TCP/IP انجام می‌شود (مثل شکل اسلاید ۸).

فیلترینگ بسته حالت یا وضعیت را به خاطر نمی‌آورد و بنابراین به این نوع فایروال، stateless firewall گویند.

Packet Filtering

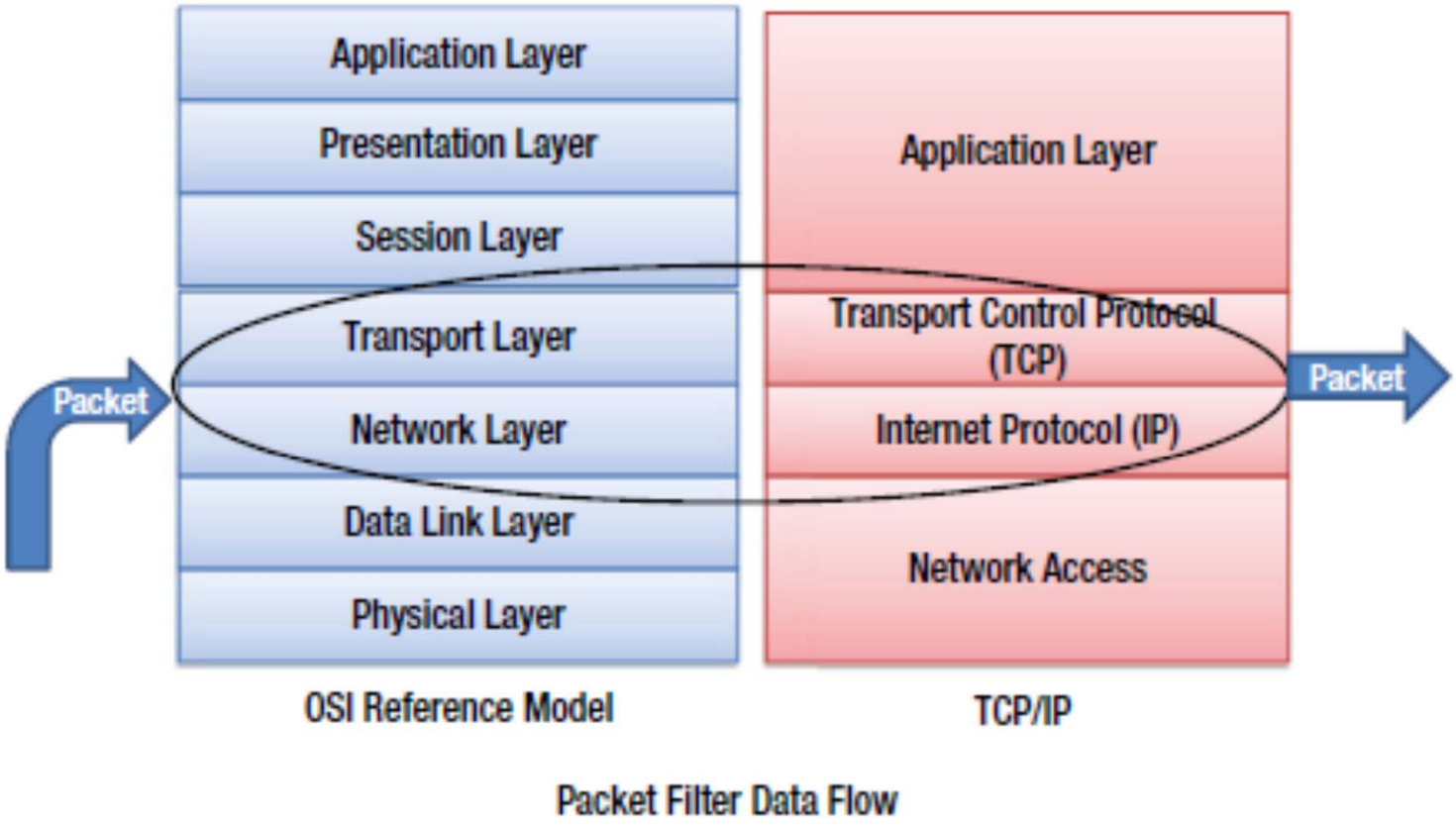


Figure 10-5. Packet Filtering related Layers

Packet Filtering

فیلترهای بسته معمولاً ترافیک شبکه را بر اساس فاکتورهای زیر **رد** یا **قبول** می‌کنند:

- ✓ آدرس‌های IP مبدا و مقصد
- ✓ پروتکلی مثل TCP، UDP یا ICMP
- ✓ آدرس‌های پورت مبدا یا مقصد پروتکل TCP یا UDP
- ✓ پرچم‌ها در سرآیند TCP مثل ACK، CLOSE و SYNC
- ✓ پرچم تکه تکه شدن IP (Fragmentation)
- ✓ جهت بسته – وارد شونده (inbound) یا خارج شونده (outbound)
- ✓ واسط فیزیکی

چگونه یک فایروال فیلترینگ بسته کار می‌کند؟

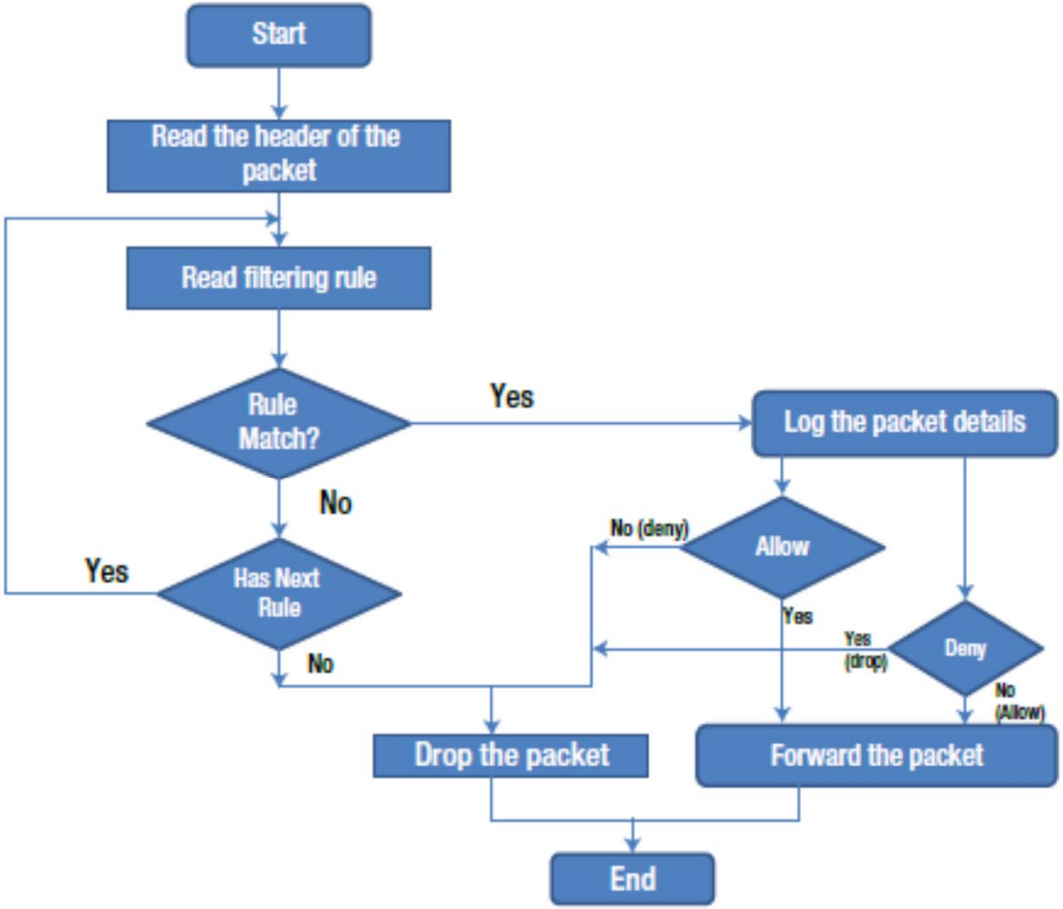


Figure 10-6. Packet filtering flow diagram

چگونه یک فایروال فیلترینگ بسته کار می‌کند؟

یک فایروال فیلترینگ بسته با **مجموعه‌ای از قوانین که برای رد یا قبول بسته تعریف می‌گردند**، پیکربندی می‌شود. وقتی که فایروال یک بسته را دریافت کرد، فیلتر قوانین تعریف شده برای آدرس IP، شماره‌ی پورت، پروتکل و غیره را چک می‌کند. اگر با قانون مطابقت داشت، بسته قبول می‌شود سپس بسته توسط شبکه پذیرفته می‌شود در غیر اینصورت بسته رد می‌شود.

برای درک پیکربندی قوانین فیترینگ بسته شما نیاز دارید که ابتدا پروتکل TCP/IP را درک کنید و این‌که بسته‌ی IP چیست و چگونه در هر لایه بسته‌های IP مدیریت می‌شوند.

RFCهای ۷۹۱ و ۷۹۳ جزئیات پروتکل IP و پروتکل TCP را عرضه می‌کند.

چگونه یک فایروال فیلترینگ بسته کار می‌کند؟

از نقطه نظر فیلترینگ بسته، سرآیند IP محتوی سه قسمت مهم اطلاعات است:

- **آدرس IP مبدا** - طول آن ۴ بایت است و معمولاً به صورت ۱۹۲.۱۶۸.۲.۳۴ نوشته می‌شود.
- **آدرس IP مقصد** – طول آن ۴ بایت است و مثل آدرس مبدا نوشته می‌شود.
- **پروتکل IP** – مشخص می‌کند که آیا بسته‌ی مربوط به پروتکل TCP، UDP و یا ICMP است.

اگر پهنای باند شبکه کوچک‌تر از پهنای باند مبدا باشد، آنگاه ممکن است بسته‌ی IP به یک سری بسته‌های کوچک‌تر که Fragment نامیده می‌شوند، تقسیم گردد. Fragmenting ساختار بسته‌ی IP را **تغییر نمی‌دهد** اما یک flag در داخل بسته‌ی IP قرار می‌دهد که توضیح می‌دهد بدنه شامل قسمتی از یک بسته می‌باشد.

چگونه یک فایروال فیلترینگ بسته کار می‌کند؟

سرآیند بسته‌ی TCP محتوی اطلاعات زیر است:

- **آدرس پورت مبدا** – یک عدد ۲ بایتی است که فرآیند کاربردی‌ای که بسته به آن **تعلق دارد** را مشخص می‌کند.
- **آدرس پورت مقصد** – یک عدد ۲ بایتی است که فرآیند کاربردی‌ای که بسته به آن **باید برسد** را مشخص می‌کند.
- **فیلد پرچم TCP** – محتوی اطلاعات پروتکل TCP مثل **ایجاد اتصال، خاتمه‌ی اتصال و سایز بسته** است.

یک نمونه از قوانین فیلترینگ بسته

به طور مثال شما می‌خواهید اجازه دهید که تمام ترافیک IP بین یک میزبان خارجی (۱۶۲.۲۲.۳۴.۵۶) و یک میزبان در داخل شبکه (کلاس A، ۱۰.۱.۱.۲)عبور کند. جدول زیر لیستی از قوانین فیلترینگ بسته را نمایش می‌دهد.

Table 10-2. Packet filtering rules

Rule	Direction	Source Address	Destination Address	Application (TCP port)	Filter Set	Action
1	Inbound	Trusted external host (162.22.34.56)	Internal (10*.*)	Http	Any	Permit
2	Outbound	Internal	Trusted External host (162*.*)	SMTP	Any	Permit
3	Inbound or Outbound	Any	Any	TFTP	Any	Deny

یک نمونه از قوانین فیلترینگ بسته

چند نمونه از قوانین فیلترینگ بسته به شرح زیر است:

- سرویس‌های e-mail و HTTP را اجازه می‌دهد اما سرویس‌هایی مثل TFTP و Telnet را بلوکه می‌کند.
- تمامی اتصالات ورودی از سیستم‌های خارجی به غیر از اتصالات SMTP را بلوکه می‌کند.
- پورت ۴۴۳ برای تمامی آدرس‌های مقصد را اجازه می‌دهد. (HTTPS)
- پورت ۸۰ برای تمامی آدرس‌های مقصد را اجازه می‌دهد. (HTTP)

مزایا و معایب فیلترینگ بسته

مهم‌ترین **مزیت** فایروال فیلترینگ بسته قوانین ساده‌ی آن است: allow یا deny.

- ✓ اگر محل قرارگیری فایروال فیلترینگ بسته درست انتخاب شود می‌تواند کل شبکه را محافظت کند. بیشتر **روترها فیلترینگ بسته** را پشتیبانی می‌کنند. اگر شما یک روتر بعد از سرویس‌دهنده‌ی اینترنت داشته باشید که فیلترینگ بسته‌ی آن فعال باشد آنگاه شما می‌توانید تمام شبکه را بدون در نظر گرفتن سایز شبکه، محافظت کنید.
- ✓ فیلترینگ بسته در اکثر روترها وجود دارد. فروشنده‌های برجسته‌ی شبکه مثل سیسکو، ژونیپر و HP، فیلترینگ بسته را در روترهای edge و core خود با عنوان Access Control Lists (ACL) قرار داده‌اند.

مزایا و معایب فیلترینگ بسته

فایروال‌های فیلترینگ بسته **معایبی** نیز دارند:

- ✓ پیکربندی قوانین فیلترینگ بسته سخت است. شما نیاز به مهارت بسیار زیاد و استراتژی مناسب برای پیکربندی درست آن دارید.
- ✓ حتی اگر آن‌را پیکربندی کردید، بسیار سخت است که به طور کامل آن‌را تست کنید و تایید کنید که آیا به درستی کار می‌کند یا نه؟
- ✓ این نوع فایروال یک ماشین **بدون وضعیت** است. **یعنی وضعیت بسته‌ی قبلی را به خاطر نمی‌آورد.** فایروال‌های فیلترینگ بسته‌ی بدون وضعیت در برابر حمله‌ها آسیب‌پذیر هستند. بنابراین بعضی حمله‌ها ، spoofing، می‌توانند به راحتی از قوانین فایروال عبور کنند.

فیلترینگ بسته stateful

مهم‌ترین عیب فایروال‌های فیلترینگ بسته این بود که **بدون وضعیت** بودند. یعنی وضعیت بسته‌ی قبلی را به خاطر نمی‌آورد. این موضوع باعث می‌شد که بسیاری از بسته‌های نامطلوب از فایروال عبور کنند.

این خطرها برای فایروال‌های اولیه‌ی فیلترینگ بسته غیرقابل اجتناب بود. از این‌رو تمامی فایروال‌های مدرن فراتر از فایروال‌های فیلترینگ بسته عمل می‌کنند و همه‌ی آنها **stateful** هستند. **یعنی فایروال ردپای وضعیت اتصال برای تمامی بسته‌ها در دو جهت (ورود و خروج به فایروال) را نگهداری می‌کند.** فایروال‌های stateful **همچنین تمامی آدرس‌های IP که اخیراً به فایروال متصل شدند را نگهداری می‌کند.**

مزیت اصلی فایروال stateful این است که admin نیاز نیست قوانین فیلترینگ گسترده‌ای بنویسد که مشخص کند تمامی سرویس‌های TCP مجاز هستند یا غیرمجاز.

Network Address Translator (NAT)

طول آدرس IP ۳۲ بیت است و با الگوی جاری حداکثر تعداد میزبانی که می‌توانیم داشته باشیم حدود ۴ میلیارد می‌باشد. این موضوع تعداد میزبان‌هایی که می‌توانند به اینترنت وصل شوند را محدود می‌کند. از آنجایی که اکثر میزبان‌هایی که در شرکت‌ها هستند نیاز به ارتباط با اینترنت دارند، ۴ میلیارد آدرس به زودی به پایان می‌رسد. در سال ۱۹۹۴راه حل کوتاه مدتی برای این مشکل با نام NAT پیشنهاد شد.NAT نه تنها مشکل قبلی را حل می‌کرد بلکه یکی از روش‌هایی بود که از طریق آن هویت شبکه‌ی داخلی محافظت می‌شد. RFC791 مجموعه‌ای از آدرس‌های IP در هر کلاس را به عنوان ادرس‌های خاص تعریف می‌کند که فقط در شبکه‌ی خصوصی استفاده می‌شوند و بقیه‌ی آدرس‌ها می‌توانند به عنوان آدرس عمومی استفاده شوند.

Network Address Translator (NAT)

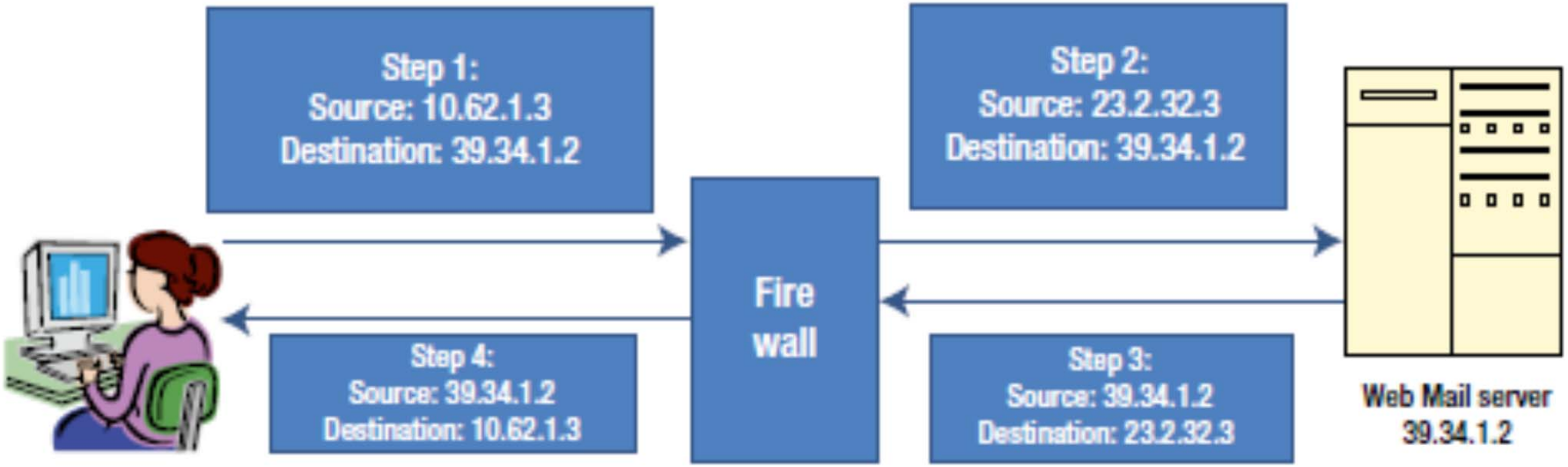
بازه‌ی رزرو شده برای شبکه‌ی خصوصی به شرح زیر است:

- 10.0.0.0 – 10.255.255.255 (10/8 prefix)
- 172.16.0.0 – 172.31.255.255 (172.16/12 prefix)
- 192.168.0.0 – 192.168.255.255 (192.168/16 prefix)

دلیل عمده برای این موضوع اطمینان از این است که آدرس‌های IP به صورت کارا (کارآمد) تخصیص داده شوند. بازه‌ی خصوصی آدرس IP، به طور مثال 10.0.0.0/8، در اینترنت استفاده نمی‌شود، وقتی‌که بخواهیم به دنیای خارج وصل شویم این آدرس باید با یک آدرس عمومی جایگزین شود. این کار با استفاده از NAT انجام می‌شود. به طور مثال، یک میزبان که آدرس IP آن (آدرس IP مبدا) 10.62.1.3 است. بعد از NATing آدرس مبدا بوسیله‌ی آدرس عمومی 23.2.23.3 جایگزین می‌شود.

Network Address Translator (NAT)

کامپیوتر (میزبان) مقصد فقط آدرس IP عمومی را می‌بیند و آدرس شبکه‌ی داخلی هیچگاه در جهان خارج شناخته نمی‌شود. بنابراین NAT محافظت از منابع شبکه‌ی داخلی را فراهم می‌کند. این فرآیند در شکل زیر نمایش داده شده است.



Network Address Translator (NAT)

بوسیله‌ی NATing، شرکت‌ها می‌توانند فقط یک آدرس IP عمومی داشته باشند. هر میزبان داخلی که می‌خواهد به اینترنت یا یک شبکه‌ی خارجی وصل شود در فایروال عمل NAT روی آن انجام می‌شود. میزبان داخلی هیچگاه نمی‌داند که NATing انجام شده است. بنابراین NAT آدرس‌های IP را ذخیره می‌کند. اگر بیش از یک سیستم کامپیوتری داخلی بخواهد با اینترنت ارتباط برقرار کند کاری که NAT در فایروال انجام می‌دهد این است که آدرس IP مبدا را تغییر می‌دهد، شماره پورت مبدا را نیز با یک شماره پورت جدید بالاتر از ۱۰۲۳ جایگزین می‌کند و به صورت موقتی شرایط جدید را در مدت اتصال نگهداری می‌کند.

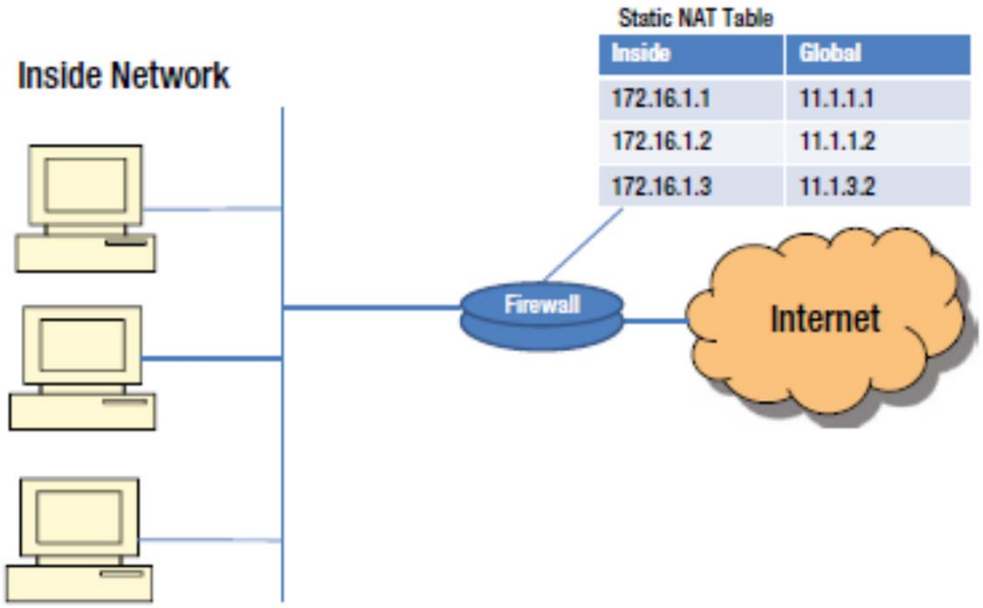
NATing به عنوان یک اقدام امنیتی اساسی به کار می‌رود که می‌تواند حمله‌کننده‌ی خارجی را برای به دست آوردن آدرس IP شبکه‌ی داخلی به زحمت بیاندازد. هنگامی‌که NATing انجام می‌شود، فایروال آدرس IP مبدا را بازنویسی می‌کند و آدرس مبدا تغییریافته و آدرسIP مقصد را در سرآیند IP قرار می‌دهد.

Network Address Translator (NAT) - Static Translation

NAT می‌تواند ترجمه (نگاشت) استاتیک یا داینامیک (پویا) داشته باشد. در NAT استاتیک، شکل ترجمه همیشه یک روش خاص ثابت است. در NAT استاتیک، تعداد زیادی آدرس‌های IP داخلی به تعداد زیادی آدرس‌های خارجی به صورت یک به یک ترجمه می‌شوند. هنگامی که این روش پیکربندی شد، به صورت ثابت باقی می‌ماند و تغییری نمی‌کند. این روش برای وب سروری که از طریق آدرسی ثابت دراینترنت در دسترس است، مفید می‌باشد.

Network Address Translator (NAT) - Static Translation

شکل زیر مثالی از NAT استاتیک را نمایش می‌دهد. هر آدرس داخلی (۱۷۲.۱۶.۱.۱، ۱۷۲.۱۶.۱.۲ و ۱۷۲.۱۶.۱.۳) به صورت یک به یک به آدرس‌های جهانی (۱۱.۱.۱.۱، ۱۱.۱.۱.۲ و ۱۱.۱.۳.۲) ترجمه شده‌اند.



Static NAT

Network Address Translator (NAT) - Dynamic Translation

در NAT پویا، ترجمه به وصرت استاتیک نیست. ترجمه بر اساس آدرس IP موجود از مخزنی از آدرس‌های عمومی می‌باشد. وقتی‌که میزبان داخلی شبکه درخواست دسترسی به اینترنت را می‌دهد، NAT پویا یک آدرس IP که تخصیص داده نشده و توسط هیچ میزبانی استفاده نشده را از مخرن آدرس‌ها برداشته و به میزبان اختصاص می‌دهد. NAT پویا هنگامی‌که آدرس‌های کمی موجود باشد و تعداد زیادی میزبان بخواهند به اینترنت متصل شوند، مفید است.

Port Address Translation (PAT)

وقتی که یک آدرس جهانی داشته باشید و چندین میزبان در داخل LAN بخواهند به اینترنت متصل گردند آنگاه ما از چیزی به نام Port Address Translation (PAT) باید استفاده کنیم. این موقعیت را overloading (اضافه بار) گویند. NAT/PAT box به یک روش برای نگهداری آدرس‌های محلی که می‌خواهند به اینترنت وصل شوند، نیاز دارد. این ترجمه توسط پورت‌های TCP/UDP انجام می‌شود. TCP/UDP از شماره‌ی پورت‌های ۱۶ بیتی استفاده می‌کند که اجازه می‌دهد ۶۵۵۳۶ سرویس متفاوت قابل شناسایی باشند. وقتی ترجمه انجام می‌شود، PAT سعی می‌کند اگر شماره‌ی پورت اصلی استفاده نشده باشد از شماره‌ی پورت اصلی استفاده کند. اگر شماره پورت اصلی در دسترس نبود آنگاه از شماره پورت موجود بعدی استفاده می‌کند.

Port Address Translation (PAT)

مزایا:

- ✓ چند میزبان داخلی میتوانند یک آدرس جهانی را به اشتراک بگذارند.
- ✓ شبکه‌ی داخلی هیچگاه در معرض دید شبکه عمومی خارجی قرار نمی‌گیرد بنابراین حمله از خارج بسیار سخت است.

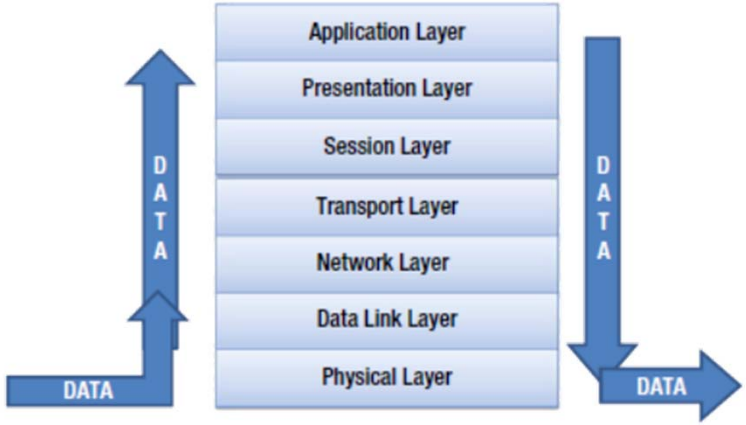
معایب:

تعداد اتصال‌های سخت‌افزاری محدودی را پشتیبانی می‌کند. به این معنی که اگر در یک زمان تعداد زیادی میزبان درخواست اتصال داشته باشند آنگاه سخت افزار پورت‌های آزادش ممکن است تمام شود.

Application Level Gateway (Application Proxy)

همانطور که از نامش مشخص است، Application Level Gateway (ALG) تمامی بسته‌ها تا لایه‌ی کاربرد را بررسی می‌کند و تعیین می‌کند که آیا یک بسته مجاز است یا غیرمجاز؟

ALG امنیت بالاتری نسبت به packet filtering دارد به خاطر این‌که بررسی بسته‌ها تا لایه‌ی کاربرد انجام می‌شود (شکل زیر). اما به زمان پردازش CPU بیشتر و اطلاعات ضروری در مورد پروتکل‌های لایه‌ی کاربرد نیاز دارد.



Application Level Gateway Data Flow

How the Application Level Gateway Works

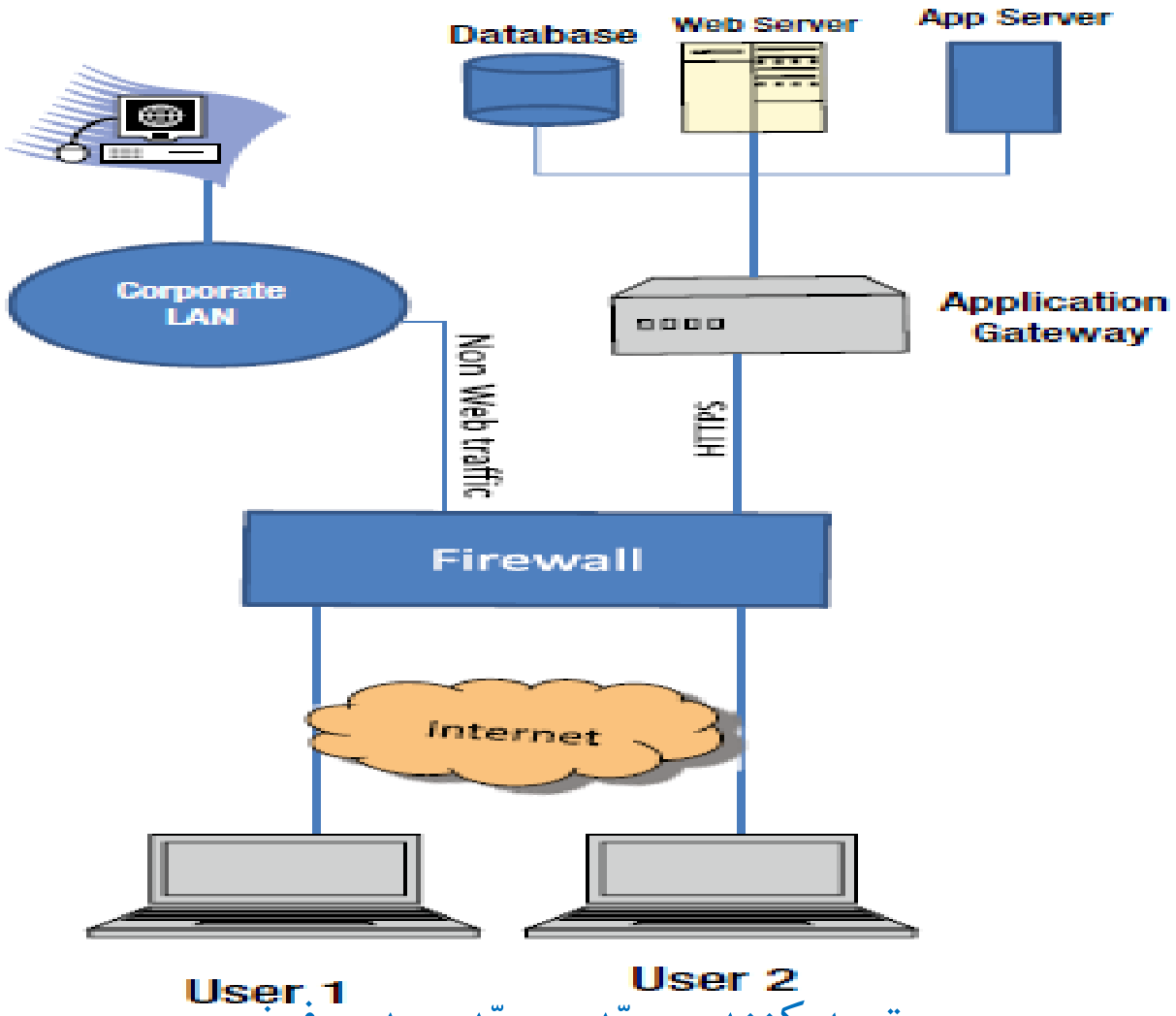
Application Level Gateway (Application Proxy) - cont.

ALG به صورت مستقل اجرا می‌شود، اطلاعات را کپی و از طریق gateway ارسال می‌کند و به عنوان proxy server کار می‌کند.

ALG از ارتباط مستقیم بین سرور مورد اعتما یا کلاینت و میزبان غیرقابل اعتماد جلوگیری می‌کند. Proxyها مخصوص کاربرد هستند. هر کاربرد جدید که به داخل شبکه وارد می‌شود ضروری است که به application proxy اطلاع دهد. برای این‌که قوانین باید ایجاد و برای آن کاربرد اجرا شوند.

ALG بین فایروال شبکه و میزبان مورد اعتماد قرار می‌گیرد (شکل اسلاید بعد) و می‌تواند بسته‌های لایه‌ی کاربرد را فیلتر کند.

Application Level Gateway (Application Proxy) - cont.



Application Level Gateway (Application Proxy) - cont.

ALG حالت اتصال TCP و sequencing را به طور کامل نگهداری می‌کند. ALGها پشت NAT یا فایروال استفاده می‌شوند. در زیر مزایا و معایب ALG ذکر شده است:

مزایا

- اتصال مستقیم بین میزبان‌های داخلی و خارجی مجاز نیست.
- تایید سطح کاربر پشتیبانی می‌شود.
- بسته تا داده‌ی کاربرد بررسی می‌شود.

Application Level Gateway (Application Proxy) - cont.

معایب

- توان پردازشی بیشتری مورد نیاز است.
- از packet filtering کندتر است.
- تمام پروتکل‌های لایه‌ی کاربرد پشتیبانی نمی‌شود. هنگامی‌که یک کاربرد جدید آمد Proxyهای متناظر باید پیاده‌سازی شود.