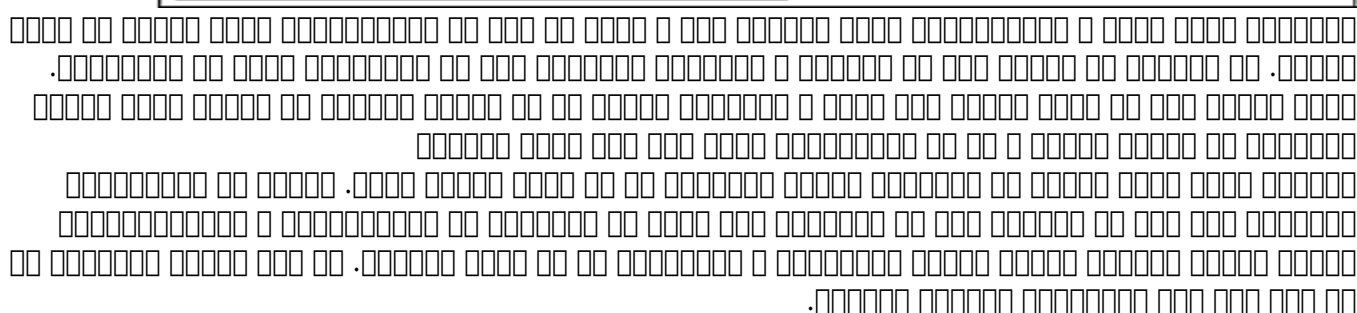


[illegible]

□ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □

၀၀၀၀၀၀၀၀ ၀၀၀၀ ၀၀၀၀၀၀ ၀၀ ၀၀ ၀၀၀၀၀၀ ၀၀၀ ၀၀၀၀၀၀၀၀ 1764 ၀၀၀ ၀၀ ၀၀၀ ၀၀၀၀၀ «၀၀၀၀၀၀၀၀» ၀၀ «၀၀၀၀၀၀၀၀၀» ၀၀၀၀
 ၀၀၀ ၀၀ ၀၀၀၀၀၀၀၀၀၀ ၀၀၀၀၀၀၀၀ ၀၀၀၀၀၀ ၀၀ ၀၀၀၀ ၀၀၀ .၀၀၀၀၀ ၀၀၀၀၀၀၀၀ ၀၀၀၀၀၀၀၀၀ ၀၀၀၀၀၀၀၀ ၀၀၀ ၀၀ ၀၀၀ ၀၀၀၀၀၀ ၀၀
 ၀၀၀၀၀၀၀ .၀၀၀၀၀၀ ၀၀၀၀၀၀၀၀ ၀၀၀၀၀၀၀၀၀ ၀၀ ၀၀၀၀၀၀၀ ၀၀၀၀၀၀၀၀ ၀၀၀၀ ၀၀၀၀၀၀၀၀ ၀၀ ၀၀၀၀ ၀၀၀၀ ၀၀၀၀၀၀၀၀ ၀၀၀၀ 1980
 ၀၀၀၀၀ ၀၀၀၀၀ ၀ ၀၀၀၀၀ ၀၀၀၀ ၀၀၀၀၀၀၀၀၀၀ ၀၀၀၀၀၀၀၀၀ ၀၀၀ ၀၀ ၀၀ ၀၀၀ ၀၀၀၀၀၀၀၀ ၀၀ ၀၀၀၀၀၀၀၀၀၀ ၀၀ ၀၀၀၀၀ ၀၀
 ၀၀၀ ၀၀၀၀၀၀၀ ၀၀၀၀၀၀ ၀၀၀၀၀၀၀၀ ၀၀ ၀၀၀၀ ၀၀ ၀၀၀၀၀၀၀ ၀ ၀၀၀၀၀၀၀ .၀၀၀၀၀၀ ၀၀၀၀ ၀၀ ၀၀၀၀ ၀၀၀ ၀၀ ၀၀ ၀၀၀ ၀၀၀၀၀၀၀
 .၀၀၀၀၀၀၀ ၀၀၀၀၀၀ Rule ၀၀၀၀၀

0 000000 0000 000000 000 :0000 0000 000000 000000 00 000 000 00 000 00000 0000000 00 000000
 0000 0000000 00 0000 00000000 0000 00 0000 00000000 000000000 .000000 0000 000000 0000 000000

1. **Access Control List (ACL) 1**

2. **Access Control List (ACL) 2**

3. **Access Control List (ACL) 3**

4. **Access Control List (ACL) 4**

Rule	Direction	Source Address	Dest. Address	Protocol	Source Port	Dest. Port	Action
A	In	External	Internal	TCP	> 1023	25	Permit
B	Out	Internal	External	TCP	25	> 1023	Permit
C	Out	Internal	External	TCP	> 1023	25	Permit
D	In	External	Internal	TCP	25	> 1023	Permit
E	Either	Any	Any	Any	Any	Any	Deny

5. **Access Control List (ACL) 5**

6. **Access Control List (ACL) 6**



7. **Access Control List (ACL) 7**

8. **Access Control List (ACL) 8**

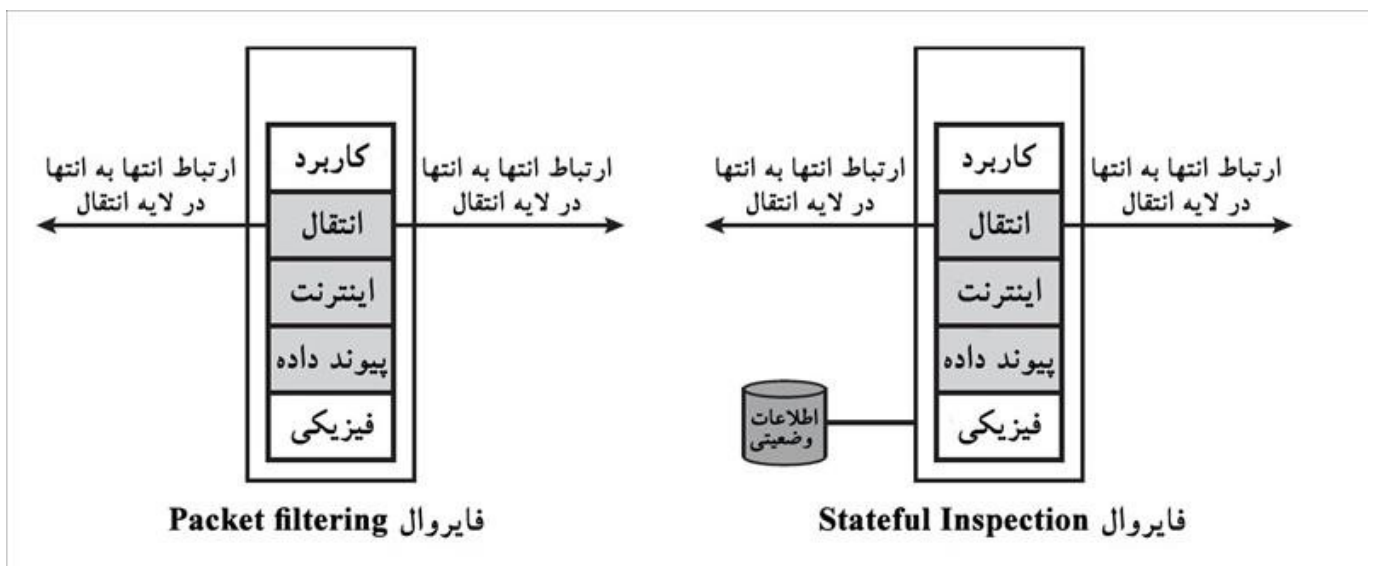
9. **Access Control List (ACL) 9**

10. **Access Control List (ACL) 10**

این روش‌ها معمولاً در روترها و فایروال‌ها استفاده می‌شود. Packet Filtering (فیلتر کردن بسته‌ها) ساده‌ترین و سریع‌ترین روش است. Stateful Inspection (فیلتر کردن بسته‌ها با حفظ وضعیت) روشی پیشرفته‌تر است که وضعیت هر بسته را در حافظه می‌نگارد. Application-Level Gateway (گیت‌واهی سطح کاربردی) روشی پیچیده‌تر است که در سطح پروتکل کاربردی (مانند HTTP) ترافیک را بررسی می‌کند. Circuit-Level Gateway (گیت‌واهی سطح مدار) روشی دیگر است که فقط ارتباطات را بررسی می‌کند.

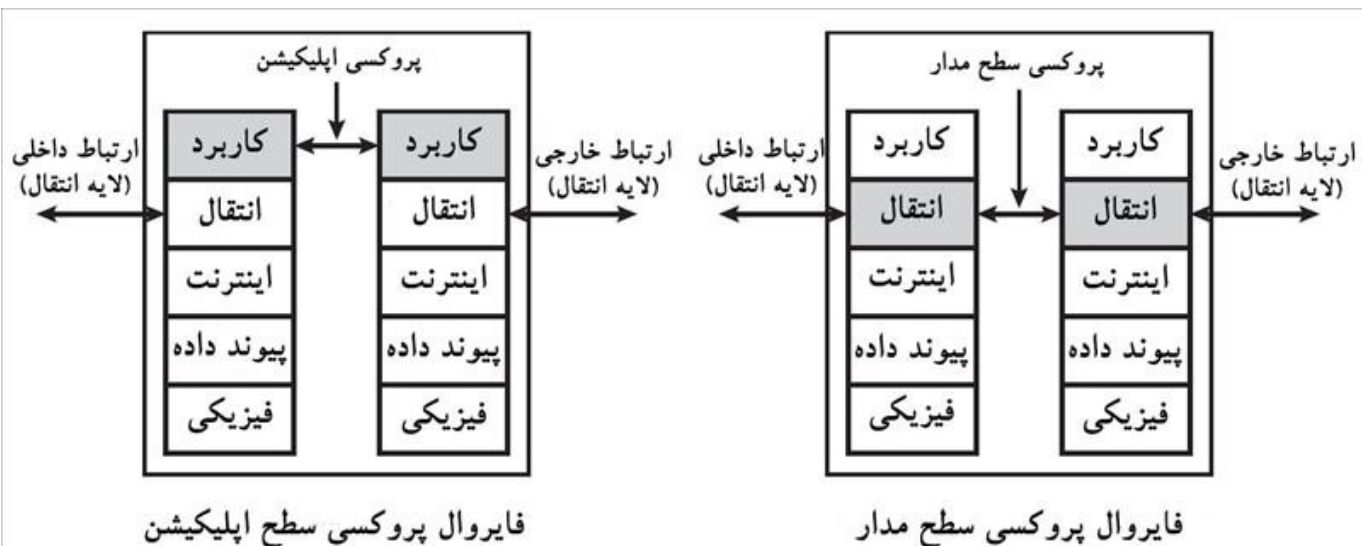
فیلتر کردن بسته‌ها

فیلتر کردن بسته‌ها (Packet Filtering) یکی از ساده‌ترین و سریع‌ترین روش‌ها برای کنترل ترافیک شبکه است. این روش در سطح IP عمل می‌کند و بر اساس آدرس‌های IP، پورت‌ها و پروتکل‌ها تصمیم می‌گیرد که یک بسته مجاز به عبور باشد یا نه. Stateful Inspection (فیلتر کردن بسته‌ها با حفظ وضعیت) روشی پیشرفته‌تر است که علاوه بر آدرس‌های IP، پورت‌ها و پروتکل‌ها، وضعیت هر بسته را نیز در حافظه می‌نگارد. Application-Level Gateway (گیت‌واهی سطح کاربردی) روشی پیچیده‌تر است که در سطح پروتکل کاربردی (مانند HTTP) ترافیک را بررسی می‌کند. Circuit-Level Gateway (گیت‌واهی سطح مدار) روشی دیگر است که فقط ارتباطات را بررسی می‌کند. Stateless (بدون حالت) روشی است که هیچ حافظه‌ای برای وضعیت بسته‌ها ندارد. Stateful (با حفظ وضعیت) روشی است که وضعیت بسته‌ها را در حافظه می‌نگارد. Stateful Packet Inspection (SPI) یا Stateful Packet Filtering (فیلتر کردن بسته‌ها با حفظ وضعیت) روشی است که وضعیت بسته‌ها را در حافظه می‌نگارد و بر اساس این وضعیت تصمیم می‌گیرد که یک بسته مجاز به عبور باشد یا نه. این روش 2 نوع دارد: Network-Level و Application-Level.



2 - فایروال‌های سطح کاربردی (Application-Level Gateway)

فایروال‌های سطح کاربردی (Application-Level Gateway) یا Application Proxy، در سطح پروتکل کاربردی (مانند HTTP) ترافیک را بررسی می‌کنند. این روش 7 نوع دارد: 1. HTTP Proxy، 2. FTP Proxy، 3. SMTP Proxy، 4. POP3 Proxy، 5. IMAP Proxy، 6. NNTP Proxy، 7. Telnet Proxy. این روش‌ها معمولاً در سرورهای وب استفاده می‌شوند.

[illegible][illegible]

□ □ □ □ □ □ □ □ □ □ □ □



□□ □□ □□□□□□□□ □□□□ □□□□ □□□□ □□□□

امنیت شبکه با استفاده از فایروال

فایروال یک سیستم امنیتی است که ترافیک ورودی و خروجی شبکه را کنترل می‌کند. این سیستم بر اساس قوانین (rules) تعریف شده عمل می‌کند و می‌تواند ترافیک را بر اساس آدرس IP، پورت و پروتکل مسدود یا اجازه دهد. فایروال می‌تواند به صورت سخت‌افزاری یا نرم‌افزاری پیاده‌سازی شود. در این مقاله، ما به بررسی انواع فایروال و نحوه پیکربندی آن خواهیم پرداخت.

انواع فایروال

فایروال‌ها را می‌توان به دو دسته فایروال مبتنی بر پورت و فایروال مبتنی بر محتوا تقسیم کرد. فایروال مبتنی بر پورت فقط بر اساس آدرس IP و پورت ترافیک را کنترل می‌کند، در حالی که فایروال مبتنی بر محتوا ترافیک را بر اساس محتوای آن نیز کنترل می‌کند.

:انواع فایروال

فایروال مبتنی بر پورت

:فایروال مبتنی بر محتوا

فایروال مبتنی بر پورت

فایروال مبتنی بر محتوا

فایروال مبتنی بر پورت

:فایروال مبتنی بر محتوا

12:10 - 30/11/1396

:فایروال

فایروال - فایروال - فایروال - فایروال - NGFW - Next Generation Firewalls
فایروال - فایروال - Application-Level Gateway فایروال - فایروال

فایروال

<https://www.shabakeh-mag.com/networking-technology/11378/%D8%AF%DB%8C%D9%88%D8%A7%D8%B1-%D8%A2%D8%AA%D8%B4%E2%80%8C%D9%87%D8%A7-%DA%86%DA%AF%D9%88%D9%86%D9%87-%D9%85%D9%89%E2%80%8C%D8%AA%D9%88%D8%A7%D9%86%D9%86%D8%AF-%D8%A7%D8%B2-%D8%B4%D8%A8%DA%A9%D9%87%E2%80%8C%D9%87%D8%A7-%D9%88-%D8%B3%D8%A7%D9%85%D8%A7%D9%86%D9%87%E2%80%8C%D9%87%D8%A7%D9%89-%DA%A9%D8%A7%D9%85%D9%BE%DB%8C%D9%88%D8%AA%D8%B1%D9%89-%D9%85%D8%AD%D8%A7%D9%81%D8%B8%D8%AA>