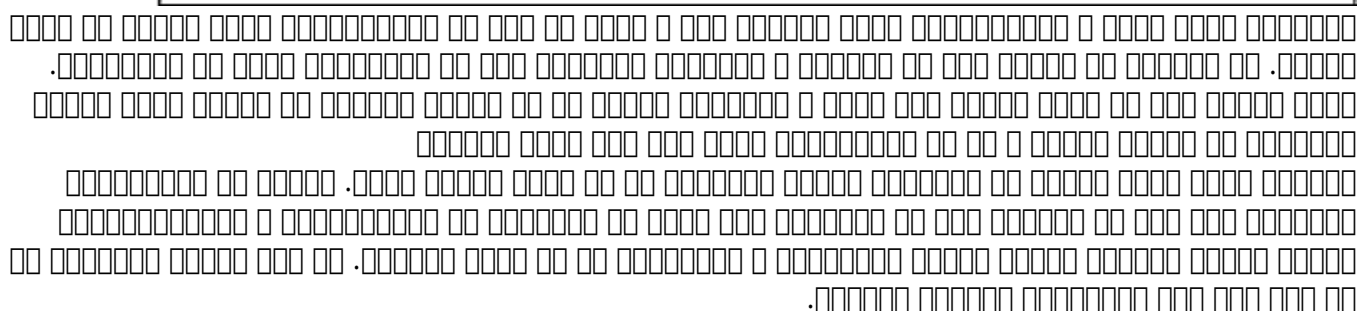




□ □ □ □ □    □ □ □ □    □ □    □ □    □ □ □ □ □    □ □    □    □ □ □ □    □ □ □ □ □ □ □ □

[illegible]

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**

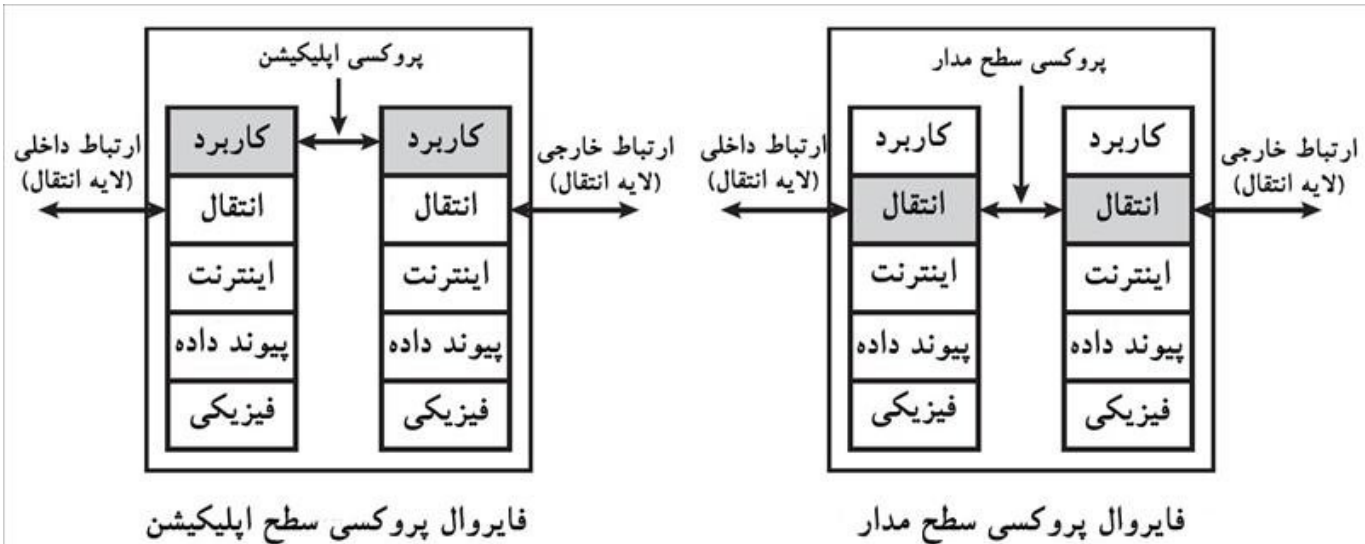
10. **Access Control List (ACL) 10**

The diagram illustrates two types of firewalls: Packet filtering and Stateful Inspection.

**Packet filtering:** On the left, a vertical stack of boxes represents the OSI model layers: کاربر (User), انتقال (Network), اینترنت (Internet), پیوند داده (Data Link), and فیزیکی (Physical). A horizontal line with arrows at both ends passes through the 'انتقال' layer, labeled 'ارتباط انتها به انتها در لایه انتقال' (End-to-end connection in the transport layer). Below this is the label 'فایروال Packet filtering'.

**Stateful Inspection:** On the right, a similar vertical stack of layers is shown. A horizontal line with arrows at both ends passes through the 'انتقال' layer, labeled 'ارتباط انتها به انتها در لایه انتقال'. Below this stack is a cylinder labeled 'اطلاعات وضعیتی' (Stateful information), which is connected to the 'انتقال' layer. Below this is the label 'فایروال Stateful Inspection'.

0000 000000 000000 000 000 00000000 00 Application Proxy 00 Application-Level Gateway 00000000  
 00000 0 000000 00000000 0 0000000 0000 0000 0 000000 000 000000000 .00000 00000 00 7 00000 00 000000  
 0000000 0 00 000000 00 000000000 0000 00 HTTP 0000000 000 00000 00000000 000 000 .000000 00 0000000000  
 (3 000) .000 000000 00000000 00 00 000000 000000000 0000 000000000000000000 00 0000 00 HTTP



3 - پروکسی سطح اپلیکیشن و پروکسی سطح مدار

پروکسی سطح اپلیکیشن (Application Proxy) یک سرور میانی است که ترافیک بین کاربران و سرورهای مقصد را مدیریت می‌کند. این پروکسی می‌تواند ترافیک را در سطح پروتکل TCP (Transmission Control Protocol) بررسی کند و می‌تواند ترافیک را بر اساس قوانین تعریف شده فیلتر کند. پروکسی سطح اپلیکیشن می‌تواند ترافیک را در سطح پروتکل TCP (Transmission Control Protocol) بررسی کند و می‌تواند ترافیک را بر اساس قوانین تعریف شده فیلتر کند. پروکسی سطح اپلیکیشن می‌تواند ترافیک را در سطح پروتکل TCP (Transmission Control Protocol) بررسی کند و می‌تواند ترافیک را بر اساس قوانین تعریف شده فیلتر کند. (3 پروکسی)

## NGFW(Next Generation Firewalls) پروکسی سطح اپلیکیشن

پروکسی سطح اپلیکیشن (Application Proxy) یک سرور میانی است که ترافیک بین کاربران و سرورهای مقصد را مدیریت می‌کند. این پروکسی می‌تواند ترافیک را در سطح پروتکل TCP (Transmission Control Protocol) بررسی کند و می‌تواند ترافیک را بر اساس قوانین تعریف شده فیلتر کند. پروکسی سطح اپلیکیشن می‌تواند ترافیک را در سطح پروتکل TCP (Transmission Control Protocol) بررسی کند و می‌تواند ترافیک را بر اساس قوانین تعریف شده فیلتر کند. پروکسی سطح اپلیکیشن می‌تواند ترافیک را در سطح پروتکل TCP (Transmission Control Protocol) بررسی کند و می‌تواند ترافیک را بر اساس قوانین تعریف شده فیلتر کند. VoIP (Voice over IP) یک فناوری است که امکان انتقال صدا و تصویر را از طریق اینترنت فراهم می‌کند. NGFW (Next Generation Firewall) یک فایروال نسل بعدی است که علاوه بر فیلتر کردن ترافیک بر اساس قوانین تعریف شده، می‌تواند ترافیک را بر اساس پروتکل‌های مختلف (مانند TLS/SSL) بررسی کند. NGFW می‌تواند ترافیک را در سطح پروتکل OSI (Open Systems Interconnection) بررسی کند و می‌تواند ترافیک را بر اساس قوانین تعریف شده فیلتر کند. malware (مال‌ویر) یک برنامه مخرب است که می‌تواند به سیستم‌ها آسیب بزند. پروکسی سطح اپلیکیشن می‌تواند ترافیک را در سطح پروتکل OSI (Open Systems Interconnection) بررسی کند و می‌تواند ترافیک را بر اساس قوانین تعریف شده فیلتر کند. malware (مال‌ویر) یک برنامه مخرب است که می‌تواند به سیستم‌ها آسیب بزند. پروکسی سطح اپلیکیشن می‌تواند ترافیک را در سطح پروتکل OSI (Open Systems Interconnection) بررسی کند و می‌تواند ترافیک را بر اساس قوانین تعریف شده فیلتر کند. malware (مال‌ویر) یک برنامه مخرب است که می‌تواند به سیستم‌ها آسیب بزند.

پروکسی سطح اپلیکیشن



پروکسی سطح اپلیکیشن

## روش های مختلف برای تشخیص نفوذ

در این مقاله به روش های مختلف برای تشخیص نفوذ در شبکه های کامپیوتری پرداخته می شود. این روش ها شامل روش های مبتنی بر تحلیل ترافیک شبکه، روش های مبتنی بر تحلیل رفتار کاربران، روش های مبتنی بر تحلیل رفتار سیستم ها و روش های مبتنی بر تحلیل رفتار دستگاه های متصل به شبکه می باشد. این روش ها می توانند به مدیران شبکه کمک کنند تا بتوانند نفوذ را تشخیص دهند و اقدامات لازم را برای جلوگیری از نفوذ انجام دهند. این روش ها می توانند به مدیران شبکه کمک کنند تا بتوانند نفوذ را تشخیص دهند و اقدامات لازم را برای جلوگیری از نفوذ انجام دهند. این روش ها می توانند به مدیران شبکه کمک کنند تا بتوانند نفوذ را تشخیص دهند و اقدامات لازم را برای جلوگیری از نفوذ انجام دهند.

## روش های مختلف

در این مقاله به روش های مختلف برای تشخیص نفوذ در شبکه های کامپیوتری پرداخته می شود. این روش ها شامل روش های مبتنی بر تحلیل ترافیک شبکه، روش های مبتنی بر تحلیل رفتار کاربران، روش های مبتنی بر تحلیل رفتار سیستم ها و روش های مبتنی بر تحلیل رفتار دستگاه های متصل به شبکه می باشد. این روش ها می توانند به مدیران شبکه کمک کنند تا بتوانند نفوذ را تشخیص دهند و اقدامات لازم را برای جلوگیری از نفوذ انجام دهند. این روش ها می توانند به مدیران شبکه کمک کنند تا بتوانند نفوذ را تشخیص دهند و اقدامات لازم را برای جلوگیری از نفوذ انجام دهند. این روش ها می توانند به مدیران شبکه کمک کنند تا بتوانند نفوذ را تشخیص دهند و اقدامات لازم را برای جلوگیری از نفوذ انجام دهند.

:روش های مختلف

روش های مختلف

:روش های مختلف

روش های مختلف

روش های مختلف

روش های مختلف

:روش های مختلف

12:10 - 30/11/1396

:روش های مختلف

روش های مختلف - روش های مختلف - روش های مختلف - روش های مختلف - NGFW - Next Generation Firewalls  
روش های مختلف - روش های مختلف - Application-Level Gateway روش های مختلف - روش های مختلف

روش های مختلف

<https://www.shabakeh-mag.com/tricks/network-tricks/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>