درس ۱۲: فایروال (دیواره آتش)

فهرست مطالب

مقدمه

- گسترش ارتباطات شبکه‌ای
- نیاز به استفاده از زیرساخت اینترنت توسط هر فرد
- ایجاد تعامل بین شبکه‌های مختلف
- مشکل بودن ایجاد امنیت در هر سیستم درون سازمانی
- نیاز به یک لایه دفاعی جلوی جبهه با استفاده از فایروال
- فایروال به عنوان بخشی از استراتژی کلی تامین امنیت است.

فایروال چیست؟

- نقطه کنترل و نظارت شبکه
- امکان اتصال شبکه‌ها با سطوح اعتماد مختلف با یکدیگر
- ترافیک گذرنده از داخل به خارج و برعکس، باید از داخل فایروال عبور کند.
- تنها اطلاعات و اشخاص مجاز، با توجه به سیاست‌های شبکه محلی، می‌توانند از فایروال عبور کنند.
- فایروال خود باید در مقابل نفوذ امن باشد (با استفاده از trusted system).

سرویس‌های فراهم شده توسط فایروالهای تجاری

- امکان بازرسی و کنترل دسترسی به شبکه و منابع و سرویس‌های آن
- امکان ثبت جریان ترافیک
- پالایش بر اساس محتوای بسته‌ها
- فراهم‌سازی ترجمه نشانی NAT و نظارت بر استفاده
- پیاده‌سازی شبکه خصوصی مجازی (VPN) مبتنی بر IPsec

فهرست مطالب

- مقدمه
- **ویژگی‌های فایروال**
- انواع فایروال‌ها

سازوکارهای کنترلی در فایروال

- Service Control
  - چه سرویس‌هایی قابل دسترسی هستند.
- Direction Control
  - درخواست به یک سرویس از کدام سمت می‌تواند ارسال و پاسخ داده شود.
- User Control
  - کنترل دسترسی به سرویس بر اساس شخص درخواست‌کننده

محدودیتهای فایروال

- فایروال‌ها نمی‌توانند با حملات زیر مقابله کنند:

☜ حملاتی که ترافیک آنها از فایروال عبور نمی‌کنند.

- اتصال کارکنان از طریق مودم Dial-up یا ADSL

☜ خطرات داخلی

- کارمندان ناراضی یا ساده لوح!

☜ ممانعت کامل از انتقال ویروس‌ها و فایل‌های اجرایی مخرب

- با توجه به تنوع سیستم عامل‌ها و انواع فایل‌های مورد پشتیبانی آنها

☜ ترافیک رمز شده

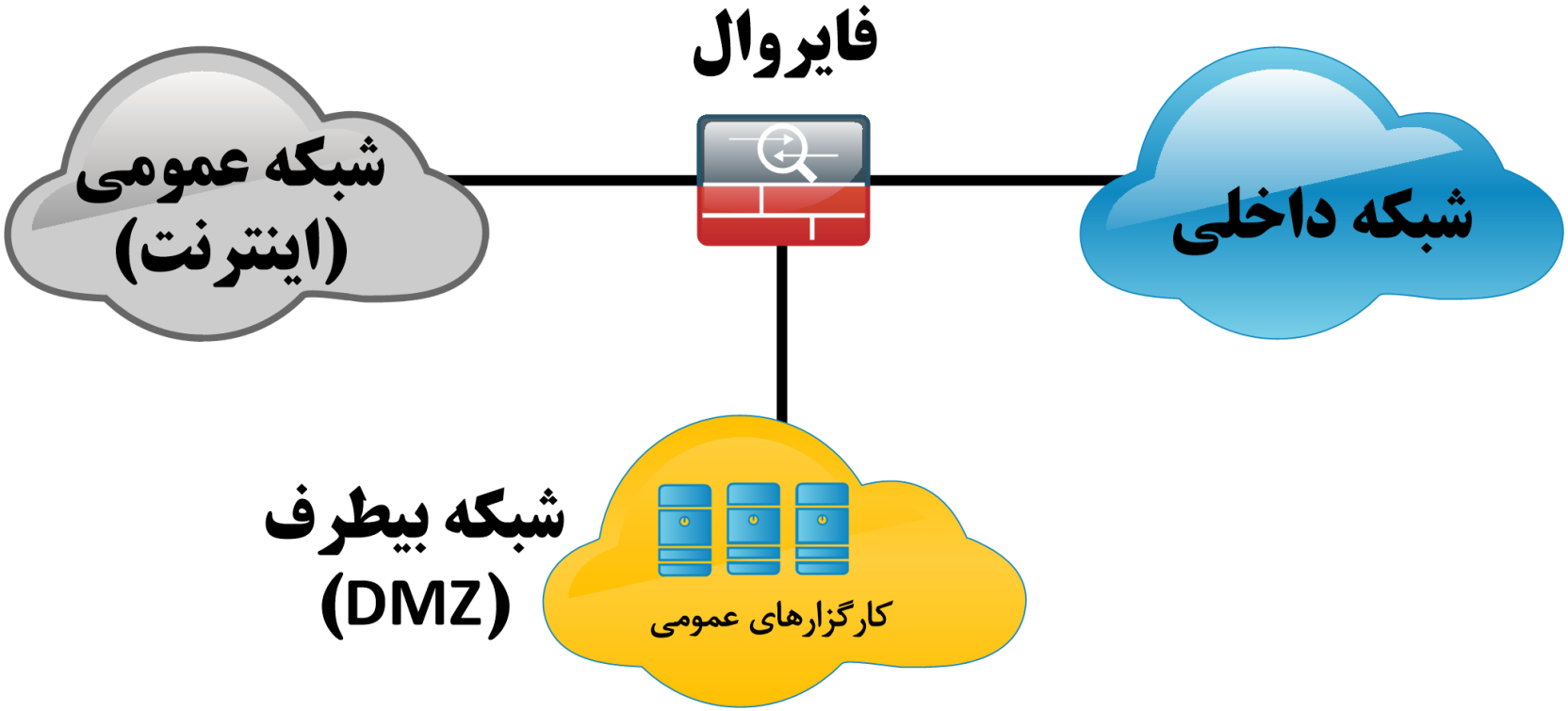
فهرست مطالب

انواع فایروال‌ها

- **فایروال شخصی (Personal):** روی یک میزبان نصب می‌شود، و ترافیک شبکه ورودی و خروجی به آن را کنترل می‌کند.
  - مثال: iptables و Windows Firewall
  - مزیت: قادر است به ترافیک نهایی که روی میزبان رمزگشایی می‌شود دسترسی داشته باشد.
  - اشکال: دید محدودی نسبت به شبکه دارد.
- **فایروال شبکه:** در بخشی از شبکه نصب شده و ترافیک ورودی و خروجی به آن بخش از شبکه را کنترل می‌کند.
  - مثال: ASA سیسکو، pfsense

مثال: ASA سیسکو

جایدهی فایروال در شبکه



DMZ: Demilitarized Zone

Packet Filter

- مبنای کلیه سیستم‌های فایروال است.
- هر بسته IP را چک کرده (صرف نظر از محتوا) و بر اساس قواعد امنیتی درباره عبور آن تصمیم می‌گیرد:
  - اجازه عبور: Permit
  - ممانعت از عبور: Deny
- قواعد بر اساس سرآیند IP و لایه انتقال (TCP/UDP/...) تعریف می‌شوند.
- پالایش در هر دو جهت قابل اِعمال است.

Packet Filter

- دسترسی به سرویس‌ها قابل کنترل است (با استفاده از پورت‌ها).
- مزیت: سادگی و پنهانی از دید کاربران
- ضعف:
  - عدم پشتیبانی از تصدیق هویت
  - اعمال قواعد متناسب با برنامه مشکل است.
- دو سیاست **پیش‌فرض** می‌تواند وجود داشته باشد:
  - Discard / Block = هر آنچه که صریحاً اجازه داده نشده، غیرمجاز است.
  - Forward / Allow = هر آنچه که صریحاً ممنوع نشده، مجاز است.

روش پالایش بسته در Packet Filter

- نوع پروتکل (IP، TCP، ICMP، ...)
- نشانی IP مبدأ و مقصد
- پورت مبدأ و مقصد
- حالت ارتباط (پرچم‌های SYN، ACK یا RST در TCP، Related، Established)
- زمان: فعال کردن سرویس در یک بازه زمانی خاص
- واسط ورودی/خروجی (eth0، eth1)

مثال ۱

- **توضیح:** قواعد از بالا به پایین و به واسط ورودی اعمال می‌شوند.
- ایمیل‌های ورودی از ENEMY (1.2.3.*) مسدود می‌شوند.
- ایمیل‌های ورودی (پورت ۲۵ از SMTP) فقط می‌توانند به میزبان SMTP_GW (213.233.161.*) فرستاده شوند.

	action	ourhost	port	theirhost	port	comment
A	block	*	25	ENEMY	*	we don't trust these people
	allow	SMTP_GW	25	*	*	connection to our SMTP port

مثال ۲

- بیان سیاست پیش‌فرض (default = deny).
- این قاعده به صورت صریح در انتهای مجموعه قواعد می‌آید.

B	action	ourhost	port	theirhost	port	comment
	block	*	*	*	*	default

مثال ۳

- هر گره از داخل شبکه می‌تواند به بیرون از شبکه ایمیل ارسال کند.

☜این قاعده به واسط خروجی اعمال می‌شود.

- **مشکل:** ممکن است بجای سرویس ایمیل، سرویس دیگری روی پورت ۲۵ قرار گرفته باشد. در این صورت نفوذگر می‌تواند بسته‌ای با پورت مبدأ ۲۵ را به هر ماشین در داخل شبکه ارسال کند!

	action	ourhost	port	theirhost	port	comment
C	allow	*	*	*	25	connection to their SMTP port

مثال ۴

- بسته هایی که مبدأ آنها متعلق به لیست ماشین‌های میزبان داخلی و مقصد آنها، پورت ۲۵ از TCP باشند، اجازه عبور دارند.
- بسته های ورودی با پورت مقصد ۲۵ از TCP اجازه عبور دارند، به شرطی که پرچم ACK آنها روشن باشد.
- پرچم ACK تأیید می‌کند که بسته‌ها از طرف مقابل در تأیید بسته‌های ارسالی رسیده‌اند.

	action	src	port	dest	port	flags	comment
D	allow	{our hosts}	*	*	25		our packets to their SMTP port
	allow	*	25	*	*	ACK	their replies

حملات وارده به Packet Filter – ۱

- **جعل نشانی IP:** فرستادن بسته از خارج با نشانی مبدأ داخلی جعلی (با هدف دسترسی به سرویس‌هایی که صرفاً نشانی IP مبدأ را برای دسترسی کنترل می‌نمایند).

  ☜ **راه حل:** انسداد بسته‌های فوق توسط فایروالها.

- **مسیردهی از مبدأ:** فرستنده، مسیر انتقال بسته را مشخص و همراه آن می‌فرستد و بدین ترتیب فایروال را دور می‌زند. (گزینه source routing در سرآیند IP).

  ☜ **راه حل:** انسداد بسته‌های حاوی اطلاعات مسیر توسط مسیریابها.

حملات وارده به Packet Filter – ۲

- **بسته های IP قطعه‌قطعه شده:** سرآیند بسته اصلی در بسته‌های کوچکتر شکسته می‌شود.

☜ **راه حل:** انسداد بسته‌های کوچکی که گزینه تقسیم IP آنها set شده است و یا ابتدا بازسازی بسته اصلی و سپس کنترل آن.

فایروال‌های حالتمند (Stateful)

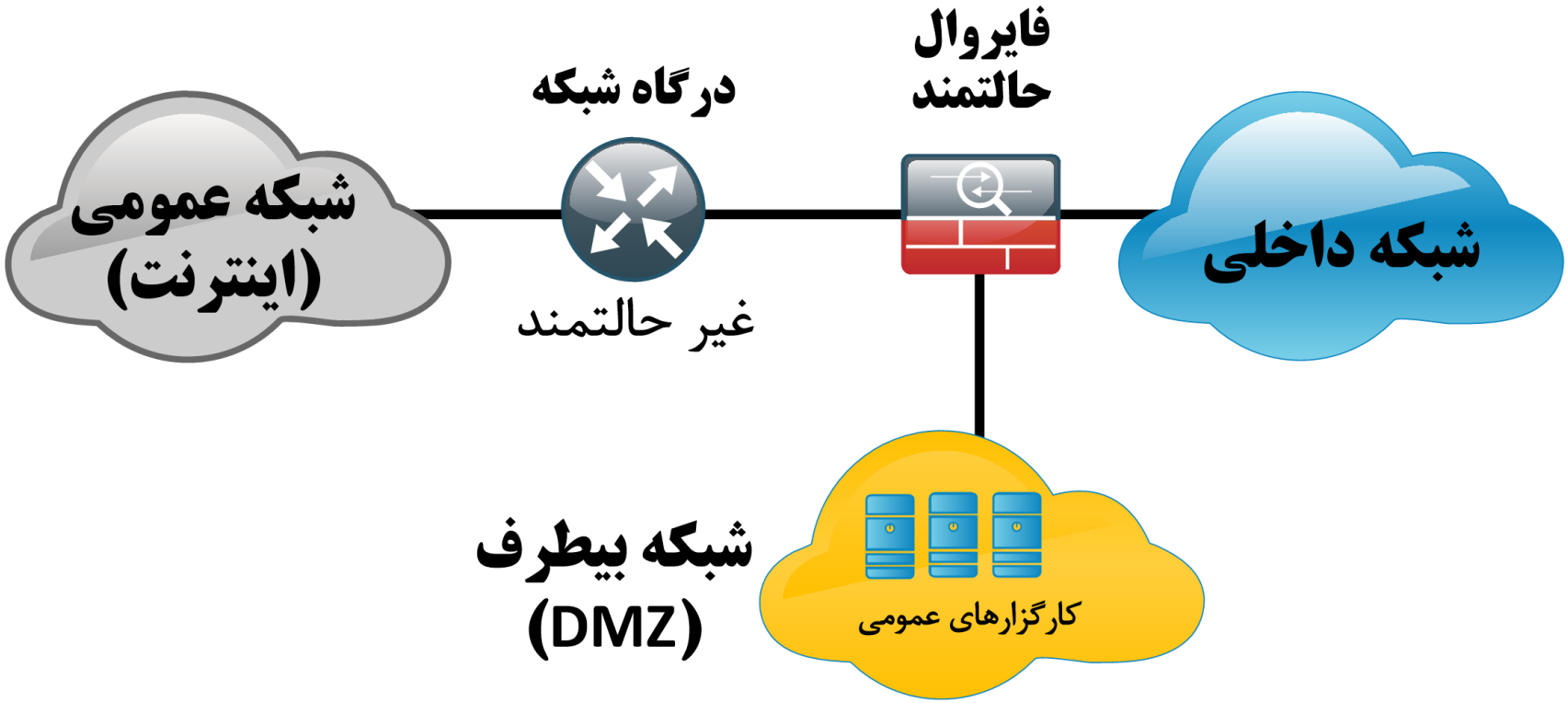
- **SPI:** Stateful Packet Inspection
  - وارسی بسته‌ها فقط منحصر به اطلاعات سرآیند آنها نیست.
  - هر بسته بخشی از یک اتصال است، و باید در context آن اتصال وارسی شود.
  - **مثال ۱:** کارگزار موجود در DMZ حق ندارد شروع کننده اتصال به بیرون باشد، و فقط حق دارد به اتصالی که از بیرون برقرار شده پاسخ دهد.
  - **مثال ۲:** FTP در حالت Active

فایروال‌های حالتمند

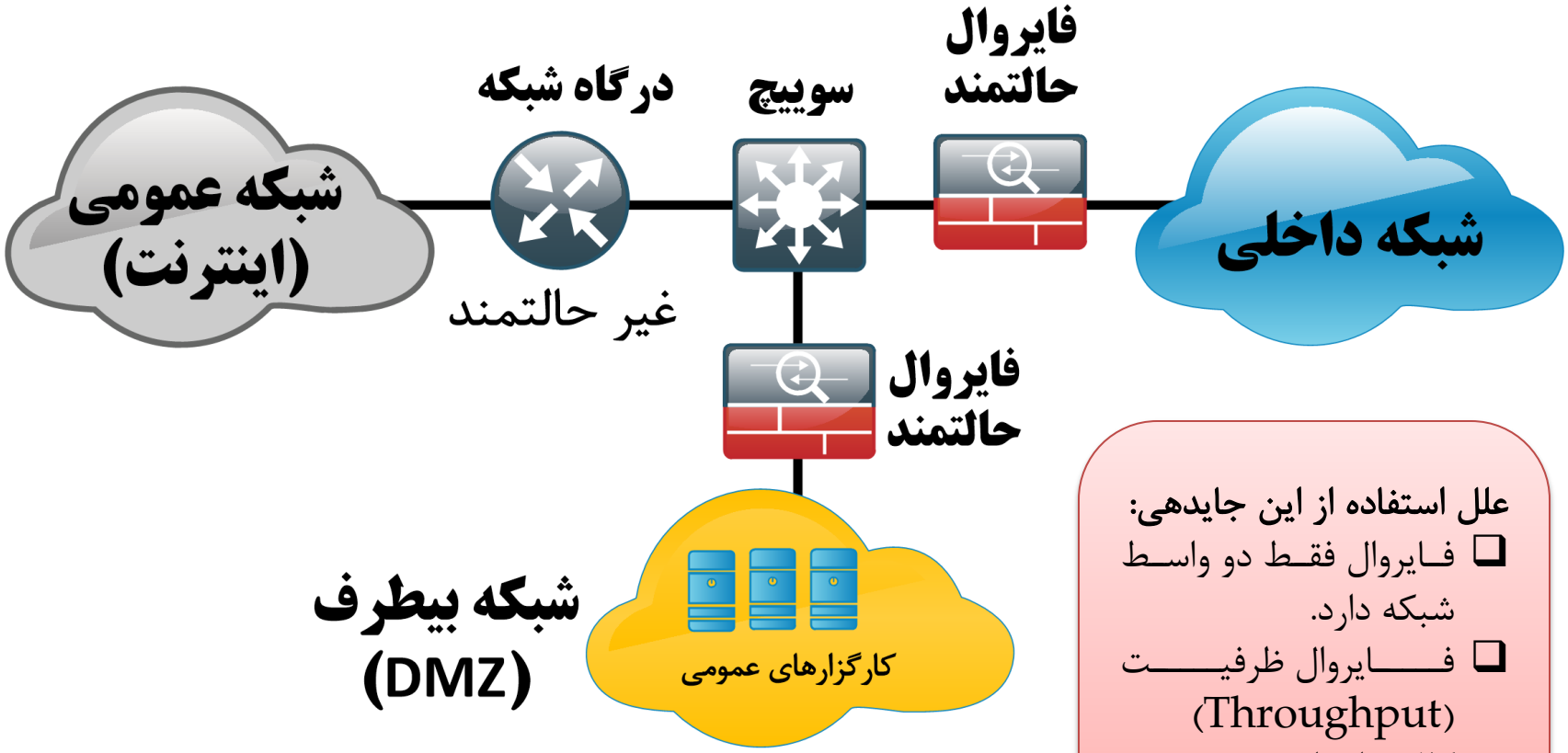
- اطلاعات مربوط به اتصالات برقرار شده را نگهداری می‌نمایند.

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING
TCP	127.0.0.1:1541	127.0.0.1:5354	ESTABLISHED
UDP	127.0.0.1:1542	127.0.0.1:5354	ESTABLISHED
UDP	127.0.0.1:1570	127.0.0.1:15485	ESTABLISHED
TCP	127.0.0.1:1576	127.0.0.1:27015	ESTABLISHED
TCP	127.0.0.1:5555	127.0.0.1:14181	TIME_WAIT
TCP	192.168.1.4:14198	74.125.71.19:443	TIME_WAIT
TCP	192.168.1.4:14199	74.125.71.99:443	TIME_WAIT

جایدهی فایروال حالتمند در شبکه



جایدهی دیگر فایروال حالتمند در شبکه



علل استفاده از این جایدهی:

- فایروال فقط دو واسط شبکه دارد.
- فایروال ظرفیت (Throughput) کافی را ندارد.
- دفاع چند لایه

فایروال لایه کاربرد

- فایروالهای از نوع Packet Filter تنها می‌توانند بسته‌ها را در لایه شبکه و انتقال وارسی کنند.
- امروزه لازم است حملات در سطح لایه کاربرد نیز وارسی شود.
  - ایجاد فایروالهایی خاص یک یا چند پروتکل لایه کاربرد
- انواع معروف فایروال لایه کاربرد:
  - Web Application Firewall (یا WAF): شامل قوانینی برای جلوگیری از حملاتی نظیر XSS یا SQL Injection
    - **مثال:** ModSecurity برای کارگزارهای وب آپاچی، IIS و NGINX
  - DB Firewall

پایان