یا ذاالامن والامان

امنیت داده و شبکه

فایروال (دیواره آتش)

مرتضی امینی - نیمسال دوم ۱۴۰۰-۱۳۹۹

مرکز امنیت داده و شبکه شریف
http://dnsl.ce.sharif.edu

فهرست مطالب

- مقدمه
- ویژگی‌های فایروال
- انواع فایروال‌ها
- پیکربندی فایروال‌ها
- آشنایی با فایروال iptables

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).

فایروال چیست؟

- سرویس‌های فراهم شده توسط فایروالهای تجاری:
  - امکان بازرسی و کنترل دسترسی به شبکه و منابع و سرویس‌های آن
  - امکان ثبت جریان ترافیک (netflow)
  - پالایش بر اساس محتوای بسته‌ها (filtering)
  - فراهم‌سازی ترجمه آدرس NAT و نظارت بر استفاده
  - پیاده‌سازی شبکه خصوصی مجازی (VPN) مبتنی بر IPSec

فهرست مطالب

- مقدمه
- **ویژگی‌های فایروال**
- انواع فایروال‌ها
- پیکربندی فایروال‌ها
- آشنایی با فایروال iptables

مکانیزم‌های کنترلی در فایروال

- Service Control
  - سرویس‌های اینترنتی قابل دسترسی
  - اعمال کنترل بر اساس آدرس IP و پورت
  - استفاده از پروکسی برای سرویس‌های استاندارد (FTP، Telnet،...)
- Direction Control
  - اینکه درخواست 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 از فایروال عبور نمی‌کنند.
    - مثال: اتصال کارکنان از طریق مودم 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

فهرست مطالب

- مقدمه
- ویژگی‌های فایروال
- **انواع فایروال‌ها**
- پیکربندی فایروال‌ها
- آشنایی با فایروال iptables

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

انواع فایروال‌ها

- از منظر لایه‌ای که در آن به کنترل می‌پردازند:
  - **Packet Filters**
  - **Application-Level Gateways**
  - **Circuit-Level Gateways**

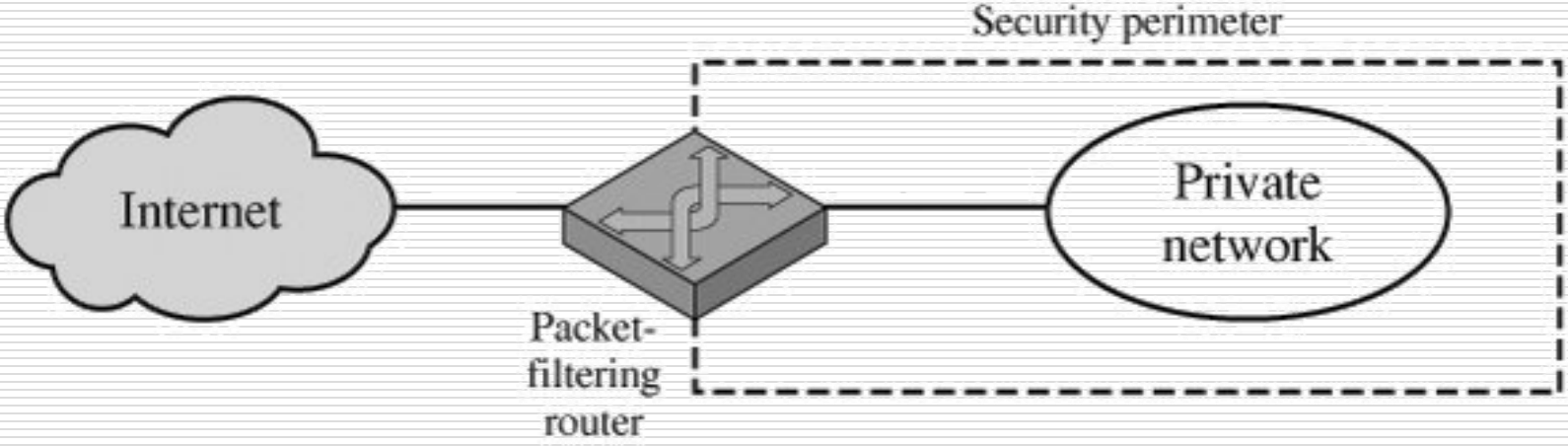
انواع فایروال‌ها
Packet Filters

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

انواع فایروال‌ها
Packet Filters

- دسترسی به سرویس‌ها قابل کنترل است (با استفاده از پورت‌ها).
- مزیت: سادگی و پنهانی از دید کاربران
- ضعف:
  - عدم پشتیبانی از احراز 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.

انواع فایروال‌ها
Packet Filters



انواع فایروال‌ها
Packet Filters

- پالایش بسته‌ها در این نوع فایروال‌ها بر اساس فیلدهای زیر صورت می‌گیرد:
  - نوع پروتکل (IP، TCP، ICMP، ...)
  - آدرس IP مبدا و مقصد
  - پورت مبدا 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)

انواع فایروال‌ها
Packet Filters

- مثال ۱ (توضیح : قواعد از بالا به پایین اعمال می‌شوند)
  - ایمیل‌های ورودی از SPIGOT (81.31.159.*) مسدود می‌شوند.
  - ایمیل‌های ورودی (پورت ۲۵ از SMTP) از شبکه‌هایی غیر از SPIGOT فقط می‌توانند به میزبان OUR_GW (213.233.161.*) فرستاده شوند.

	action	ourhost	port	theirhost	port	comment
A	block	*	25	SPIGOT	*	we don't trust these people
	allow	OUR-GW	25	*	*	connection to our SMTP port

انواع فایروال‌ها
Packet Filters

- 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

انواع فایروال‌ها
Packet Filters

- مثال ۳

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

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

انواع فایروال‌ها
Packet Filters

- مثال ۴

- بسته هایی که مبدا 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 تایید می‌کند که بسته‌ها از طرف مقابل در تایید 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 Filters

- جعل آدرس IP: فرستادن بسته از خارج با آدرس مبدا داخلی جعلی (با هدف دسترسی به سرویس‌هایی که صرفاً آدرس IP مبدا را برای دسترسی، کنترل می‌نمایند).
  - راه حل: انسداد بسته‌های فوق توسط فایروالها.
- تعیین مسیر توسط مبدأ: فرستنده مسیر انتقال بسته را مشخص و همراه آن می‌فرستد و بدین ترتیب فایروال را دور می‌زند.
  (options-0-3,9/control-source routing از سرآیند IP).
  - راه حل: انسداد بسته‌های حاوی اطلاعات مسیر توسط مسیریابها.
- بسته های IP قطعه قطعه 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)

- در اتصال به سرورها،
  - آدرس پورت سرور معمولاً زیر ۱۰۲۴ و شناخته شده است.
  - آدرس پورت مشتری می تواند هر مقدار بزرگتر مساوی ۱۰۲۴ باشد.
  - لذا نمی‌توان قاعده‌ای را برای پورت مبدا در بسته‌های ارسالی و پورت مقصد در بسته‌های دریافتی در نظر گرفت.
- پالایش حالتمند، این نیاز را برطرف می‌کند.
- می‌توان جهت اتصال را با آن مشخص و صرفا اجازه دریافت بسته بابت اتصالات برقرار شده را صادر کرد.

فایروال‌های حالتمند

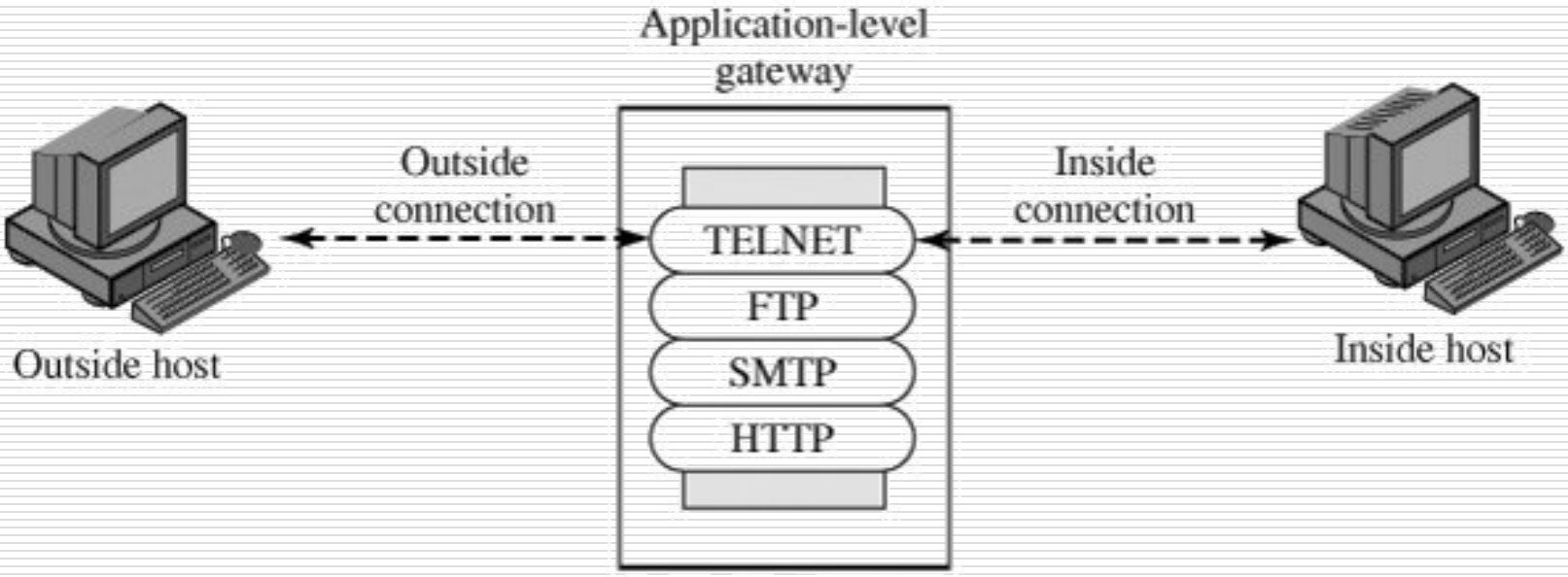
- اطلاعات مربوط به اتصالات برقرار شده را نگهداری می‌نمایند.
  - صرفاً بسته‌های دریافتی در صورت تعلق به یکی از اتصالات جاری پذیرفته می‌شوند.

Source Address	Source Port	Destination Address	Destination Port	Connection State
192.168.1.100	1030	210.9.88.29	80	Established
192.168.1.102	1031	216.32.42.123	80	Established
192.168.1.101	1033	173.66.32.122	25	Established
192.168.1.106	1035	177.231.32.12	79	Established
223.43.21.231	1990	192.168.1.6	80	Established
219.22.123.32	2112	192.168.1.6	80	Established

انواع فایروال‌ها
Application-Level Gateway

- 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: برای مقابله با حملات به پایگاه داده مانند SQL Injection

انواع فایروال‌ها
Application-Level Gateway



انواع فایروال‌ها
Application-Level Gateway

- بیشتر به عنوان Proxy Server اطلاق می‌شود.
- اصولا نقش واسط انتقال ترافیک در لایه کاربرد را ایفا می‌کند:
  - کاربر از proxy تقاضای سرویس می‌کند.
  - Proxy صلاحیت کاربر برای استفاده از سرویس را بررسی می‌کند و قواعد کنترلی را اعمال می‌کند.
  - Proxy با سرور اصلی تماس می‌گیرد و قطعات TCP را منتقل می‌کند.
  - اگر سرویس موردنظر در proxy پیاده‌سازی نشده باشد، سرویس غیرقابل دسترسی خواهد بود.

انواع فایروال‌ها
Application-Level Gateway

مزایا

- تنها با لیست محدودی از برنامه‌های کاربردی سروکار دارد.
- ترافیک ورودی به سادگی قابل ردیابی و بازرسی است.
- نسبت به حمله DoS مقاوم‌تر است.
- امکان پالایش بر اساس محتوای بسته‌ها وجود دارد.

در مجموع امنیت بیشتری فراهم می‌کند.

انواع فایروال‌ها
Application-Level Gateway

معایب

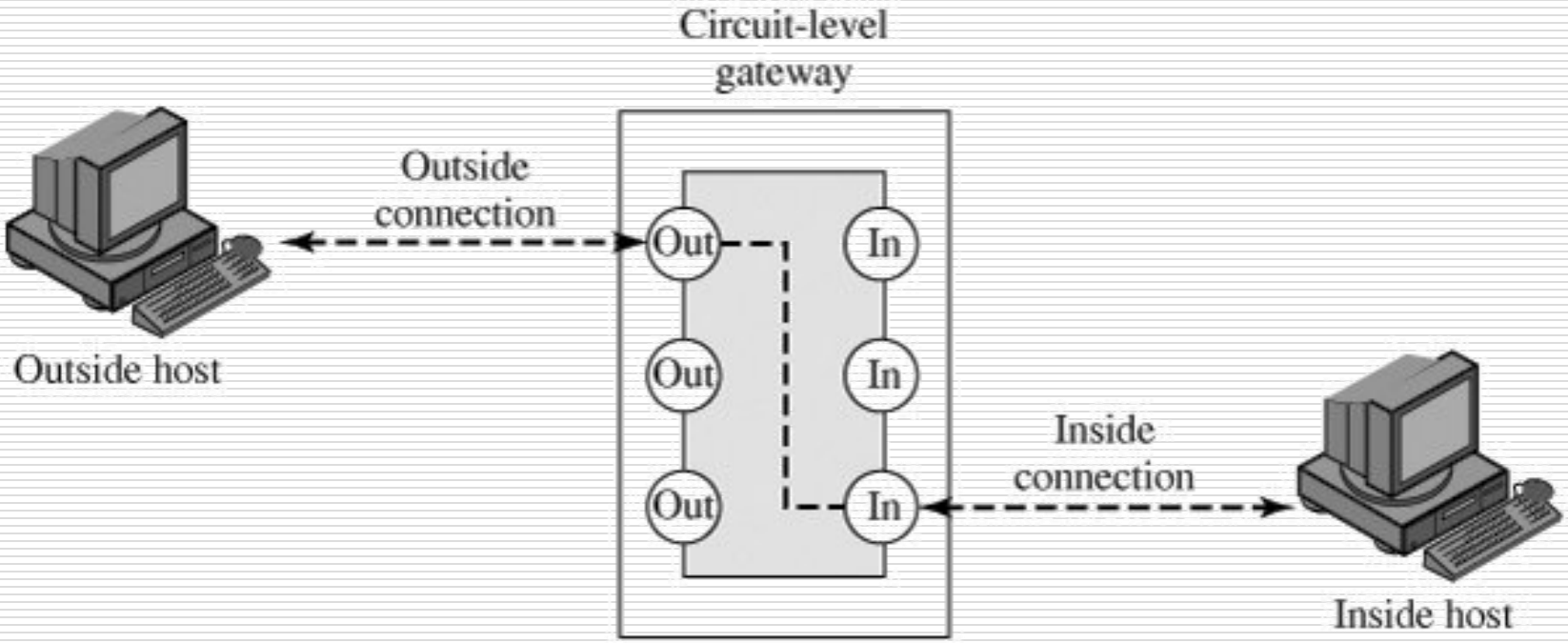
- سربار بوجود آمده برای ایجاد هر اتصال جدید.
- طرفین با هم ارتباط مستقیم ندارند.

در مجموع کارآیی کمتری دارد.

انواع فایروال‌ها
Circuit-Level Gateway

- در واقع در لایه نشست (بین لایه TCP و لایه برنامه کاربردی) عمل می‌کند.
- ارتباط انتها به انتها بین میزبان بیرونی و میزبان درون شبکه برقرار نمی‌شود.
- با وجود فایروال Circuit-Level، دو ارتباط جداگانه TCP، یکی با میزبان داخلی و یکی با میزبان خارجی برقرار می‌شود.
- ترافیک بدون کنترل محتوای داخلی آن منتقل می‌شود و صرفاً کنترل می‌کند که یک ارتباط برقرار شود یا نه.
- احراز هویت هم می‌تواند توسط فایروال Circuite-Level انجام شود.
- مزیت اصلی آن پنهان‌سازی شبکه داخلی است.

انواع فایروال‌ها
Circuit-Level Gateway



انواع فایروال‌ها
Circuit-Level Gateway

- عموما وقتی کاربران داخلی قابل اعتماد هستند، به کار می‌رود. در این حالت :
  - برای ارتباطات ورودی از proxy استفاده می‌شود.
  - برای ارتباطات خروجی از circuit-level gateway استفاده می‌شود، تا دسترسی به سرویس‌های بیرونی کنترل شود.
- SOCKS یکی از پیاده‌سازی‌های circuit-level gateway است که نسخه ۵ آن در RFC 1928 آمده است.

فهرست مطالب

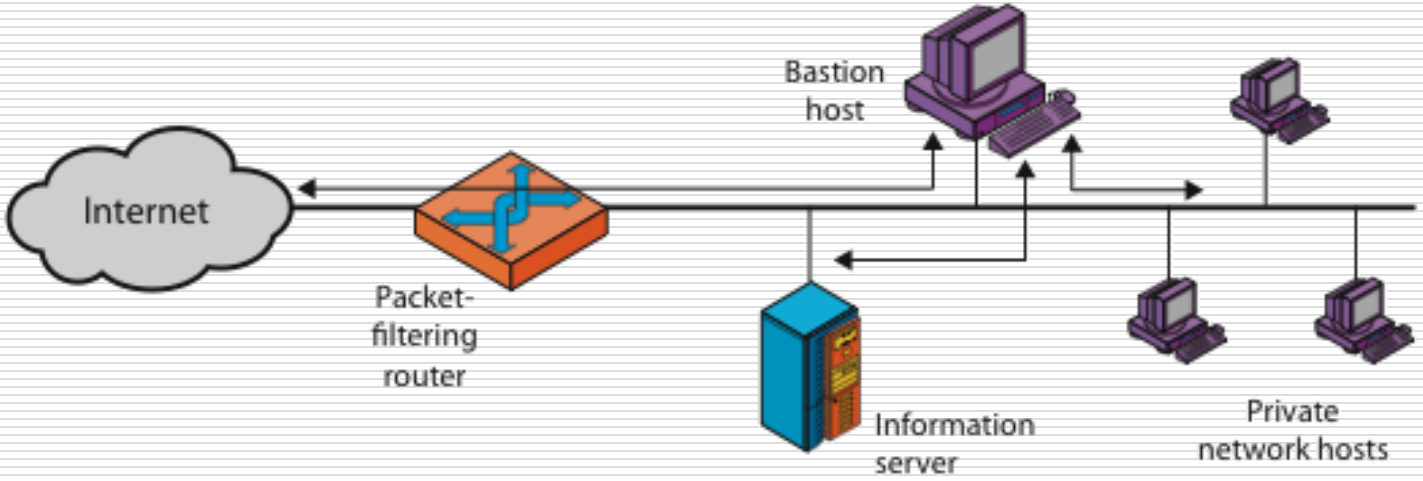
- مقدمه
- ویژگی‌های فایروال
- انواع فایروال‌ها
- **پیکربندی فایروال‌ها**
- آشنایی با فایروال iptables

Bastion Host

- یک نقطه بحرانی از نظر امنیت و قابل اعتماد در شبکه داخلی است.
- عموما Proxy Server ها یا Circuit-level Gateway ها روی آن نصب می‌شوند.
- یک نسخه امن سیستم عامل روی آن اجرا می‌شود.
- Proxyها زیرمجموعه‌ای از ویژگیهای سرویسها را پشتیبانی می‌کنند.
- Proxyها دسترسی به میزبان‌های خاصی را مجاز می‌شمارند.
- Proxyها جزییات وقایع امنیتی را ثبت می‌کنند.
- Proxyها از همدیگر مستقل هستند.
- بجز خواندن فایل پیکربندی در ابتدای زمان راه اندازی، دسترسی به دیسک ندارند (امنیت بیشتر در مقابل ویروسها و اسبهای تروا).

پیکربندی فایروالها
Single-Homed Bastion Host

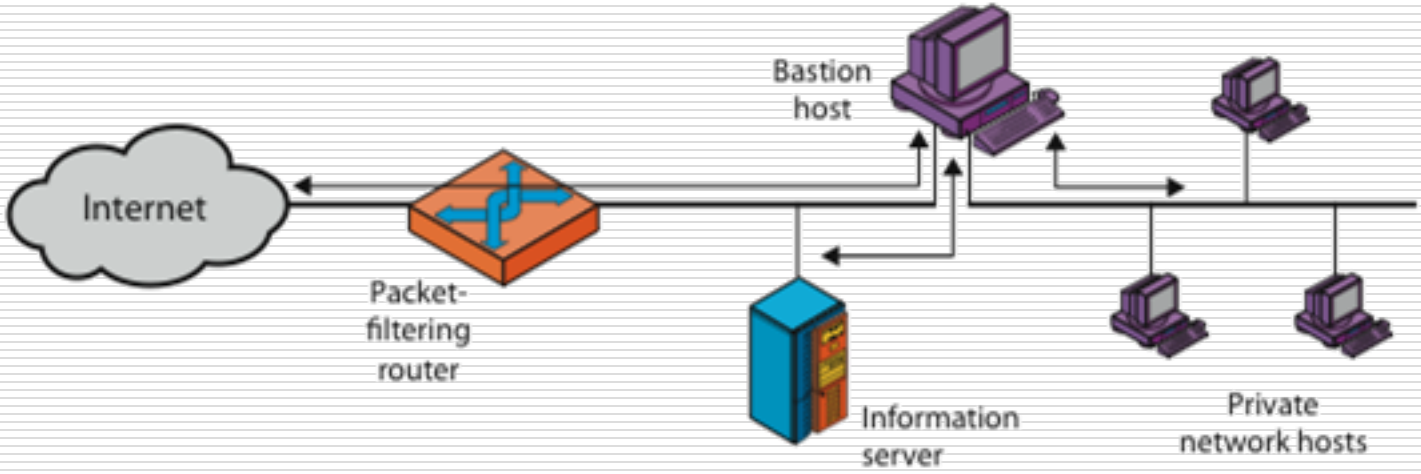
- Bastion Host + Packet-Filter router
- بسته‌های ورودی فقط به مقصد Bastion Host می‌توانند فرستاده شوند.
- بسته ها فقط از مبداء Bastion Host می توانند به خارج فرستاده شوند.



(a) Screened host firewall system (single-homed bastion host)

پیکربندی فایروالها
Dual-Homed Bastion Host

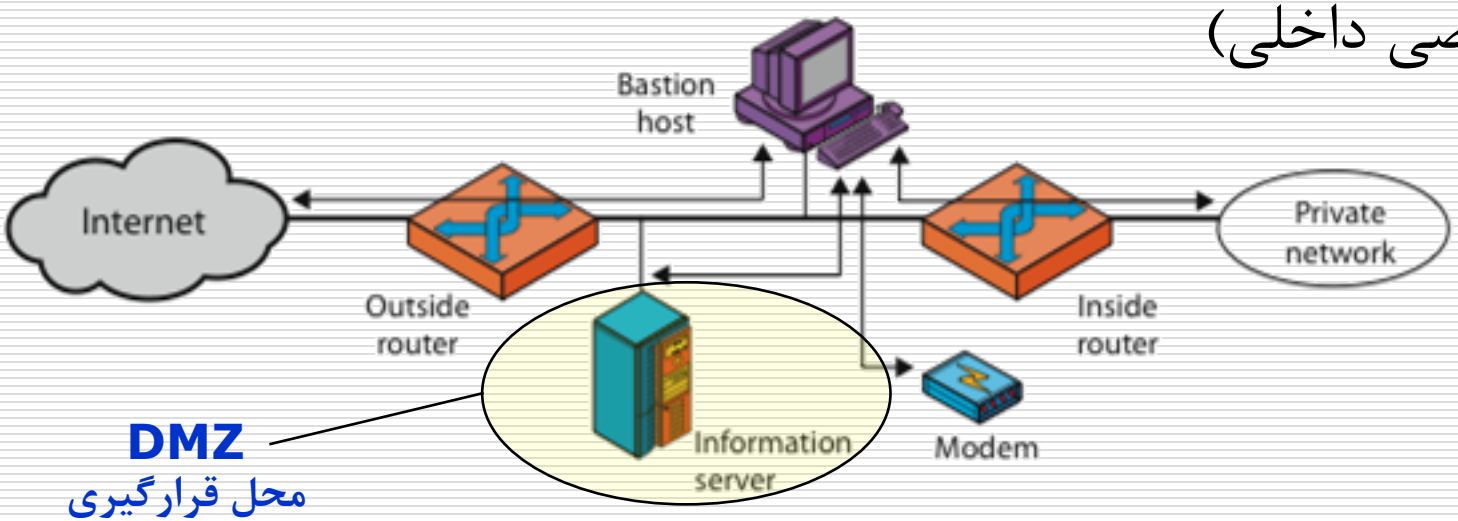
- از لحاظ فیزیکی، امکان دسترسی مستقیم به شبکه داخلی وجود ندارد.
- کارگزار اطلاعات یا سایر میزبان‌ها (در صورت لزوم) می‌توانند مستقیماً با مسیریاب (شامل Packet Filter) ارتباط داشته باشند.



(b) Screened host firewall system (dual-homed bastion host)

پیکربندی فایروالها
Screened-subnet Firewall

- ایجاد یک محیط ایزوله با استفاده از دو مسیریاب/فایروال.
- شبکه داخلی و اینترنت می‌توانند با سرویس‌های موجود در **دامنه DMZ** ارتباط داشته باشند.
- ایجاد سه لایه دفاعی و فراهم آمدن امنیت بیشتر (خصوصا برای شبکه خصوصی داخلی)



فهرست مطالب

- مقدمه
- ویژگی‌های فایروال
- انواع فایروال‌ها
- پیکربندی فایروال‌ها
- **آشنایی با فایروال iptables**

آشنایی با فایروال iptables

- iptables: فایروال سیستم عامل لینوکس
- سه زنجیره (chain) از قواعد در iptables:
  - **INPUT**: زنجیره قواعد حاکم بر بسته‌های ورودی به واسطهای شبکه
  - **OUTPUT**: زنجیره قواعد حاکم بر بسته‌های خروجی از واسطهای شبکه
  - **FORWARD**: زنجیره قواعد حاکم بر بسته‌های فورورد شده (بسته‌های ورودی که مقصد آنها خود سیستم نیستند و فقط فورورد می‌شوند)

iptables: عکس‌العمل‌های ممکن

- عکس‌العمل‌های ممکن در قواعد iptables:
  - **ACCEPT**: پذیرش بسته
  - **DROP**: دور ریختن بسته (برای زمانی که نخواهیم متوجه وجود سیستم شوند)
  - **REJECT**: رد کردن بسته و بازگرداندن خطا (برای زمانی که بخواهیم متوجه رد شدن بسته توسط فایروال شوند)

iptables: برخی دستورات مهم

برخی دستورات iptables

- -P یا --policy تعریف سیاست پیش‌فرض
- -A یا -- append اضافه کرن قاعده به انتهای زنجیره
- -I یا --insert اضافه کردن قاعده به ابتدا (یا ردیفی مشخص) در زنجیره
- -D یا --delete برای حذف کردن قاعده از زنجیره
- -L یا --list برای لیست کردن قواعد
- -F یا --flush برای پاک کردن کل قواعد

iptables: سیاست پیش‌فرض

- تعریف قواعد پیش‌فرض (به طور مثال DROP) در زنجیره‌ها

- iptables --policy INPUT DROP
- iptables --policy OUTPUT DROP
- iptables --policy FORWARD DROP

iptables: تعریف قواعد (۱)

- باز کردن loopback بر روی سیستم

  - iptables -A INPUT -i lo -j ACCEPT
  - iptables -A OUTPUT -o lo -j ACCEPT

iptables: تعریف قواعد (۲)

- باز کردن پروتکل icmp خروجی از سیستم

- iptables -A INPUT -p icmp -j ACCEPT
- iptables -A OUTPUT -p icmp -j ACCEPT

iptables: تعریف قواعد (۳)

- باز کردن پروتکل dns خروجی از سیستم
  - iptables -A INPUT -p udp --sport 53 -j ACCEPT
  - iptables -A OUTPUT -p udp --dport 53 -j ACCEPT
- در صورتی‌که سیستم ما سرور DNS باشد، عکس قواعد فوق را نیاز داریم:
  - iptables -A INPUT -p udp --dport 53 -j ACCEPT
  - iptables -A OUTPUT -p udp --sport 53 -j ACCEPT

iptables: تعریف قواعد (۴)

- باز کردن اتصالات پروتکل http (و به طور مشابه https) خروجی از سیستم به صورت حالتمند (stateful)
  - iptables -A INPUT -p tcp --sport http -m state --state ESTABLISHED -j ACCEPT
  - iptables -A OUTPUT -p tcp --dport http -m state --state NEW,ESTABLISHED -j ACCEPT
- باز کردن اتصالات ورودی http(s) (برای حالتی که سیستم ما وب‌سرور باشد) به طور مشابه می‌تواند تنظیم شود.

iptables: ذخیره و بازیابی قواعد

- قواعد تعریف شده، پس از راه‌اندازی مجدد سیستم از دست می‌روند. لذا باید قواعد تعریف شده را ذخیره و در هنگام راه‌اندازی سیستم بازیابی کرد.

- iptables-save > /etc/iptables.rules
- iptables-restore < /etc/iptables.rules

پایان

مرکز امنیت داده و شبکه شریف

http://dnsl.ce.sharif.edu

پست الکترونیکی

amini@sharif.edu