

یادداشت‌های امن و آلمان

دیوار آتش (فایروال)

مبانی امنیت اطلاعات و شبکه‌های کامپیوتری

محمد رضا رازیان*

بهار و تابستان 1395

مرکز تخصصی آفا

دانشگاه سمنان

*Homepage: www.mrazian.com



آفا دانشگاه سمنان

مرکز تخصصی آفا دانشگاه سمنان
<http://cert.semnan.ac.ir>



آزمایشگاه امنیت داده و شبکه شریف
<http://dnsl.ce.sharif.ir>



فهرست مطالب



- مقدمه
- ویژگی های فایروال
- انواع فایروال ها
- پیکربندی فایروال ها



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).



فایروال چیست؟

- 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 آدرس NAT و نظارت بر استفاده
 - پیاده‌سازی شبکه خصوصی مجازی (VPN) مبتنی بر IPsec



فایروال چیست؟

- 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 آدرس NAT و نظارت بر استفاده
 - پیاده‌سازی شبکه خصوصی مجازی (VPN) مبتنی بر IPsec



فهرست مطالب



- مقدمه
- ویژگی‌های فایروال
- انواع فایروال‌ها
- پیکربندی فایروال‌ها



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.
 - 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



فهرست مطالب



- مقدمه
- ویژگی‌های فایروال
- انواع فایروال‌ها
- پیکربندی فایروال‌ها



انواع فایروال‌ها



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
 - ممانعت از عبور: Deny
- قواعد بر اساس سرآیند IP و لایه انتقال تعریف می‌شوند.
- پالایش در هر دو جهت قابل اعمال است.



انواع فایروال‌ها

Packet Filters

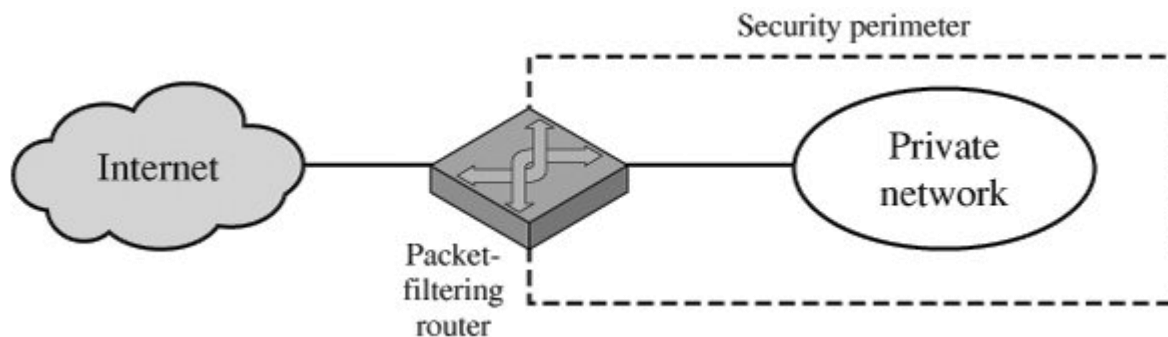


- دسترسی به سرویس‌ها قابل کنترل است (با استفاده از پورت‌ها).
- **مزیت:** سادگی و پنهانی از دید کاربران
- **ضعف:**
 - عدم پشتیبانی از احراز هویت
 - اعمال قواعد متناسب با برنامه مشکل است.
- دو سیاست پیش فرض می‌تواند وجود داشته باشد:
 - Discard / Block = هر آنچه که صریحاً اجازه داده نشده، غیرمجاز است.
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



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



انواع فایروال‌ها

Packet Filters



• مثال ۲

• بیان سیاست پیش فرض (default = deny).
• این قاعده به صورت صریح در انتهای مجموعه قواعد می آید.

	action	ourhost	port	theirhost	port	comment
B	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!

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



انواع فایروال‌ها

Packet Filters



مثال ۴

- بسته‌هایی که مبدا آنها متعلق به لیست ماشین‌های میزبان داخلی و مقصد آنها، پورت ۲۵ از TCP باشند، اجازه عبور دارند.
- بسته‌های 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



آپاداشگاه سمنان

- 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.
- بسته‌های 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 فایروال‌های قدیمی، اطلاعات لایه‌های بالاتر مربوط به بسته‌ها در پالایش آنها مورد استفاده قرار نمی‌گرفت.
- به طور مثال، کنترل دریافت بسته، بر اساس ترافیک ارسالی
- در اتصال به سرورها،
- آدرس پورت سرور معمولاً زیر ۱۰۲۴ و شناخته شده است.
- آدرس پورت مشتری می‌تواند 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.



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



- بیشتر به عنوان Proxy Server اطلاق می‌شود.
- اصولاً 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.
 - Proxy با سرور اصلی تماس می‌گیرد و قطعات TCP را منتقل می‌کند.
 - اگر کد 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



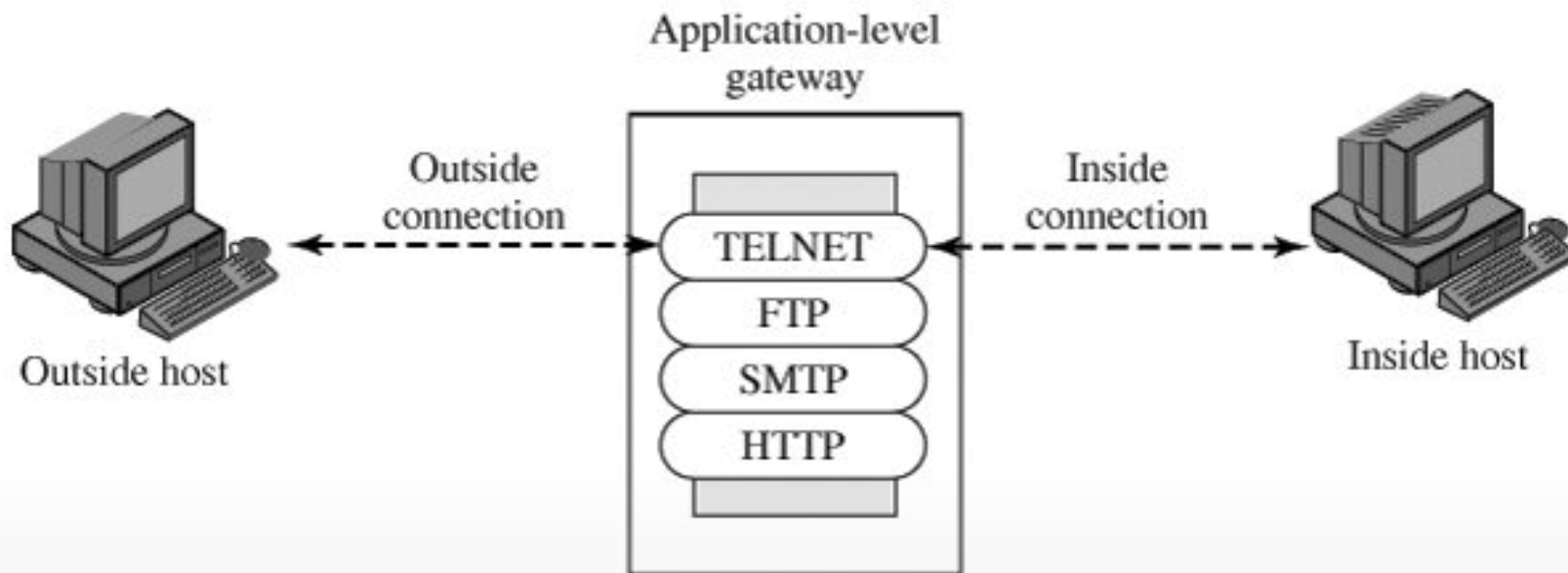
• معایب

- سربار بوجود آمده برای ایجاد هر اتصال جدید.
 - طرفین با هم ارتباط مستقیم ندارند.
 - با تغییر Proxy Server ها ممکن است مجبور به تغییر پیکربندی مشتری‌ها باشیم.
- در مجموع کارایی کمتری دارد.



انواع فایروالها

Application-Level Gateway





انواع فایروال‌ها

Circuit-Level Gateway

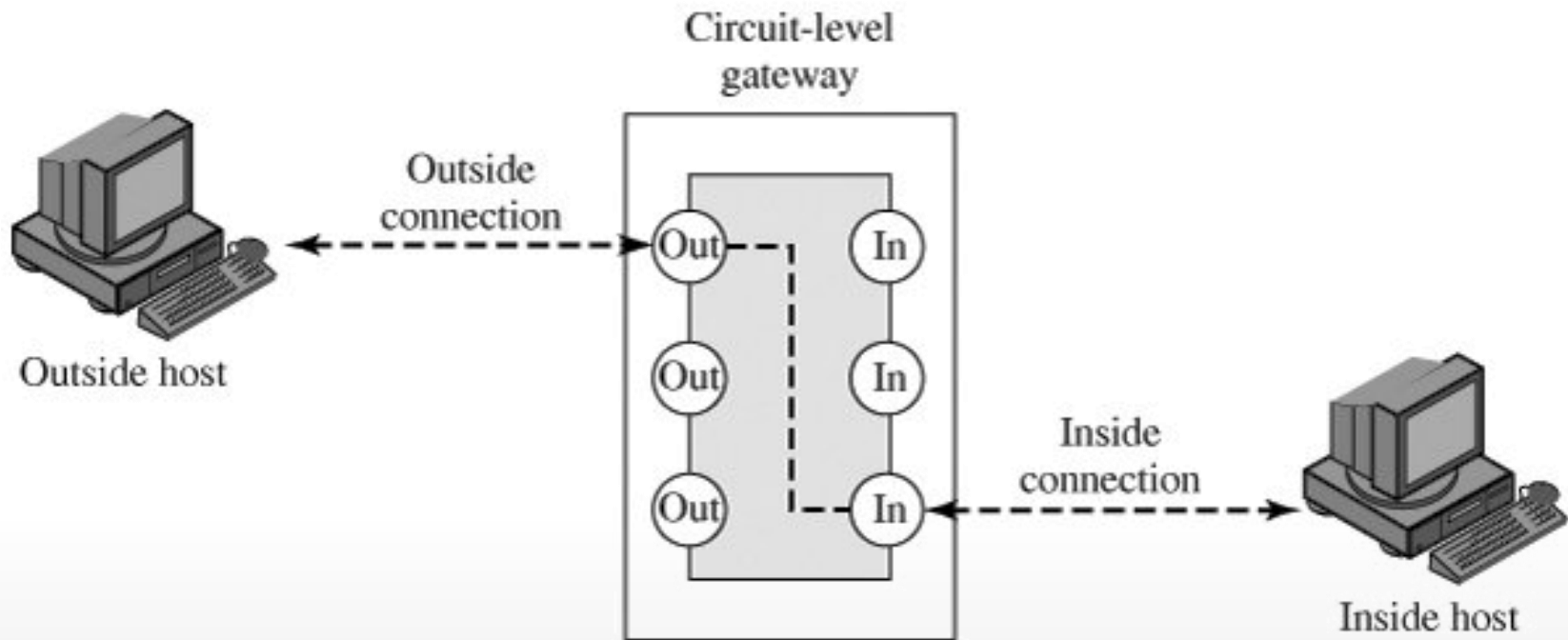


- در واقع در لایه نشست (بین لایه TCP و لایه برنامه کاربردی) عمل می‌کند.
- ارتباط انتها به انتها بین میزبان بیرونی و میزبان درون شبکه برقرار نمی‌شود.
- با وجود فایروال Circuit-Level، دو ارتباط جداگانه TCP، یکی با میزبان داخلی و یکی با میزبان خارجی برقرار می‌شود.
- ترافیک بدون کنترل محتوای داخلی آن منتقل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



انواع فایروال‌ها

Circuit-Level Gateway





انواع فایروال‌ها

Circuit-Level Gateway



- عموماً 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



آپادانشگاه سمنان

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



Bastion Host

- یک نقطه بحرانی از نظر امنیت و قابل اعتماد در شبکه داخلی است.
- عموماً Proxy Server ها یا Circuit-level Gateway ها روی آن نصب می‌شوند.
- یک نسخه امن سیستم عامل روی آن اجرا می‌شود.
- Proxy ها زیرمجموعه‌ای از ویژگیهای سرویسها را پشتیبانی می‌کنند.
- Proxy ها دسترسی به میزبان‌های خاصی را مجاز می‌شمارند.
- Proxy ها جزییات وقایع امنیتی را ثبت می‌کنند.
- Proxy ها 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).



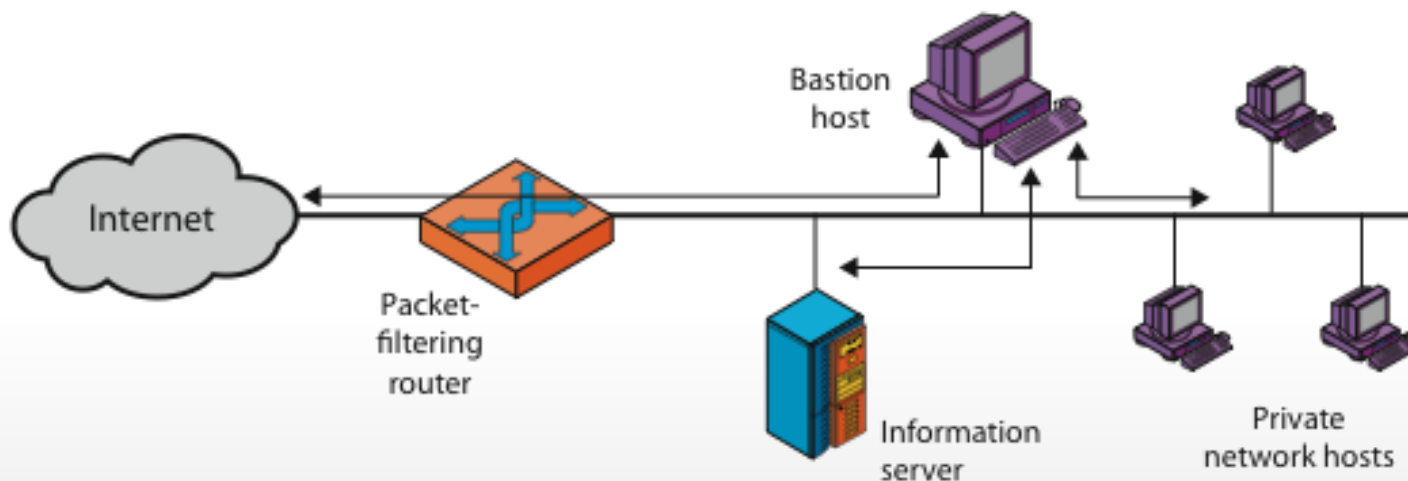
پیکربندی فایروالها

Single-Homed Bastion Host



Bastion Host + Packet-Filter router

- بسته‌های ورودی فقط به مقصد Bastion Host می‌توانند فرستاده شوند.
- بسته‌ها فقط از مبدا Bastion Host می‌توانند به خارج فرستاده شوند.



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

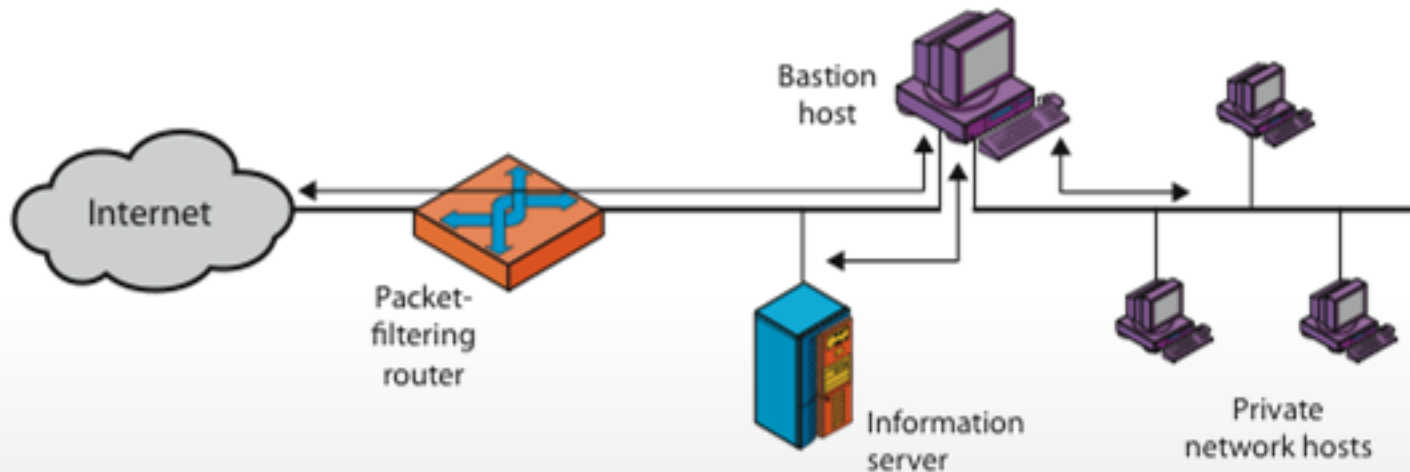


پیکربندی فایروالها

Dual-Homed Bastion Host



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



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

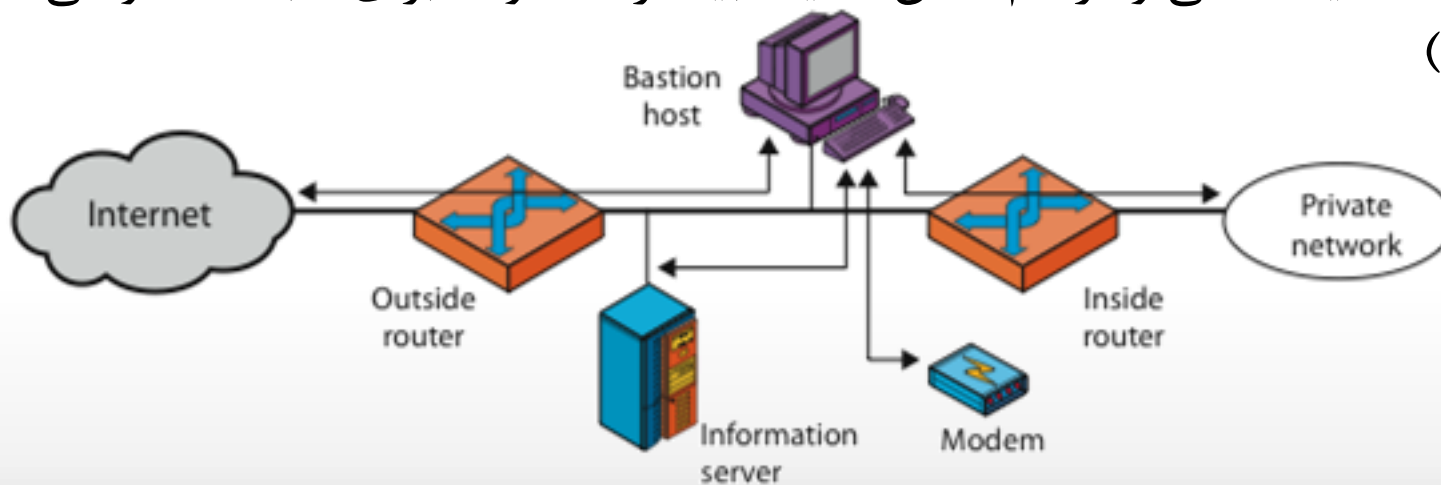


پیکربندی فایروالها

Screened-subnet Firewall



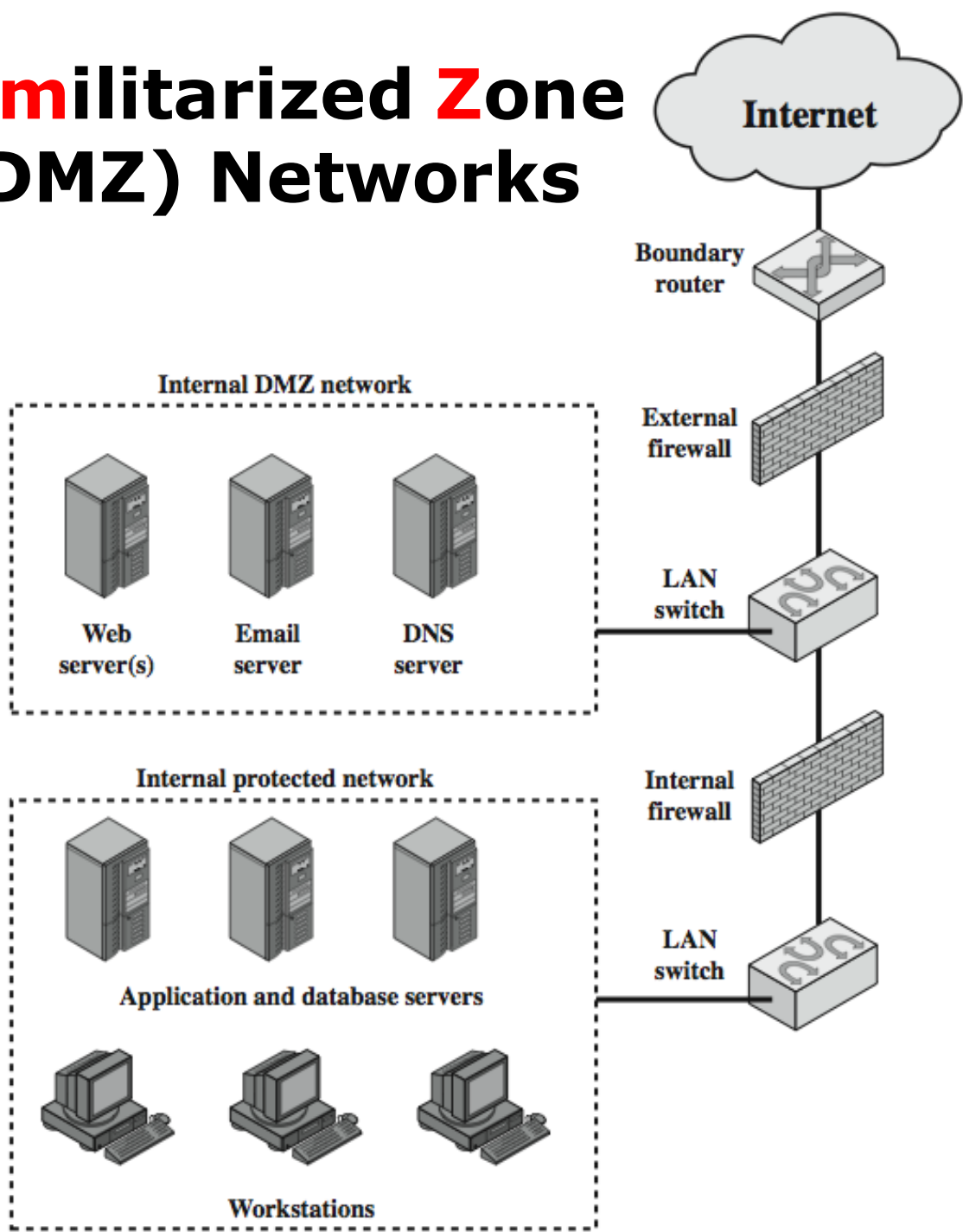
- ایجاد یک محیط ایزوله با استفاده از دو مسیر یاب.
- شبکه داخلی و اینترنت می توانند با زیر شبکه (subnet) داخلی ارتباط داشته باشند.
- ایجاد سه لایه دفاعی و فراهم آمدن امنیت بیشتر (خصوصاً برای شبکه خصوصی داخلی)

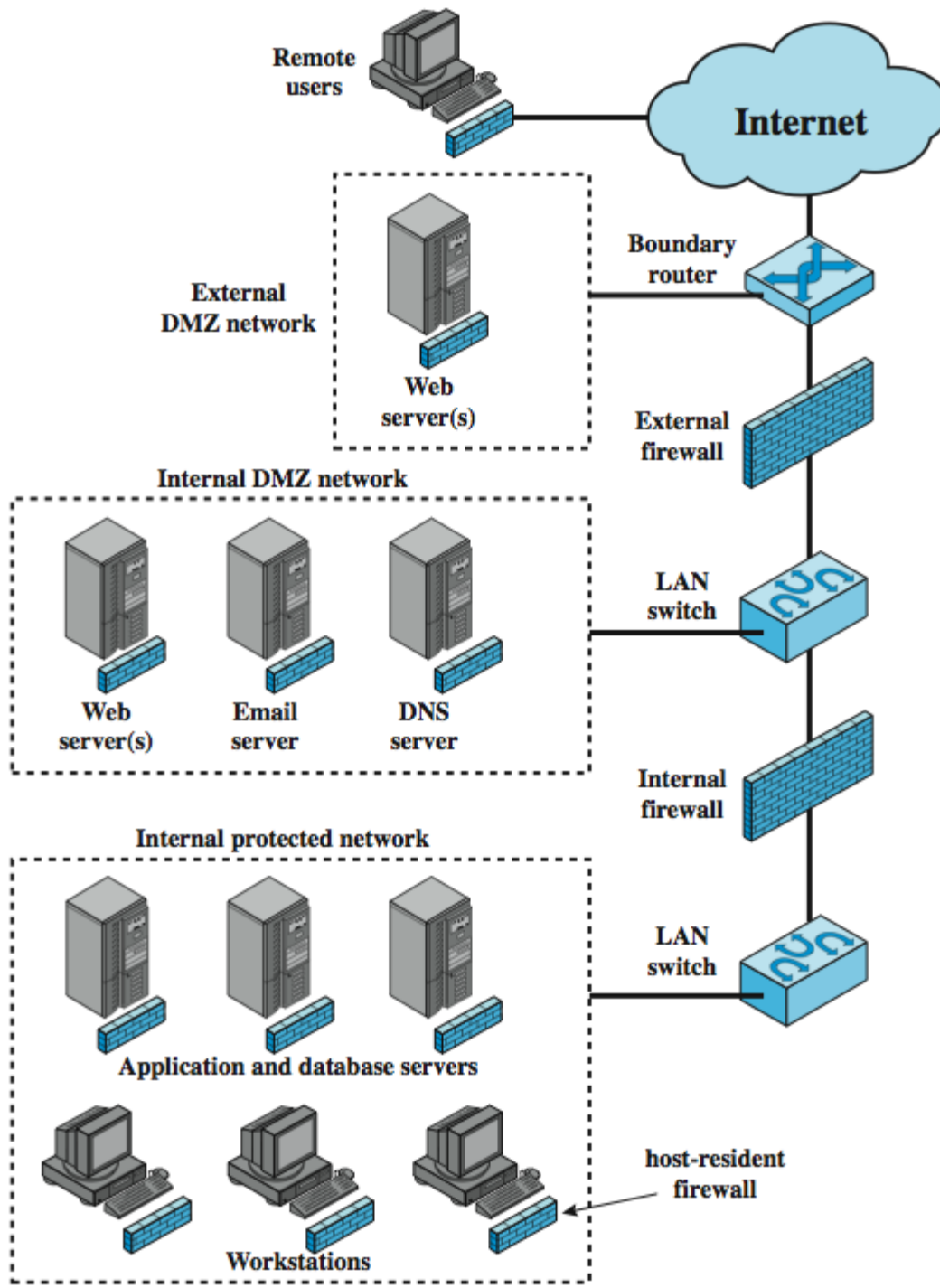


(c) Screened-subnet firewall system



Demilitarized Zone (DMZ) Networks





Distributed Firewalls



منابع



- اسلایدهای دکتر مرتضی امینی (منبع اصلی) – درس امنیت داده و شبکه
- Cryptography and Network Security Principles and Practices, By William Stallings 5th Edition