مبانی امنیت شبکه

گردآوری: محمدعلی عظیمی

بخش سوم: امنیت در لایه ها

۳-۵ فایروال

مقدمه

- فایروال دستگاه یا مجموعه دستگاه هایی است که دسترسی بین شبکه ها را کنترل می کند.
- فایروال سیستم کامپیوتری امنی است که بین شبکه مورد اعتماد و اینترنت غیرقابل اعتماد قرار گرفته، ترافیک شبکه را بررسی کرده و ترافیکی را به نظر خطرناک و غیر مناسب می رسد را بلوک می‌کند.
- فایروال از شبکه داخلی در برابر حملات اینترنتی محافظت کرده و choke point ایجاد می‌کند تا بتوان امنیت را بر آن اعمال کرد.

نقش فایروال

- اعمال محدودیت بر روی بسته های وروی و خروجی از شبکه خصوصی
- اعمال فیلتر بر اساس آدرس IP مبدا یا مقصد، شماره پورت مبدا یا مقصد
- امکان اعمال فیلترینگ در سطح لایه کاربرد
- امکان ارائه سرویس logging در فایروال
- امکان فیلتر کردن ترافیک RLOGING یا Telnet از اینترنت به شبکه داخلی

- امکان فیلتر کردن ترافیک FTP یا SMTP از شبکه داخلی به اینترنت
- محافظت در برابر رنج وسیعی از حملات مسیریابی و IP Spoofing
- امکان اعمال IPSec در مد تونل
- امکان اعمال VPN
- پنهان سازی اطلاعات شبکه داخلی از اینترنت عمومی
- امکان انجام اعمال مدیریت شبکه و NAT

Firewall Limitations

- cannot protect from attacks bypassing it
  - eg sneaker net, utility modems, trusted organisations, trusted services (eg SSL/SSH)
- cannot protect against internal threats
  - eg disgruntled or colluding employees
- cannot protect against access via WLAN
  - if improperly secured against external use
- cannot protect against malware imported via laptop, PDA, storage infected outside

Firewall characteristics

- Design goals for a firewall:
  - All traffic from inside to outside, and vice versa, must pass through the firewall
  - Only authorized traffic, as defined by the local security policy, will be allowed to pass
  - The firewall itself is immune to penetration
- Techniques that firewalls use to control access and enforce the site's security policy:

Service control

- Determines the types of Internet services that can be accessed, inbound or outbound

Direction control

- Determines the direction in which particular service requests may be initiated and allowed to flow through the firewall

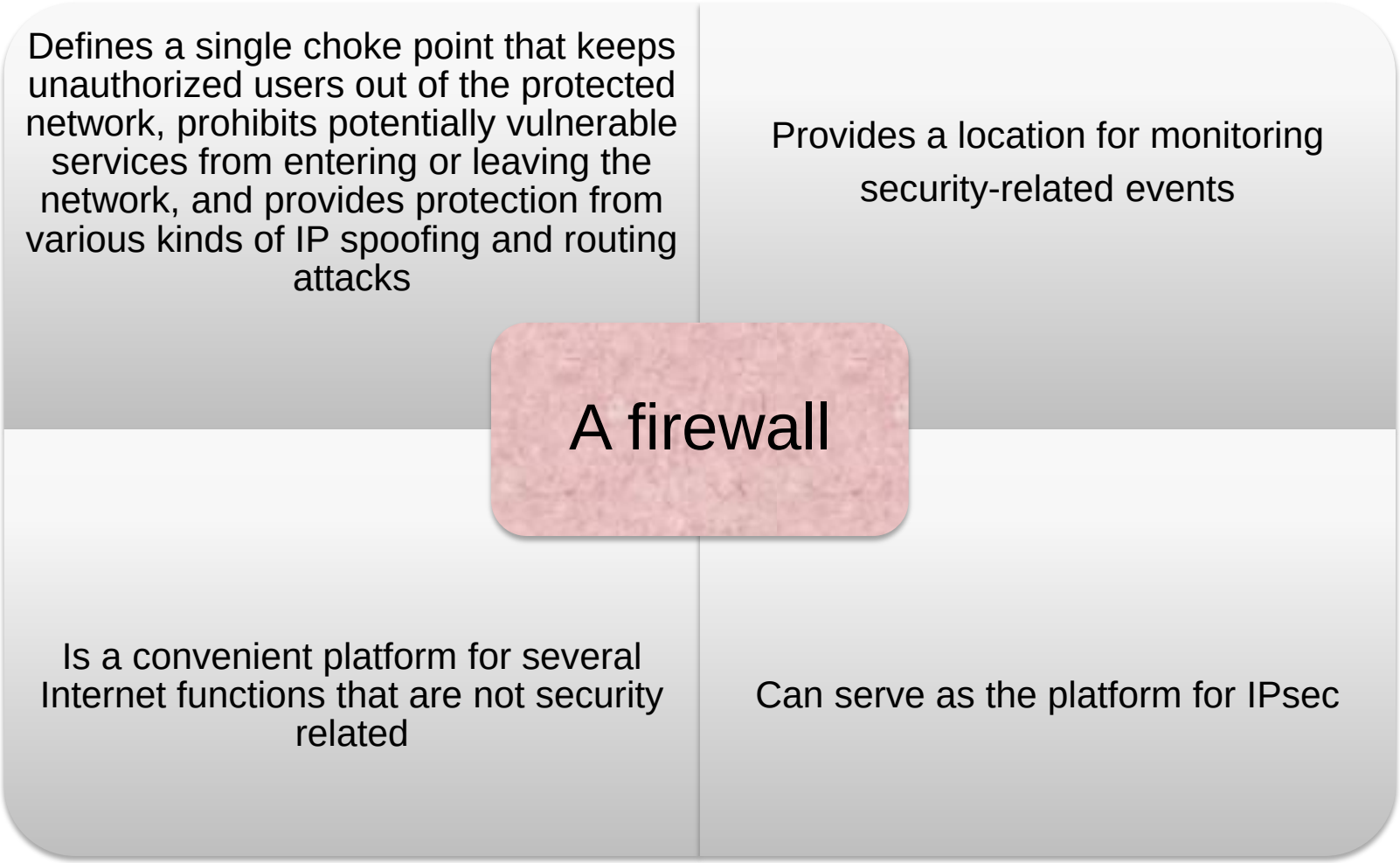
User control

- Controls access to a service according to which user is attempting to access it

Behaviour control

- Controls how particular services are used

Firewall expectations



Bastion Host

- دستگاهی است که در دسترس عموم قرار داشته و دسترسی مستقیم به اینترنت دارد.
- کل ترافیک وردی و خروجی را بررسی کرده و قوانین امنیتی را بر روی ترافیک اعمال می کند.
- در معرض حملات خارجی و داخلی قرار داشته و به همین دلیل حداقل تجهیزات نرم افزاری و سخت افزاری بر روی آن قرار می گیرد و امکان logging و اعلام خطر را دارد.

Proxy Server

- proxy server از طرف کاربران با سرورهای خارجی ارتباط برقرار می‌کند و امکان logging جزئیات ترافیکی هر اتصال را دارد، هر ارتباط proxy server برای دسترسی به یک host برقرار می شود.
- عموماً دسترسی به دیسک proxy server غیرممکن بوده و امکان نصب تروجان و برنامه های دیگر را رابرای حمله کننده کم می‌کند.
- عملکرد:
  - **دروازه در سطح کاربرد:** بسته ها را تنها در صورتی که قبلاً اتصالی برقرار شده باشد، ارسال خواهد کرد. بسته های تکی را عبور نخواهد داد. معمولاً برای ترافیک ورودی استفاده می شود.
  - **دروازه در سطح circuit:** همه بسته هایی که شماره پورت permit شده ای دارند را ارسال خواهد کرد. معمولاً برای ترافیک خروجی استفاده می شود.

SOCKS

- طرحی برای تصدیق هویت و بسط آدرس دهی IPv6 در کاربردهای مبتنی بر اتصال TCP در پروتکل های HTTP، Telnet، FTP و UDP است.
- برای برقراری اتصال با شئ از طریق فایروال، ابتدا باید درخواستی به سرور SOCKS در پورت 1080 بدهد. سرور درخواست را بررسی کرده و اتصال را برقرار می کند یا درخواست را رد می کند.

- **Choke Point** : نقطه ای است که اینترنت به شبکه داخلی دسترسی پیدا می کند، در صورت پیاده سازی درست کل ترافیک شبکه باید از این نقطه عبور کند. نصب ابزارهای مانیتورینگ و logging جامع بر روی این نقطه انجام می شود.

- **DMZ**: شبکه ای است که بین شبکه خصوصی داخلی و شبکه عمومی خارجی قرار می‌گیرد که به perimeter network هم گفته می‌شود. DMZ برای جداسازی بیشتر شبکه داخلی و خارجی استفاده می‌شود.

انواع فایروال

1. **Packet Filter**: این نوع فایروال هر بسته را بررسی کرده و لیستی از قوانین را خط به خط خوانده و بر روی بسته اعمال می کند. قوانین می تواند بر اساس آدرس IP مبدا یا مقصد یا آدرس شبکه یا پورت TCP و UDP باشد. برای هر قانون دو عمل ارسال یا دورانداختن تعریف می شود. اگر بسته با هیچ کدام از قوانین تطبیق پیدا نکند، عمل پیش فرض(ارسال یا دورانداختن) انجام می شود.

- کلیه ترافیک ورودی را به یک host ارسال کرده به این ترتیب احتمال حمله به سایر host ها در شبکه کم خواهد شد.
- نمی تواند بسته های خوب و بد را از هم تشخیص دهد.
- در معرض حمله IP Spoofingقرار دارد.

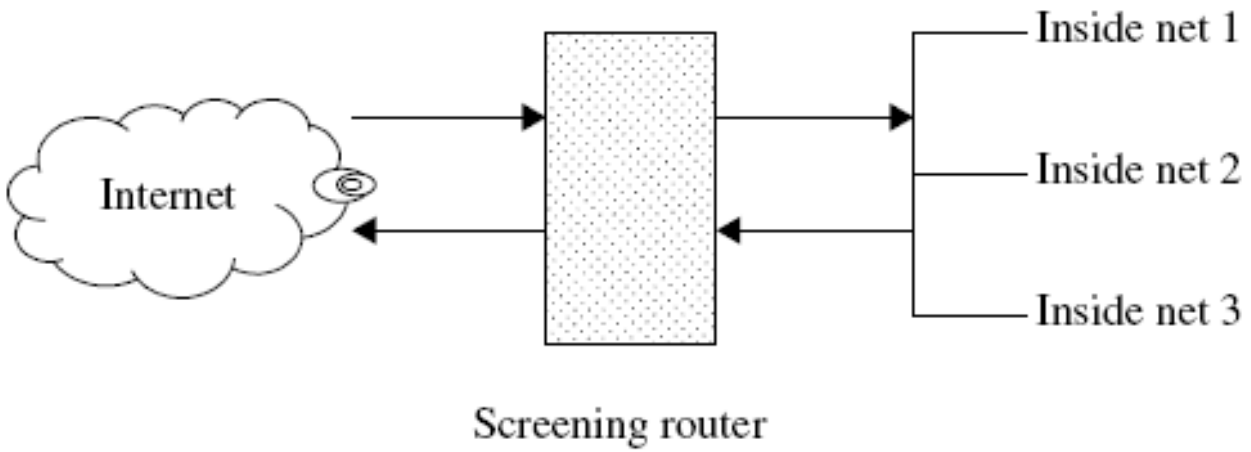


Figure 10.1 A screening router for packet filtering.

Telnet packet filter

- Telnet اجازه اتصال به کامپیوتر راه دور را از طریق اینترنت داده و ورودی صفحه کلید را به صورت متن ساده منتقل می کند. از Telnet می توان برای مدیریت UNIX و ویندوز NT استفاده کرد.

- در مثال زیر فایروال هر بسته با پورت مبدا 23 و هر بسته با پورت مقصد ۲۳ را دور می اندازد.

Table 10.1 Telnet packet-filtering example

Rule number	Action	Source IP	Source port	Destination IP	Destination port	Protocol
1	Discard	*	23	*	*	TCP
2	Discard	*	*	*	23	TCP

FTP packet filter

- FTP بر روی پورت ۲۰ یا ۲۱ است.
- **مثال :**
  - قانون ۱ به کاربران از شبکه 192.168.10.0 اجازه ایجاد نشست TCP به هر مقصد بر روی پورت ۲۱ را می دهد.
  - قانون ۲ هر مبدایی با پورت ۲۰ که بخواهد به هر مقصدی در شبکه 192.168.10.0 با پورت کمتر از ۱۰۲۴ ارتباط برقرار کند بلوک می شود.
  - قانون ۳ به هر کاربر راه دور با پورت ۲۰ اجازه می دهد با هر مقصدی در شبکه 192.168.10.0 با هر پورت برقرار کند.

Table 10.2 FTP packet-filtering example

Rule number	Action	Source IP	Source port	Destination IP	Destination port	Protocol
1	Allow	192.168.10.0	*	*	21	TCP
2	Block	*	20	192.168.10.0	<1024	TCP
3	Allow	*	20	192.168.10.0	*	TCP ACK = 1

- FTP از دو اتصال TCP کنترلی و داده برای برقراری ارتباط و انتقال داده استفاده میکند.

- **Active Mode**: سرور در پورت ۲۱ آماده دریافت دستور بوده، کاربر درخواست را از روی یک پورت آزاد میان ۱۰۲۴ تا ۶۵۵۳۵ در کانال کنترلی به پورت ۲۱ سرور ارسال می کند. سرور از پورت ۲۰ به پورت مشخص شده کاربر داده ارسال می کند.
- **Passive Mode**: کانال کنترلی همان پورت ۲۱ بوده، اما سرور پس از دریافت درخواست کاربر پورتی بین ۱۰۲۴ تا ۶۵۵۳۵ را انتخاب کرده و داده را از آن پورت ارسال میکند.

SMTP packet filter

- SMTP پروتکل ارسال email است و سرور SMTP از پورت ۲۵ گوش می کند و کاربر آن از پورت تصادفی بالای ۱۰۲۳ استفاده می‌کند.
- **مثال:**
  - اجازه ترافیک SMTP ورودی از source gatewayبا پورت ۲۵ را می دهد
  - اجازه ارسال به هر مقصد با پورت ۲۵ را داده، یعنی اجازه ارسال email را به هر host میدهد.
  - اجازه ارسال از host های شبکه داخلی به هر مقصد با پورت ۲۵ را میدهد.
  - اجازه ورود به بسته هایی که پرچم ACK آنها تنظیم شده را از پورت ۲۵ می‌ده

Table 10.3 SMTP packet-filtering examples

Case	Action	Source host	Source port	Destination host	Destination port	Protocol
A	Allow	Source gateway	25	*	*	TCP
B	Allow	*	*	*	25	TCP
C	Allow	Internal host	*	*	25	TCP
D	Allow	*	25	*	*	TCP ACK flag

2. Circuit level gateway

- اصول آن شبیه packet filter است. تمام بسته هایی که شماره پورت آنها در قوانین اجازه داده شده، از طرف gateway به سرور اصلی ارسال خواهد شد.
- امکان پیاده سازی NAT بر روی آن وجود دارد. بنابراین بسته ها با آدرس gateway در اینترنت منتشر شده و بدین وسیله اطلاعات داخلی شبکه پنهان نگه داشته می‌شود.

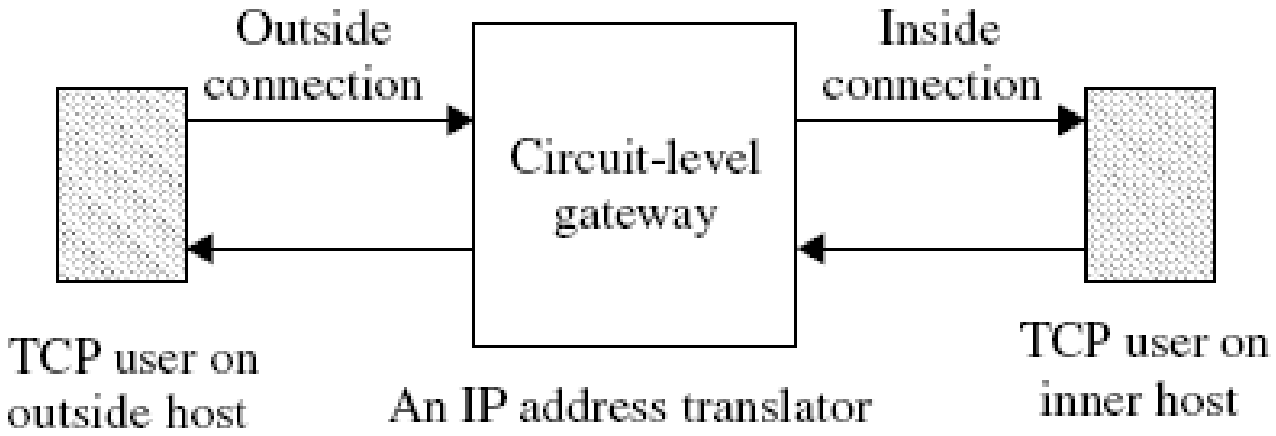
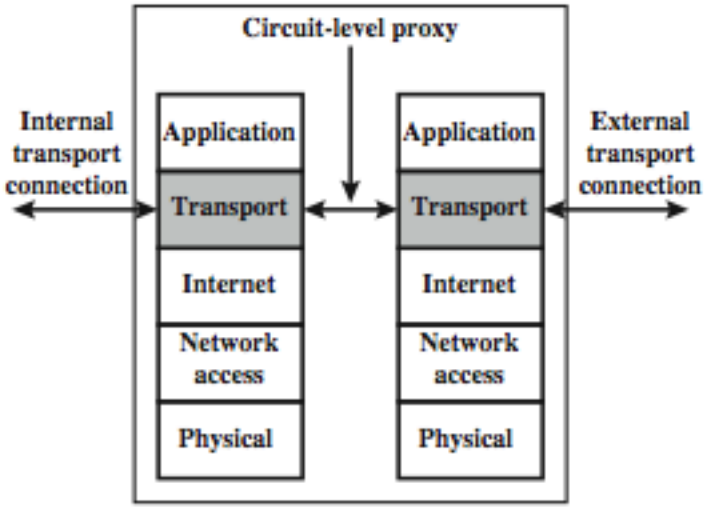
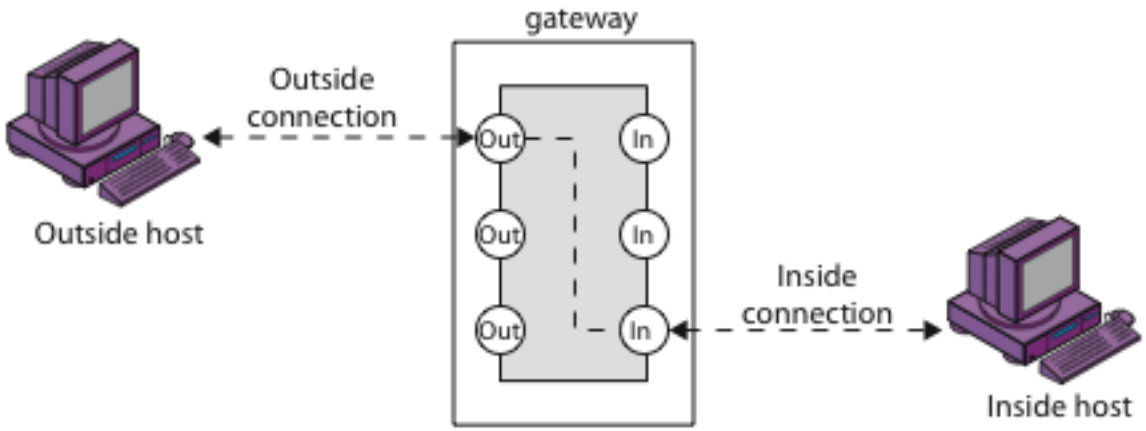


Figure 10.2 Circuit-level gateway for setting up two TCP connections.

Firewalls - Circuit Level Gateway



(e) Circuit-level proxy firewall



(c) Circuit-level gateway

Application level gateway .3

- بجای بررسی تک تک بسته ها، کل پیام را آنالیز می‌کند.
- Gateway ابتدا درخواست کاربر را گرفته و با قوانین خود چک می‌کند. سپس یک اتصال TCP/IP با سرور راه دور برقرار می کند. سرور نیز پاسخ خود را به gateway فرستاده، پاسخ دریافت شده نیز با قوانین چک شده و صحت تطابق به کاربر ارسال می‌شود.

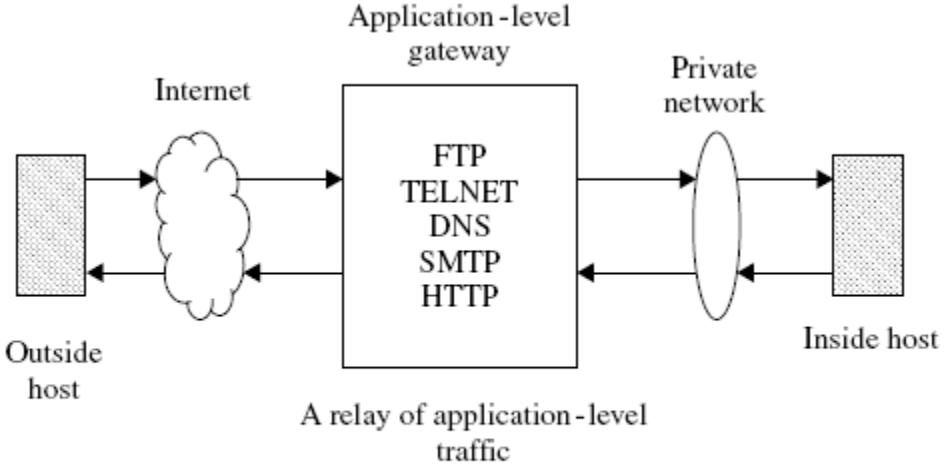
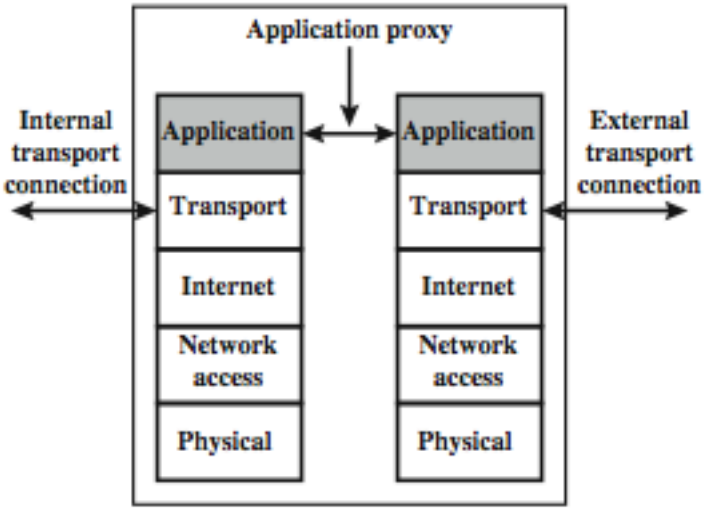
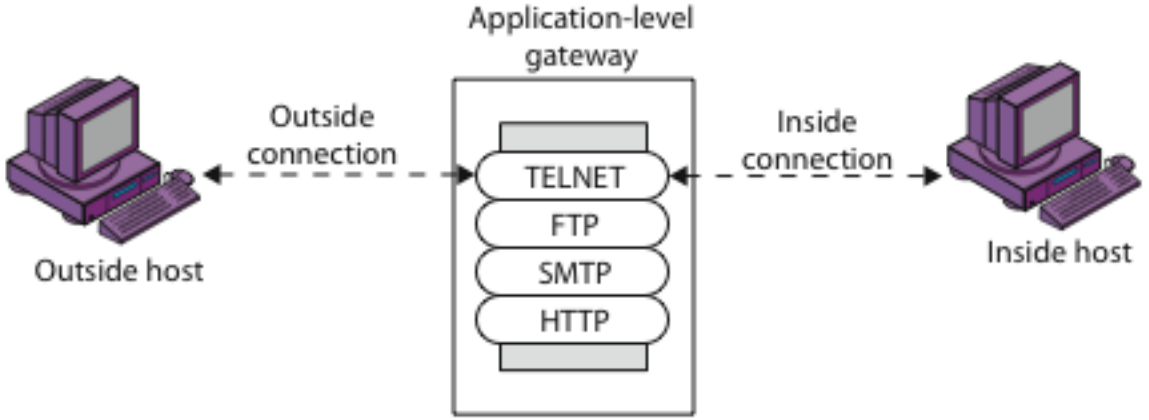


Figure 10.3 Application-level gateway for acting as a relay of application-level traffic.

Firewalls - Application Level Gateway (or Proxy)





(b) Application-level gateway

Stateful Firewall

SPI: Stateful Packet Inspection

- وارسی بسته ها فقط منحصر به اطلاعات سرآیند آنها نیست.
- هر بسته بخشی از یک اتصال است، و باید در context آن اتصال وارسی شود.
- **مثال :** کارگزار موجود در DMZ حق ندارد شروع کننده اتصاال به بیرون باشد، و فقط حق دارد به اتصالی که از بیرون برقرار شاده پاس دهد.

طراحی فایروال

- سه نوع طراحی فایروال وجود دارد

1. Screened Host Firewall (Single-Homed Bastion Host)
2. Screened Host Firewall (Dual-Homed Bastion Host)
3. Screened Subnet Firewall

- در دو طراحی اول وظیفه روتر مشاهده ترافیک شبکه و اعمال کنترل در سطح کلان است و طراحی سوم شامل روتری با خاصیت فیلتر کردن بسته نیز می‌شود که سطح امنیتی بالاتری را فراهم میکند.
- هنگامی که کاربران اینترنت بخواهند به منابع داخلی شبکه دسترسی پیدا کنند، اولین دستگاهی که به آن برمی خورند Bastion host است. Bastion host باید حداقل امکانات سخت افزاری و نرم افزاری را داشته باشد تا شانس حمله کننده برای نفود را کمتر کند. Bastion host شامل امکانات logging و اعلام خطر است.

Screened Host Firewall (Single-Homed Bastion Host)

- از bastion host با یک واسط و یک روتر با فیلترینک بسته است. Bastion host می تواند به صورت circuite level یا application level پیکریندی شود.
- با استفاده از NAT، آدرس داخلی شبکه به آدرس رجیستر شده تبدیل می‌شود.
- روتر بنحوی پیکربندی شده که تمام ترافیک ورودی را به bastion host هدایت کرده و تنها ترافیکی که از bastion host آمده باشد را به بیرون می فرستد. بنابراین bastion host به عنوان proxy برای ترافیک خروجی عمل می‌کند.
- حمله کننده می‌تواند روتر را بنحوی دستکاری کند که ترافیک را بجای ارسال به bastion host مستقیماً به میزبان داخل شبکه ارسال کند، البته حمله معمولاً موفق نیست زیرا میزبان های داخلی ترافیک خارجی را تنها به bastion host می‌فرستند.

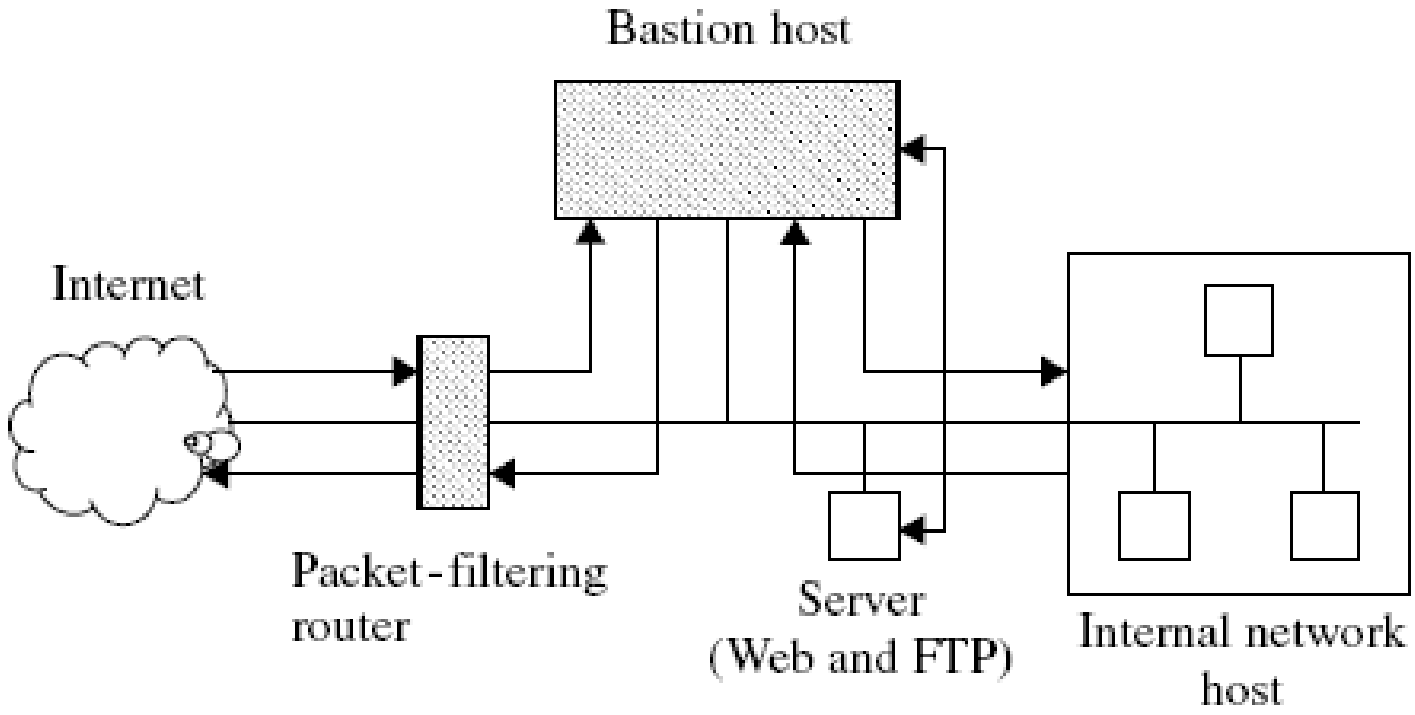


Figure 10.4 Screened host firewall system (single-homed bastion host).

Screened Host Firewall (Dual-Homed Bastion Host)

- Bastion host دارای دو واسط بوده و بین شبکه داخلی و اینترنت شکاف بیشتری ایجاد کرده و به همین دلیل نسبت به مدل قبل امنیت بیشتری فراهم میکند.
- حمله کننده ممکن است بخواهد به روتر و bastion host دسترسی پیدا کند، الگوریتم در این طراحی حمله کننده مجبور است از دو لایه امنیتی عبور کند.
- امکان پیاده سازی NAT وجود دارد.

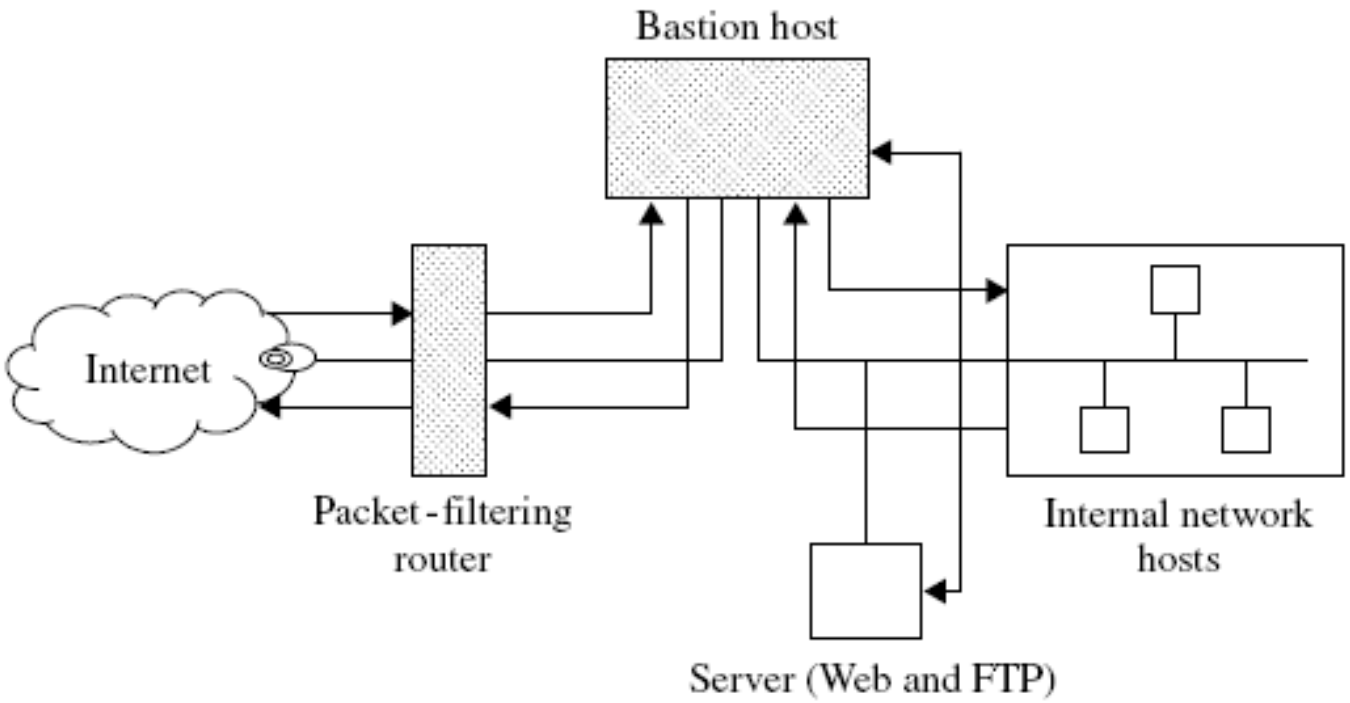


Figure 10.5 Screened host firewall system (dual-homed bastion host).

Screened Subnet Firewall

- کلیه دستگاه های در معرض عموم در شبکه تقریباً جدا شده ای به نام DMZ قرار میگیرد و به همین دلیل امن ترین طرح است.

- یک روتر خارجی و یک روتر داخلی وجود دارد. که تنها به ترافیک از/به bastion hos اجازه عبور میدهد.

- روترهای داخلی و خارجی از حملات IP spoofing و source routing جلوگیری می کند.

مزایا:

1. حمله کننده باید از سه لایه برای نفوذ به شبکه داخلی عبورکند.
2. اطلاعات داخلی شبکه از دید کاربران خارجی محفوظ می ماند
3. کاربران داخلی برای دسترسی به اینترنت باید از bastion host عبورکند

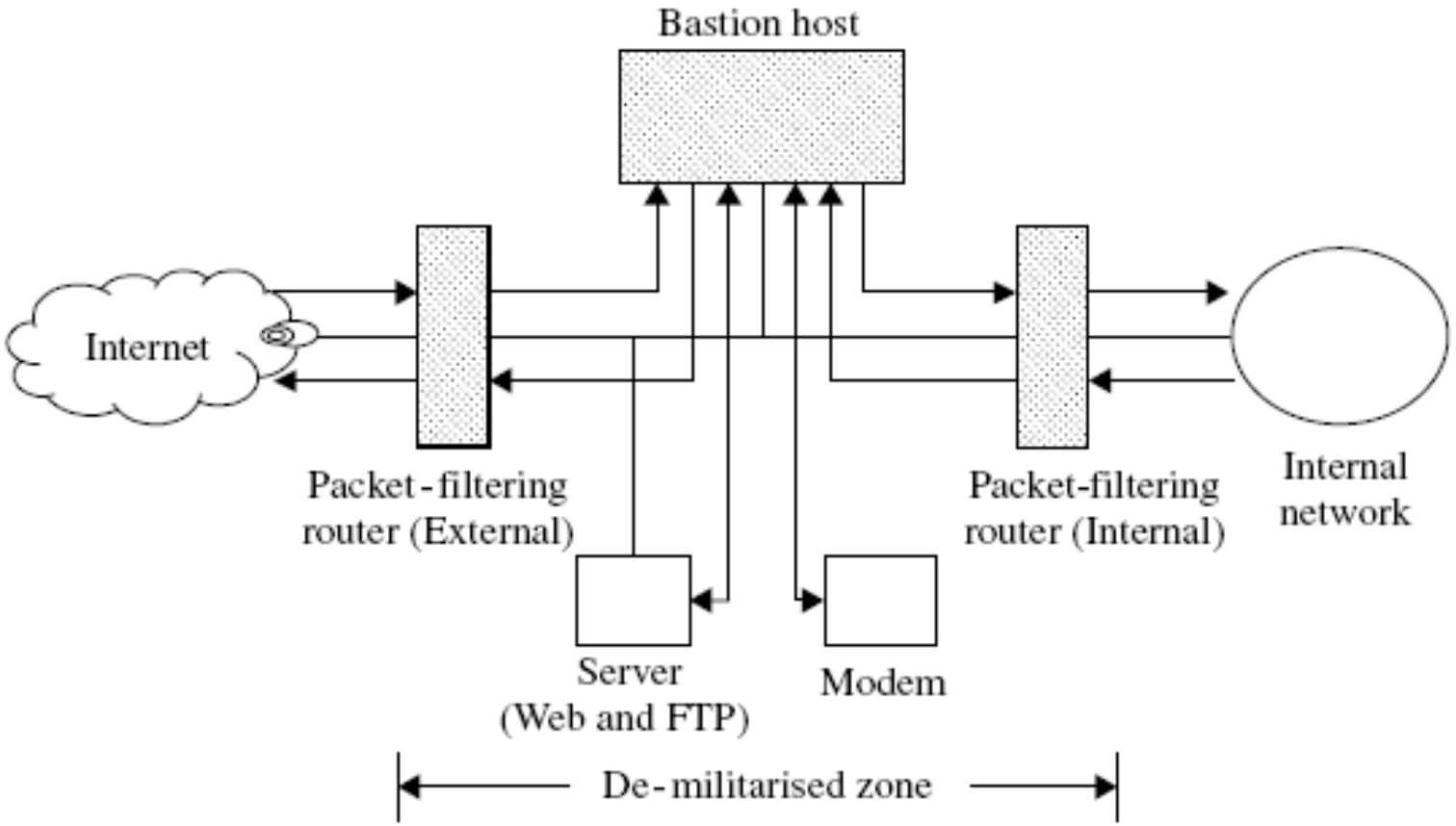
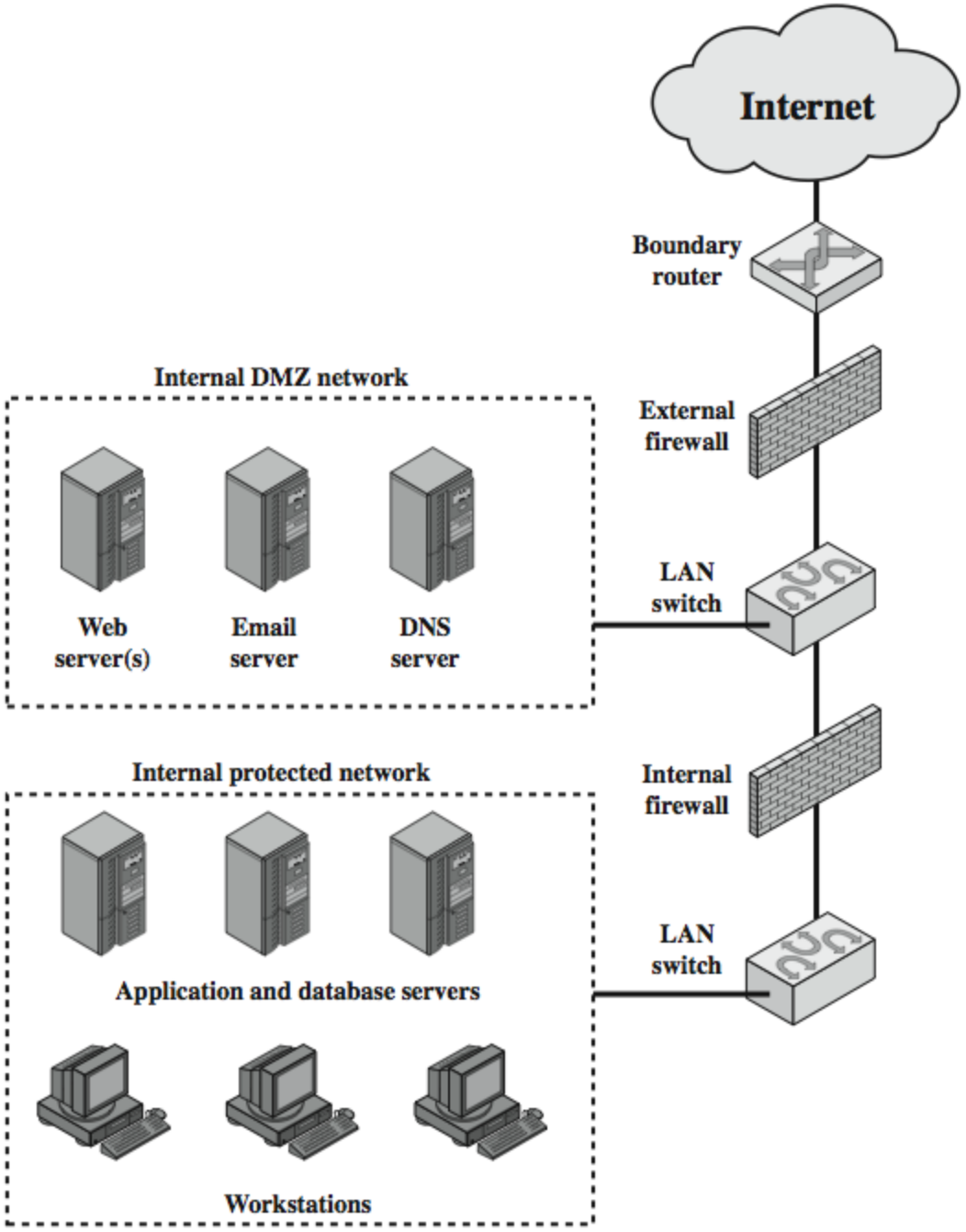


Figure 10.6 Screened subnet firewall system.

DMZ Networks



Distributed Firewalls