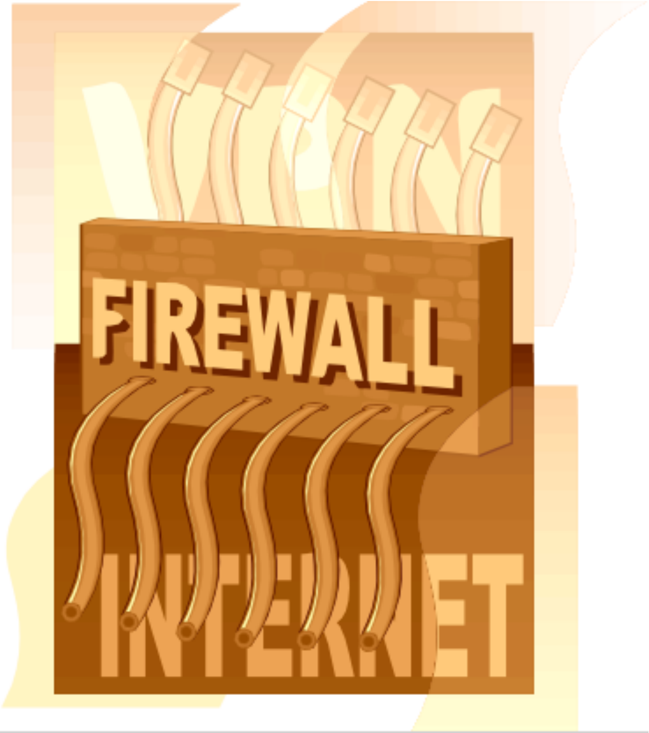
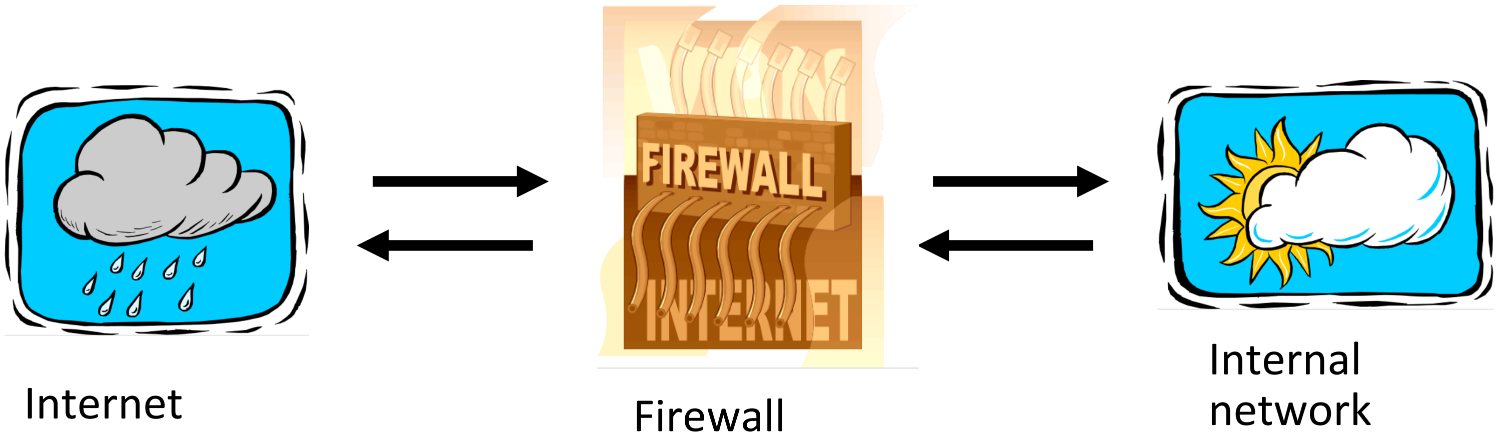
Firewalls



Firewalls



Internet

Firewall

Internal network

- Firewall decides what to let in to internal network and/or what to let out
- **Access control** for the network

Firewall as Secretary

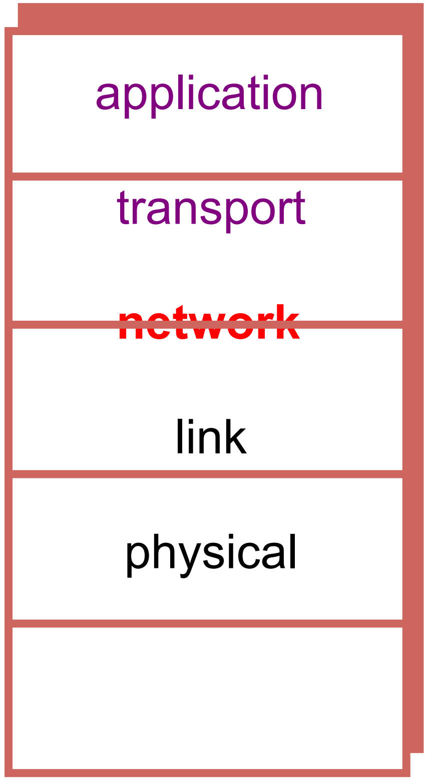
- A firewall is like a **secretary**
- To meet with an executive
  - First contact the secretary
  - Secretary decides if meeting is important
  - So, secretary filters out many requests
- You want to meet chair of CS department?
  - Secretary does some filtering
- You want to meet the POTUS?
  - Secretary does lots of filtering

Firewall Terminology

- No standard firewall terminology
- Types of firewalls
  - **Packet filter** — works at network layer
  - **Stateful packet filter** — transport layer
  - **Application proxy** — application layer
- Other terms often used
  - E.g., "deep packet inspection"

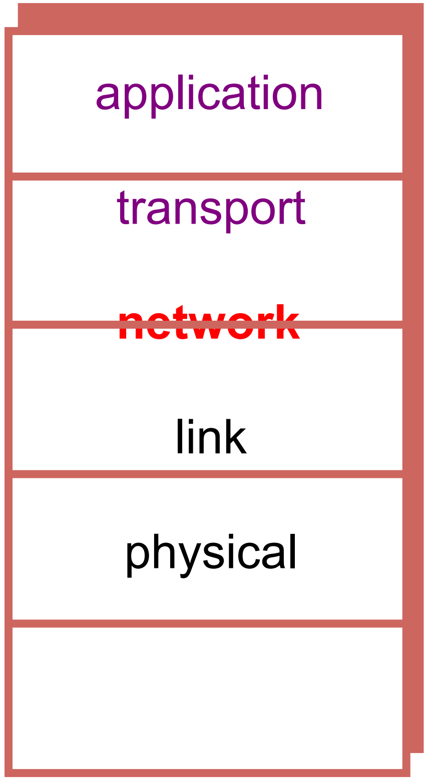
Packet Filter

- Operates at network layer
- Can filters based on…
  - Source IP address
  - Destination IP address
  - Source Port
  - Destination Port
  - Flag bits (SYN, ACK, etc.)
  - Egress or ingress



Packet Filter

- Advantages?
  - Speed
- Disadvantages?
  - No concept of state
  - Cannot see TCP connections
  - Blind to application data



Packet Filter

- Configured via Access Control Lists (ACLs)
  - Different meaning than at start of Chapter 8

Action	Source IP	Dest IP	Source Port	Dest Port	Protocol	Flag Bits
Allow	Inside	Outside	Any	80	HTTP	Any
Allow	Outside	Inside	80	> 1023	HTTP	ACK
Deny	All	All	All	All	All	All

❑ **Q**: Intention?

❑ **A**: Restrict traffic to Web browsing

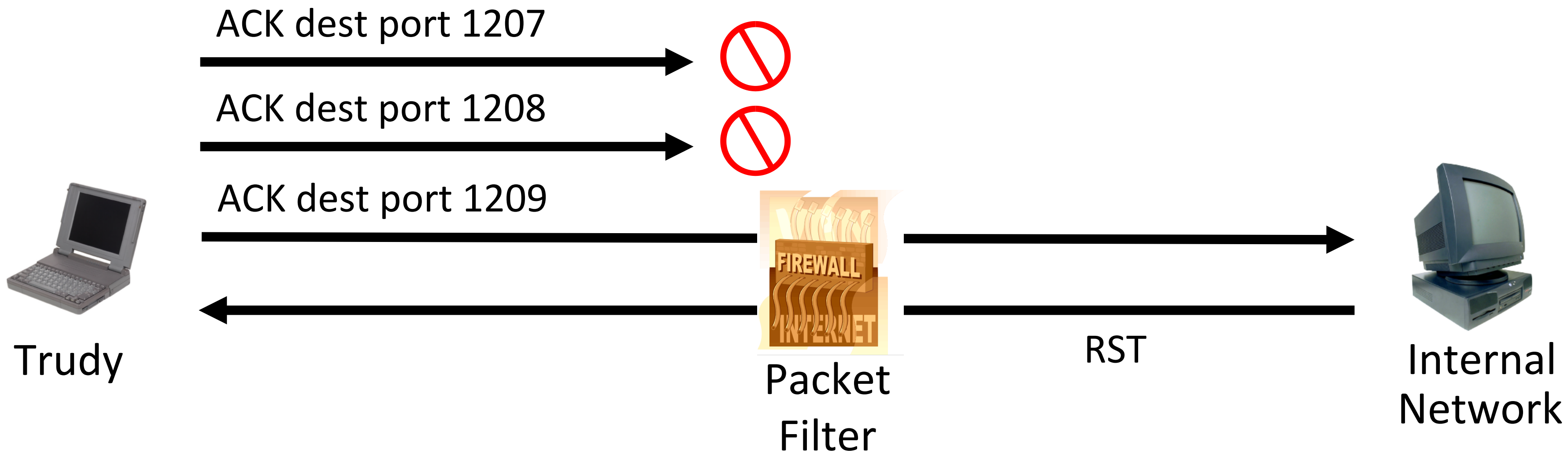
Port scan

- Check if certain port is open
- TCP scan
  - open: connection established/ closed: RST
- SYN scan
  - open: SYN-ACK/ closed: RST
- Ack scan
  - open: RST/ closed: RST
  - Used to determine Firewall rules
- FIN scan
  - open: ignore/ closed: RST

TCP ACK Scan

- Attacker scans for open ports thru firewall
  - Port scanning is *first step* in many attacks
- Attacker sends packet with ACK bit set, **without** prior 3-way handshake
  - Violates TCP/IP protocol
  - ACK packet pass thru packet filter firewall
  - Appears to be part of an ongoing connection
  - RST sent by recipient of such packet

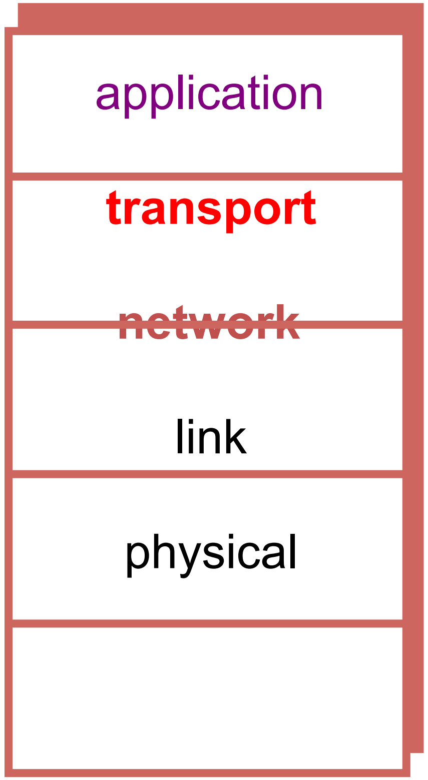
TCP ACK Scan



- Attacker knows 1209 is open
- stateless firewall: pass
- stateful firewall: drop

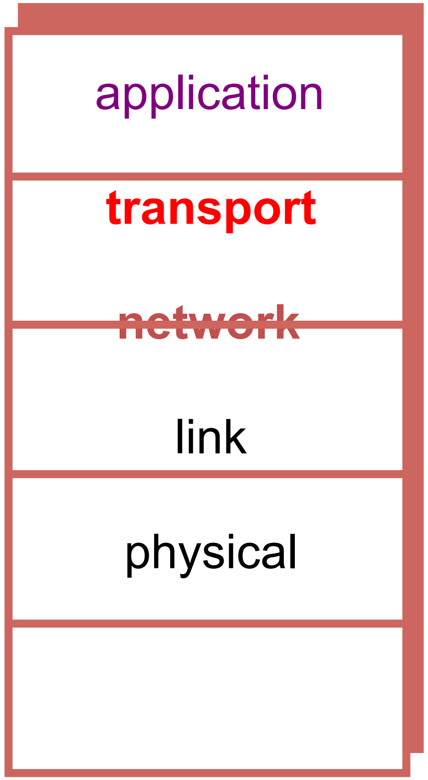
Stateful Packet Filter

- Adds **state** to packet filter
- Operates at transport layer
- ***Remembers*** TCP connections, flag bits, etc.
- Can even remember UDP packets (e.g., DNS requests)



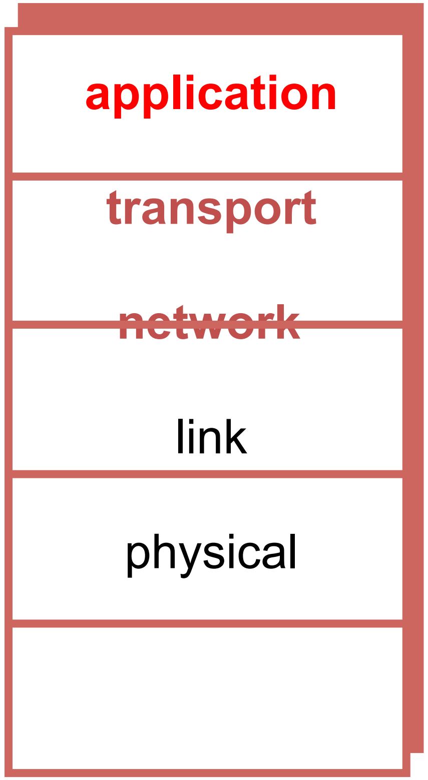
Stateful Packet Filter

- Advantages?
  - Can do everything a packet filter can do plus...
  - Keep track of ongoing connections (so prevents TCP ACK scan)
- Disadvantages?
  - Cannot see application data
  - Slower than packet filtering



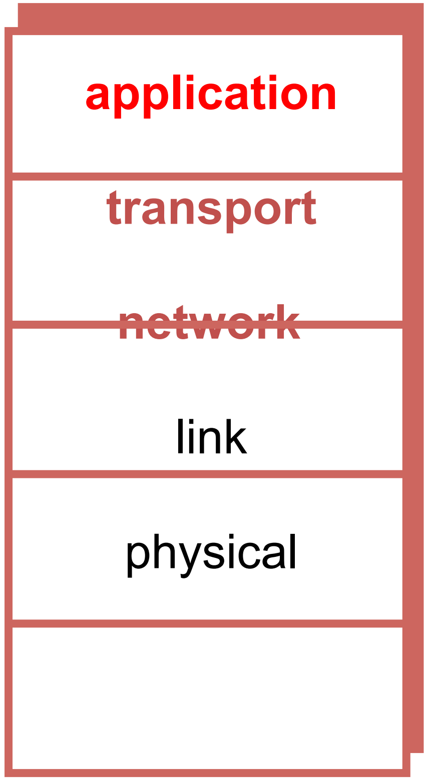
Application Proxy

- A **proxy** is something that acts on your behalf
- Application proxy looks at incoming application data
- Verifies that data is safe before letting it in



Application Proxy

- Advantages?
  - Complete view of connections and applications data
  - Filter bad data at application layer (viruses, Word macros)
- Disadvantages?
  - Speed



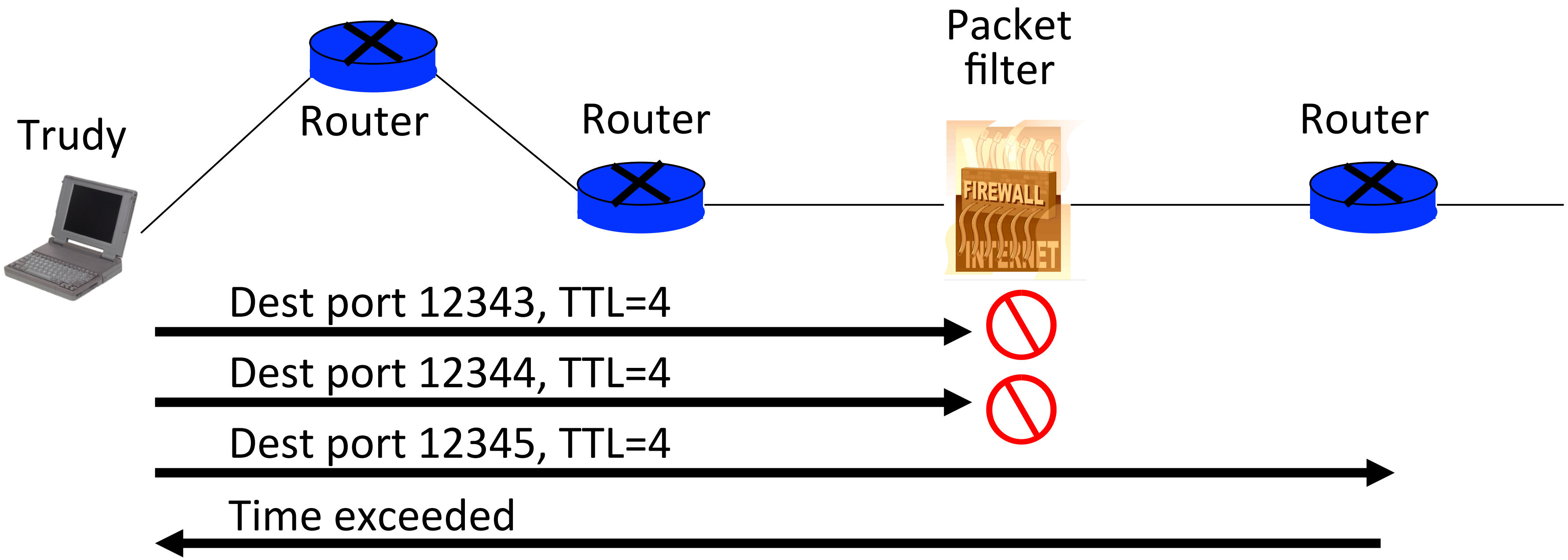
Application Proxy

- Creates a new packet before sending it thru to internal network
- Attacker must talk to **proxy** and convince it to forward message
- Proxy has complete view of connection
- Prevents some scans stateful packet filter cannot — next slides

Firewalk

- Tool to scan for open ports thru firewall
- Attacker knows IP address of firewall and IP address of one system inside firewall
  - Set TTL to 1 more than number of hops to firewall, and set destination port to N
- If firewall allows data on port N thru firewall, get ***time exceeded*** error message
  - Otherwise, no response

Firewalk and Proxy Firewall



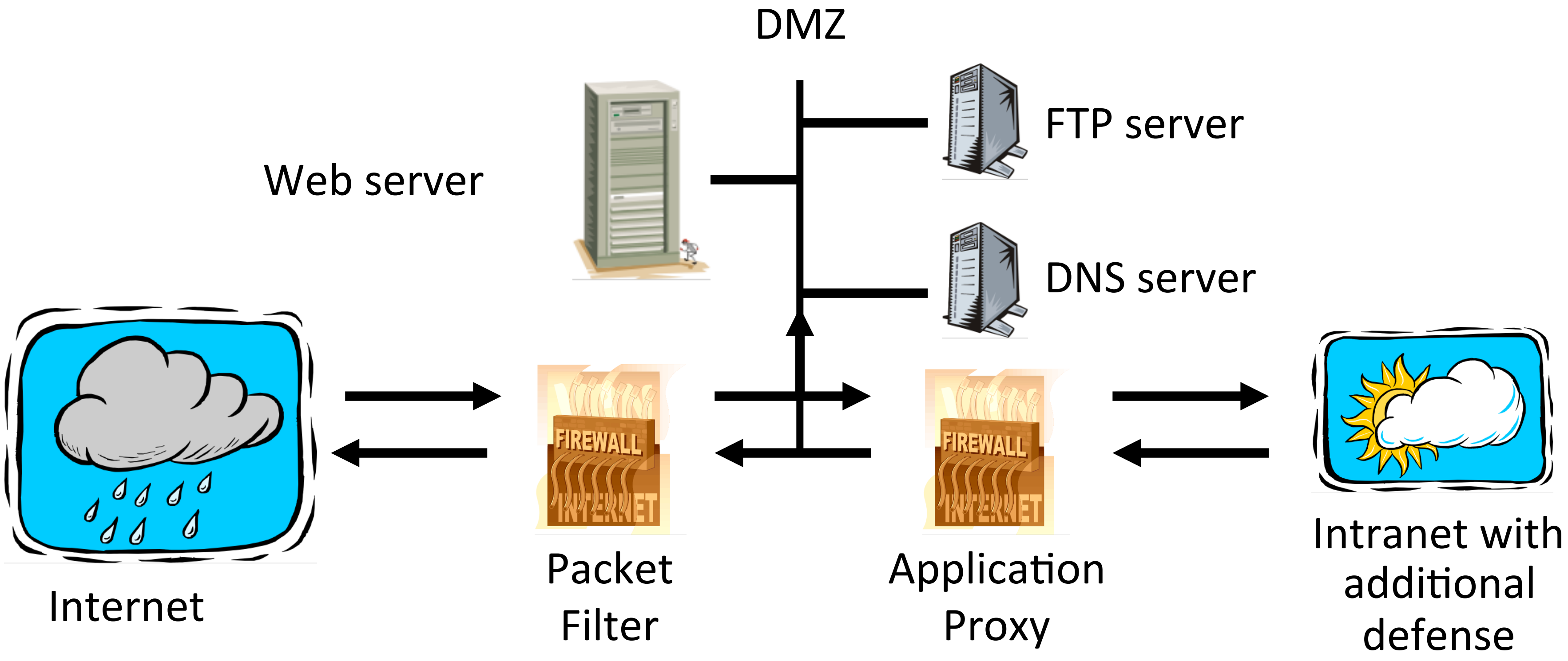
- This will **not** work thru an application proxy (why?)
- The proxy creates a new packet, destroys old TTL

Deep Packet Inspection

- Many buzzwords used for firewalls
  - One example: **deep packet inspection**
- What could this mean?
- Look into packets, but don't really "process" the packets
  - Like an application proxy, but faster

Firewalls and Defense in Depth

- Typical network security architecture


DMZ
Web server
FTP server
DNS server
Internet
Packet
Filter
Application
Proxy
Intranet with
additional
defense
FIREWALL
INTERNET
FIREWALL
INTERNET