

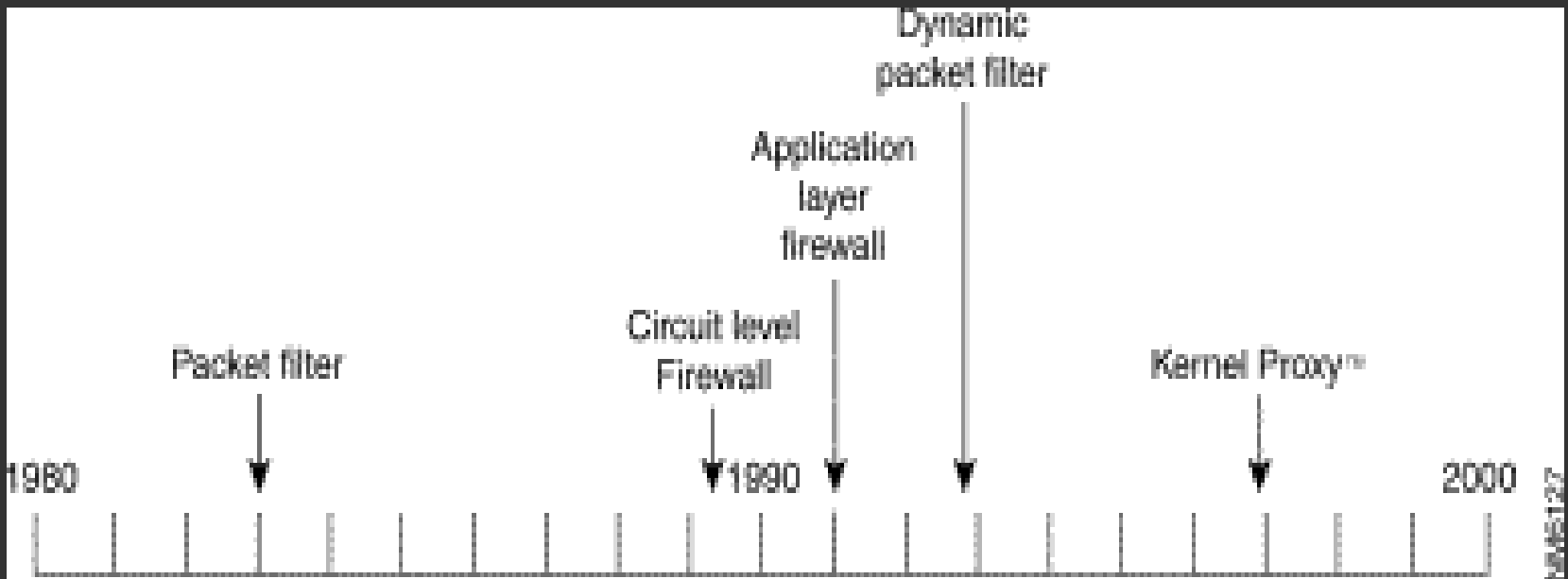
Firewalls

Presented by
Sheetal Joseph

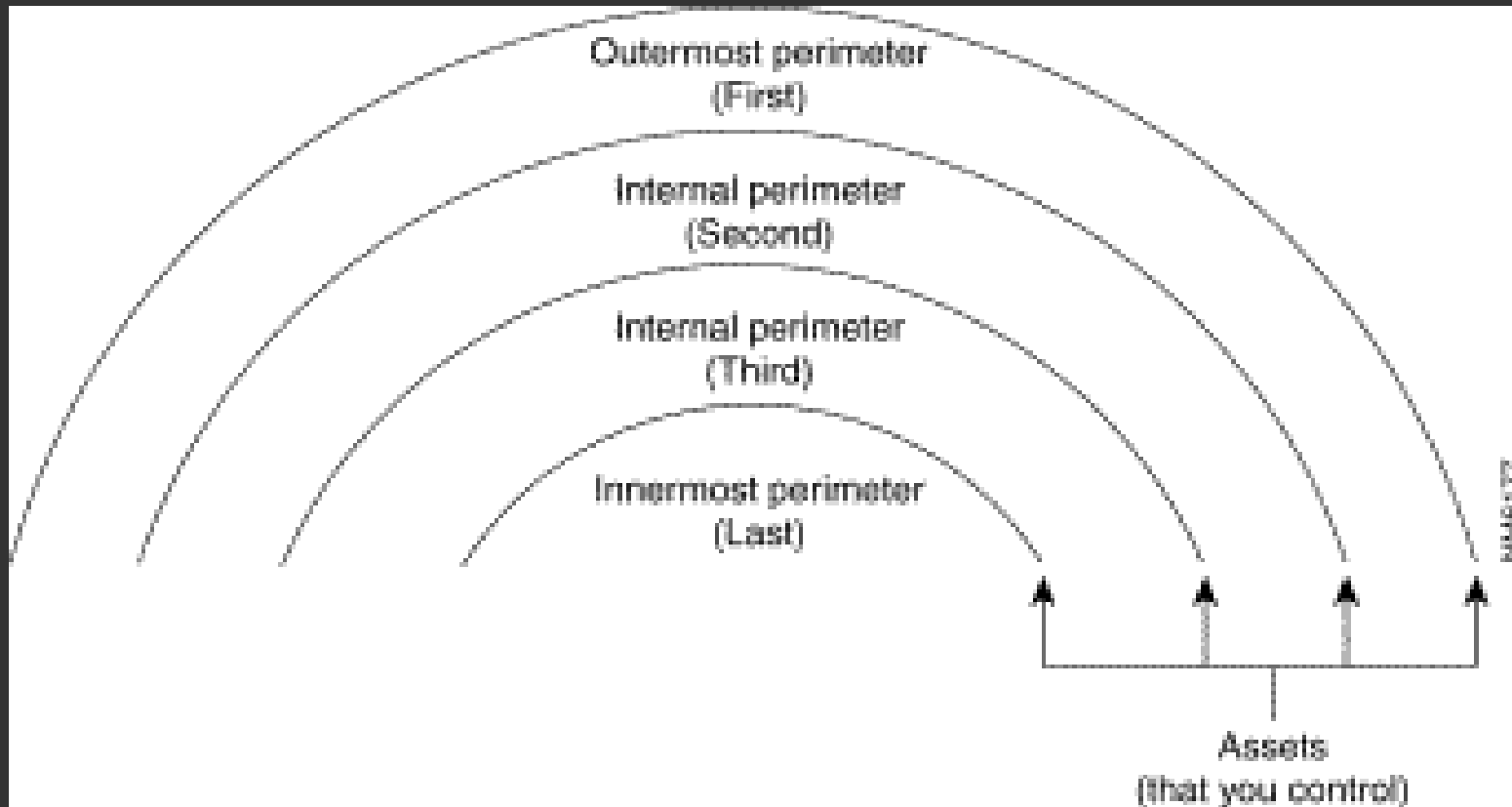
Firewalls

- A firewall is a physical manifestation of your corporate Information Security policy
- It can do the following:
 - Protect a trusted from an un-trusted network
 - Evaluate each incoming or outgoing packet
 - Against a specific criteria (“rule”)
 - Perform an action (permit – deny – modify)
 - Log the inspection / action event
 - Hide the internal network

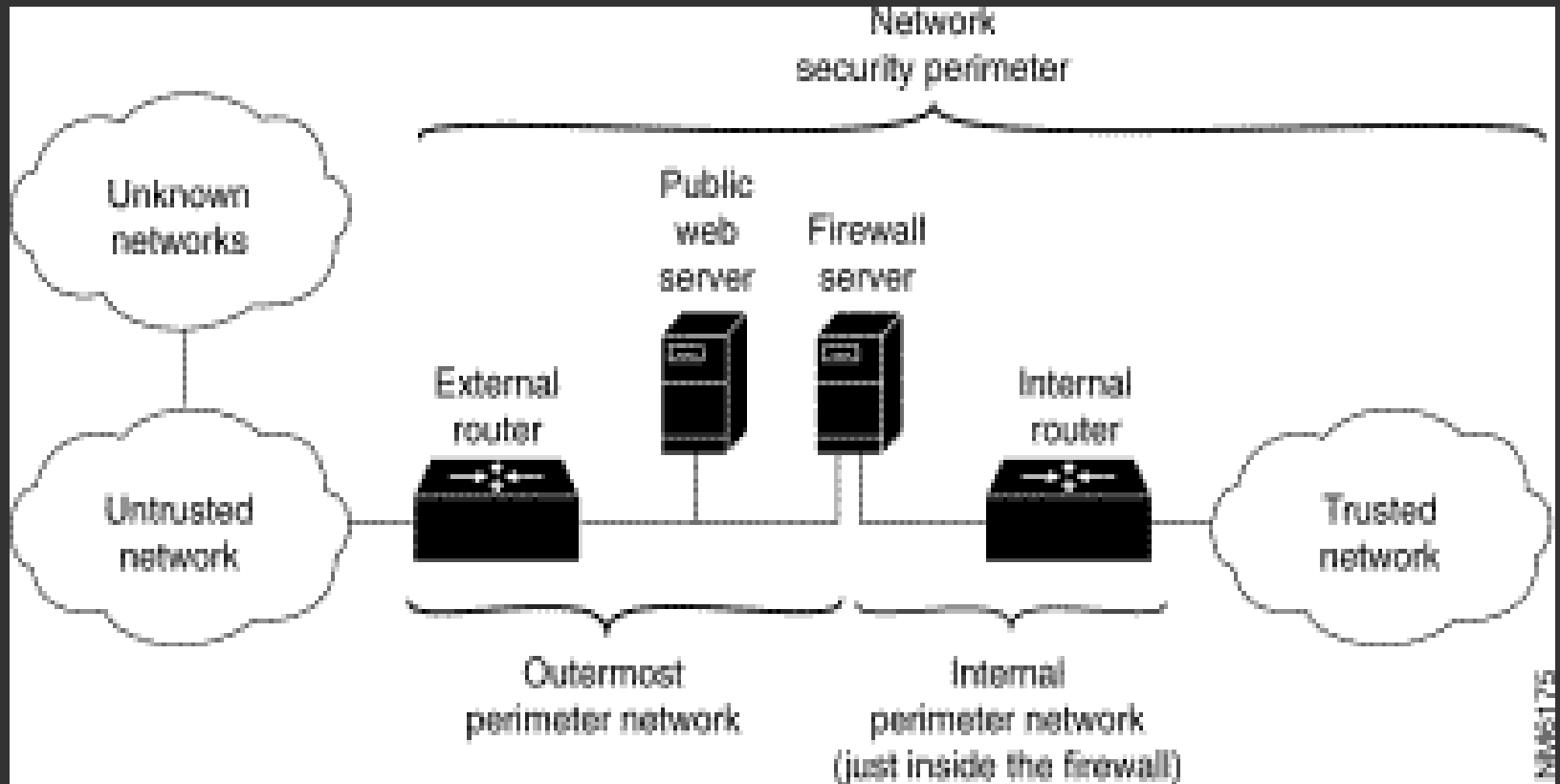
Time Line



Establishing a Security Perimeter



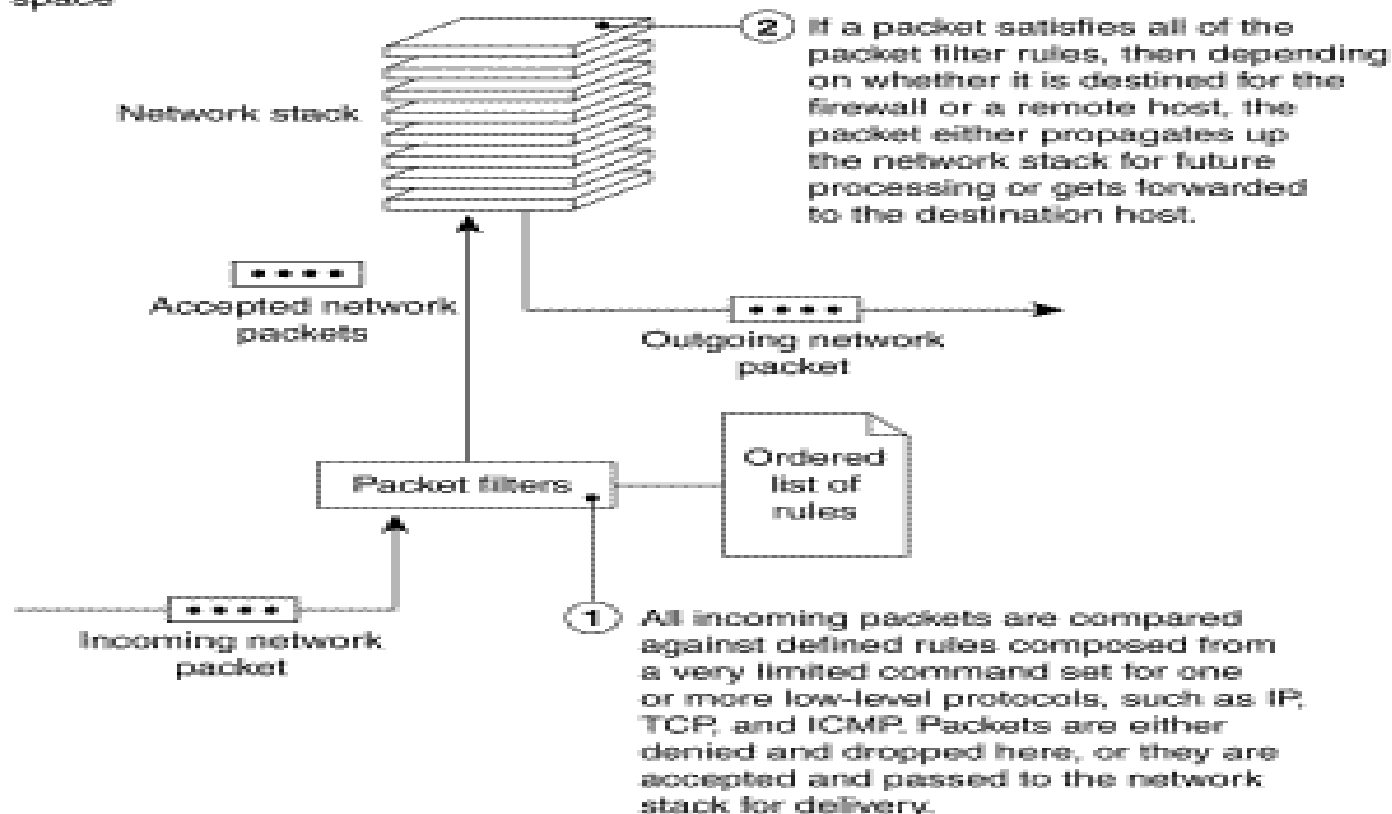
Network Security Perimeter



Packet Filters

Application space

Kernel space



Packet Filters

Packet filters typically enable you to manipulate (that is, permit or prohibit) the transfer of data based on the following controls:

- Physical network interface that the packet arrives on
- The address the data is (supposedly) coming from (source IP address)
- The address the data is going to (destination IP address)
- The type of transport layer (TCP, UDP, ICMP)
- The transport layer source port/destination port

Packet Filters-Advantages

- Packet filters are generally faster than other firewall technologies because they perform fewer evaluations. Also, they can easily be implemented as hardware solutions
- A single rule can help protect an entire network by prohibiting connections between specific Internet sources and internal computers.
- Packet filters do not require client computers to be specifically configured; the packet filters do all of the work.
- In conjunction with network address translation, you can use packet filter firewalls to shield internal IP addresses from external users.

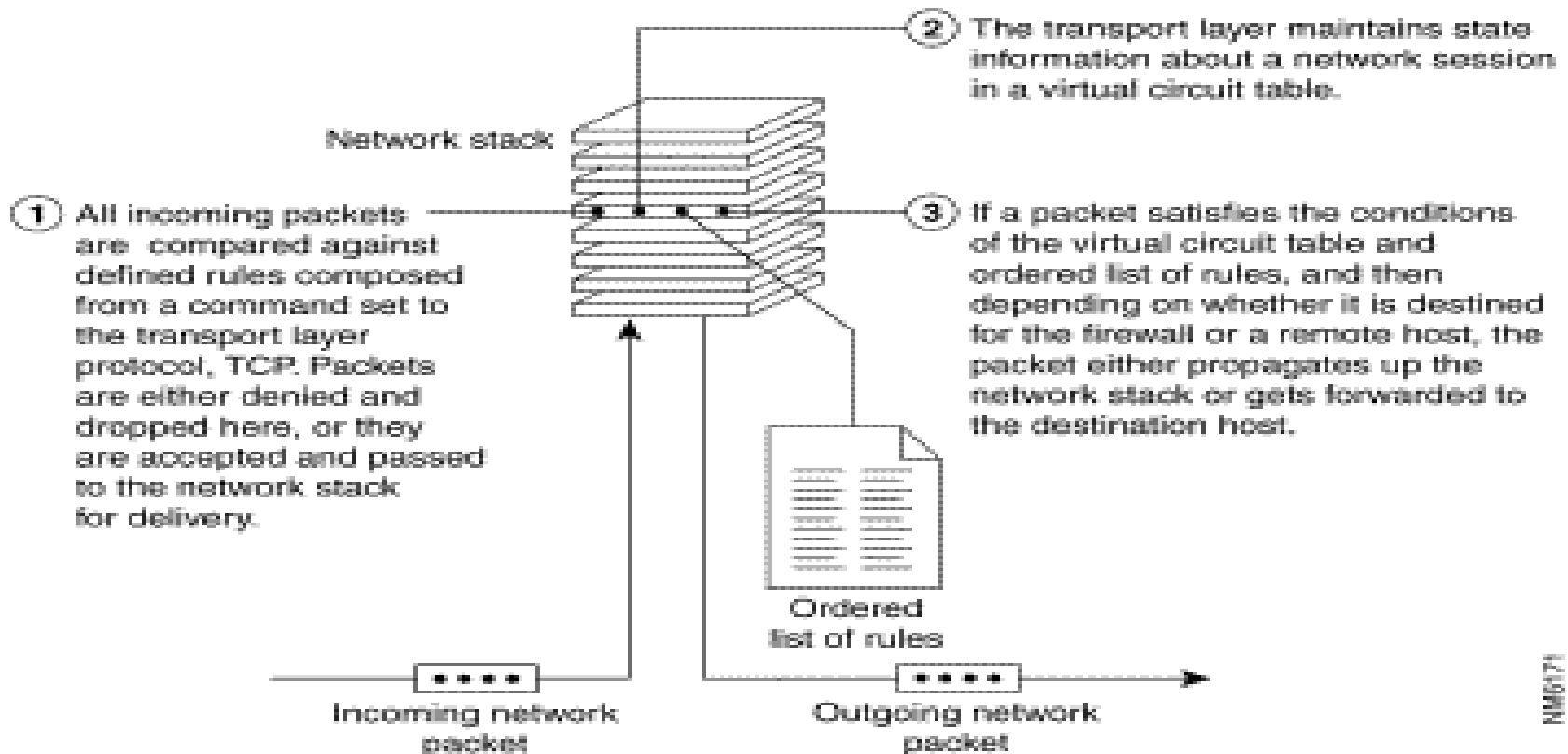
Packet Filters-Disadvantages

- Packet filters do not understand application layer protocols. They cannot restrict access to protocol subsets for even the most basic services, such as the PUT or GET commands in FTP. For this reason, they are less secure than application layer and circuit level firewalls.
- Packet filters are stateless in that they do not keep information about a session or application-derived information.
- Packet filters have very limited abilities to manipulate information within a packet.
- Packet filters do not offer value-added features, such as HTTP object caching, URL filtering, and authentication because they do not understand the protocols being used and cannot discern one from another.
- Packet filters cannot restrict what information is passed from internal computers to services on the firewall server. Packet filters only restrict what information can go *to* it. Thus, intruders can potentially access the services on the firewall server.
- Packet filters have little or no audit event generation and alerting mechanisms.
- Because of the complexity of supporting most non-trivial network services, it can be difficult to test "accept" and "deny" rules.

Circuit Level Firewall

Application space

Kernel space



Circuit Level Firewall

When a connection is set up, the circuit level firewall typically stores the following information about the connection:

- A unique session identifier for the connection, which is used for tracking purposes
- The state of the connection: *handshake*, *established*, or *closing*
- The sequencing information
- The source IP address, which is the address from which the data is being delivered
- The destination IP address, which is the address to which the data is being delivered
- The physical network interface through which the packet arrives
- The physical network interface through which the packet goes out

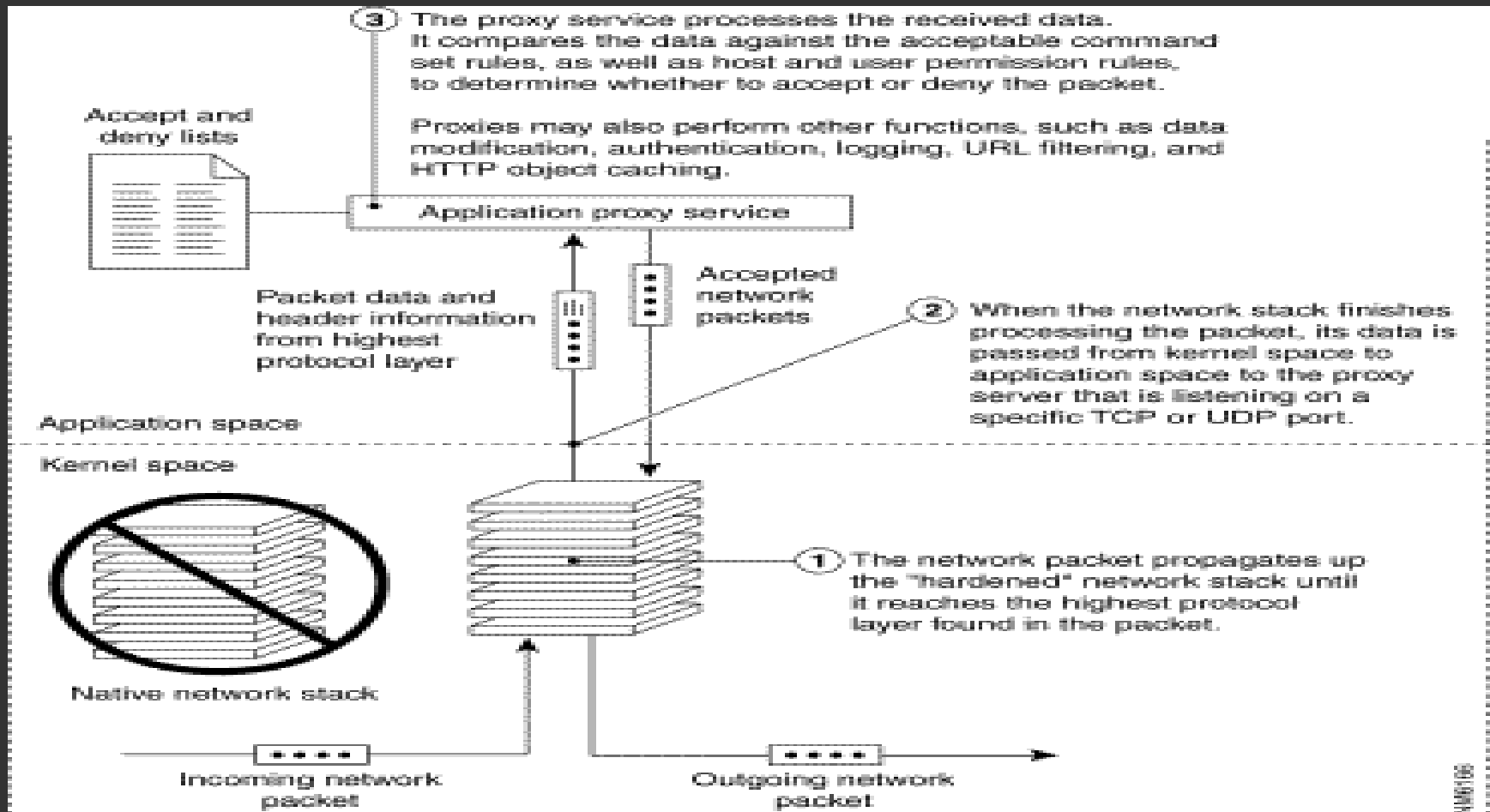
Circuit level firewalls-adv

- Circuit level firewalls are generally faster than application layer firewalls because they perform fewer evaluations.
- A circuit level firewall can help protect an entire network by prohibiting connections between specific Internet sources and internal computers.
- In conjunction with network address translation, you can use circuit level firewalls to shield internal IP addresses from external users.

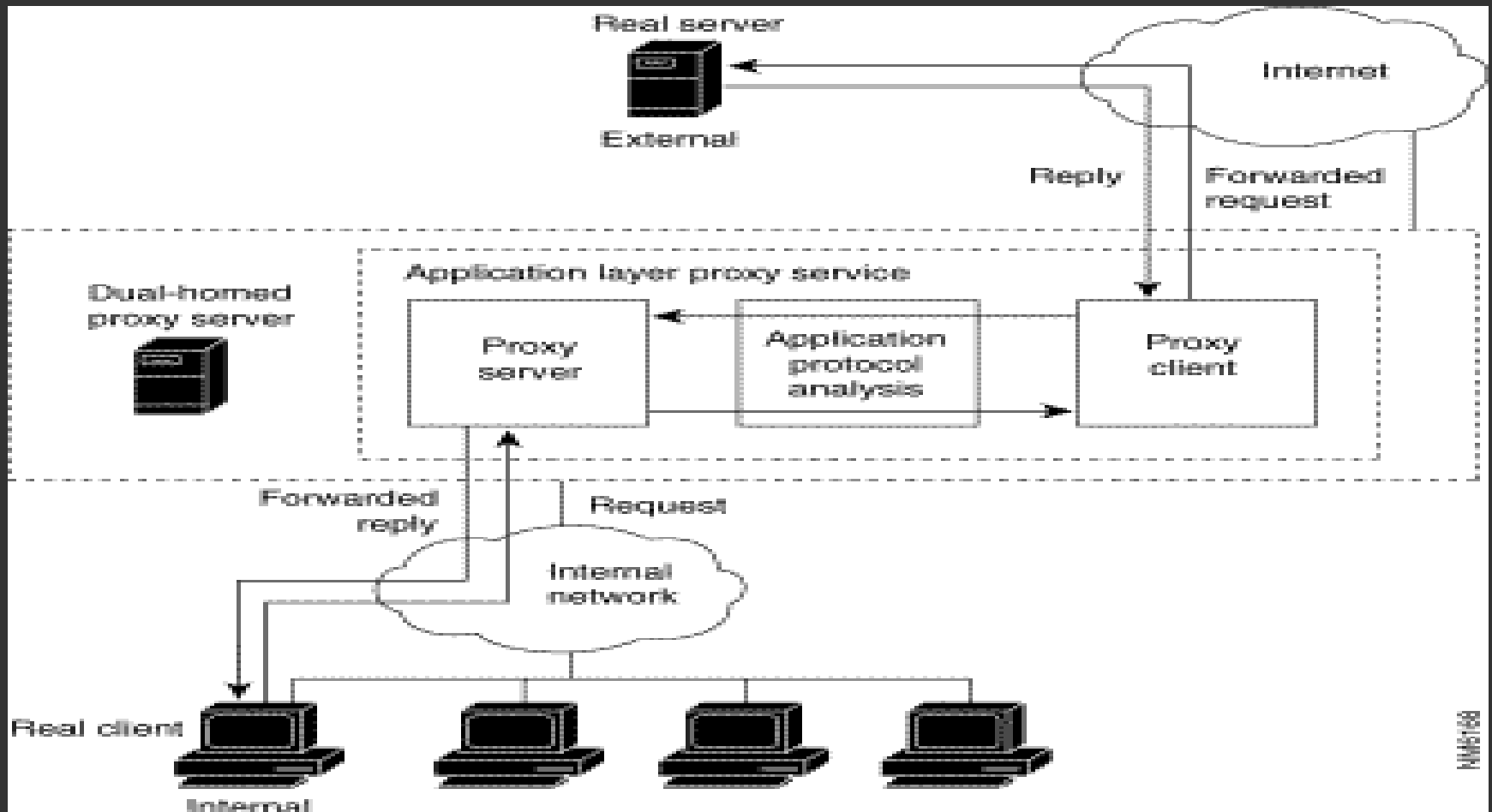
Circuit Level Firewall - Disadvantages

- Circuit level firewalls cannot restrict access to protocol subsets other than TCP.
- Circuit level firewalls cannot perform strict security checks on a higher-level protocol should the need arise.
- Circuit level firewalls have limited audit event generation abilities but can typically tie a network data packet to an application layer protocol by building limited forms of session state.
- Circuit level firewalls do not offer value-added features, such as HTTP object caching, URL filtering, and authentication because they do not understand the protocols being used and cannot discern one from another.
- It can be difficult to test "accept" and "deny" rules.

Application Layer Firewalls



How a Proxy Service Works



Dynamic Packet Filters

