SNS COLLEGE OF ENGINEERING

Kurumbapalayam(Po), Coimbatore – 641 107
Accredited by NAAC-UGC with 'A' Grade
Approved by AICTE, Recognized by UGC & Affiliated to Anna University, Chennai

Department of Artificial Intelligence & Data Science

CYBER SECURITY

Daze Thomas
AP | AI & DS

Network Encryption

- Encryption is powerful for providing privacy, authenticity, integrity and separation
- Use network encryption to encrypt data transmitted between server and client, and between server and other server.
- To read an encrypted file, you must have access to a secret decryption key or password.
- Unencrypted data is called *plain text*; encrypted data is called *cipher text*.
- A *cipher* is an encryption-decryption algorithm.

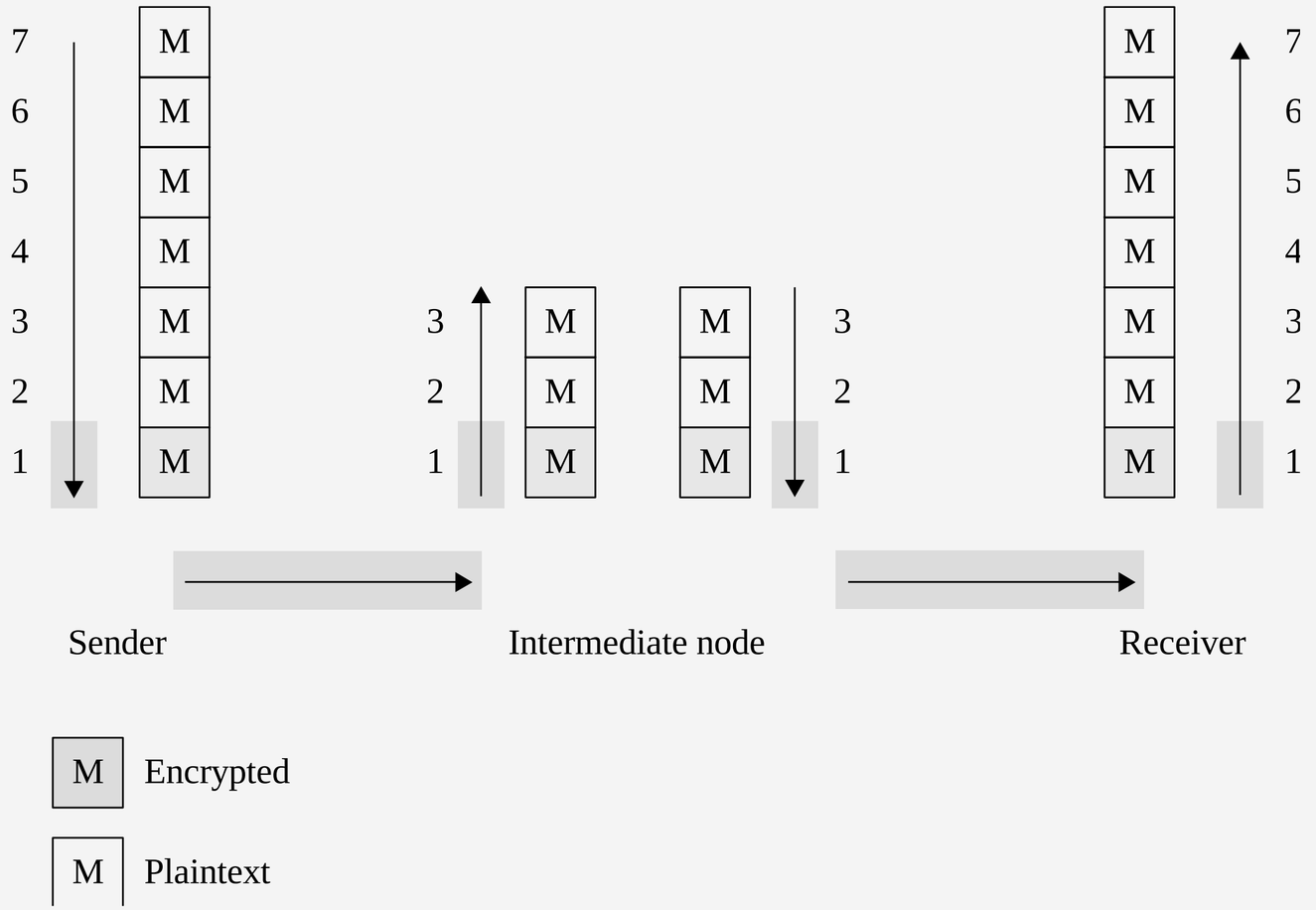
The OSI Model

7	Application Layer	Human-computer interaction layer, where applications can access the network services
6	Presentation Layer	Ensures that data is in a usable format and is where data encryption occurs
5	Session Layer	Maintains connections and is responsible for controlling ports and sessions
4	Transport Layer	Transmits data using transmission protocols including TCP and UDP
3	Network Layer	Decides which physical path the data will take
2	Data Link Layer	Defines the format of data on the network
1	Physical Layer	Transmits raw bit stream over the physical medium

Modes of Network Encryption

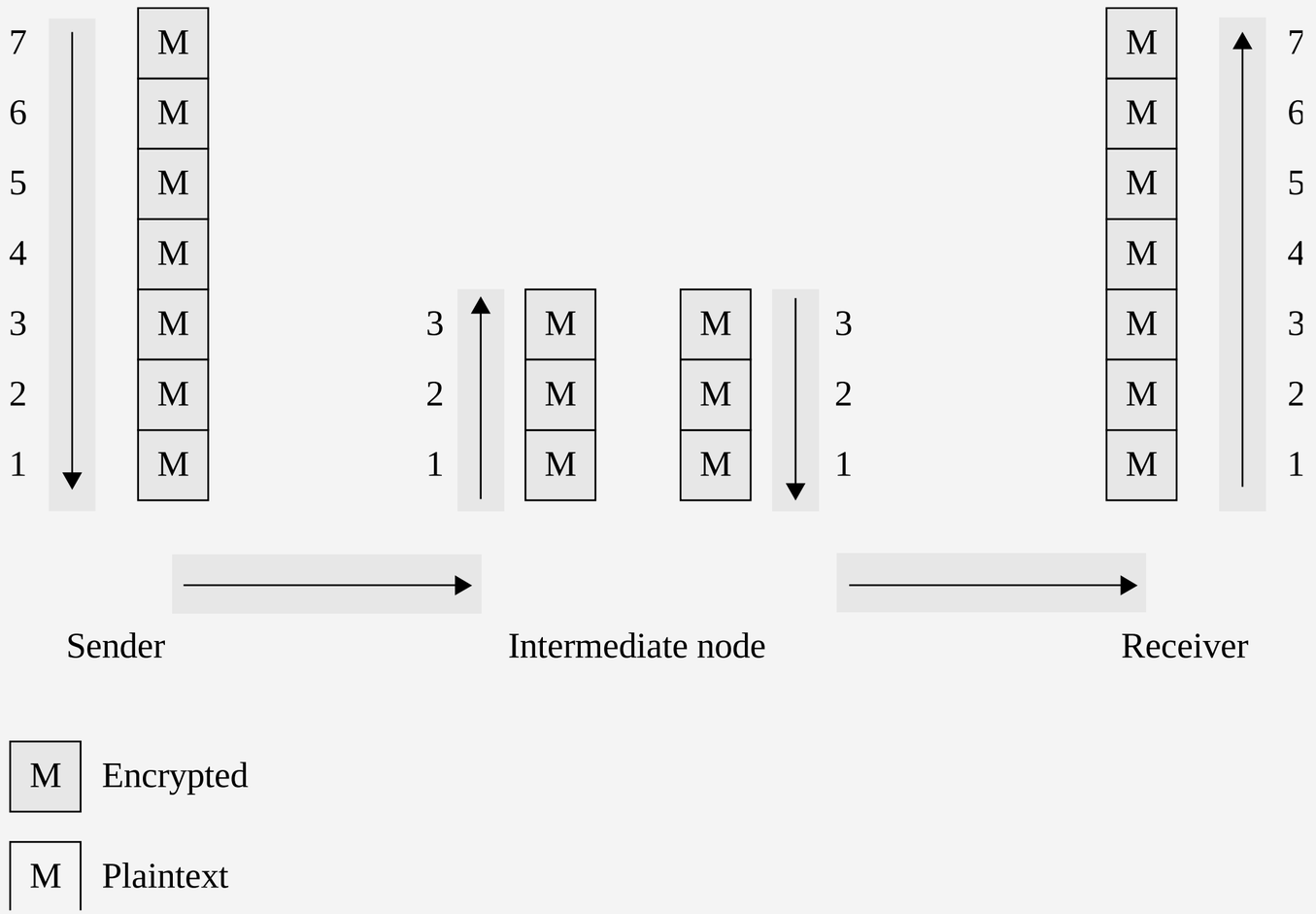
- Encryption can be employed in a network through two general modes: link and end-to end.
- They perform different functions and have different strengths and weaknesses.
- And they can even be used together, even if somewhat redundantly.

Link Encryption



- Data are encrypted just before the system places them on the physical communications link.
- Encryption occurs at layer 1 or 2 in the OSI model
- Addressing occurs at level 3
- In the intermediate node, the encryption must be removed in order to determine where next to forward the data, and so the content is exposed.

End-to-End Encryption



- Provides security from one end of a transmission to the other.
- The encryption can be applied between the user and the host by a hardware device.

Link vs. End-to-End

Link Encryption	End-to-End Encryption
Security within hosts	
Data partially exposed in sending host	Data protected in sending host
Data partially exposed in intermediate nodes	Data protected through intermediate nodes
Role of user	
Applied by sending host	Applied by user application
Invisible to user	User application encrypts
Host administrators select encryption	User selects algorithm
One facility for all users	Each user selects
Can be done in software or hardware	Usually software implementation; occasionally performed by user add-on hardware
All or no data encrypted	User can selectively encrypt individual data items
Implementation considerations	
Requires one key per pair of hosts	Requires one key per pair of users
Provides node authentication	Provides user authentication

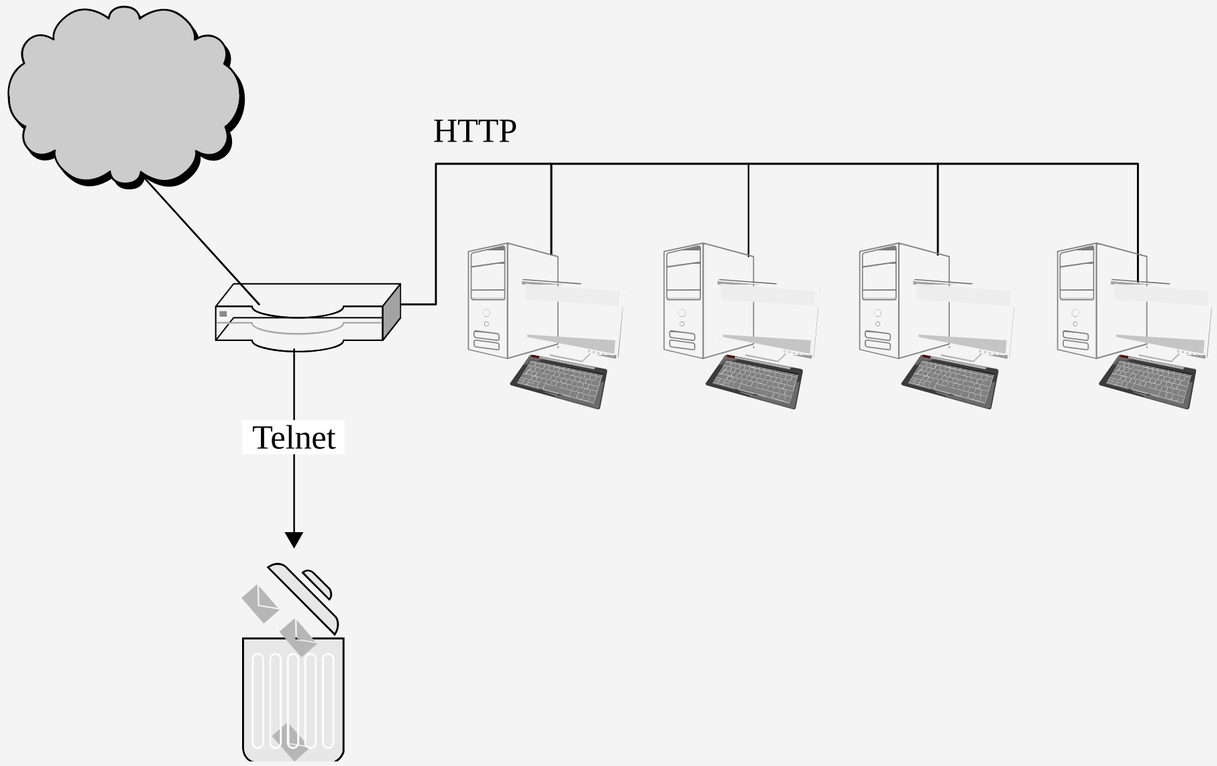
Firewalls

- A device that filters all traffic between a protected or “inside” network and less trustworthy or “outside” network
- Most firewalls run as dedicated devices
  - Easier to design correctly and inspect for bugs
  - Easier to optimize for performance
- Firewalls implement security policies, or set of rules that determine what traffic can or cannot pass through
- A firewall is an example of a reference monitor, which means it should have three characteristics:
  - Always invoked (cannot be circumvented)
  - Tamperproof
  - Small and simple enough for rigorous analysis

Types of Firewalls

- Packet filtering gateways or screening routers
- Stateful inspection firewalls
- Application-level gateways, also known as proxies
- Circuit-level gateways
- Guards
- Personal or host-based firewalls

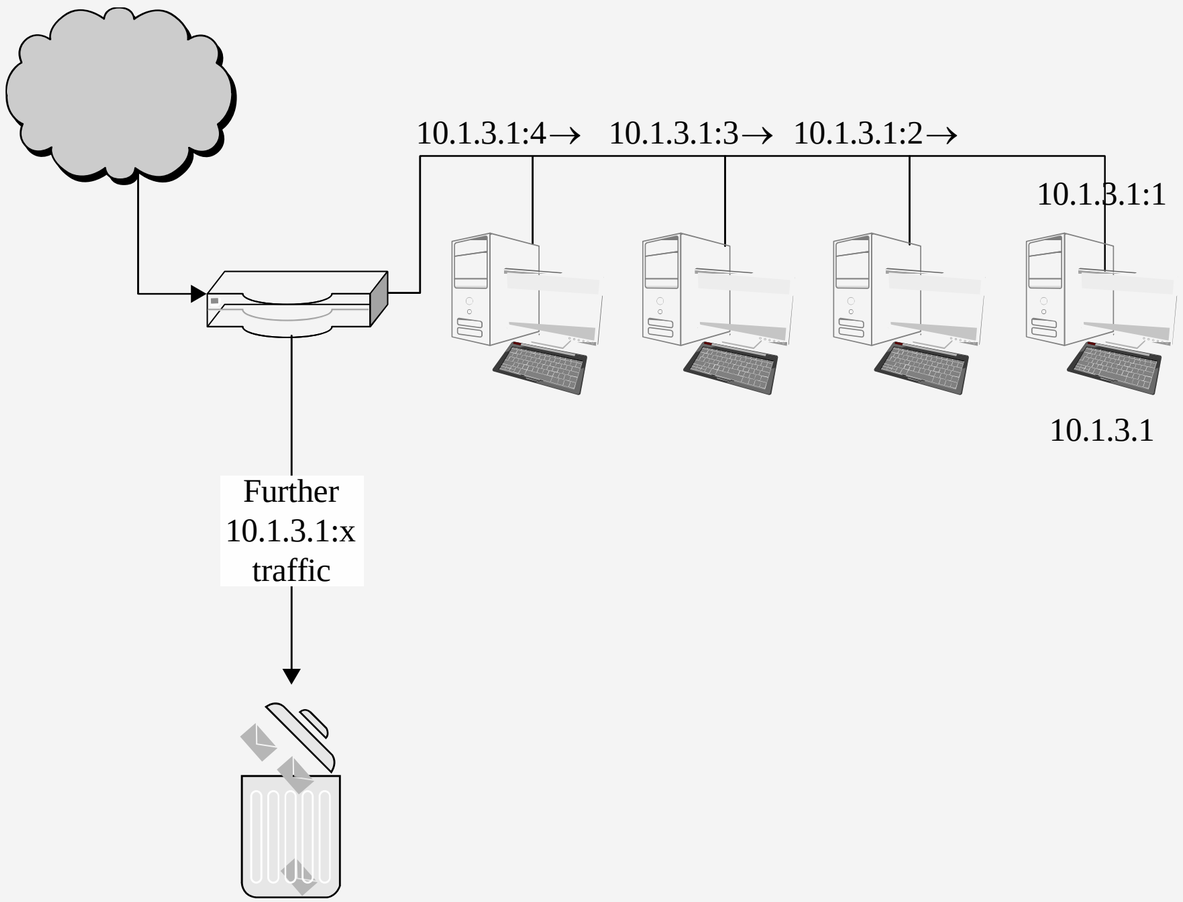
Packet-Filtering Gateways



- A packet-filtering gateway controls access on the basis of packet address and specific transport protocol type (e.g., HTTP traffic).

The firewall is filtering out Telnet traffic but allowing HTTP traffic in.

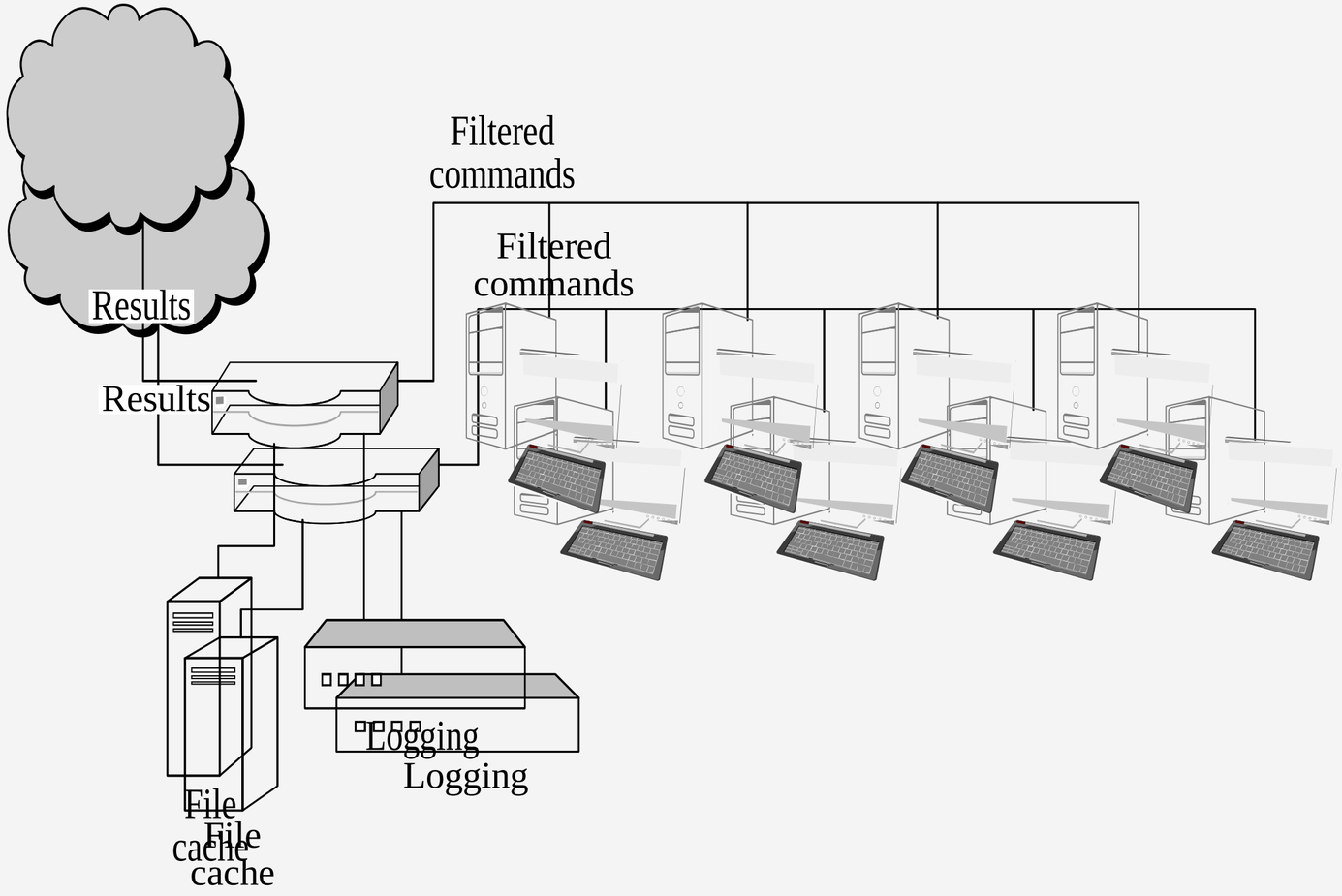
Stateful Inspection Firewall



- Maintain state information from one packet to the next

- The firewall is counting the number of systems coming from external IP 10.1.3.1; after the external system reaches out to a fourth computer, the firewall hits a configured threshold and begins filtering packets from that address.

Application Proxy

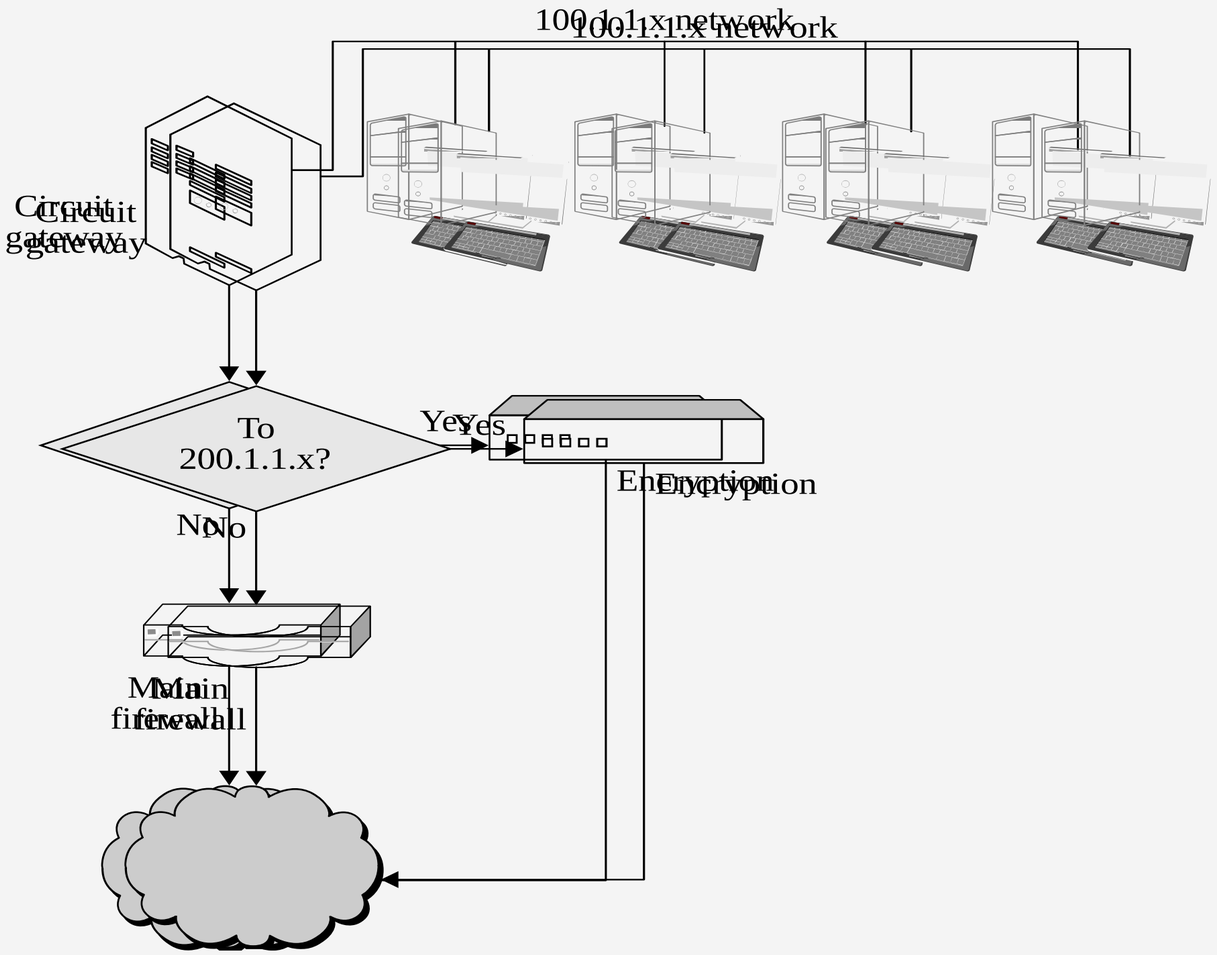


Application proxies can serve a number of purposes:

- Filtering potentially dangerous application-layer requests
- Log requests/accesses
- Cache results to save bandwidth

Perhaps the most common form of application proxies in the real world is a web proxy, which companies often use to monitor and filter employee Internet use.

Circuit-Level Gateway



- A circuit-level gateway is a firewall that essentially allows one network to be an extension of another.

- It operates at OSI layer 5, the session layer, and it functions as a virtual gateway between two networks.

- One use of a circuit-level gateway is to implement a VPN.

Guard

- A sophisticated firewall that, like an application proxy, can interpret data at the protocol level and respond
- The distinction between a guard and an application proxy can be fuzzy; the more protection features an application proxy implements, the more it becomes like a guard
- Guards may implement any programmable set of rules; for example:
  - Limit the number of email messages a user can receive
  - Limit users' web bandwidth
  - Filter documents containing the word "Secret"
  - Pass downloaded files through a virus scanner

Personal Firewalls

A personal firewall runs on a workstation or server and can enforce security policy like other firewalls.

In addition to restricting traffic by source IP and destination port, personal firewalls can restrict which applications are allowed to use the network.

In this example Windows firewall configuration dialog, an administrator can select which protocols and applications should be allowed to communicate to and from the host.

Comparison of Firewall Types

Packet Filter	Stateful Inspection	Application Proxy	Circuit Gateway	Guard	Personal Firewall
Simplest decision-making rules, packet by packet	Correlates data across packets	Simulates effect of an application program	Joins two subnetworks	Implements any conditions that can be programmed	Similar to packet filter, but getting more complex
Sees only addresses and service protocol type	Can see addresses and data	Sees and analyzes full data portion of pack	Sees addresses and data	Sees and analyzes full content of data	Can see full data portion
Auditing limited because of speed limitations	Auditing possible	Auditing likely	Auditing likely	Auditing likely	Auditing likely
Screens based on connection rules	Screens based on information across multiple packets—in either headers or data	Screens based on behavior of application	Screens based on address	Screens based on interpretation of content	Typically, screens based on content of each packet individually, based on address or content
Complex addressing rules can make configuration tricky	Usually preconfigured to detect certain attack signatures	Simple proxies can substitute for complex decision rules, but proxies must be aware of application's behavior	Relatively simple addressing rules; make configuration straightforward	Complex guard functionality; can be difficult to define and program accurately	Usually starts in mode to deny all inbound traffic; adds addresses and functions to trust as they arise