Security Countermeasures

ICT 3156

IPSITA UPASANA

Road Map

- Cryptography in Network Security
  - Browser Encryption
  - Onion Routing
  - IP Security Protocol Suite (IPsec)
  - Virtual Private Networks
- Firewalls
- Intrusion Detection and Prevention Systems
- Network Management

Browser Encryption

- Browsers can encrypt data for protection during transmission.
- The browser and the server negotiate a common encryption key. What does this imply?
- Even if an attacker hijacks a session at the TCP or IP protocol level, the attacker, not having the proper key, cannot join the application data exchange.
- SSH Encryption
- SSL and TLS Encryption
- Cipher Suite
- SSL Session

SSH Encryption

- SSH provides an authenticated and encrypted path to the shell or operating system command interpreter.
- SSH protects against spoofing attacks and modification of data in communication.
- The SSH protocol involves negotiation between local and remote sites for encryption algorithm (for example, DES or AES) and authentication (including public key and Kerberos).
- The protocol does have a known vulnerability.

SSL and TLS Encryption

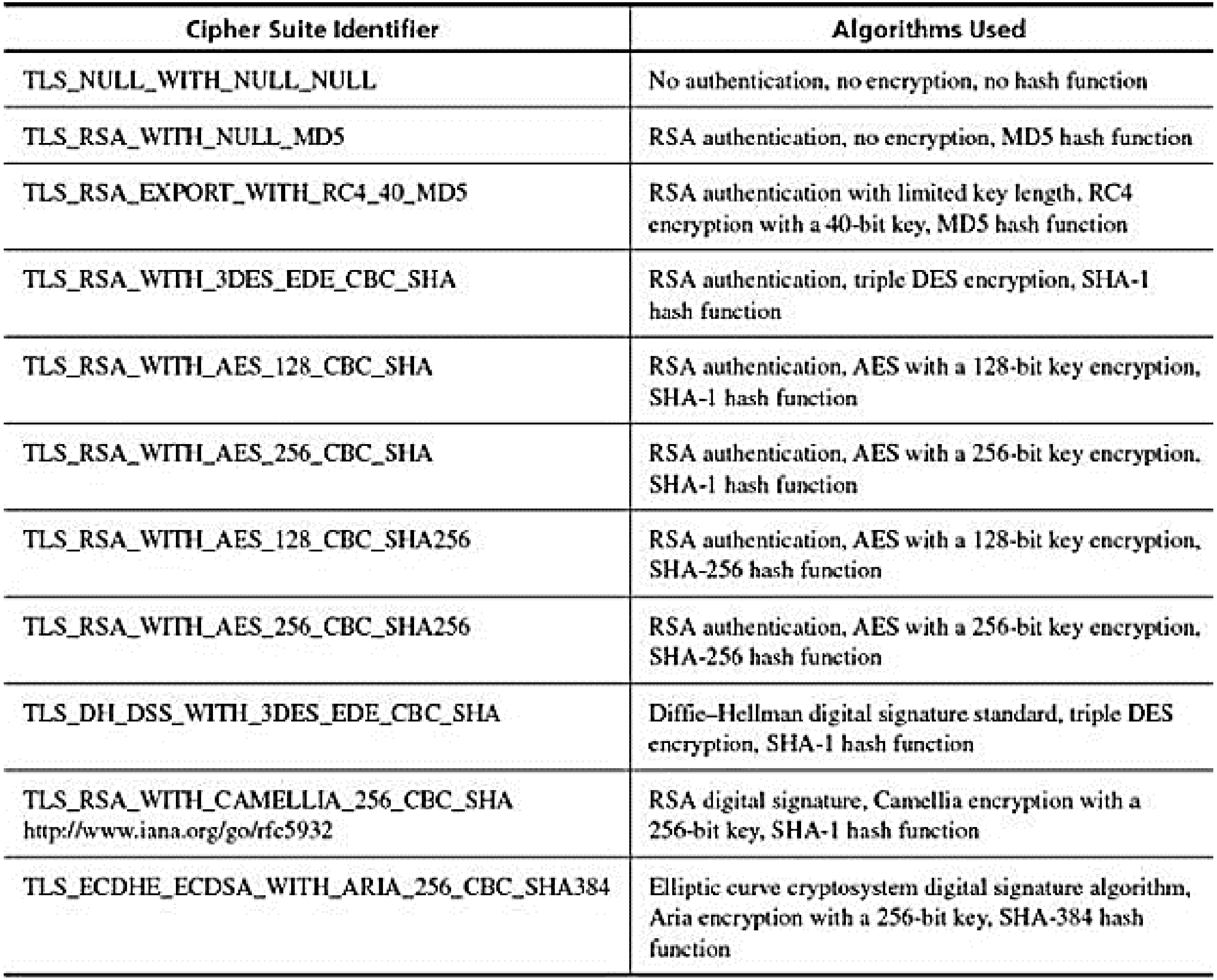
- Secure Sockets Layer (SSL) protocol
  - Originally designed by Netscape in the mid-1990s to protect communication between a web browser and server. SSL 1.0, SSL 2.0, SSL 3.0 .
- Transport Layer Security (TLS) : IETF upgraded SSL 3.0 and named the upgrade TLS.
- SSL is implemented at level 4 of OSI model.
- SSL operates between applications (such as browsers) and the TCP/IP protocols.
- It provides:
  - Server authentication.
  - Optional client authentication.
  - Encrypted communication channel between client and server.

Cipher Suite

- Client and server negotiate **cipher suite**, for authentication, session encryption, and hashing.
- The first to open an interaction states its preferred algorithms, and the second party responds with the highest one on that list it can handle.
- When client and server begin an SSL session, the server sends a set of records listing the cipher suite identifiers it can use; the client responds with its preferred selection from that set.
- IANA globally coordinates the **cipher suites**. What other things does it coordinate?
- The SSL protocol is simple but effective, and it is the most widely used secure communication protocol on the Internet.

Cipher Suite

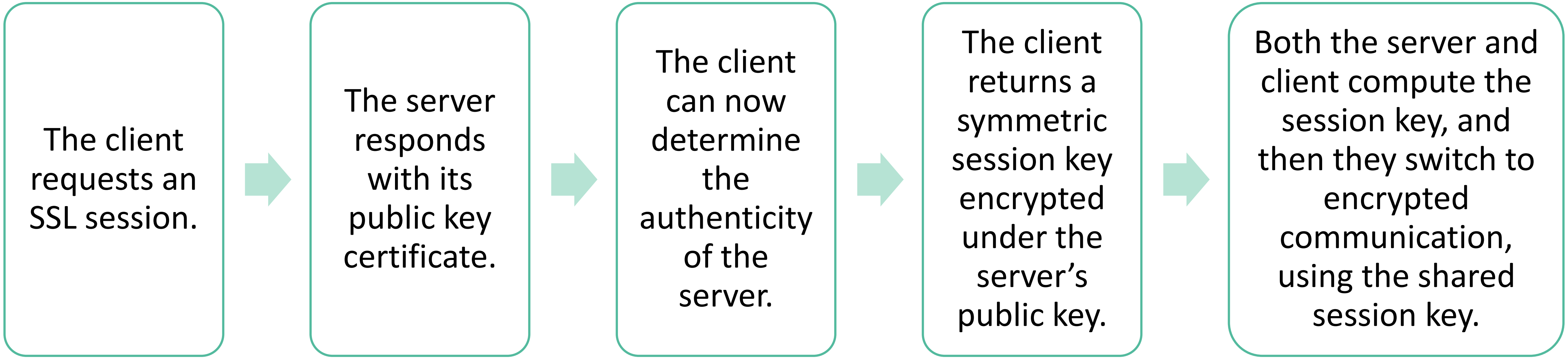
- MD5 has a flaw.
- Researchers were able to forge a seemingly valid certificate for use with SSL.
- Plaintext Injection attack.



Cipher Suite Identifier	Algorithms Used
TLS_NULL_WITH_NULL_NULL	No authentication, no encryption, no hash function
TLS_RSA_WITH_NULL_MD5	RSA authentication, no encryption, MD5 hash function
TLS_RSA_EXPORT_WITH_RC4_40_MD5	RSA authentication with limited key length, RC4 encryption with a 40-bit key, MD5 hash function
TLS_RSA_WITH_3DES_EDE_CBC_SHA	RSA authentication, triple DES encryption, SHA-1 hash function
TLS_RSA_WITH_AES_128_CBC_SHA	RSA authentication, AES with a 128-bit key encryption, SHA-1 hash function
TLS_RSA_WITH_AES_256_CBC_SHA	RSA authentication, AES with a 256-bit key encryption, SHA-1 hash function
TLS_RSA_WITH_AES_128_CBC_SHA256	RSA authentication, AES with a 128-bit key encryption, SHA-256 hash function
TLS_RSA_WITH_AES_256_CBC_SHA256	RSA authentication, AES with a 256-bit key encryption, SHA-256 hash function
TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA	Diffie–Hellman digital signature standard, triple DES encryption, SHA-1 hash function
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA http://www.iana.org/go/rfc5932	RSA digital signature, Camellia encryption with a 256-bit key, SHA-1 hash function
TLS_ECDHE_ECDSA_WITH_ARIA_256_CBC_SHA384	Elliptic curve cryptosystem digital signature algorithm, Aria encryption with a 256-bit key, SHA-384 hash function

SSL Session

- Often referred to as HTTPS.
- To use SSL:



The client requests an SSL session.

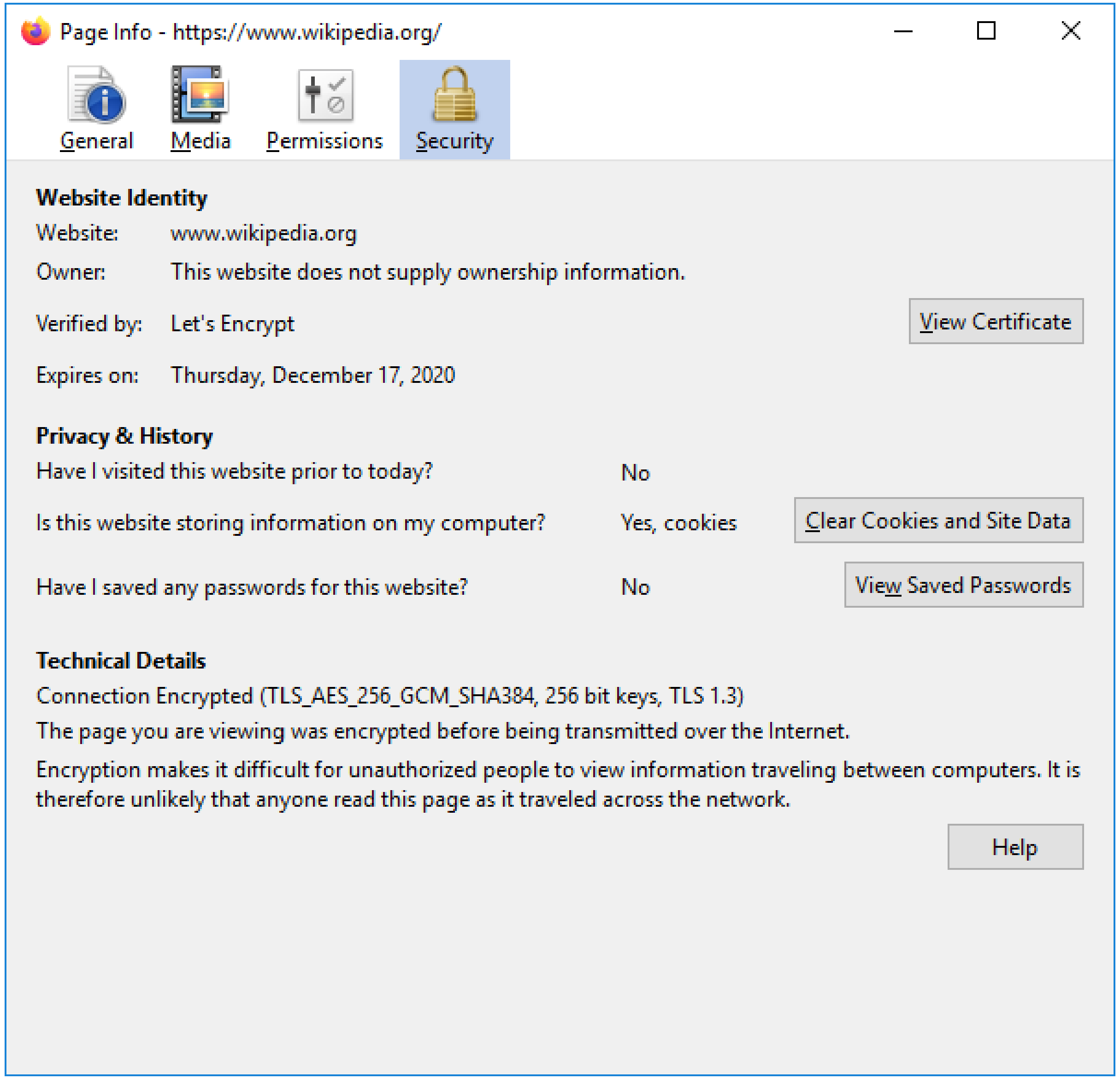
The server responds with its public key certificate.

The client can now determine the authenticity of the server.

The client returns a symmetric session key encrypted under the server's public key.

Both the server and client compute the session key, and then they switch to encrypted communication, using the shared session key.

After an SSL session has been established, the details of the session can be viewed.



Website Identity

Website: www.wikipedia.org

Owner: This website does not supply ownership information.

Verified by: Let's Encrypt

Expires on: Thursday, December 17, 2020

Privacy & History

Have I visited this website prior to today? No

Is this website storing information on my computer? Yes, cookies

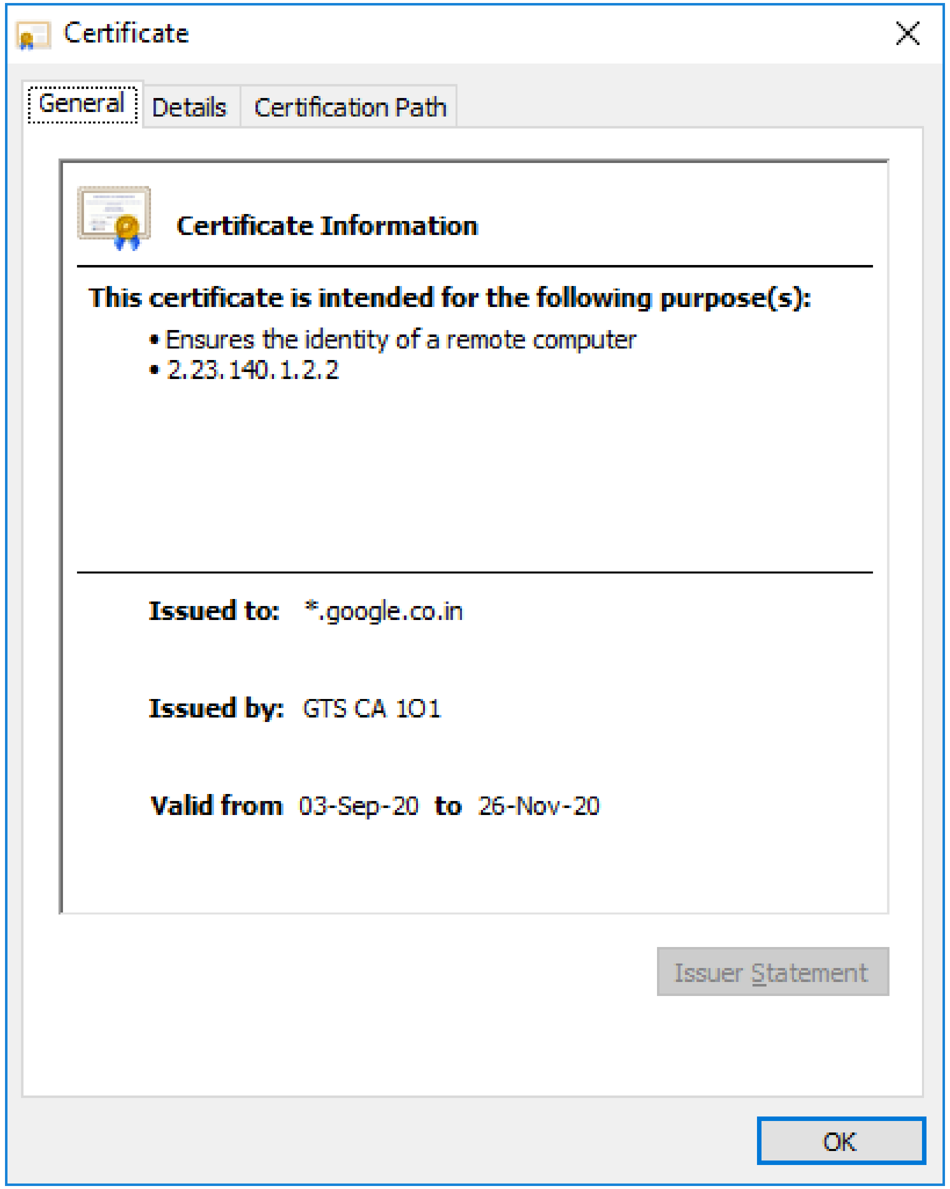
Have I saved any passwords for this website? No

Technical Details

Connection Encrypted (TLS_AES_256_GCM_SHA384, 256 bit keys, TLS 1.3)

The page you are viewing was encrypted before being transmitted over the Internet.

Encryption makes it difficult for unauthorized people to view information traveling between computers. It is therefore unlikely that anyone read this page as it traveled across the network.



Certificate Information

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer
- 2.23.140.1.2.2

Issued to: *.google.co.in

Issued by: GTS CA 1O1

Valid from 03-Sep-20 **to** 26-Nov-20

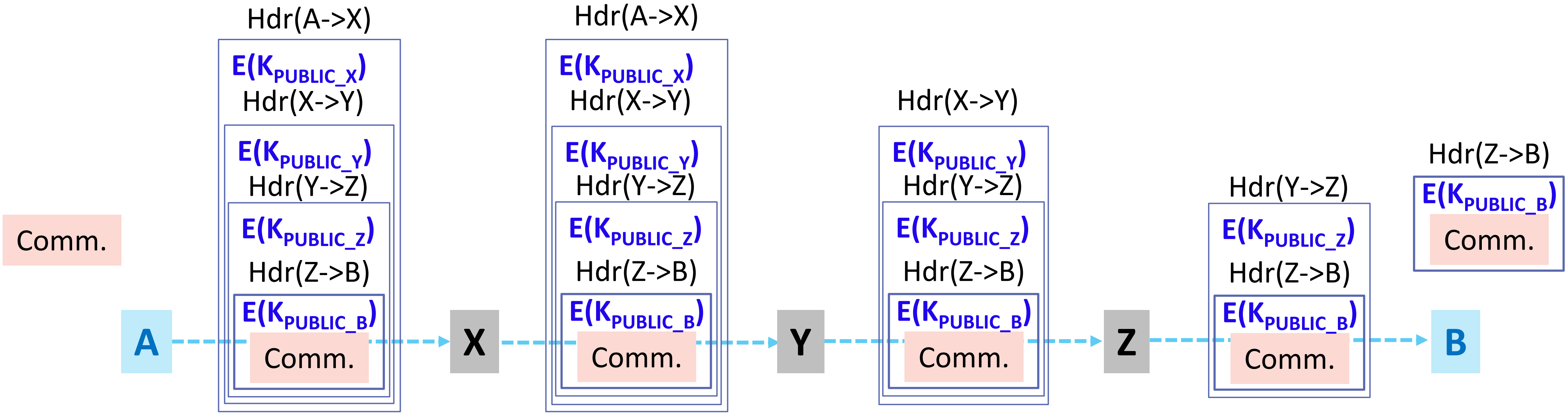
SSL Session

- The chain of certificates and signers is important because of the potential for **unscrupulous CAs.**
- **Why** should one review their set of loaded certificates?
  - The preloaded CAs are reputable, but if one CA signs a certificate for a less honorable firm, the SSL operation would still succeed.
  - SSL requires a certificate chain from a CA in the browser’s list, but all such CAs are equally credible to the browser.
  - That is why you should review your set of loaded certificates to ensure that you would trust anything signed by any of them.
- SSL encryption protects only from the browser to the destination decryption point. Vulnerabilities before encryption or after decryption are unaffected.

Onion Routing

- **Tor**—onion routing—prevents an eavesdropper from learning source, destination, or content of data in transit in a network.
- Packages for onion routing can be any network transmissions.
- Most popular uses: covert email and private web browsing.
- Tor protects by transferring communications around a distributed network of relays run by volunteers all around the world.
- The model uses a collection of forwarding hosts, each of whom knows only from **where a communication was received and to where to send it next**.

Onion Routing



IP Security Protocol Suite (IPsec)

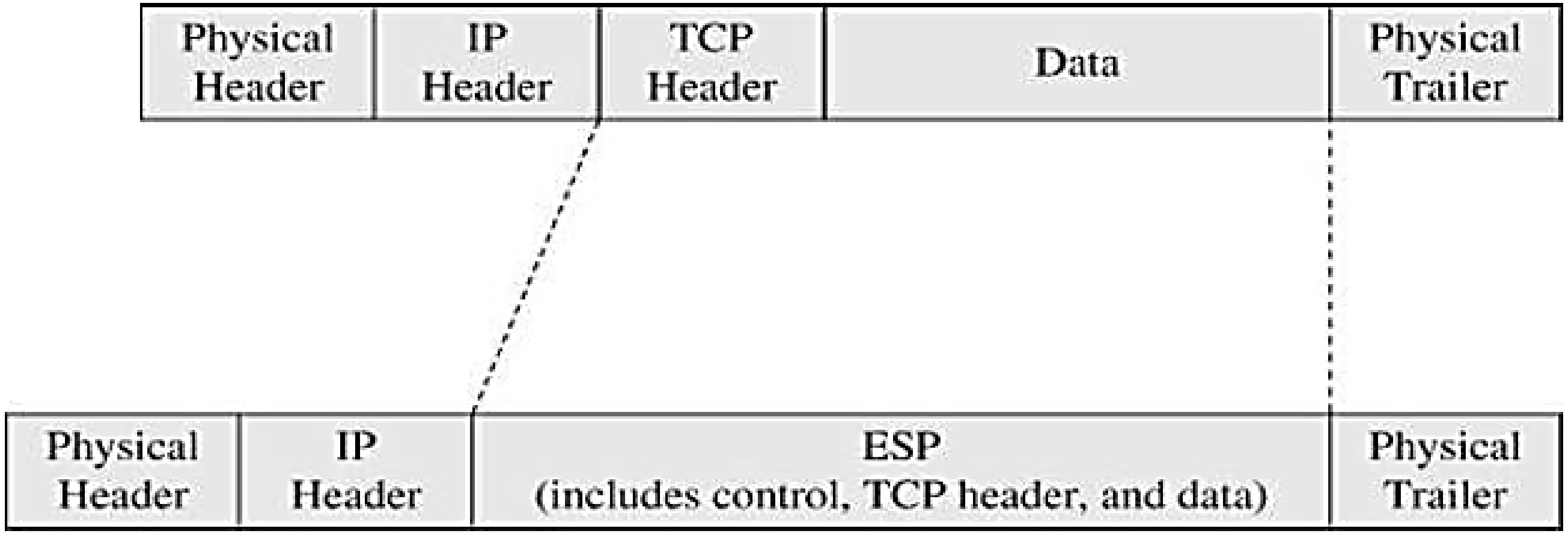
- IPsec was adopted as a part of the IPv6 suite.
- IPsec protocol defines a standard means for handling encrypted data.
- Designed to address fundamental shortcomings such as being subject to spoofing, eavesdropping, and session hijacking.
- IPsec requires **no change** to the existing large number of TCP and UDP protocols or applications. Why so?
- Implemented at the IP layer 3. So it protects data produced in all layers above it.
- IPsec is somewhat similar to SSL. How?
- IPsec implements encryption and authentication in the Internet protocols.

IPsec Security Association

- The basis of IPsec is a **security association**.
- It is essentially the set of security parameters for a secured communication channel.
- A security association includes:
    - Encryption algorithm and mode .
    - Encryption key.
    - Encryption parameters.
    - Authentication protocol and key
    - Life span of the association.
    - Address of the opposite end of association.
    - Sensitivity level of protected data (usable for classified data).

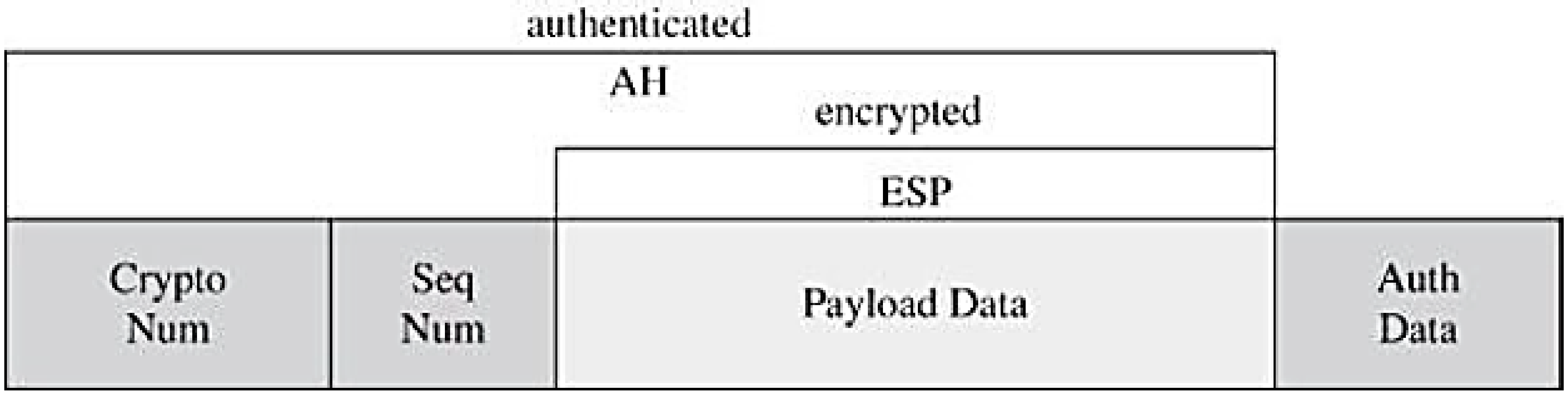
IPsec Headers and Data

- The fundamental data structures of IPsec are the authentication header (AH) and the encapsulated security payload (ESP).
- The ESP replaces (includes) the conventional TCP header and data portion of a packet.



IPsec Headers and Data

- The ESP contains both an authenticated portion and an encrypted portion.
- IPsec encapsulated security payload contains descriptors to tell a recipient how to interpret encrypted content.

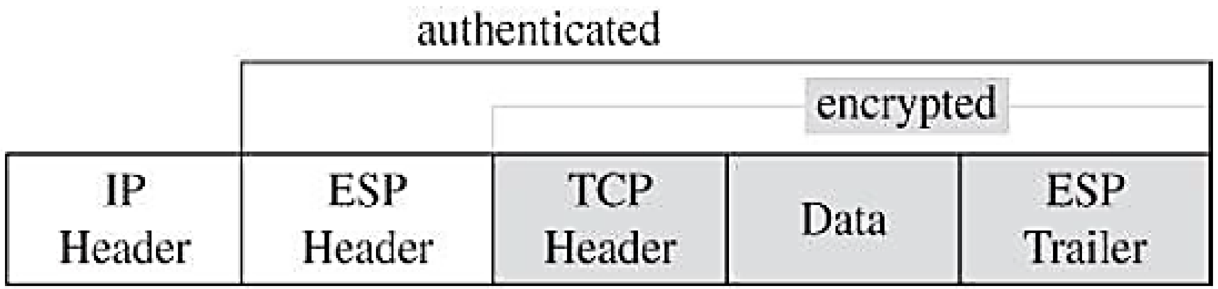


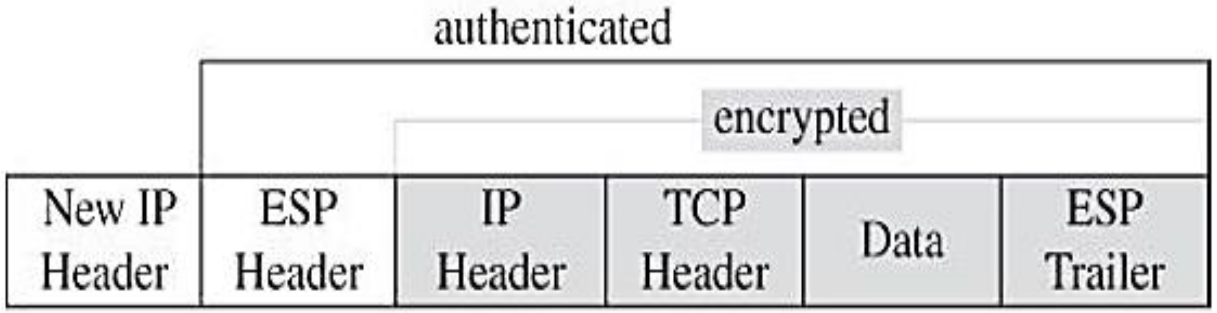
IPsec Key Management

- The critical element is key management.
- Addressed by Internet Security Association Key Management Protocol, or **ISAKMP**.
- ISAKMP requires that a distinct key be generated for each security association.
- ISAKMP is implemented through the ISAKMP key exchange, or **IKE**.
- IKE provides a way to agree on and manage protocols, algorithms, and keys.
- The exchange can be accomplished in two messages, with an optional two more messages for authentication.

IPsec Modes of Operation

- IPsec can enforce either or both of confidentiality and authenticity.
- Two modes of operation :
  - Transport Mode
  - Tunnel Mode





Transport mode (normal operation) : the IP address header is unencrypted.

Tunnel mode : the recipient’s address is concealed by encryption, and IPsec substitutes the address of a remote device, such as a firewall, that will receive the transmission and remove the IPsec encryption.

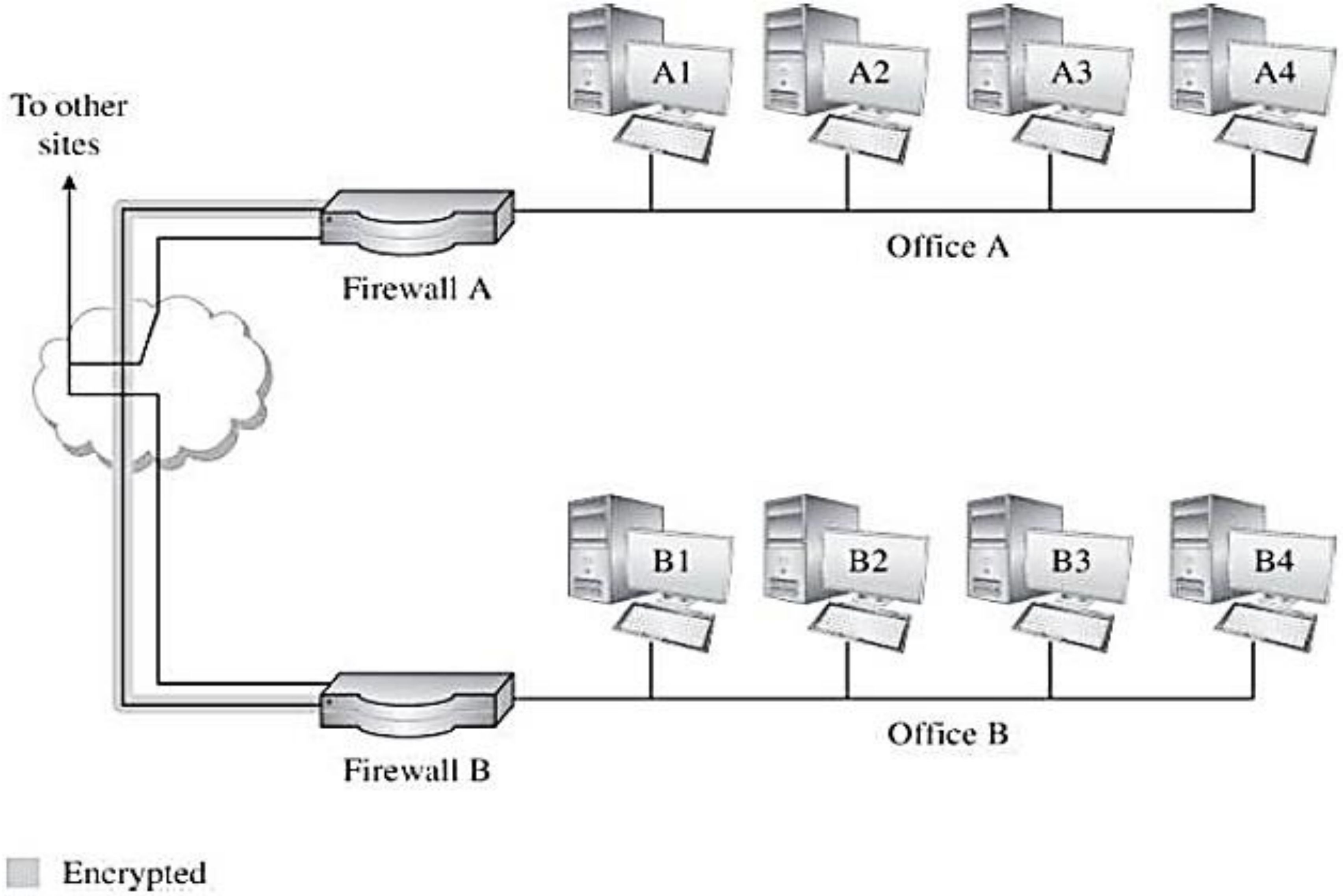
Virtual Private Networks (VPNs)

- Link encryption can give a network’s users the sense that they are on a private network, even when it is part of a public network.
- If applied at the link level, the encrypting and decrypting are invisible to users.
- A **virtual private network** simulates the security of a dedicated, protected communication line on a shared network.
- Two approaches for private network:
    - By acquiring, managing, and maintaining their own network equipment to provide a private link between the two sites.
    - By implementing VPN.

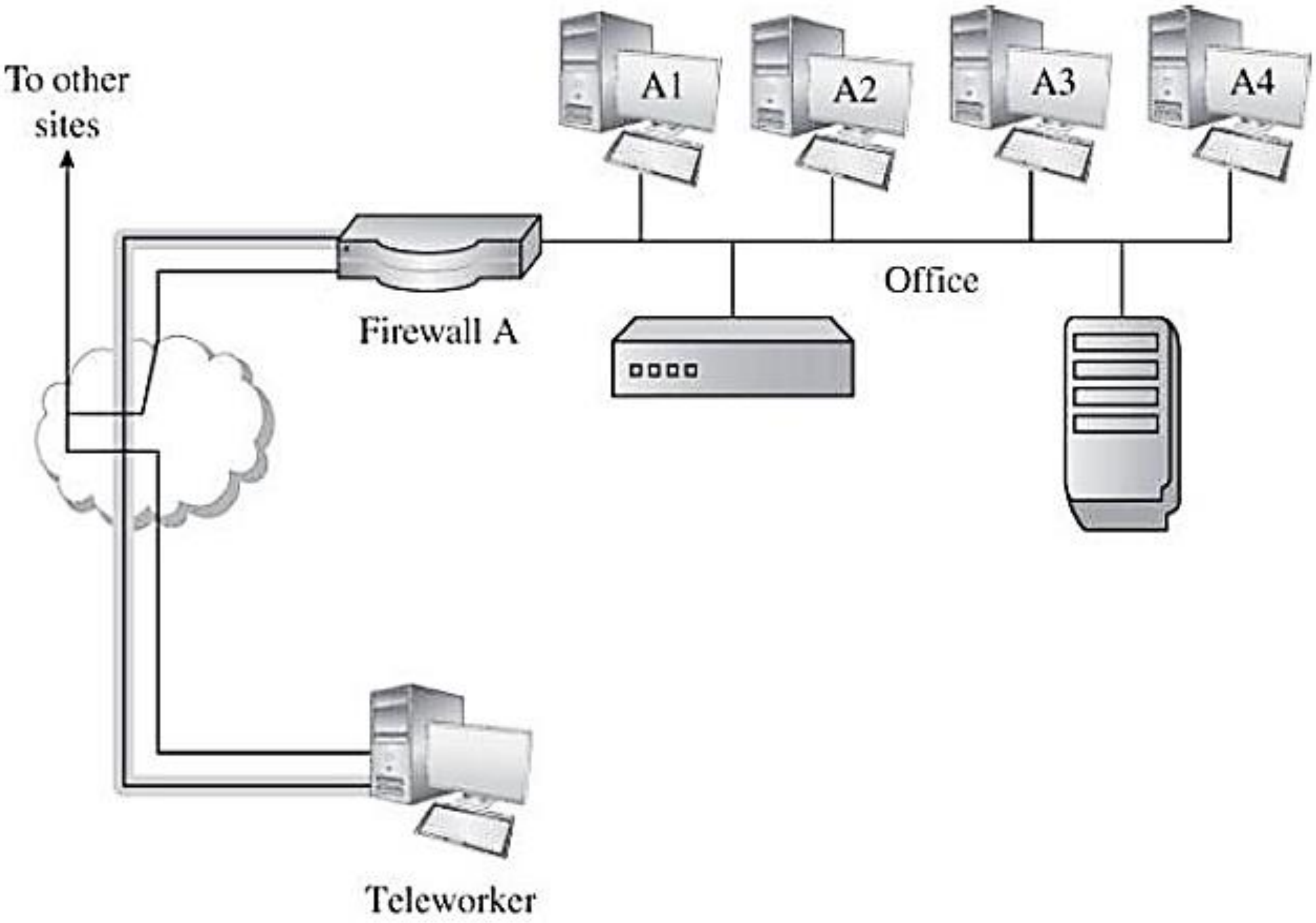
VPN

- **Firewalls** can implement a VPN.
- When a user first establishes a communication with the firewall, the user can request a VPN session with the firewall.
- The firewall may pass user authentication data to the authentication server.
- Upon confirmation of the authenticated identity, the firewall provides the user with appropriate security privileges.
- The user's client and the firewall negotiate a session encryption key.
- The firewall and the client subsequently use that key to encrypt all traffic between the two.

VPN


To other sites
A1
A2
A3
A4
Firewall A
Office A
B1
B2
B3
B4
Firewall B
Office B
▨ Encrypted

VPN : WFH



Firewalls

A firewall is a computer traffic cop that permits or blocks data flow between two parts of a network architecture. It is the only link between parts.

- A firewall is a device that filters all traffic between a protected or “inside” network and a less trustworthy or “outside” network.
- Usually a firewall runs on a dedicated device. Why?
  - Because it is a single point through which traffic is channeled, performance is important, which means that only firewall functions should run on the firewall machine.
- In practice, a firewall is a full-fledged computer.
- A firewall system typically does not have compilers, linkers, loaders, general text editors, debuggers, programming libraries, or other tools. Why?

Firewall

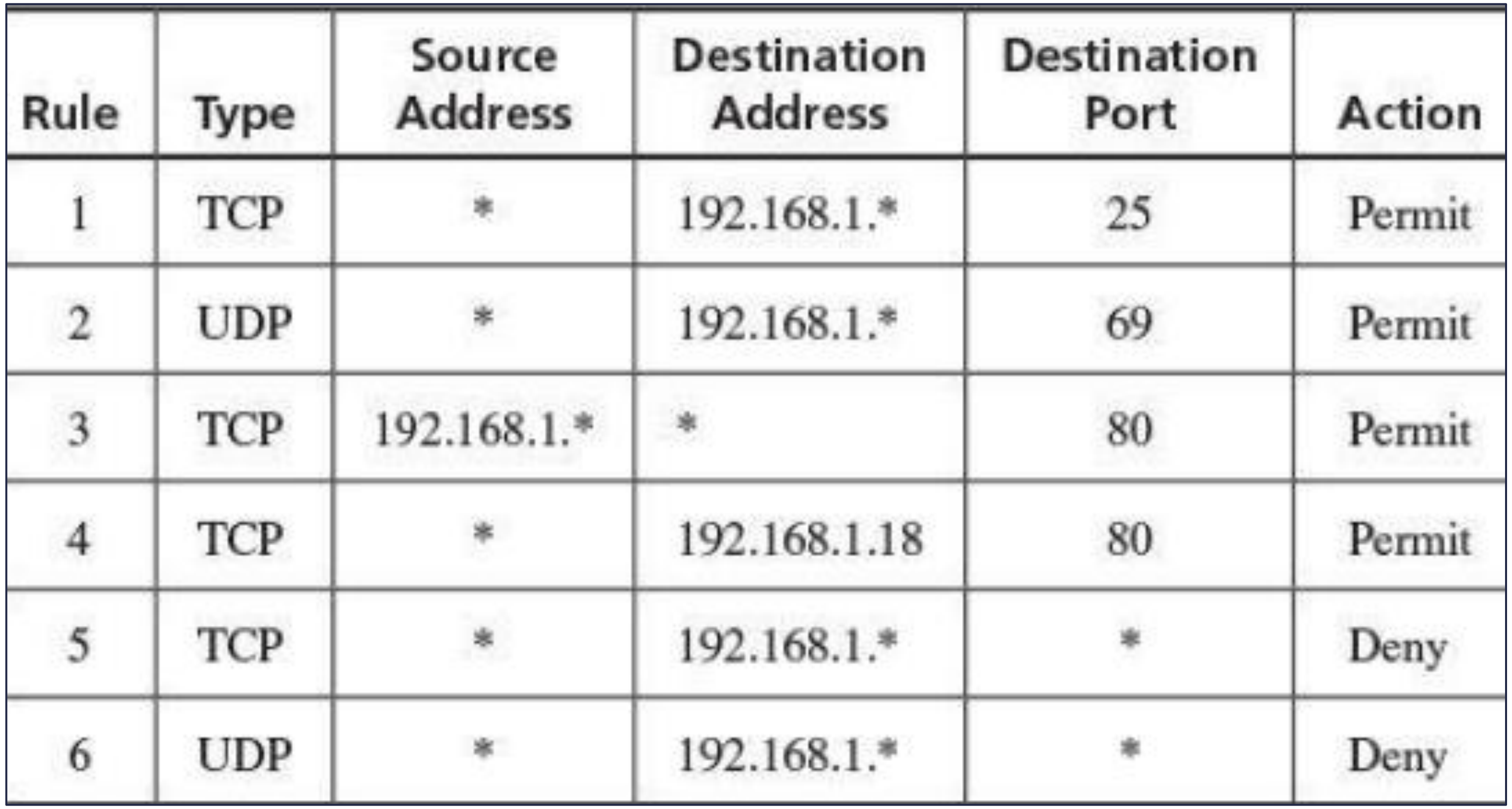
- Policy. Firewalls enforce predetermined rules governing what traffic can flow.
- Default Permit
  - “That which is not expressly forbidden is permitted”
- Default Deny
  - “That which is not expressly permitted is forbidden”
- Users, always interested in new features, prefer the former.
- Security experts strongly counsel the latter.

Firewall Design

- Two qualities lead to the effectiveness: a well-understood traffic flow policy and a trustworthy design and implementation.
- Policy
- Trust

Firewall Design: Policy

- A firewall implements a **security policy**.
- It is a set of rules that determine what traffic can or cannot pass through the firewall.
- Firewalls come with example policies, but each network administrator needs to determine what traffic to allow into a particular network.



Rule	Type	Source Address	Destination Address	Destination Port	Action
1	TCP	*	192.168.1.*	25	Permit
2	UDP	*	192.168.1.*	69	Permit
3	TCP	192.168.1.*	*	80	Permit
4	TCP	*	192.168.1.18	80	Permit
5	TCP	*	192.168.1.*	*	Deny
6	UDP	*	192.168.1.*	*	Deny

Firewall Design: Trust

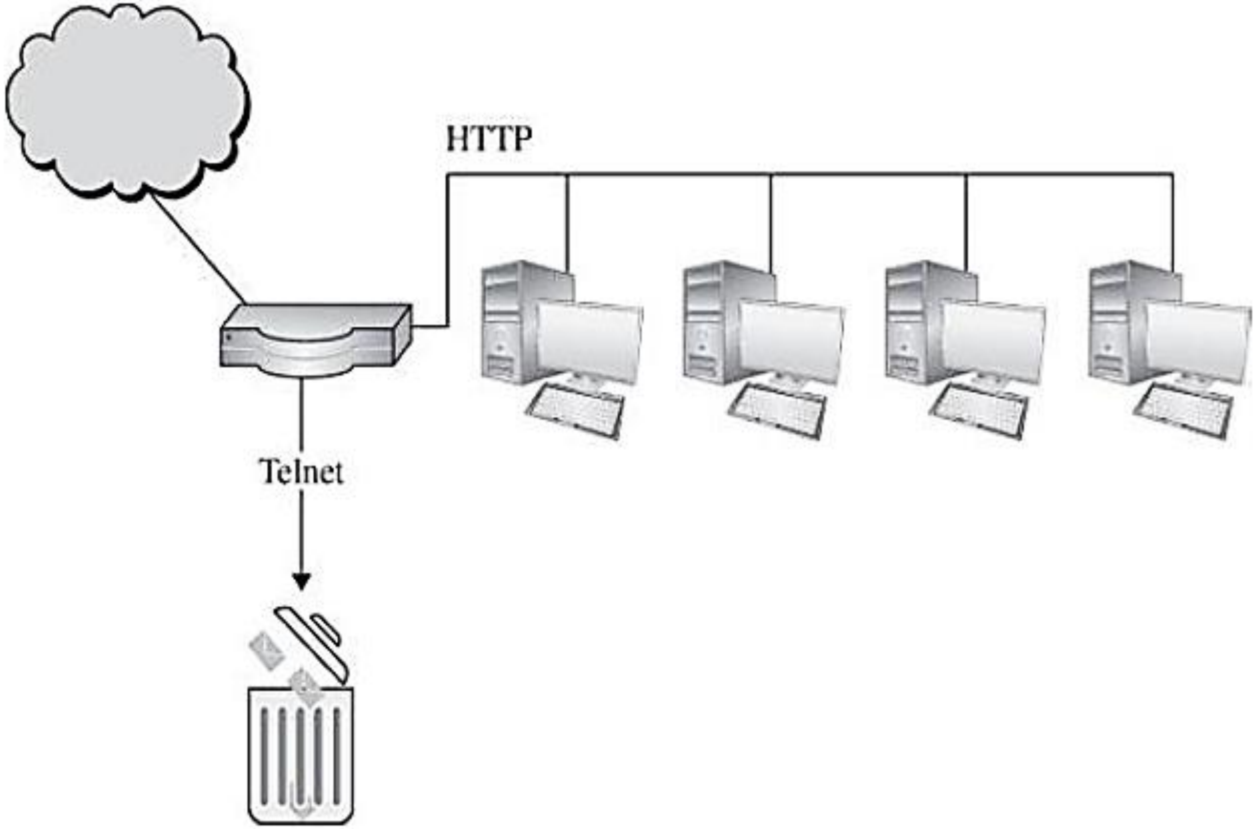
- A firewall is an example of the reference monitor.
- A reference monitor has three characteristics:
    - ❑Always invoked
    - ❑Tamperproof
    - ❑Small and simple enough for rigorous analysis
- A firewall is positioned as the single physical connection between a protected (internal) network and an uncontrolled (external) one.
- A firewall is typically well isolated, making it highly immune to modification.
- Firewall designers strongly recommend keeping the functionality of the firewall simple.

Types of Firewalls

- Packet Filtering Gateways or Screening Routers
- Stateful Inspection Firewalls
- Application-level Gateways, also known as Proxies
- Circuit-level Gateways
- Guards
- Personal Firewalls

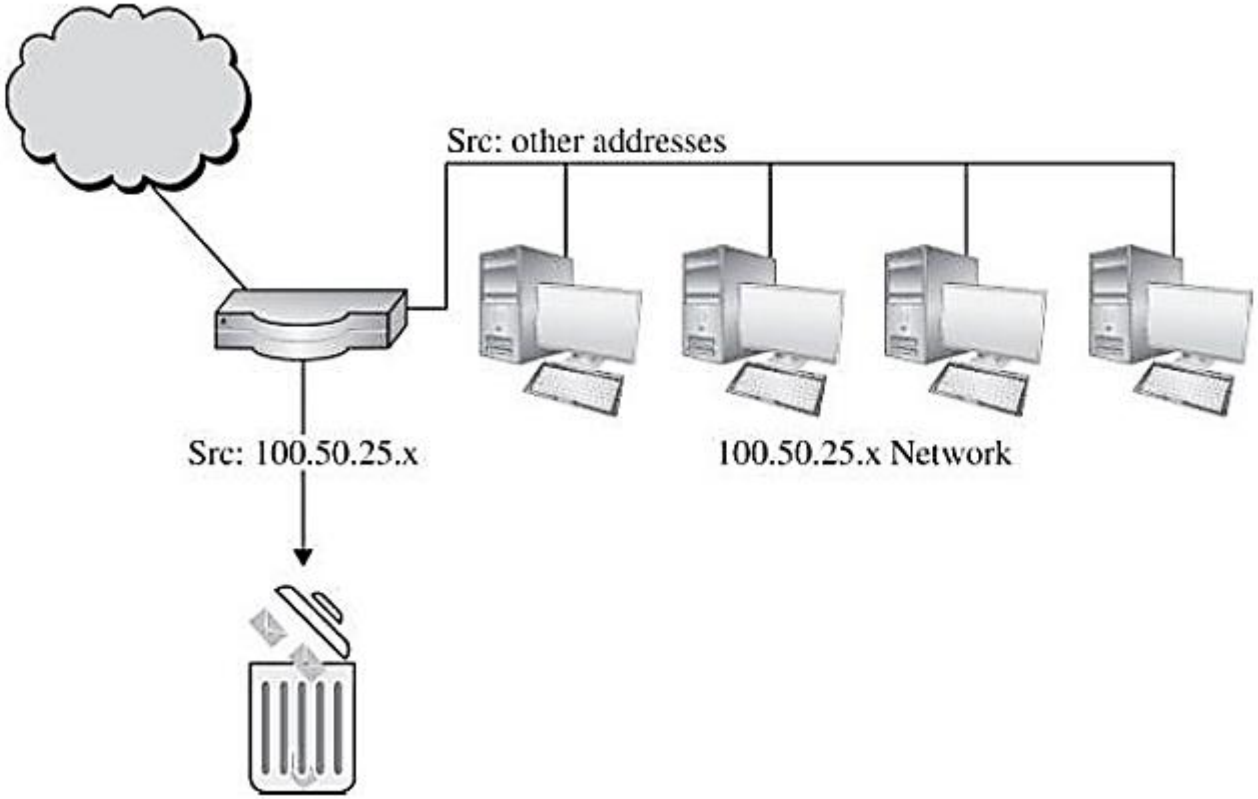
Packet Filtering Gateway

- **Packet filters—screening routers**—limit traffic based on packet header data: addresses and ports on packets (control information).
- A firewall can screen traffic before it gets to the protected network.
- Packet filters operate at OSI level 3.
- Packet filters do not “see inside” a packet; any details in the packet’s data field is beyond the capability of a packet filter.



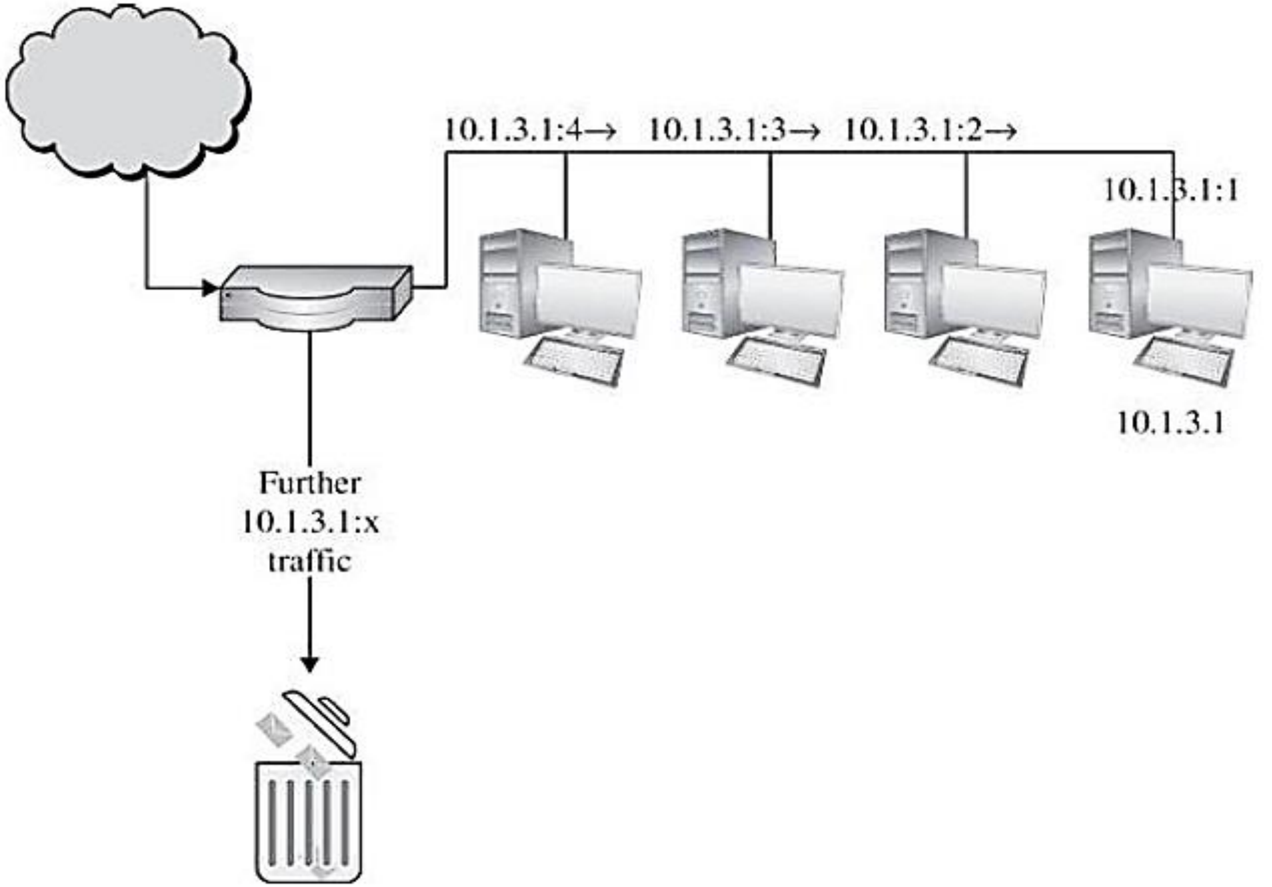
Packet Filtering Gateway

- Packet filters can perform the important service of ensuring the validity of inside addresses.
- A packet filter sits between the inside network and the outside net, so it can determine if a packet from the outside is forging an inside address. How?
- Primary disadvantage: a combination of simplicity and complexity.
- The router’s inspection is simplistic; a detailed rules set will be complex and therefore prone to error.



Stateful Inspection Firewalls

- Stateful inspection firewalls judge according to information from multiple packets.
- Maintains state information from one packet to another in the input stream.
- Port Scanning example. By itself, a probe against port 1 is meaningless, but it could also signal the start of a port scan attack.
- Attackers: break an attack into multiple packets by forcing some packets to have very short lengths.
- A stateful inspection firewall would track the sequence of packets and conditions from one packet to another to thwart such an attack.



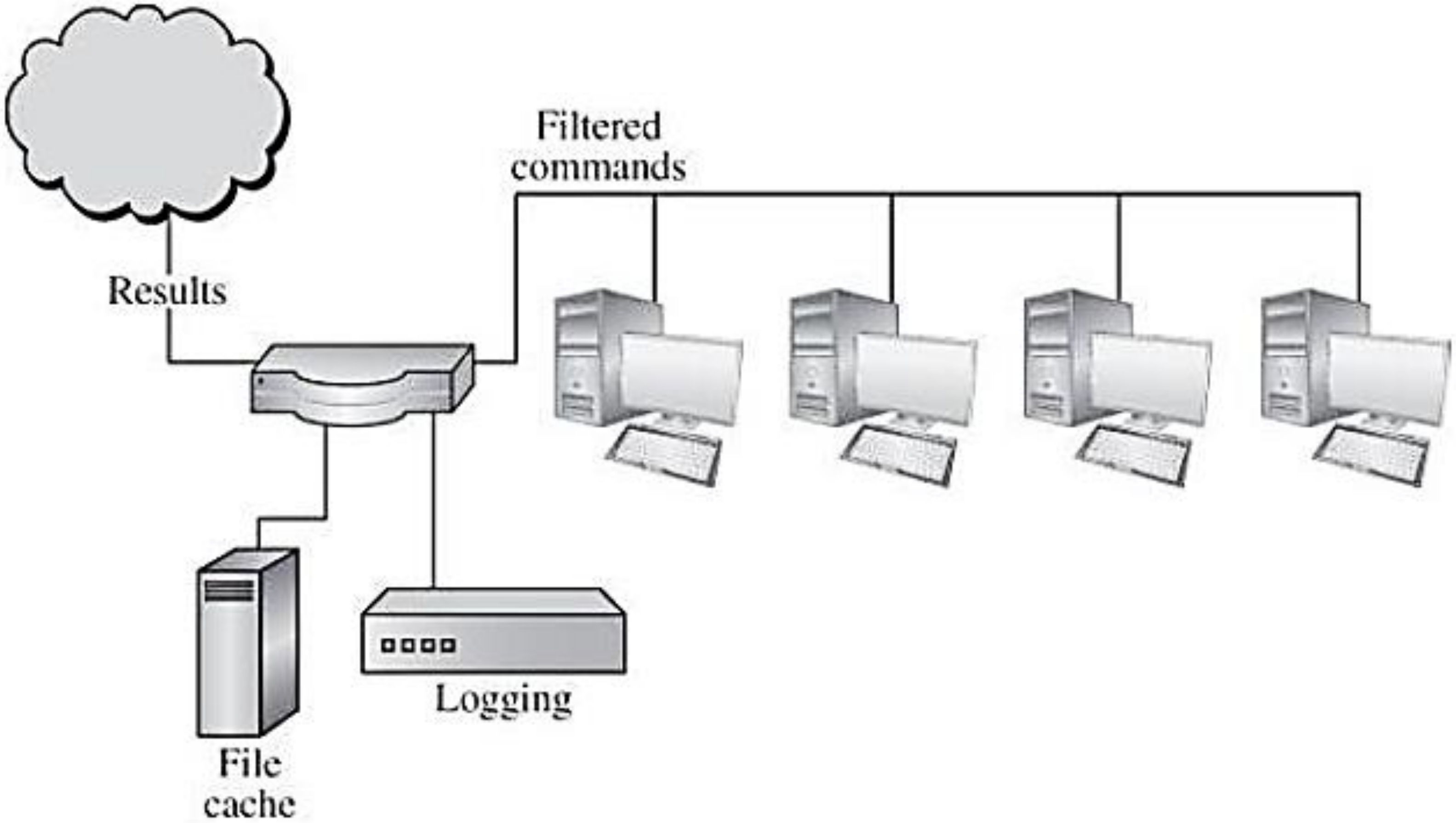
Application Proxy

- Packet filters look only at the headers of packets, not at the data inside the packets. Implications?
- An application proxy (**bastion host**) simulates the behavior of a protected application on the inside network, allowing in only safe data.
- Simulates the (proper) effects of an application at level 7 so that the application receives only requests to act properly.
- A proxy gateway is a two-headed device.
- An application proxy runs pseudo-applications. Example?
- Mail application. The proxy in the middle has the opportunity to screen the mail transfer, ensuring that only acceptable email protocol commands and content are sent in either direction.

Application Proxy Examples

Requirement	Solution
Shopping Website wanting to display only price list.	Monitor the FTP data to ensure that only the price list file was accessed (only read)
Keeping a tab on student page visits for effective caching.	Logging procedure as part of the web browser
Govt. agency responding to DB queries with screening.	Special-purpose proxy performing queries but filtering the output.
A company with multiple offices wants to encrypt the data portion of all email	A firewall application could encrypt and decrypt specific email messages.

Application Proxy Examples



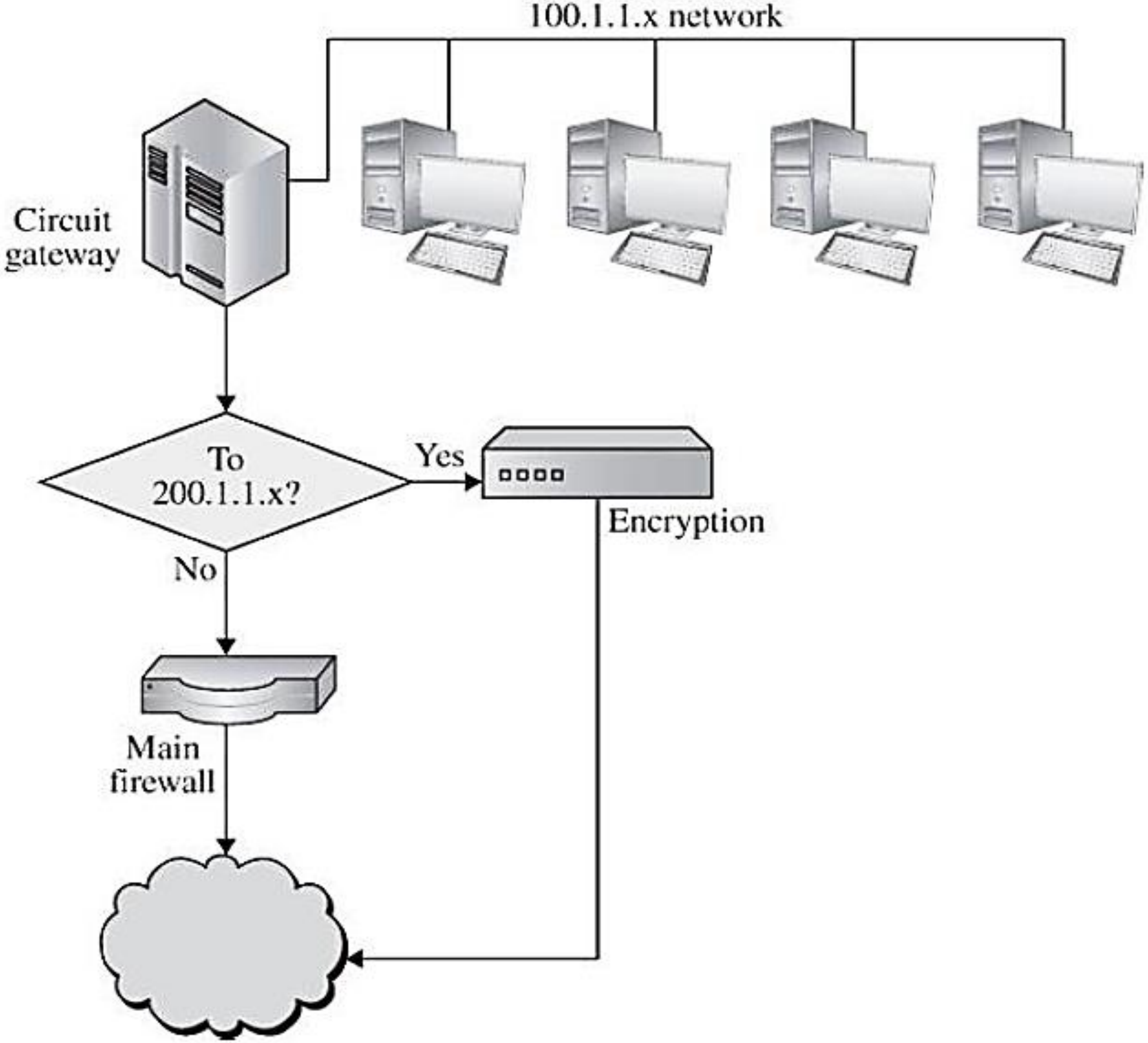
Application Proxy

- Can be tailored to specific requirements, such as logging details about accesses.
- Can present a common user interface to what may be dissimilar internal functions. Example?
    - Suppose the internal network has a mixture of operating system types, none of which support strong authentication.
    - The proxy can demand strong authentication and validate it.
    - Then it pass on only simple name and password authentication details in the form required by a specific internal host's operating system.
- Distinction between a proxy and a screening router?
- The proxy interprets the protocol stream as an application would, to control actions through the firewall on the basis of things visible within the protocol, not just on external header data.

Circuit-Level Gateway

- A **circuit-level** gateway connects two separate subnetworks as if they were one contiguous unit.
- Essentially allows one network to be an extension of another.
- Operates at OSI level 5, the session level.
- Functions as a virtual gateway between two networks.
- The firewall verifies the circuit when it is first created.
- Subsequent data transferred over the circuit are not checked.
- Circuit-level gateways can limit which connections can be made through the gateway.
- One use for a circuit-level gateway is to implement a virtual private network

Circuit-Level Gateway Example



Guards

- Sophisticated firewall.
- Like a proxy firewall, it receives PDUs, interprets them, and emits the same or different PDUs that achieve either the same result or a modified result.
- The degree of control a guard can provide is limited only by what is computable.
- Guards and proxy firewalls are similar enough that the distinction between them is sometimes fuzzy.
- A guard can implement any programmable set of conditions, even if the program conditions become highly sophisticated.

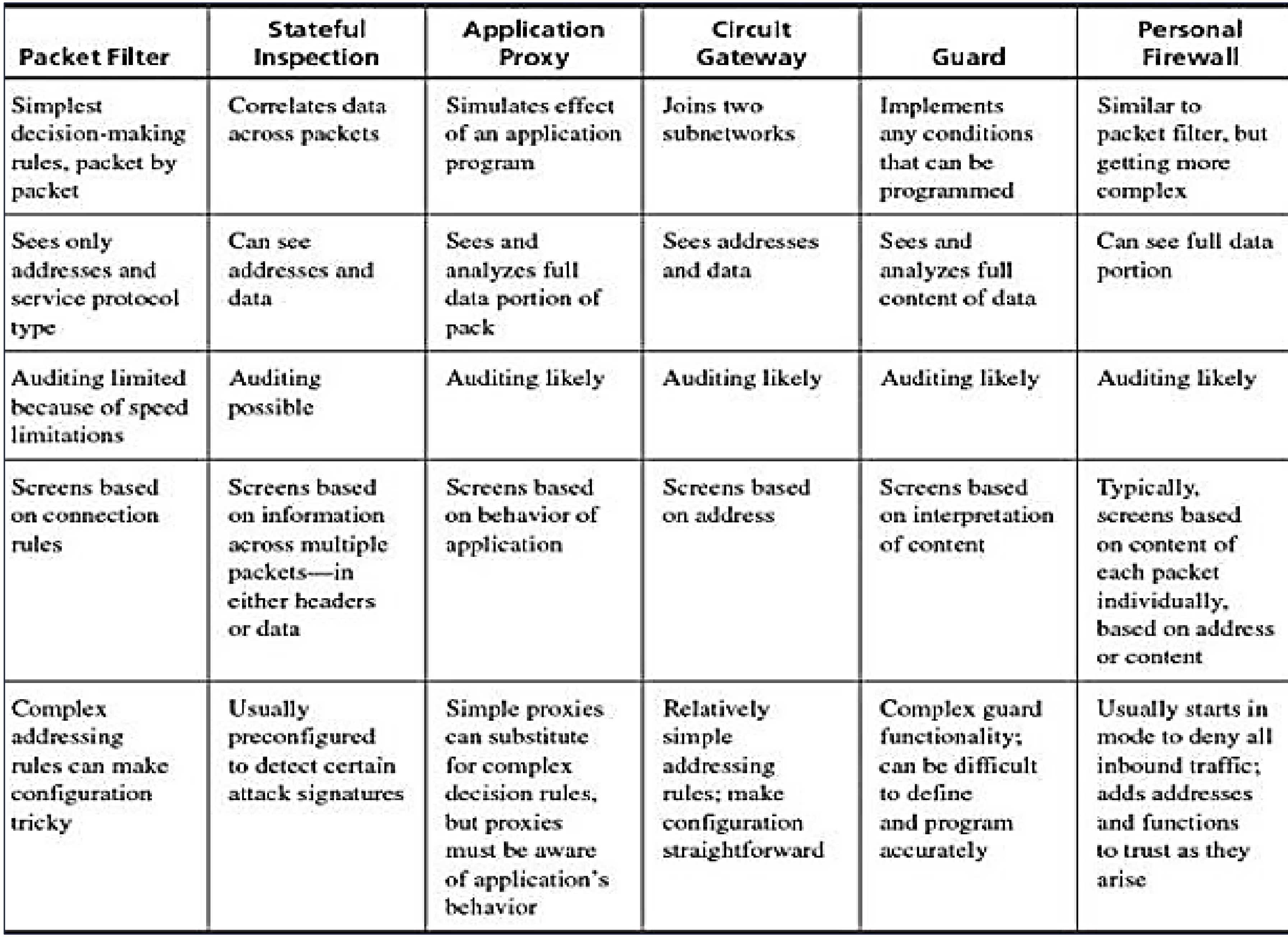
Guards Example

- Restricting users of an organization to a limit in emails sent.
- Managing connection capability to web by allowing text mode and simple graphics but disallowing complex graphics, video, music, or the like.
- Show partials of copyrighted document.
- Replace certain terms with other terms to maintain privacy of a company. This example shows that a firewall or guard can just as easily screen outbound traffic.
- A company scanning all FTP downloaded data through virus scanners.

Personal Firewalls

- A personal firewall is a program that runs on a single host to monitor and control traffic to that host.
- It can only work in conjunction with support from the operating system.
- Commercial implementations of personal firewalls include SaaS Endpoint Protection from McAfee, F-Secure Internet Security, Microsoft Windows Firewall, and Zone Alarm from CheckPoint.
- The personal firewall is configured to enforce some policy.
- With the combination of a virus scanner and a personal firewall, the firewall directs all incoming email to the virus scanner, which examines every attachment the moment it reaches the target host and before it is opened.
- Holes in the firewalls.

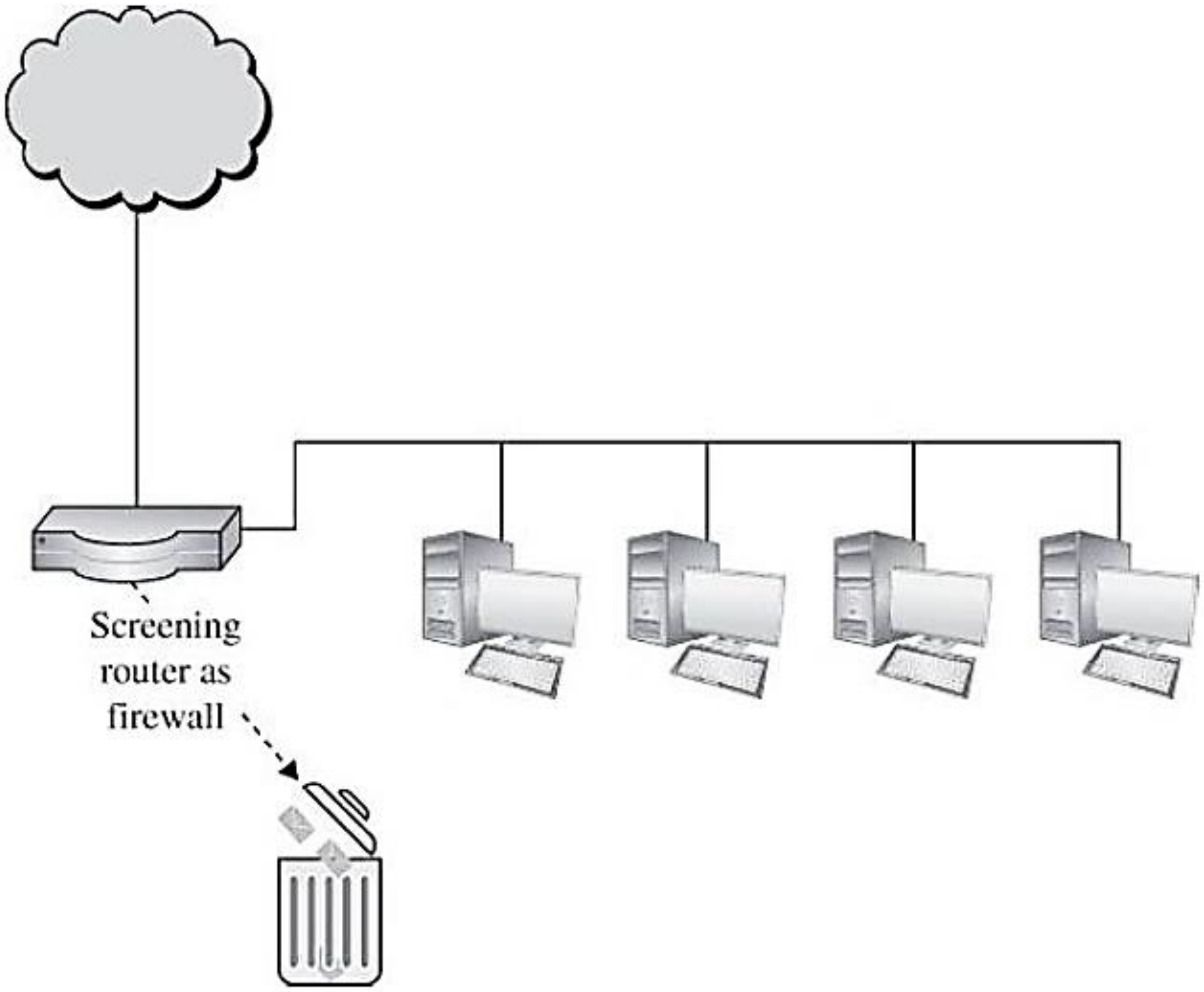
Comparison of Firewall Types



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

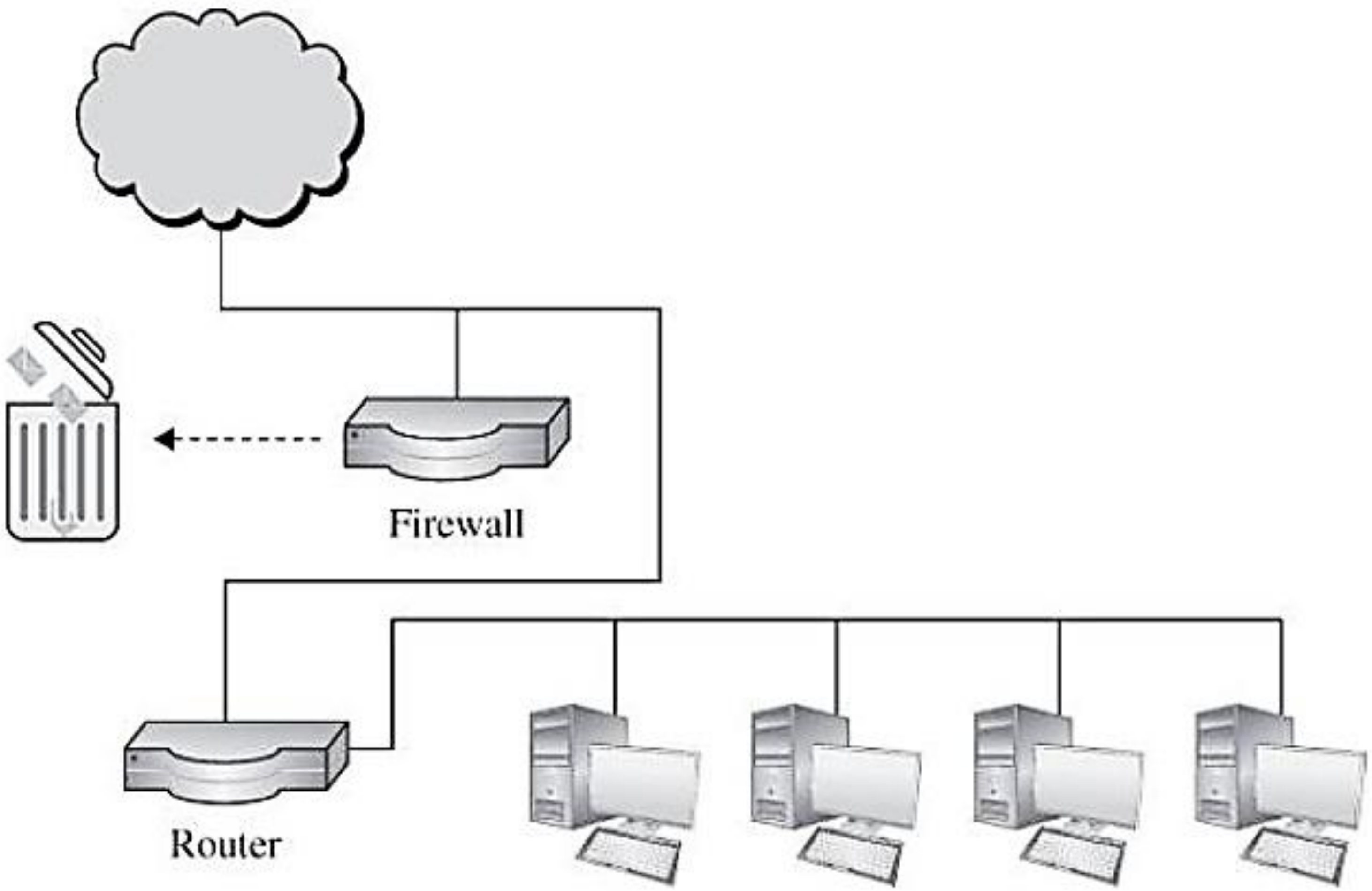
Firewall Example

- Screening Router



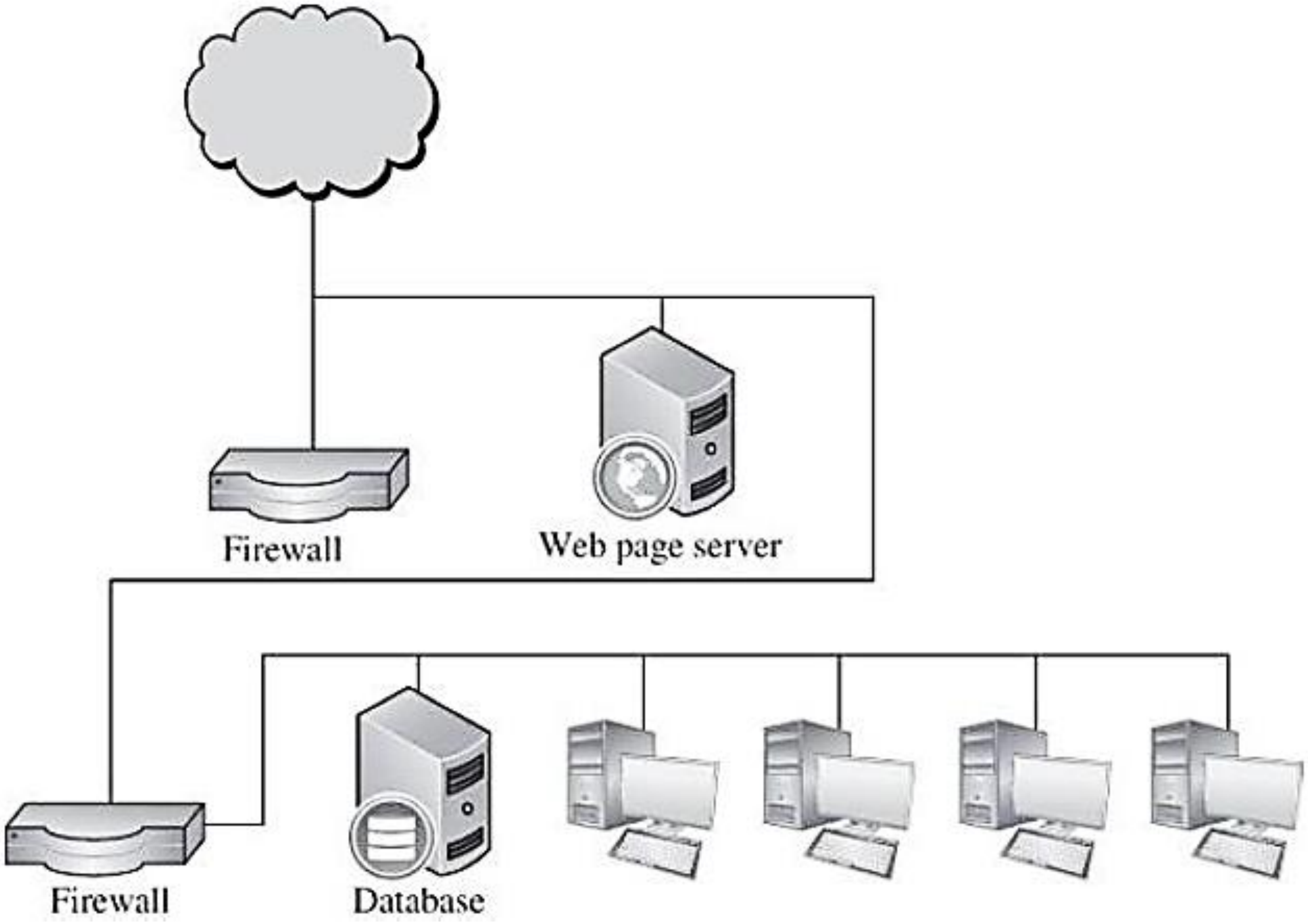
Firewall Example

- Firewall on Separate LAN



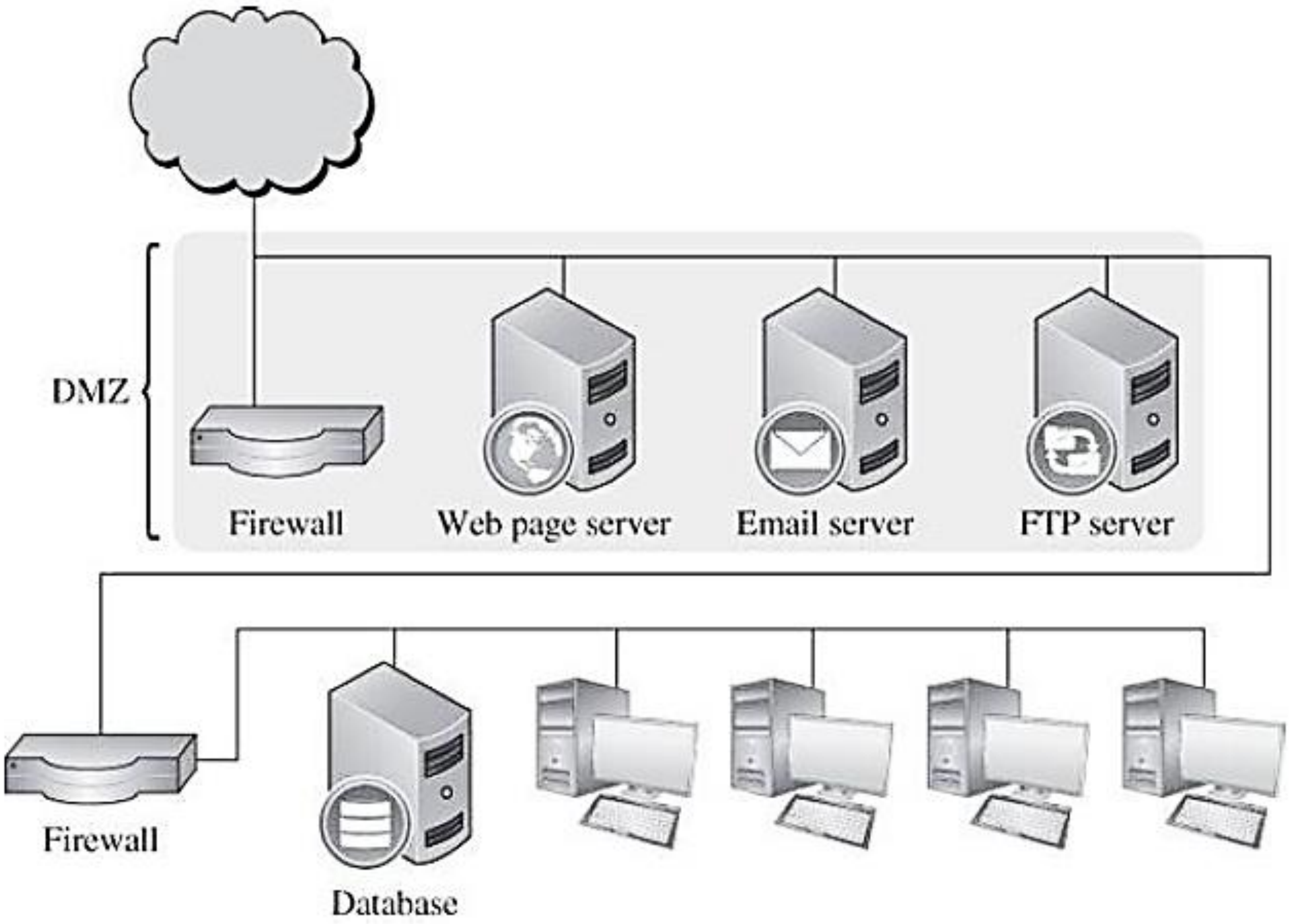
Firewall Example

- Application Proxy



Firewall Example

- Demilitarized Zone



Intrusion Detection and Prevention Systems

- Why do we need Intrusion Detection System (IDS)?
  - Most of the controls (firewalls, authentication and access controls) are preventive: They block known bad things from happening.
  - Most computer security incidents are caused by insiders or people impersonating them.
  - The vast majority of harm from insiders is not malicious. There are the potential malicious outsiders who have somehow passed the screens of firewalls and access controls.
  - Prevention, although necessary, is not a complete computer security control; **detection** during an incident copes with harm that cannot be prevented in advance.
  - IDSs complement these preventive controls as the next line of defense.

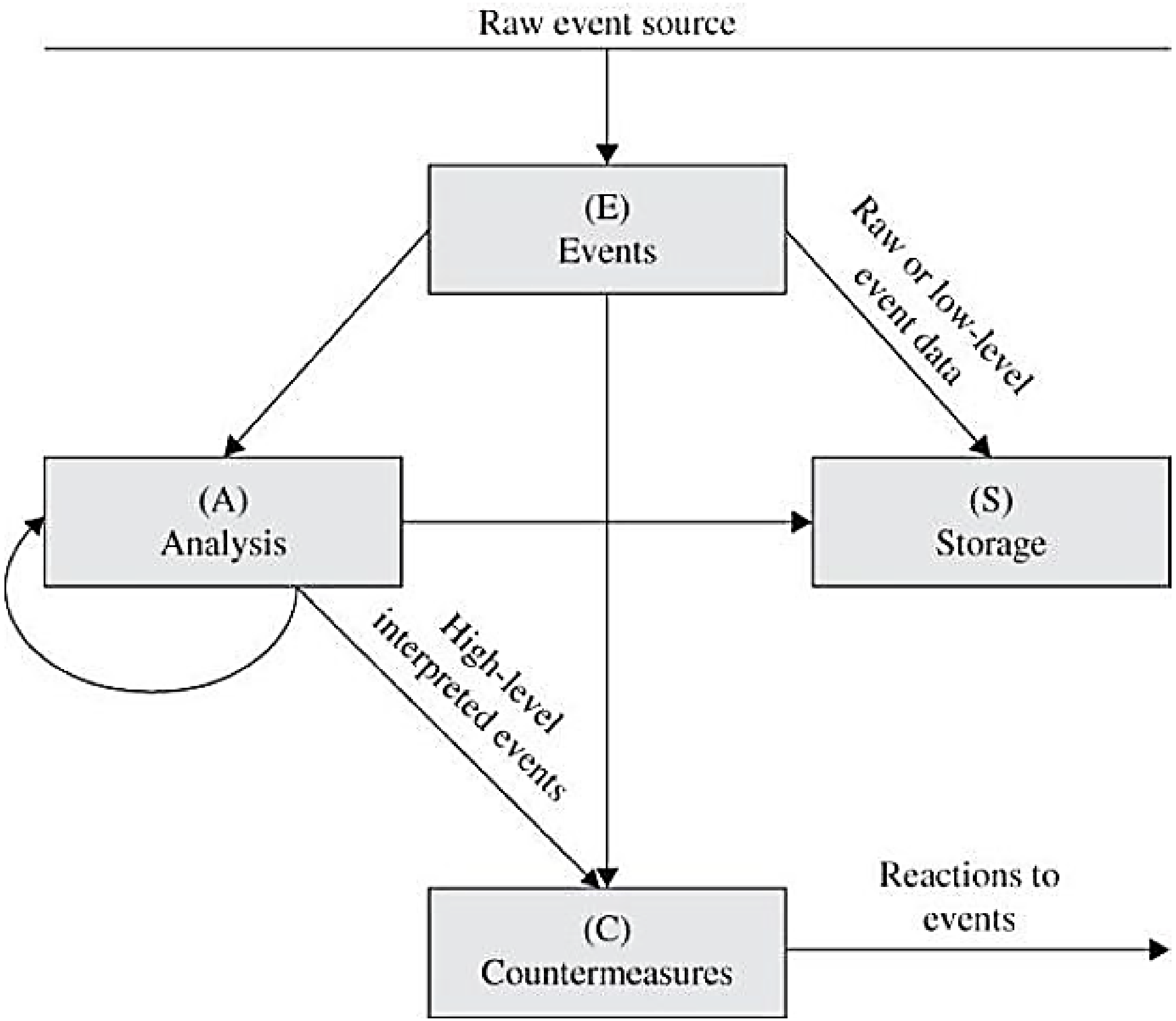
Intrusion Detection and Prevention Systems

- An IDS is a device that monitors activity to identify malicious or suspicious events.
- An IDS is a sensor that raises an alarm if specific things occur.
- IDSs have a response function. Alert a human team that will then decide what further action is warranted.
- If an IDS goes into protection mode to isolate a suspected intruder and constrain access, it is called an Intrusion Protection System (IPS).

Intrusion Detection System: Model

An IDS receives raw inputs from sensors.

It saves those inputs, analyzes them, and takes some controlling action.



IDS: Functions

No one IDS performs all of these functions.

- Monitoring users and system activity.
- Auditing system configuration for vulnerabilities and misconfigurations.
- Assessing the integrity of critical system and data files.
- Recognizing known attack patterns in system activity.
- Identifying abnormal activity through statistical analysis.
- Managing audit trails and highlighting user violation of policy or normal activity.
- Correcting system configuration errors.
- Installing and operating traps to record information about intruders.

Types of IDSs

Signature-based IDSs look for patterns; heuristic ones learn characteristics of unacceptable behavior over time.

- Two general types of intrusion detection systems are:
- **Signature based IDS.**
    - Perform simple pattern-matching and report situations that match a pattern (signature) corresponding to a known attack type.
- **Heuristic IDS. (Anomaly based IDS)**
    - Build a model of acceptable behavior and flag exceptions to that model.
    - The administrator can mark a flagged behavior as acceptable – IDS will now treat it as acceptable rather than unclassified.
    - Heuristic IDS can learn what constitute anomalies or improper behavior.
    - The **inference engine** (AI component) identifies pieces of attacks and rates the degree to which these pieces are associated with malicious behavior.

Signature-Based Intrusion Detection

- Tend to use statistical analysis.
- Uses tools: To obtain sample measurements of key indicators.

  To determine whether the collected measurements fit the predetermined attack signatures.
- Signatures should match every instance of an attack, match subtle variations of the attack, but not match traffic that is not part of an attack.
- Signature-based IDSs are limited to known patterns. Cannot detect a new attack for which no signature has yet been installed in the database.
- Example of patterns: Port Scan, Large ICMP packet size.

Signature-Based Intrusion Detection

What an attacker might do?

- Modify a basic attack in such a way that it will not match the known signature of that attack.
- Convert lowercase to uppercase letters.
- Convert “blank space” to its character code equivalent %20.
- Cause a pattern mismatch: insert spurious packets that the IDS will see, or shuffle the order of reconnaissance probes.
- Each of these variations could be detected by an IDS, but more signatures require additional work for the IDS, thereby reducing performance.

Signature-Based Intrusion Detection

- Where it works easily?
  - Certain types of DoS attacks, like ping and echo-chargen attacks.
- Where it is rather difficult?
  - Teardrop attack.
  - SYN flooding.
- Why?
  - Packet fragmentation is a characteristic of most traffic. Similarly, SYN–ACK is part of the three-way TCP handshake.
  - The IDS would need to maintain data on virtually all traffic to identify Teardrop attack.
  - A SYN flood is recognized only by a profusion of unmatched SYN–ACK responses.

Heuristic Intrusion Detection

- The inference engine of an IDS continuously analyzes the system, raising an alert when the system’s dirtiness exceeds a threshold or when a combination of factors signals likely malicious behavior.
- Example.
- Inference engines work in two ways. State-based and Model-based (**misuse intrusion detection**).
- State-based: See the system going through changes of overall state or configuration. They try to detect when the system has veered into unsafe modes.
- Model-based: Current activity matches the model to a certain degree. Accessing a password file apart from the normal reasons.
- To a heuristic intrusion detection system, all activity is classified in one of three categories: **good/benign, suspicious, or unknown**. Over time, specific kinds of actions can move from one of these categories to another

Types of IDSs

- Intrusion detection devices can be **network based(NIDS)** or **host based (HIDS)**.
- A network-based IDS is a stand-alone device attached to the network to monitor traffic throughout that network.
- The **goal** of a NIDS is to protect the entire network or some set of specific sensitive resources, such as a collection of servers holding critical data.
- A host-based IDS runs on a single workstation or client or host, to protect that one host.
- The **goal** of a host-based system is to protect one machine and its data.

HIDS

- Protects a single host against attack. Collects and analyzes data for that one host.
- OS supplies some of that data to the IDS.
- The device either analyzes data itself or forwards the data to a separate machine for analysis and perhaps correlation with HIDSs on other hosts.
- Being a process on the target computer also exposes the HIDS to the vulnerability of being detected.

NIDS

- Separate network appliance that monitors traffic on an entire network.
- It receives data from firewalls, operating systems of the connected computers, other sensors such as traffic volume monitors and load balancers, and administrator actions on the network.
- The detection software can also monitor the content of packets communicated across the network, to detect unusual actions by one host against another.
- Which IDS is better able to protect itself against detection or compromise? Why?
- Network IDS can operate in so-called stealth mode, observing but never sending data onto the network.
- NIDS can send alarms on a separate network from the one being monitored. That way an attacker will not know the attack has been recognized.

Intrusion Prevention System (IPS)

- Detecting the attack gets easier as the attack unfolds.
- Premise of IDS: being able to detect bad things before they cause too much harm.
- An IPS tries to block or stop harm.
- It is an IDS with a built-in response capability.
- The response is not just raising an alarm; the automatic responses include cutting off a user’s access, rejecting all traffic from address a.b.c.d, or blocking all users’ access to a particular file or program.

Intrusion Response

- Intrusion detection is probabilistic.
- In taking action, especially if a tool causes the action automatically, a network administrator has to weigh the consequences of action against the possibility that there is no attack.
- Responding to alarms.

Responding to Alarms

- What are possible responses?
- Responses fall into **three** major categories:
- Monitor, collect data, perhaps increase amount of data collected.
    - Appropriate for an attack of modest (initial) impact. Watch the intruder's actions. Record all traffic from a given source for future analysis (should be invisible to the attacker).
- Protect, act to reduce exposure.
    - Increase access controls, make a resource unavailable, possibly sever the network connection the attacker is using. Protecting may be very visible to the attacker.
- Signal an alert to other protection components.
- Call a human.

Goals for Intrusion Detection Systems

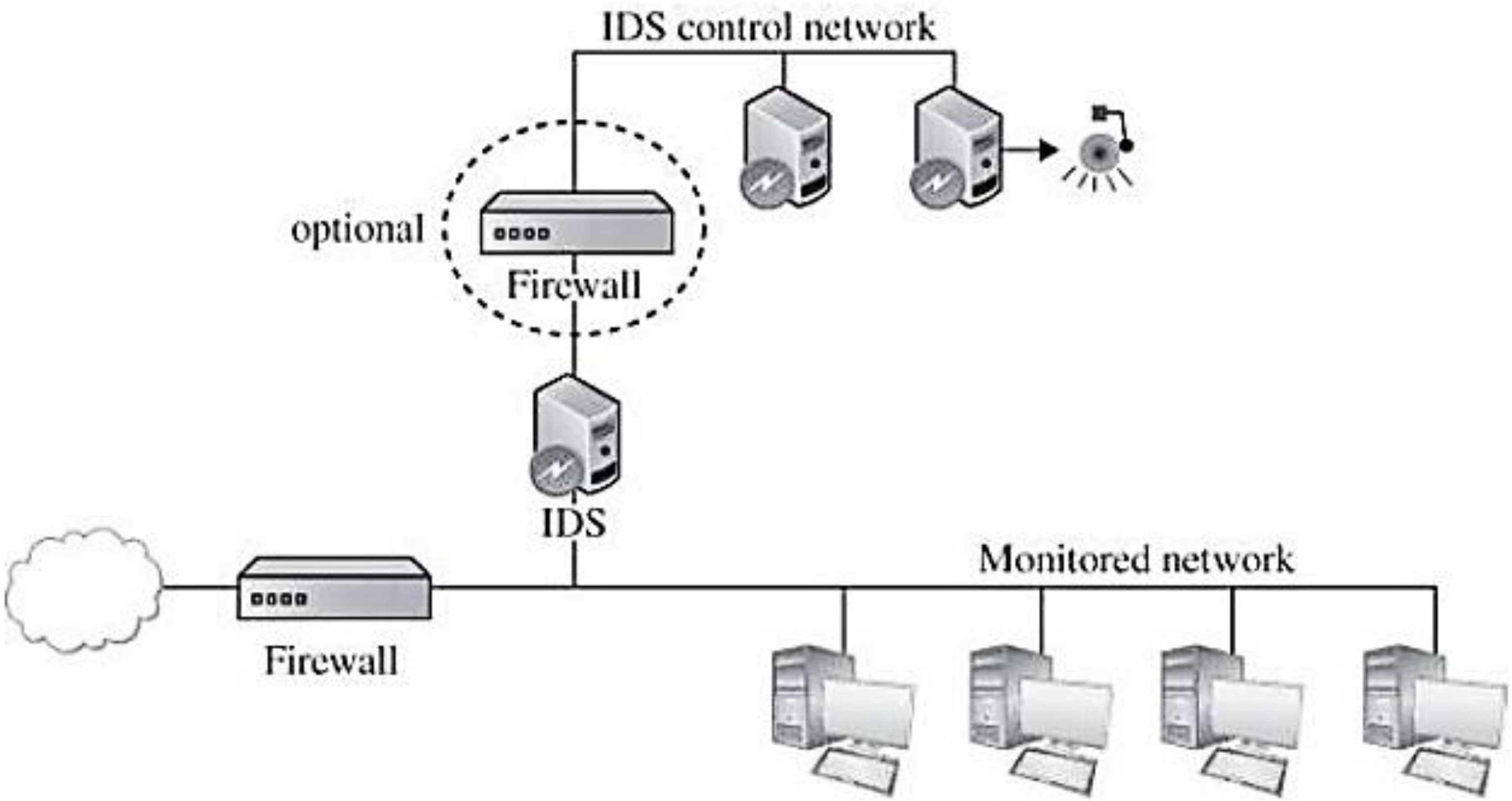
- An IDS should be fast, simple, and accurate, while at the same time being complete.
- It should detect all attacks with negligible performance penalty. <Accurate Situation Assessment>
- An IDS could use some—or all—of the following design approaches:
    - Filter on packet headers. Filter on packet content.
    - Maintain connection state.
    - Use complex, multipacket signatures.
    - Use minimal number of signatures with maximum effect.
    - Filter in real time, online.
    - Hide its presence. <Stealth Mode>
    - Use optimal sliding-time window size to match signatures.

Goals for Intrusion Detection Systems

- Wouldn’t the attacker try to disable the IDS?
- Most IDSs run in **stealth mode** - an IDS has **two** network interfaces:
- For the network it is monitoring.
  - Input only- it never sends packets out through that interface.
  - No published address through the monitored interface; that is, no router can route anything directly to that address.
- To generate alerts and perhaps perform other administrative needs.

Stealth mode IDS prevents the attacker from knowing an alarm has been raised.

Goals for IDS: Stealth Mode



Goals for IDS

Accurate Situation Assessment

- Too many false positives.
  - The administrator will be less confident of the IDS's warnings, perhaps leading to a real alarm's being ignored.
- False negatives.
  - Real attacks are passing the IDS without action.
- Most IDS implementations allow the administrator to tune the system's sensitivity in order to strike an acceptable balance between false positives and negatives.

Network Management

- Management to Ensure Service
- Security Information and Event Management (SIEM)

Network Management

- Management to Ensure Service
  - Capacity Planning
  - Load Balancing
  - Network Tuning
  - Shunning
  - Blacklisting and Sinkholing

A load balancer is an appliance that redirects traffic to different servers while working to ensure that all servers have roughly equivalent workloads.
Network load balancing directs incoming traffic to resources with available capacity.

Network administrators can set edge routers to drop packets engaging in a DoS attack.
Essentially filters out all traffic from implicated addresses.

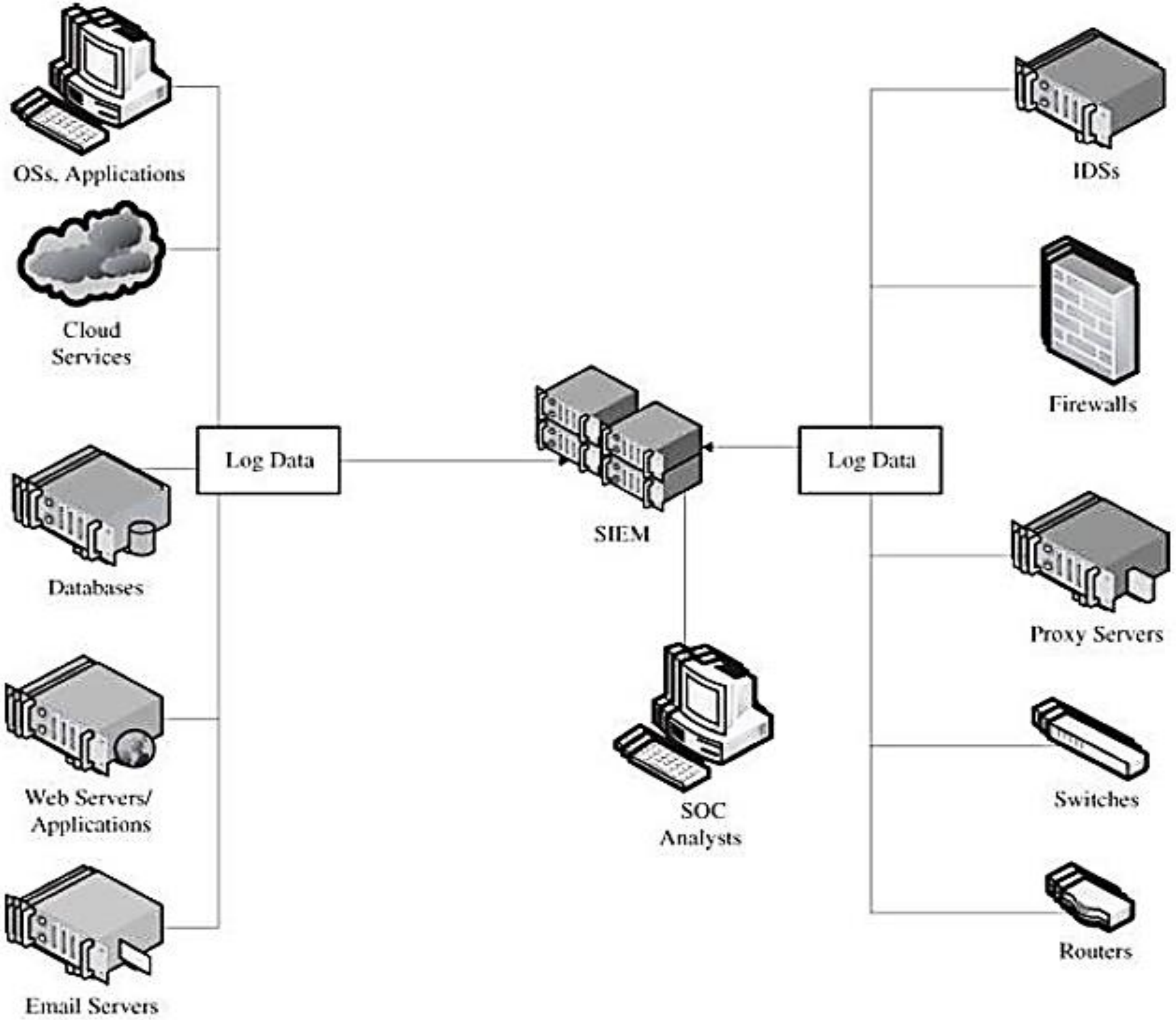
Blacklist the target address: no traffic goes to that address, from legitimate or malicious sources alike.
Sinkholing: redirect traffic to a valid address where the incoming traffic can be analyzed.

- Shunning and sinkholing are extreme network countermeasures blocking all traffic from or to a specific address.

Network Management: SIEM

- Security Operations Center (SOC): A team of security personnel dedicated to monitoring a network for security incidents and investigating and remediating those incidents.
- Need for SIEM?
  - Manually logging in to every device to check status and look for alerts makes it difficult to identify even simple attack patterns.
  - SIEMs are software systems that collect security-relevant data from a variety of hardware and software products in order to create a unified security dashboard for SOC personnel.

SIEM Dashboard



SIEM Challenges

- **Cost**.
- **Data portability**. Knowledge stored in the SIEM, such as saved searches or data visualizations, tends to be SIEM specific and you will likely need to rebuild such knowledge bases when you switch products.
- **Log-source compatibility**. Some SIEMs can read data logs as it is, some may require a bit of configuration, and some would require agents.
- **Deployment complexity**. Deployment will likely require a variety of configuration changes, some of which will be unpredictable side effects of the intricacies of your environment.
- **Customization**. How much of the functionality is either built-in or easy to acquire, and how much will need to be developed (customized).

SIEM Challenges

- **Data storage**. Log files listing IDS alerts are relatively sparse, while full packet capture can result in gigabytes of new data per second.
- **Segregation and access control**. SIEMs generally have robust segregation and role-based access control capabilities that allow administrators to limit users' access to data and functionality, but mitigating insider risks posed by security personnel is a perpetual challenge.
- **Full-time maintenance**. SIEMs are inherently complex, so deploying, maintaining, and customizing them are expert skills in themselves.
- **User training**. SOC analysts are generally trained in incident detection, investigation, and response, but they may not know how to use the particular tools deployed in a organization.

Book

- Pfleeger C. P., Pfleeger S. L. and Margulies J., Security in Computing (5e), Prentice Hall, 2015, Chapter 6.