UNIT V SECURITY PRACTICES

Firewalls and Intrusion Detection Systems: Intrusion Detection Password Management, Firewall Characteristics Types of Firewalls, Firewall Basing, Firewall Location and Configurations. Blockchains, Cloud Security and IoT security

5.1 INTRUSION DETECTION

INTRUDER

An intruder refers to an unauthorized person or entity attempting to gain access to a computer system, network, or data without permission. Generally referred to as hacker or cracker.

Three classes of intruders are as follows:

1. **Masquerader** – an individual who is not authorized to use the computer and whopenetrates a system's access controls to exploit a legitimate user's account.
2. **Misfeasor** – a legitimate user who accesses data, programs, or resources for which such access is not authorized, or who is authorized for such access but misuse his or her privileges.
3. **Clandestine user** – an individual who seizes supervisory control of the system and uses this control to evade auditing and access controls or to suppress audit collection.

The masquerader is likely to be an outsider; the misfeasor generally is an insider; and the clandestine user can be either an outsider or an insider.

Intrusion Techniques

The objective of the intruders is to gain access to a system or to increase the range of privileges accessible on a system.

The password files can be protected in one of the two ways:

One-way encryption – The system stores only an encrypted form of user's password.

Access control – Access to the password file is limited to one or a very few accounts.

The following techniques are used for learning passwords.

1.Try default passwords used with standard accounts that are shipped with the system.

Many administrators do not bother to change these defaults.

2. Exhaustively try all short passwords.

3. Try words in the system's online dictionary or a list of likely passwords.

4. Collect information about users such as their full names, the name of their spouse and children, pictures in their office and books in their office that are related to hobbies.

5. Try user's phone number, social security numbers and room numbers.

6. Try all legitimate license plate numbers.

7. Use a torjan horse to bypass restriction on access.

8. Tap the line between a remote user and the host system.

Two principle countermeasures:

1. Detection – concerned with learning of an attack, either before or after its success.
2. Prevention – challenging security goal

INTRUSION DETECTION

Intrusion detection is based on the assumption that the behaviour of the intruder differs from that of alegitimate user in ways that can be quantified. Although the typical behaviour of an intruder differs from the typical behaviour of an authorized user, there is an overlap in these behaviours.

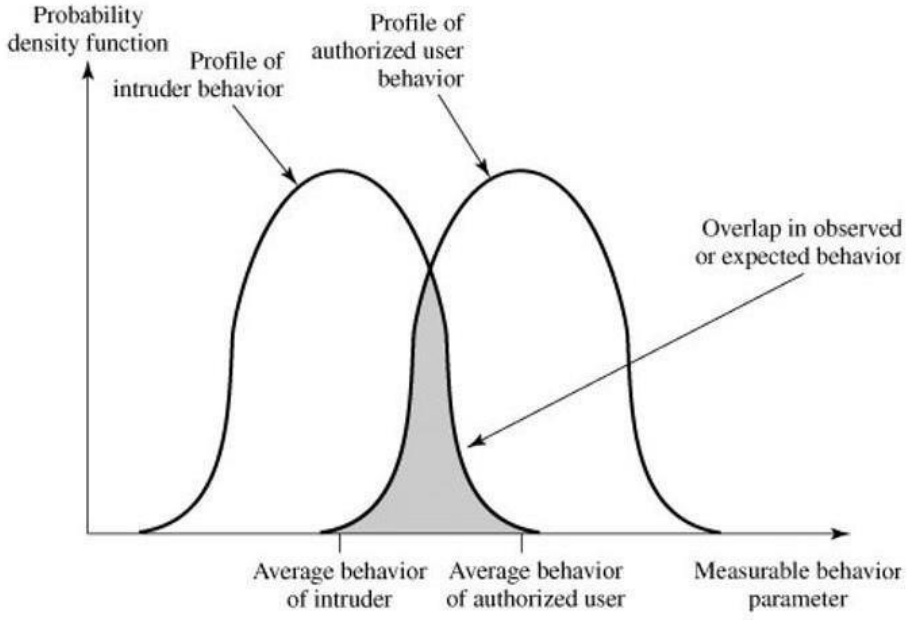


Figure: Profiles of Behavior of Intruders and Authorized Users

Approaches to intrusion detection

1. Statistical anomaly detection

2. Rule-based detection:
3. Distributed Intrusion Detection
4. Honeypot

1. Statistical anomaly detection:

Involves the collection of data relating to the behaviour of legitimate users over a period of time.

Then statistical tests are applied to observed behaviour to determine with a high level of confidence whether that behaviour is not legitimate user behaviour.

a) Threshold detection: This approach involves defining thresholds, independent of user,for the frequency of occurrence of various events.

b) Profile based: A profile of the activity of each user is developed and used to detect changes in the behaviour of individual accounts.

2. Rule-based detection:

Involves an attempt to define a set of rules that can be used to decide that a given behaviour is that of an intruder.

a) **Anomaly detection**: Rules are developed to detect deviation from previous usage patterns.

b) **Penetration identification**: An expert system approach that searches for suspicious behaviour.

A fundamental tool for intrusion detection is the **audit record.** Some record of ongoing activity by users must be maintained as input to an intrusion detection system.

Basically, two plans are used:

1.**Native audit records**: Virtually all multiuser operating systems include accounting software that collects information onuser activity. The advantage of using this information is that no additional collection software is needed.

2.**Detection-specific audit records**: A collection facilitycan be implemented that generates audit records containing only that information required by the intrusion detection system. The disadvantage is the extra overhead involved in having, in effect, two accounting packages running on a machine.

Each audit record contains the following fields:

• Subject: Initiators of actions. A subject is typically a terminal user but might also be a process acting on behalf of users or groups of users.

• Action: Operation performed by the subject on or with an object; for example, login, read, perform I/O, execute.

• Object: Receptors of actions. Examples include files, programs, messages, records, terminals, printers, and user- or program-created structures

• Exception-Condition: Denotes which, if any, exception condition is raised on return.

• Resource-Usage: A list of quantitative elements in which each element gives the amount used of some resource

• Time-Stamp: Unique time-and-date stamp identifying when the action took place.

3. Distributed Intrusion Detection

Traditional focus is on single systems. But typically have networked systems. More effective defense has these working together to detect intrusions

- Dealing with varying audit record formats
- Integrity & confidentiality of networked data
- Centralized or decentralized architecture

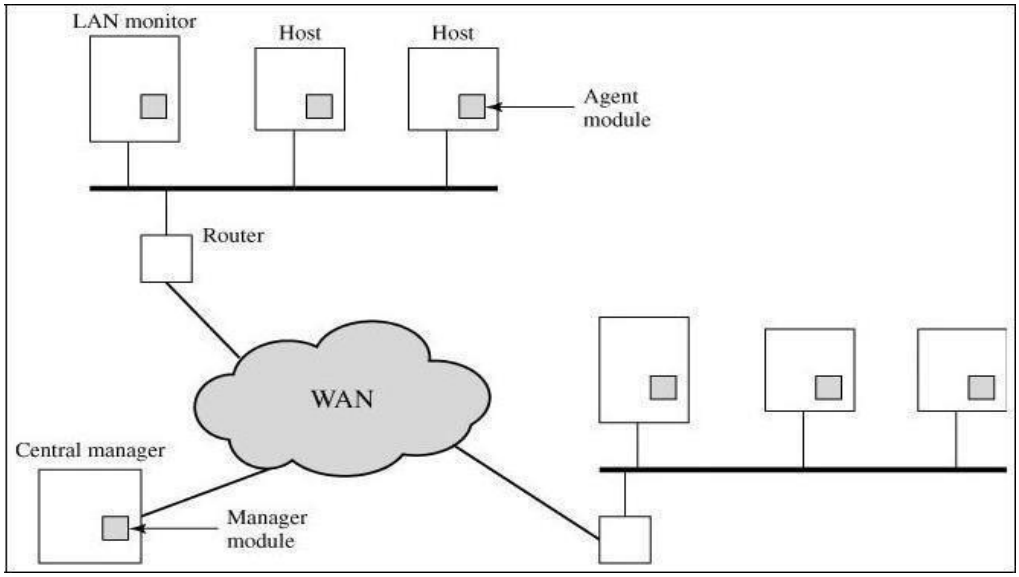


Figure. Architecture for Distributed Intrusion Detection

Three main components

1. **Host agent module**: An audit collection module operating as a background process on a monitored system. Its purpose is to collect data on security-related events on the host and transmit these to the central manager.

2. **LAN monitor agent module**: Operates in the same fashion as a host agent module except that it analyses LAN traffic and reports the results to the central manager.

3. **Central manager module**: Receives reports from LAN monitor and host agents and processes and correlates these reports t2o detect intrusion.

Agent Architecture

The agent captures each audit record produced by the native audit collection system.

1. Filter is applied that retains only those records that are of security interest.
2. These records are then reformatted into a standardized format referred to as the host audit record (HAR).
3. Next, a template-driven logic module analyzes the records for suspicious activity.
4. At the lowest level, the agent scans for notable events that are of interest independent of any past events.
5. At the next higher level, the agent looks for sequences of events, such as known attack patterns (signatures).
6. Finally, the agent looks for anomalous behaviour of an individual user based on a historical profile of that user, such as number of programs executed, number of files accessed, and the like.
7. When suspicious activity is detected, an alert is sent to the central manager.
8. The central manager includes an expert system that can draw inferences from received data.
9. The manager may also query individual systems for copies of HARs to correlate with those from other agents.
10. The LAN monitor agent also supplies information to the central manager.
11. The LAN monitor agent audits host-host connections, services used, and volume of traffic.
12. It searches for significant events, such as sudden changes in network load, the use of security-related services, and network activities such as rlogin.

4. Honeypots

Honeypots are decoy systems that are designed to lure a potential attacker away from critical systems. Honeypots are designed to

- Divert an attacker from accessing critical systems
- Collect information about the attacker's activity
- Encourage the attacker to stay on the system long enough for administrators to respond

5.2 PASSWORD MANAGEMENT

- The front line of defense against intruders is the password system, where a user provides a name/login identifier (ID) and a password.
- The password serves to authenticate the ID of the individual logging on to the system.
- Passwords are usually stored encrypted rather than in the clear

The Vulnerability of Passwords: let us consider a scheme that is widely used on UNIX:

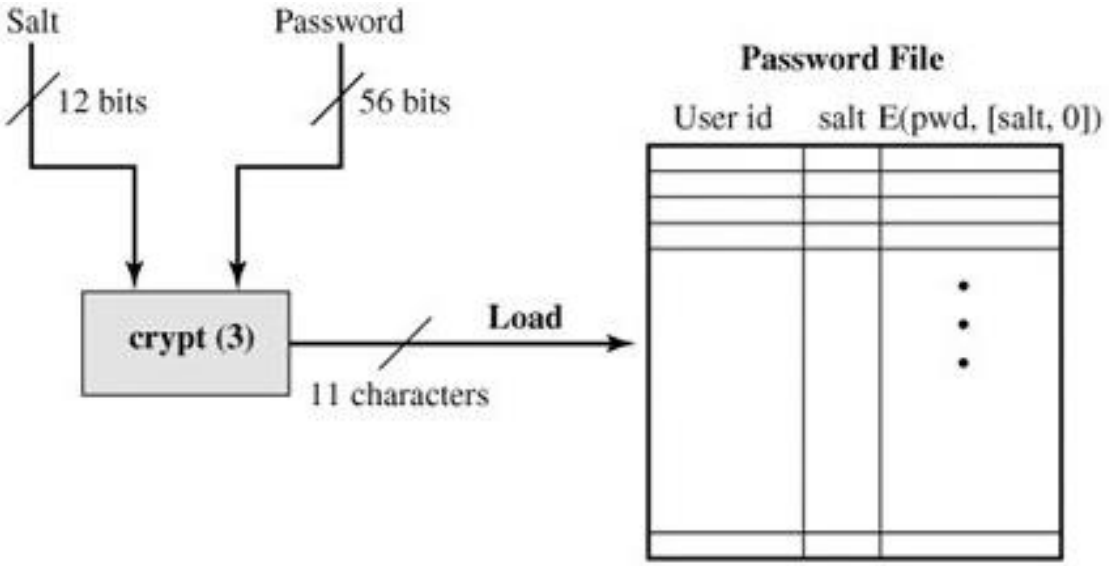
- Each user selects a password up to eight characters.
- This is converted into a 56-bit value (key input to an encryption routine).
- The encryption routine is based on DES. The DES algorithm is modified using a 12-bit.
- This value is related to the time at which the password is assigned to the user.
- The modified DES algorithm is exercised with a data input consisting of a 64-bit block of zeros.
- The output of the algorithm then serves as input for a second encryption.
- This process is repeated for a total of 25 encryptions.
- The resulting 64-bit output is then translated into an 11-character sequence.
- The hashed password is then stored, together with a plaintext copy of the salt, in the password file

The salt serves three purposes:

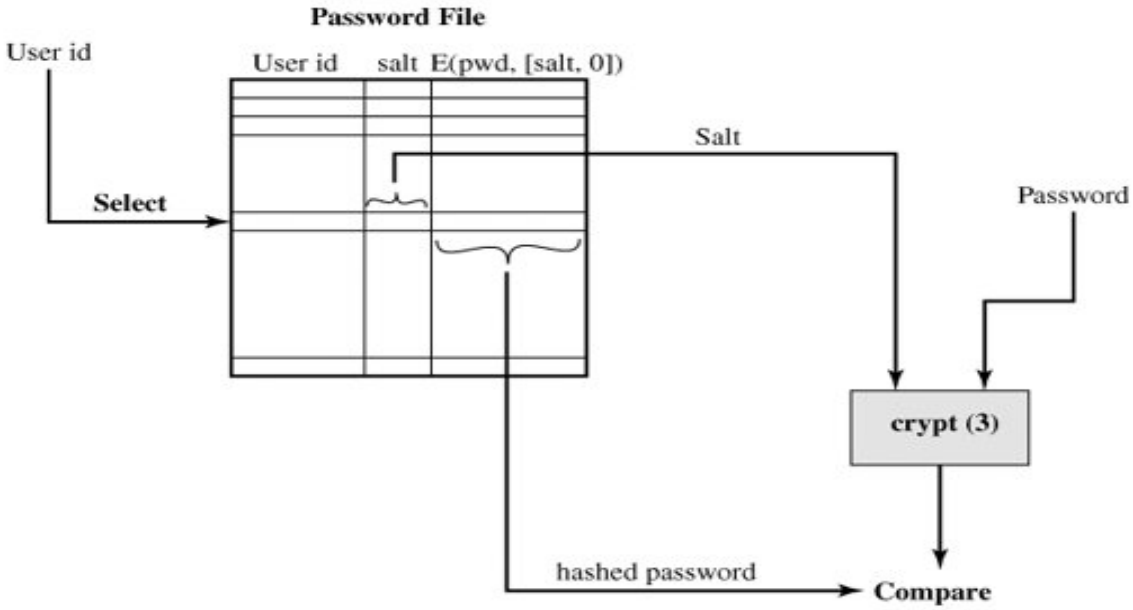
- It prevents duplicate passwords from being visible in the password file.

- It effectively increases the length of the password without requiring the user to remember additional characters.

Access Control: One way to thwart a password attack is to deny the opponent access to the password file. If the encrypted password portion of the file is accessible only by a privileged user, then the opponent cannot read it without already knowing the password of a privileged user.



(a) Loading a new password



(b) Verifying a password

Password Selection Strategies: The goal is to eliminate guessable passwords while allowing the user to select a password that is memorable. Four basic techniques are in use:

- User education.
- Computer-generated passwords.
- Reactive password checking.
- Proactive password checking.

User education

- Users can be told the importance of using hard-to-guess passwords and can be provided with guidelines for selecting strong passwords.

Computer-generated passwords

- passwords are quite random in nature

Reactive password checking

- the system periodically runs its own password cracker to find guessable passwords. The system cancels any passwords that are guessed

Proactive password checking

- user is allowed to select his or her own password. However, at the time of selection, the system checks to see if the password is allowable and, if not, rejects it.

The first approach is a simple system for rule enforcement, enforcing say guidelines from user education. May not be good enough. Another approach is to compile a large dictionary of possible "bad"passwords, and check user passwords against this disapproved list. But this can be very large & slow to search. A third approach is based on rejecting words using either a Markov model of guessable passwords, or a Bloom filter. Both attempt to identify good or bad passwords without keeping large dictionaries.

5.3 FIREWALLS

Firewall Characteristics

- Firewalls can be an effective means of protecting a local system or network of systems from network-based security threats while at the same time affording access to the outside world via wide area networks and the Internet.
- A firewall is inserted between the premises network and the Internet to establish a controlled link and to create an outer security wall or perimeter, forming a single choke point where security and audit can be imposed.

A firewall:

1.Defines a single choke point that keeps unauthorized users out of the protected network,

2. provides a location for monitoring security-related events

3. is a convenient platform for several Internet functions that are not security related, such as NAT and Internet usage audits or logs

4. A firewall can serve as the platform for IPSec to implement virtual private networks.

5. The firewall itself must be immune to penetration, since it will be a target of attack.

Firewall Limitations

- cannot protect from attacks bypassing it
    - eg sneaker net, trusted organisations, trusted services (eg SSL/SSH)
- cannot protect against internal threats
    - eg disgruntled employees
- cannot protect against transfer of all virus infected programs or files
    - because of huge range of O/S & file types

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

Behavior control

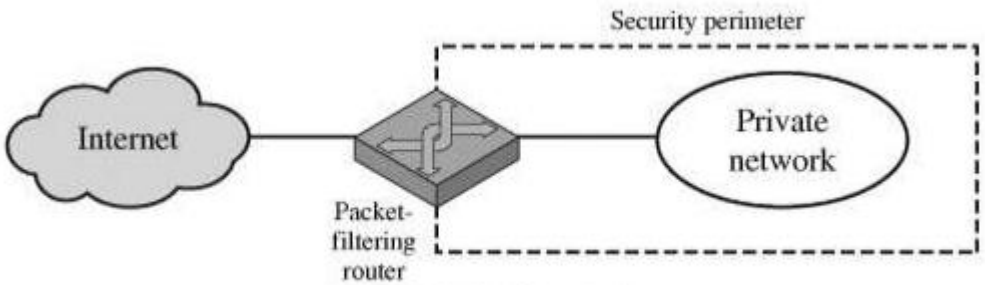
- Controls how particular services are used

5.4 TYPES OF FIREWALLS

- Packet Filters
- Application-Level Gateways
- Circuit-Level Gateways

1. Packet filtering Router

- A packet filtering router applies a set of rules to each incoming IP packet and then forwards or discards the packet.
- The router is typically configured to filter packets going in both directions.
- Filtering rules are based on the information contained in a network packet:
    - Source IP address
    - Destination IP address
    - Source and destination transport level address Interface
    - Interface



(a) Packet-filtering router

- The packet filter is typically set up as a list of rules based on matches to fields in the IP or TCP header.
- If there is a match to one of the rules, that rule is invoked to determine whether to forward or discard the packet. If there is no match to any rule, then a default action is taken.

- Two default policies are possible:
    - Default = discard: That which is not expressly permitted is prohibited.
    - Default = forward: That which is not expressly prohibited is permitted.

Some of the attacks that can be made on packet-filtering routers

• IP address spoofing: where intruder transmits packets from the outside with internal host source IP address

• Source routing attacks: where source specifies the route that a packet should take to bypass security measures

• Tiny fragment attacks: intruder uses the IP fragmentation option to create extremely small fragments and force the TCP header information into a separate fragment to avoid filtering rules needing full header info

Example

Rule	Direction	Src address	Dest addresss	Protocol	Dest port	Action
A	In	External	Internal	TCP	25	Permit
B	Out	Internal	External	TCP	>1023	Permit
C	Out	Internal	External	TCP	25	Permit
D	In	External	Internal	TCP	>1023	Permit
E	Either	Any	Any	Any	Any	Deny

Advantages of packet filter router

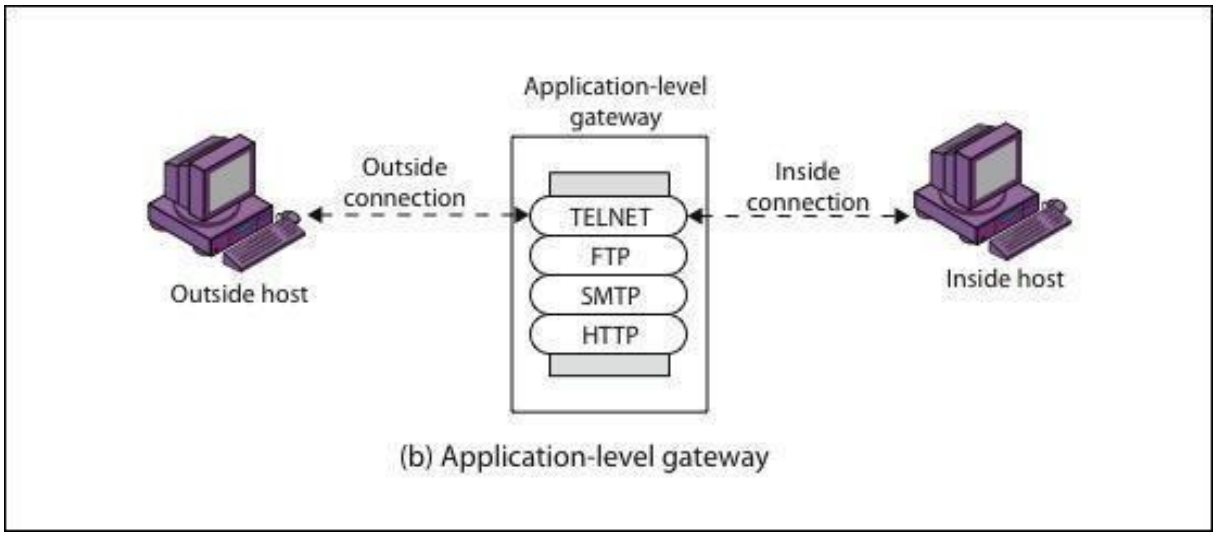
- Simple
- Transparent to users
- Very fast

Weakness of packet filter firewalls

- Because packet filter firewalls do not examine upper-layer data, they can not prevent attacks that employ application specific vulnerabilities or functions.
- The logging functionality present in packet filter firewall is limited.
- It does not support advanced user authentication schemes.
- They are generally vulnerable to attacks such as layer address spoofing.

2. Application level gateway

- An Application level gateway, also called a proxy server, acts as a relay of application level traffic.
- The user contacts the gateway using a TCP/IP application, such as Telnet or FTP, and the gateway asks the user for the name of the remote host to be accessed.
- When the user responds and provides a valid user ID and authentication information, the gateway contacts the application on the remote host and relays TCP segments containing the application data between the two endpoints.
- Application level gateways tend to be more secure than packet filters. It is easy to log and audit all incoming traffic at the application level.
- A prime disadvantage is the additional processing overhead on each connection.

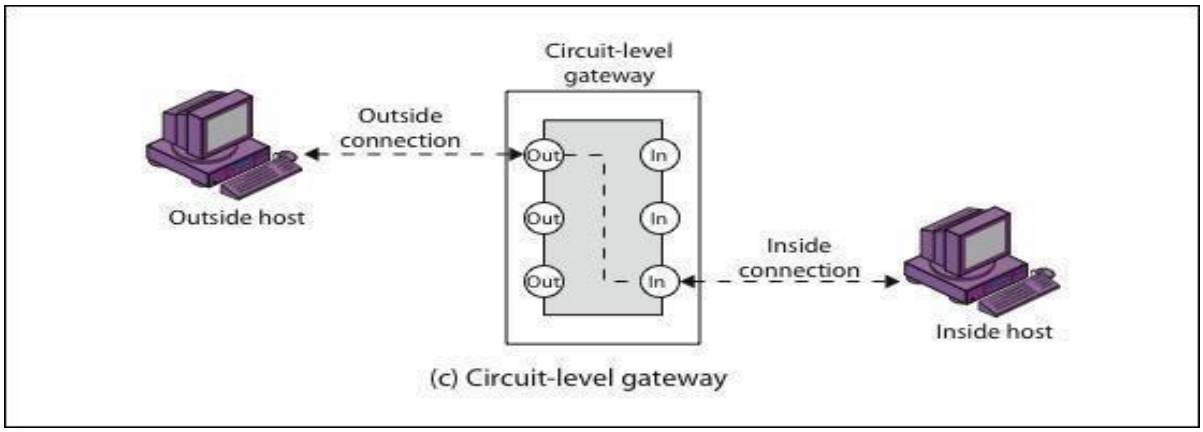


(b) Application-level gateway

3. Circuit-Level Gateway

- Circuit level gateway can be a stand-alone system or it can be a specified function performed by an application level gateway for certain applications.
- A Circuit level gateway does not permit an end-to- end TCP connection; rather, the gateway sets up two TCP connections,
    - between itself and a TCP user on an inner host
    - between itself and a TCP user on an outer host.

- Once the two connections are established, the gateway typically relays TCP segments from one connection to the other without examining the contents.
- The security function consists of determining which connections will be allowed.
- A typical use of circuit-level gateways is a situation in which the system administrator trusts the internal users.
- The gateway can be configured to support application-level or proxy service on inbound connections and circuit-level functions for outbound connections.
- Example of implementation is the SOCKS package



(c) Circuit-level gateway

5.5 FIREWALL BASING

It is common to base a firewall on a standalone machine running a common operating system, such as UNIX or Linux.

Firewall functionality can also be implemented as a software module in a router or LAN switch.

Several options for locating firewall:

- Bastion host
- Individual host-based firewall
- Personal firewall

Bastion Host

- A bastion host is a system identified by thefirewall administrator as a critical strong point in the network's security, serving as a platform for an application-level or circuit-level gateway, or for external services

Common characteristics of a bastion host are as follows

- Executes a secure version of its operating system, making it a trusted system.
- Only essential services are installed on the bastion host. E.g: DNS, FTP
- May require additional authentication before a user is allowed access to the proxy services
- Each proxy is configured to support only a subset of the application's command set.
- Each proxy is configured to allow access only to specific host systems.
- Each proxy maintains detailed audit information by logging all traffic, each connection, and the duration of each connection.
- Each proxy is independent of other proxies on the bastion host

Host-Based Firewalls

A host-based firewall is a software module used to secure an individual host. Such modules are available in many operating systems or can be provided as an add-on package.

- Like conventional standalone firewalls, host-resident firewalls filter and restrict the flow of packets.
- A common location for such firewalls is a server

Advantages:

- Custom-made filter rules for specific host needs
- Protection from both internal/external attacks, Independent of topology
- Additional layer of protection to organization firewall when used with a standalone firewall

Personal Firewall

A personal firewall controls the traffic between a personal computer or workstation on one side, and the Internet or enterprise network on the other side.

Features

- Controls the traffic between a personal computer or workstation on one side and the Internet or enterprise network on the other side
- Can be used in the home environment and on corporate intranets
- Typically, is a software module on the personal computer

- Can also be housed in a router that connects all of the home computers to a DSL, cable modem, or other Internet interface
- Primary role is to deny unauthorized remote access to the computer
- Can also monitor outgoing activity in an attempt to detect and block worms and other malware

5.6 FIREWALL LOCATION AND CONFIGURATIONS

DMZ networks

- An external firewall is placed at the edge of a local or enterprise network,
- One or more internal firewalls protect the bulk of the enterprise network.
- Between these two types of firewalls are one or more networked devices in a region referred to as a **DMZ (demilitarized zone) network**.
- Systems that are externally accessible but need some protections are usually located on DMZ networks.
- Typically, the systems in the DMZ require or foster external connectivity, such as a corporate Web site, an e-mail server, or a DNS (domain name system) server.
- The external firewall provides a measure of access control and protection for the DMZ systems consistent with their need for external connectivity.
- In this type of configuration, internal firewalls serve three purposes:
    1. The internal firewall adds more stringent filtering capability
    2. The internal firewall provides two-way protection with respect to the DMZ.
    3. Multiple internal firewalls can be used to protect portions of the internal network from each other.

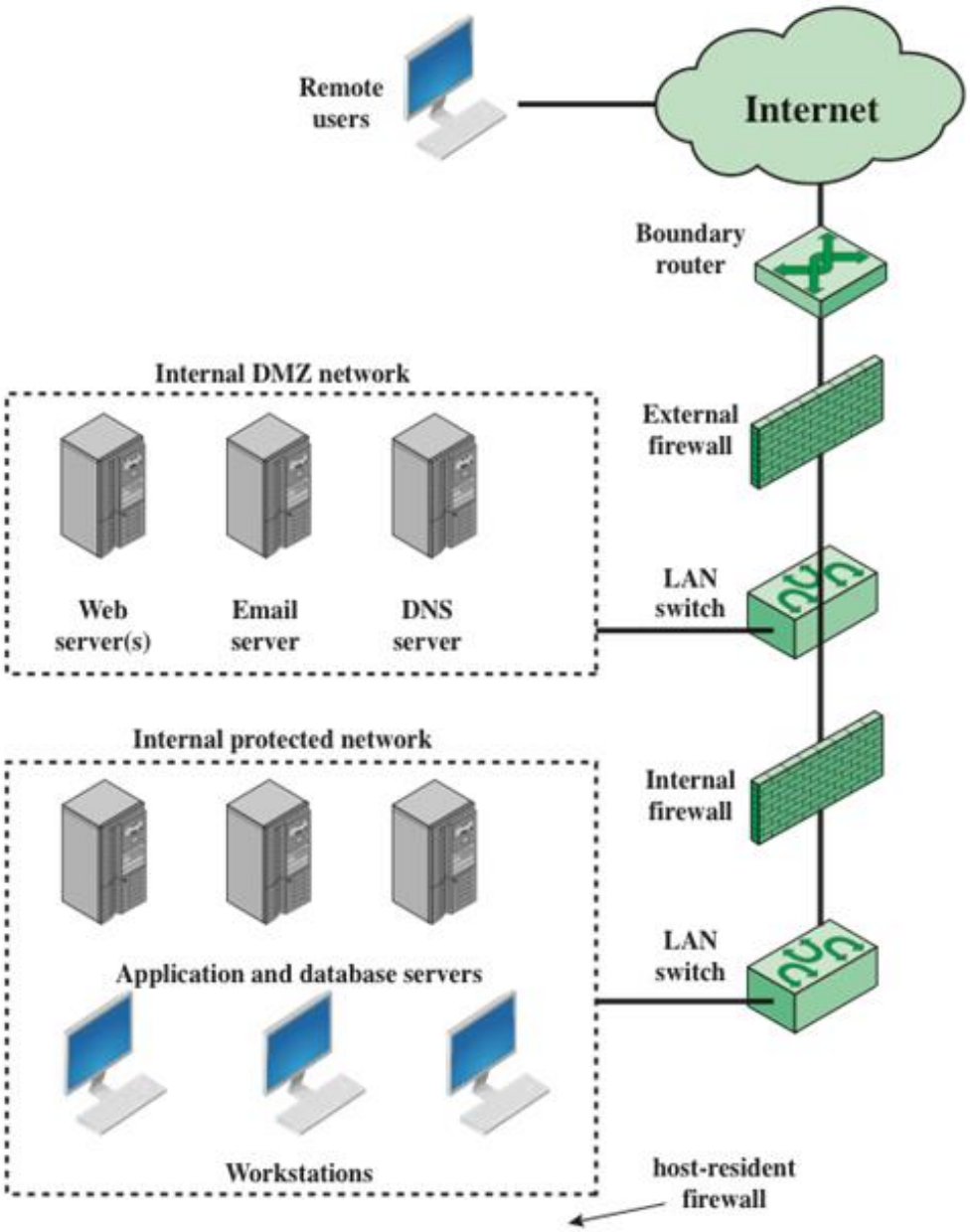


Figure 12.3 Example Firewall Configuration

Virtual private network (VPN)

- VPN consists of a set of computers that interconnect by means of a relatively unsecure network and that make use of encryption and special protocols to provide security.
- VPN uses encryption and authentication in the lower protocol layers to provide a secure connection through an otherwise insecure network, typically the Internet.

- VPNs are generally cheaper than real private networks using private lines but rely on having the same encryption and authentication system at both ends.

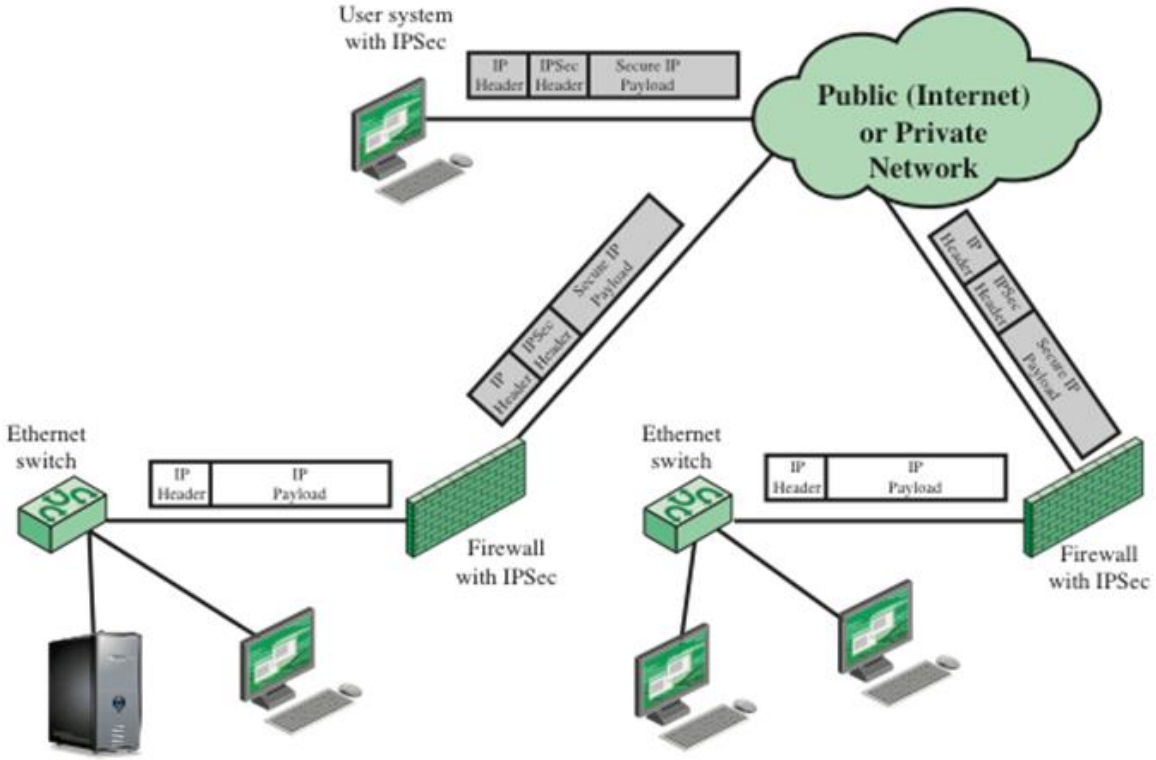


Figure 12.4 A VPN Security Scenario

Distributed firewall

A distributed firewall configuration involves stand-alone firewall devices plus host-based firewalls working together under a central administrative control.

Distributed firewall configuration

- Administrators can configure host-resident firewalls on hundreds of servers and workstations as well as configure personal firewalls on local and remote user systems.
- Network administrator set policies and monitor security across the entire network. These firewalls protect against internal attacks and provide protection tailored to specific machines and applications.

- With distributed firewalls, it may make sense to establish both an internal and an external DMZ.
- Web servers that need less protection because they have less critical information on them could be placed in an external DMZ, outside the external firewall.
- An important aspect of a distributed firewall configuration is security monitoring.

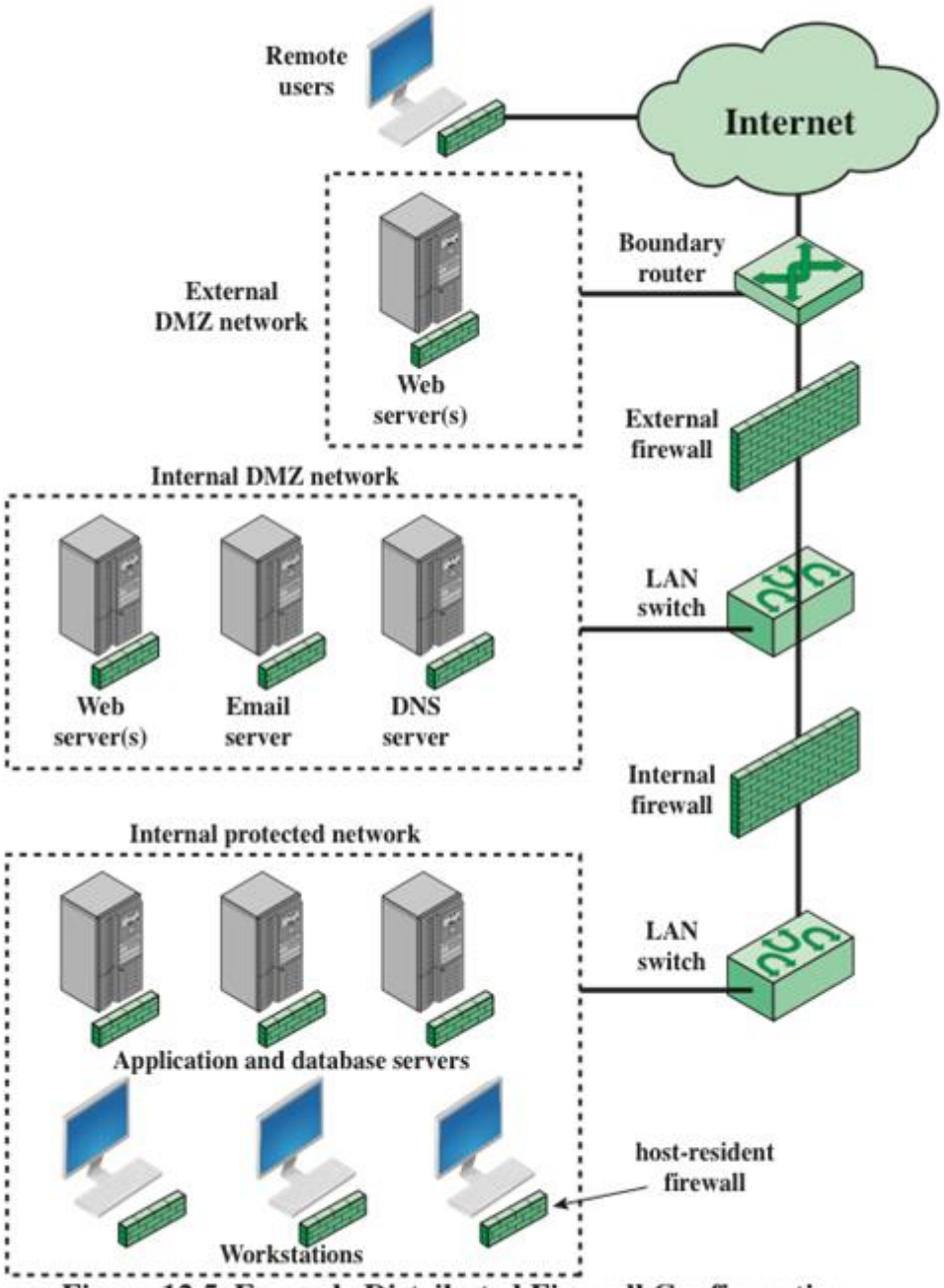


Figure 12.5 Example Distributed Firewall Configuration

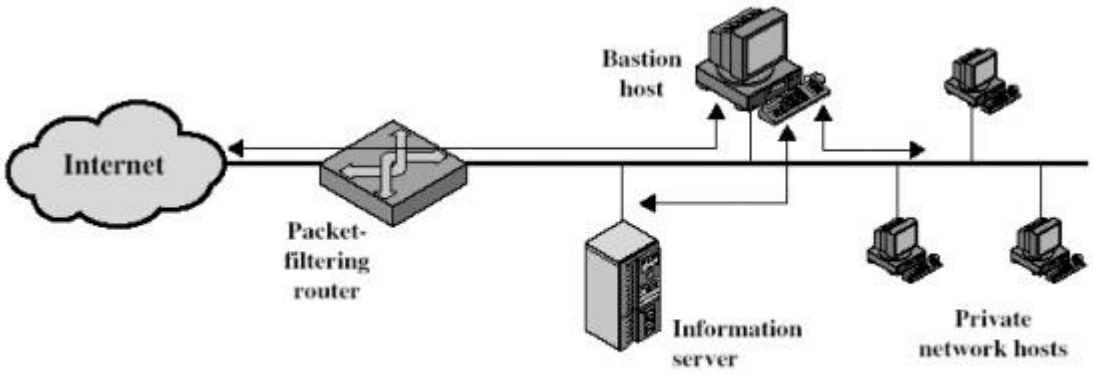
- The primary step in designing a secure firewall is obviously to prevent the firewall devices from being compromised by threats. To provide a certain level of security, the three basic firewall designs are considered:
  1. Single-homed bastion host
  2. Dual-homed bastion host
  3. Screened subnet firewall

1. Screened Host Firewall (Single-Homed Bastion Host)

In this configuration, the firewall consists of two systems: a packet filtering router and a bastion host. Typically, the router is configured so that

o For traffic from the internet, only IP packets destined for the basiton host are allowed in.

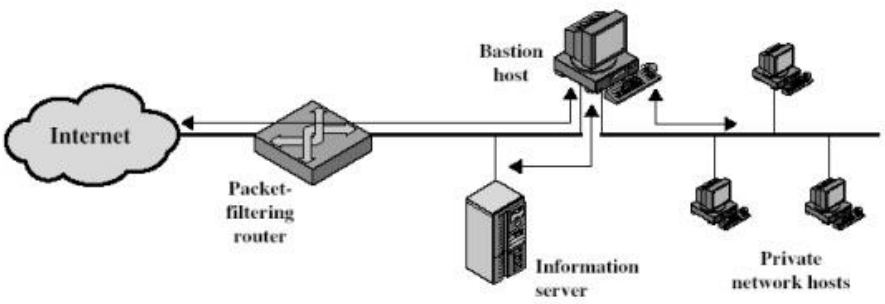
o For traffic from the internal network, only IP packets from the basiton host are allowed out.



(a) Screened host firewall system (single-homed bastion host)

2. Screened host firewall, dual homed basiton configuration

In the previous configuration, if the packet filtering router is compromised, traffic could flow directly through the router between the internet and the other hosts on the private network. This configuration physically prevents such a security break.



(b) Screened host firewall system (dual-homed bastion host)

3. Screened subnet firewall configuration

In this configuration, two packet filtering routers are used, one between the basiton host and internet and one between the basiton host and the internal network. This configuration creates an isolated subnetwork.

5.7 Blockchain

Blockchain is a type of register that stores and maintains transaction records. It stores the information in regular batches called blocks that link together to form a continuous chain. The data contained in each block is stored with a valid transaction as a block. These blocks are connected to the batches that grow as a new block of information is added.

How does it work?

A blockchain is a system that shares the data blocks with all the members linked in a chain created over the network. Each block contains the previous block's hash, followed to develop a growing transaction history. Any tampering with a block will lead to rejection by the network community, reducing the chances of hacking into the network.

Benefits of using Blockchain in Cybersecurity

- Data Transparency and Traceability
- Enhanced Customer Trust
- No Chance of Failure
- Safe Data Transfers
- Secure Data Storage and Processing

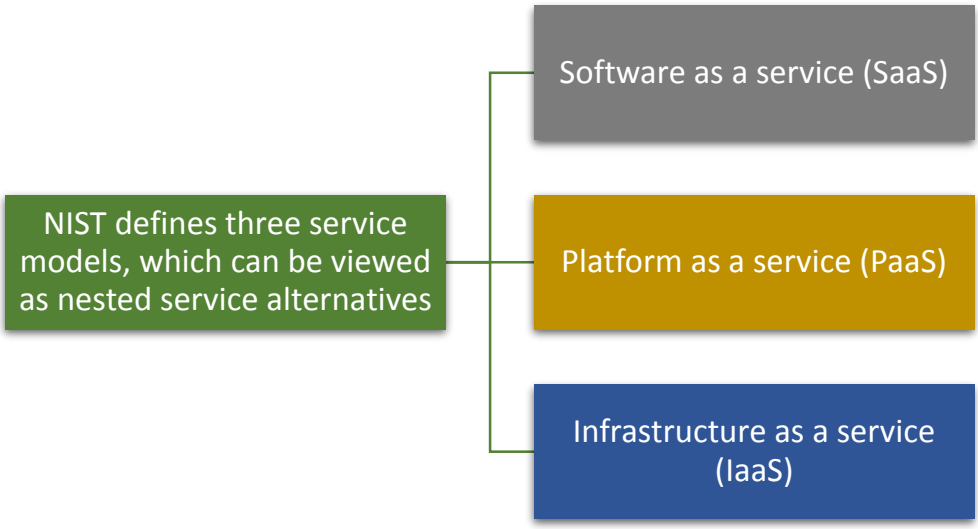
5.8 Cloud Security and IoT security

CLOUD SECURITY

The essential characteristics of cloud computing include the following:

- Broad network access
- Rapid elasticity
- Measured service
- On-demand self-service
- Resource pooling

Cloud Service Models



Security Issues for Cloud Computing

- Security is a major consideration when augmenting or replacing on-premises systems with cloud services
- Availability is another major concern
- Auditability of data must be ensured
- Businesses should perform due diligence on security threats both from outside and inside the cloud
    - Cloud users are responsible for application-level security
    - Cloud vendors are responsible for physical security and some software security
    - Security for intermediate layers of the software stack is shared between users and vendors
- Cloud providers must guard against theft or denial-of-service attacks by their users and users need to be protected from one another

Control Functions and Classes

Technical	Operational	Management ...
Access Control Audit and Accountability Identification and Authentication System and Communication Protection	Awareness and Training Configuration and Management Contingency Planning Incident Response Maintenance Media Protection Physical and Environmental Protection Personnel Security System and Information Integrity	Certification, Accreditation and Security Assessment Planning Risk Assessment System and Services Acquisitio

Risks and Countermeasures

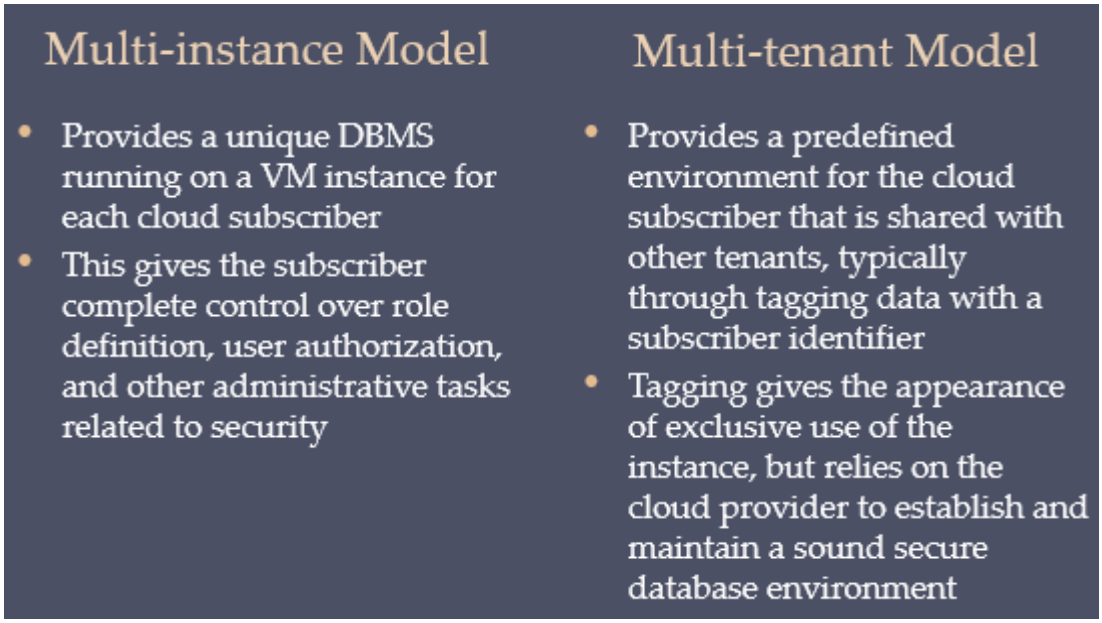
The Cloud Security Alliance lists the following as the top cloud-specific security threats:

- Abuse and immoral use of cloud computing
    - Countermeasures include:
        - Stricter initial registration and validation processes
        - Enhanced credit card fraud monitoring and coordination
        - Comprehensive inspection of customer network traffic
        - Monitoring public blacklists for one's own network blocks
- Insecure interfaces and APIs
    - Countermeasures include:
        - Analyzing the security model of CSP interfaces
        - Ensuring that strong authentication and access controls are implemented in concert with encrypted transmission
        - Understanding the dependency chain associated with the API
- Malicious insiders
    - Countermeasures include:
        - Enforce strict supply chain management and conduct a comprehensive supplier assessment
        - Specify human resource requirements as part of legal contract
        - Require transparency into overall information security and management practices, as well as compliance reporting
        - Determine security breach notification processes
- Shared technology issues
    - Countermeasures include:

- Implement security best practices for installation/configuration
- Monitor environment for unauthorized changes/activity
- Promote strong authentication and access control for administrative access and operations
- Enforce SLAs for patching and vulnerability remediation
- Conduct vulnerability scanning and configuration audits

Data Protection in the Cloud

There are many ways to compromise data. Deletion or alteration of records without a backup of the original content is an obvious example.



Cloud Security as a Service

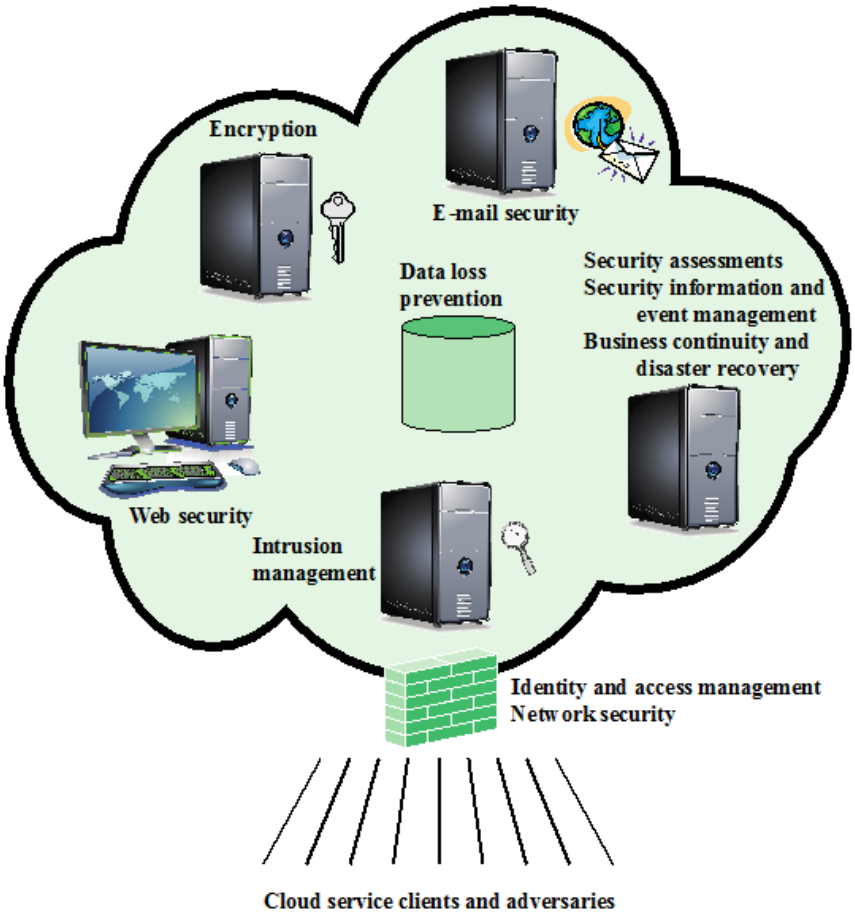


Figure . Elements of Cloud Security as a Service

- In the context of cloud computing, cloud security as a service, designated SecaaS, is a segment of the SaaS offering of a CSP
- The CSA defines SecaaS as the provision of security applications and services via the cloud either to cloud-based infrastructure and software, or from the cloud to the customers' on-premise systems

IoT SECURITY

- IoT is a term that refers to the expanding interconnection of smart devices, ranging from appliances to tiny sensors
    - A dominant theme is the embedding of short-range mobile transceivers into a wide array of gadgets and everyday items, enabling new forms of communication between people and things, and between things themselves

- The Internet supports the interconnectivity usually through cloud systems

Elements

- At the center of the network are the application platforms, data storage servers, and network and security management systems. These central systems gather data from sensors, send control signals to actuators, and are responsible for managing the IoT devices and their communication networks.
- At the edge of the network are IoT-enabled devices, some of which are quite simple constrained devices, and some of which are more intelligent unconstrained devices. As well, gateways may perform protocol conversion and other networking service on behalf of IoT devices.

Figure illustrates a number of typical scenarios for interconnection and the inclusion of security features.

The shading in Figure indicates the systems that support at least some of these functions.

- Typically, gateways will implement secure functions, such as TLS and IPsec.
- Unconstrained devices may or may not implement some security capability.
- Constrained devices generally have limited or no security features.
- As suggested in the figure, gateway devices can provide secure communication between the gateway and the devices at the center, such as

application platforms and management platforms.

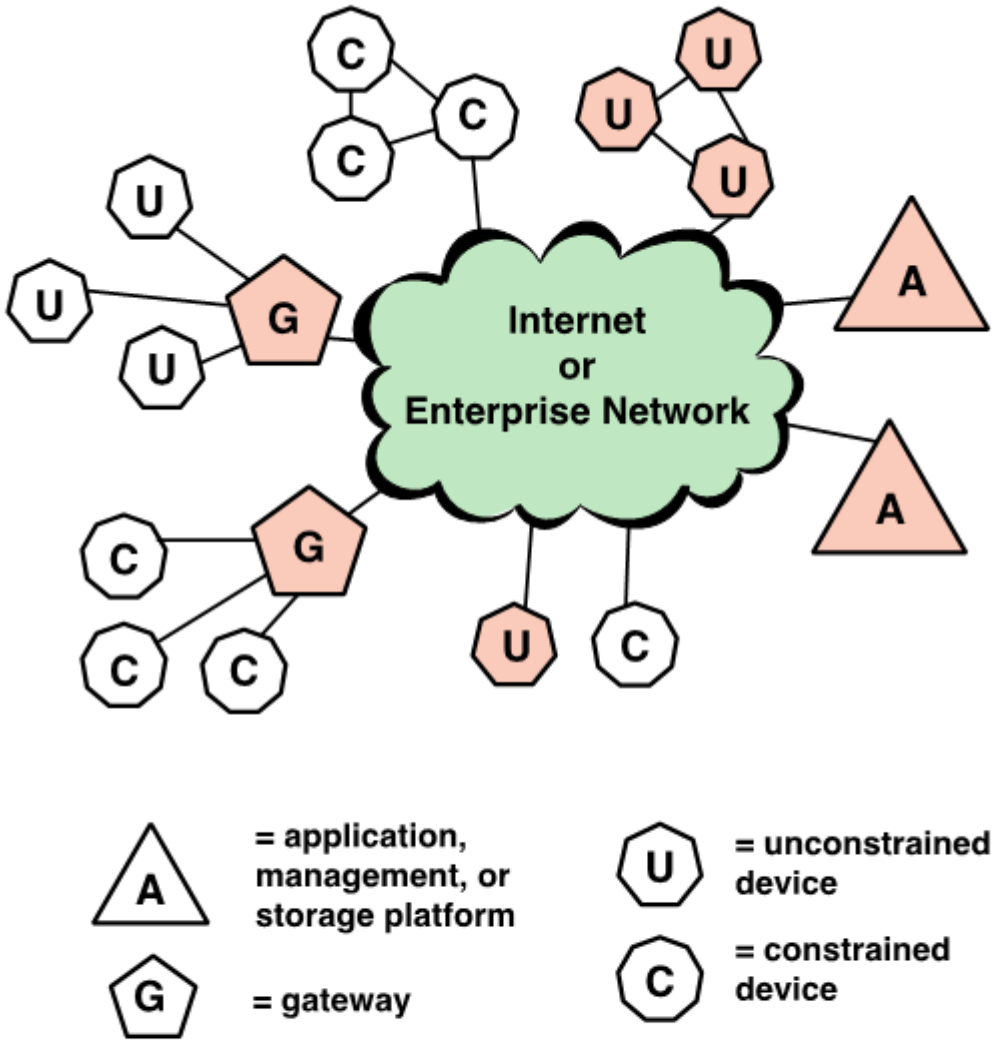


Figure IoT Security: Elements of Interest

IoT Security and Privacy Requirements

- The requirements are:
    - Communication security
    - Data management security
    - Service provision security
    - Integration of security policies and techniques
    - Mutual authentication and authorization
    - Security audit

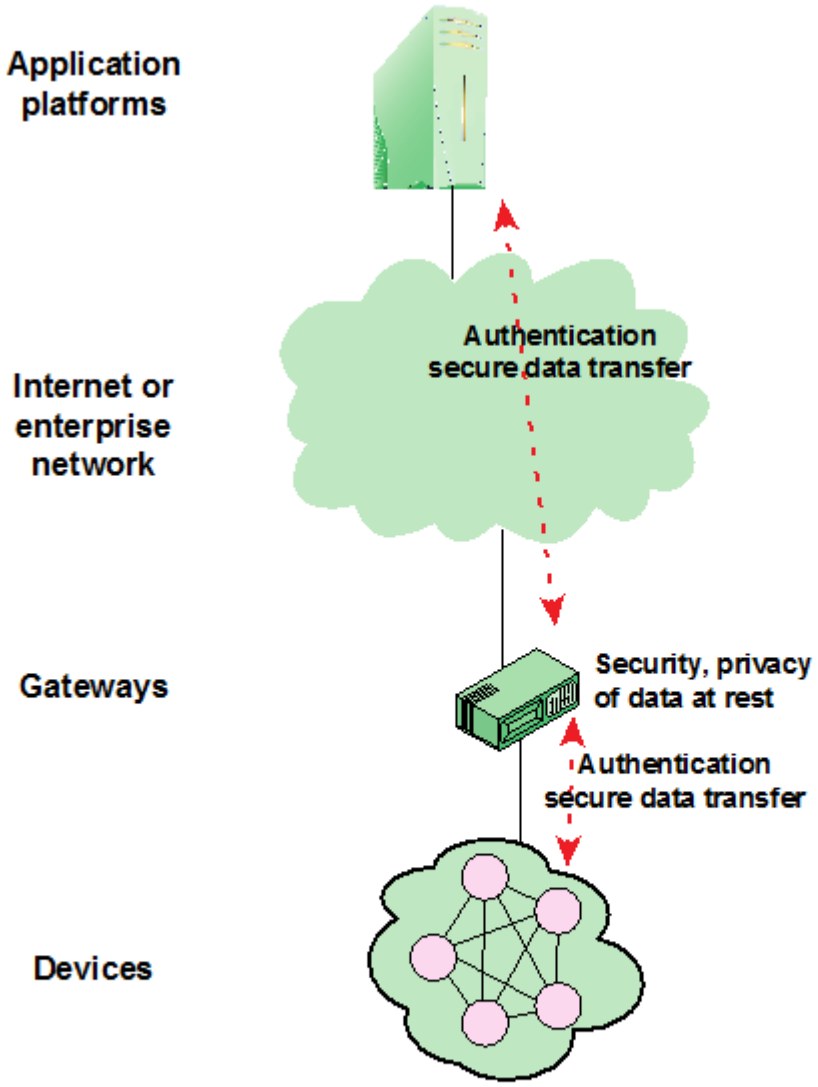


Figure . IoT Gateway Security Functions

A key element in providing security in an IoT deployment is the gateway.

Functions of Gateway

- Support identification of each access to the connected devices.
- Support authentication with devices.
- Support mutual authentication with applications.
- Support the security of the data that are stored in devices and the gateway, or transferred between the gateway and devices, or transferred between the gateway and applications.

IoT Security Environment

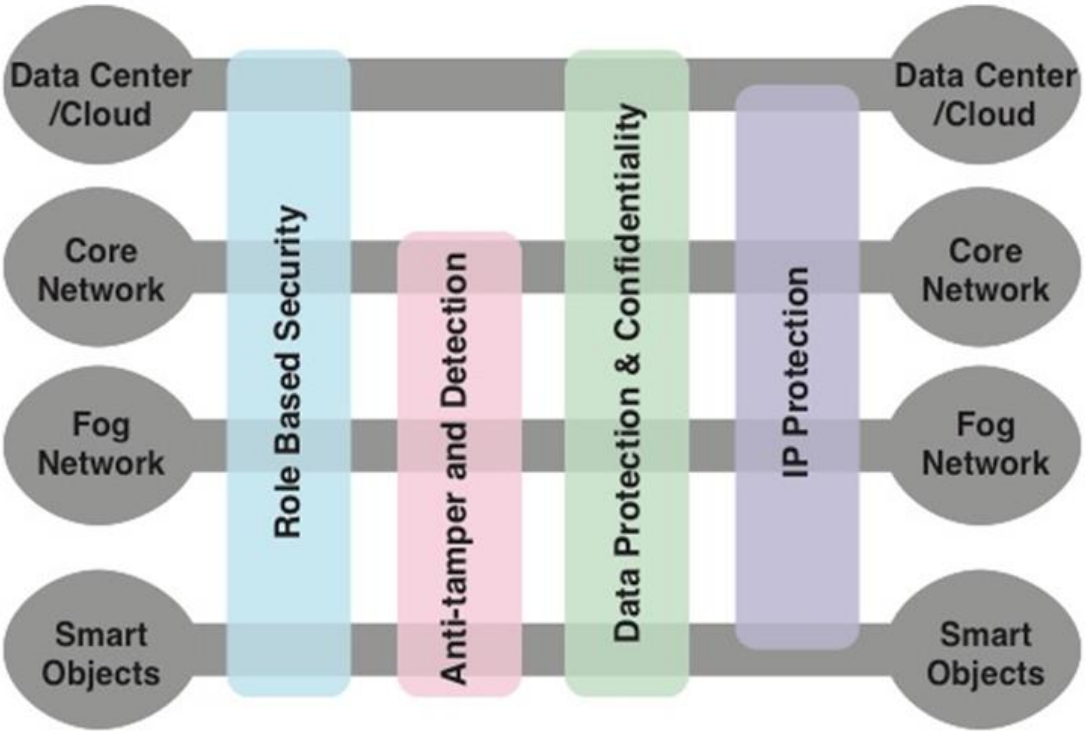


Figure IoT Security Environment

IoT model

It consists of the following levels:

- Smart objects/embedded systems
- Fog/edge network
- Core network
- Data center/cloud
- Role-based security
- Anti-tamper and detection
- Data protection and confidentiality
- Internet protocol protection

Figure maps specific security functional areas across the four layers of the IoT model.

MiniSec

- MiniSec is an open-source security module that is part of the TinyOS operating system

- It is designed to be a link-level module that offers a high level of security, while simultaneously keeping energy consumption low and using very little memory
- MiniSec provides confidentiality, authentication, and replay protection
- MiniSec has two operating modes, one tailored for single-source communication, and another tailored for multi-source broadcast communication