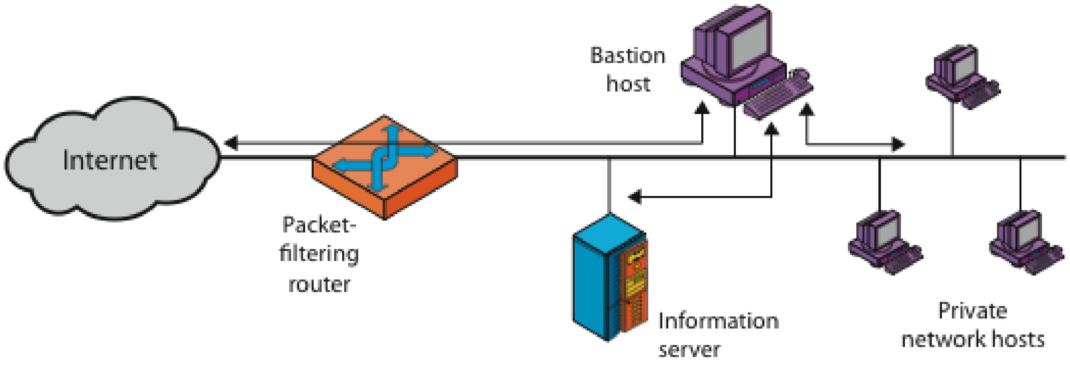
SOCKS consists of the following components:
● The SOCKS server, which runs on a UNIX-based firewall.
● The SOCKS client library, which runs on internal hosts protected by the firewall.
● SOCKS-ified versions of several standard client programs such as FTP and TELNET.

2.Describe the different Firewall Configurations with diagrams.

Three common firewall configurations:

1.screened host firewall, single-homed bastion configuration
2. Screened host firewall, dual-homed bastion configuration
3. Screened subnet firewall configuration

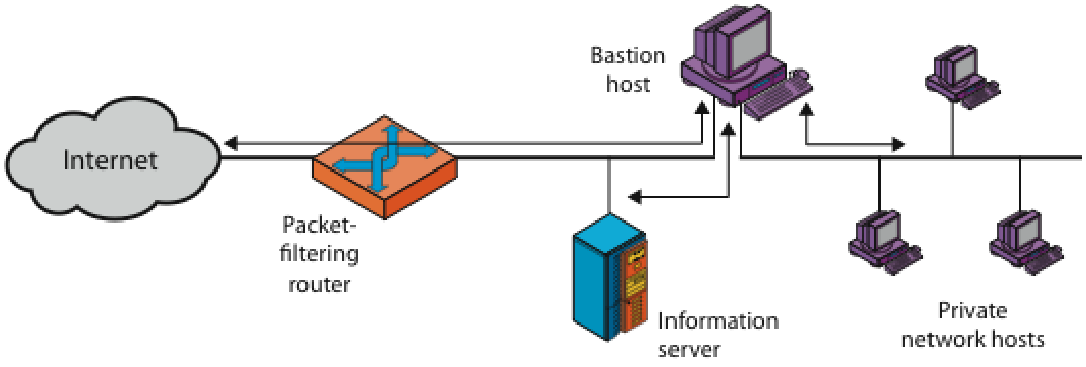
1. Screened host firewall, single-homed bastion configuration:



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

- Consists of two systems:
  - a **packet-filtering router** - allows Internet packets to/from bastion only
  - a **bastion host** - performs authentication and proxy functions
- This configuration has greater security, as it implements both packet-level & application-level filtering, forces an intruder to generally penetrate two separate systems to compromise internal security.
- Also affords flexibility in providing direct Internet access to specific internal servers (e.g. web) if desired.

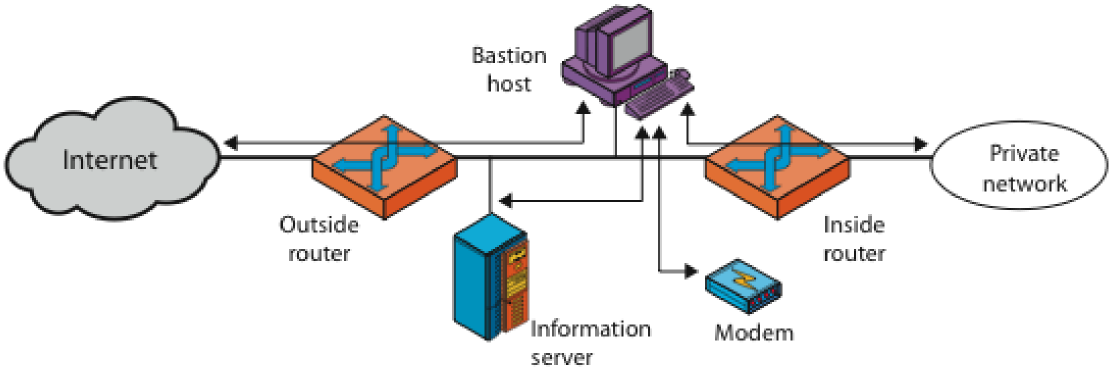
2. Screened host firewall, dual-homed bastion configuration:



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

- Physically separates the external and internal networks, ensuring two systems must be compromised to breach security.
- The advantages of dual layers of security are also present here.
- Again, an information server or other hosts can be allowed direct communication with the router if this is in accord with the security policy, but are now separated from the internal network.

3. Screened subnet firewall configuration



(c) Screened-subnet firewall system

- It has two packet-filtering routers, one between the bastion host and the Internet and the other between the bastion host and the internal network, creating an isolated sub network.
- This may consist of simply the bastion host but may also include one or more information servers and modems for dial-in capability.
- Typically, both the Internet and the internal network have access to hosts on the screened subnet, but traffic across the screened subnet is blocked.

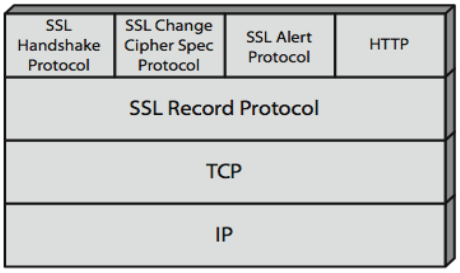
3. Explain four phases of handshake protocol with diagram.

- The most complex part of SSL is the Handshake Protocol.

- **Phase 2. Server Authentication and Key Exchange** - the server begins this phase by sending its certificate if it needs to be authenticated.
- **Phase 3. Client Authentication and Key Exchange** - the client should verify that the server provided a valid certificate if required and check that the server_hello parameters are acceptable
- **Phase 4. Finish** - this phase completes the setting up of a secure connection. The client sends a change_cipher_spec message and copies the pending CipherSpec into the current CipherSpec
- Client then immediately sends the finished message under the new algorithms, keys, and secrets.
- The finished message verifies that the key exchange and authentication processes were successful. The content of the finished message is the concatenation of two hash values:
  - MD5(master_secret || pad2 || MD5(handshake_messages ||
  - Sender || master_secret || pad1))
  - SHA(master_secret || pad2 || SHA(handshake_messages ||
  - Sender || master_secret || pad1))

4.Explain SSL architecture with a SSL protocol stack.

- SSL is the most widely used Web security mechanism.
- Its implemented at the Transport layer
- SSL is designed to make use of TCP to provide a reliable end-to-end secure service.
- SSL is not a single protocol but rather two layers of protocol.



SSL Architecture

- The SSL Record Protocol provides basic security services to various higher-layer protocols.
- In particular, the Hypertext Transfer Protocol (HTTP), which provides the transfer service for Web client/server interaction, can operate on top of SSL.
- **Three higher-layer protocols** are also defined as part of SSL:
  - the Handshake Protocol,

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 behavior 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 behavior is that of an intruder.

a.A**nomaly detection**: Rules are developed to detect deviation from previous usage patterns.

b.Penetration identification: An expert system approach that searches for suspicious behavior.

3.Audit Records

- A fundamental tool for intrusion detection is the audit record.
- Two plans are used:
  - **Native audit records**: Virtually all multiuser operating systems include accounting software that collects information on user activity
  - **Detection-specific audit records:** A collection facility can be implemented that generates audit records containing only that information required by the intrusion detection system.

7.Explain Rule-Based Intrusion Detection/ Rules that can be used to assign degrees of suspicion to activities and its attacks.

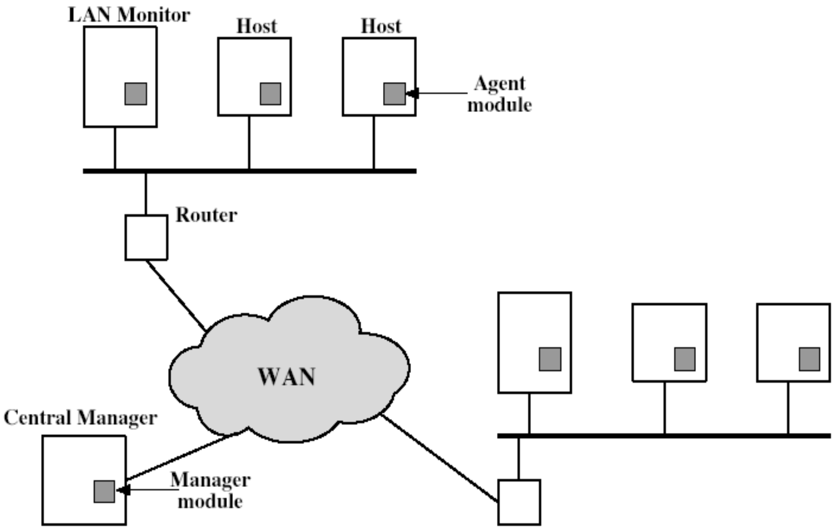
- Rule-based techniques detect intrusion by observing events in the system and applying a set of rules that lead to a decision regarding whether a given pattern of activity is or is not suspicious.
- There are two types:
- **Rule-based anomaly detection** is similar in terms of its approach and strengths to statistical anomaly detection. With the rule-based approach, historical audit records are analyzed to identify usage patterns and to generate automatically rules that describe those patterns. Rules may represent past behavior patterns of users, programs, privileges, time slots, terminals, and so on.
- **Rule-based penetration identification** takes a very different approach to intrusion detection, one based on expert system technology.
- The key feature of such systems is the use of rules for identifying known penetrations or penetrations that would exploit known weaknesses.
- Rules can also be defined that identify suspicious behavior, even when the behavior is within the bounds of established patterns of usage.

Rules that can be used to assign degrees of suspicion to activities:

1.Users should not read files in other users' personal directories.

6. Try all legitimate **license plate** numbers for this state.
7. Use a **Trojan horse** to bypass restrictions on access.
8. Tap the line between a remote user and the host system.

13. Explain the Distributed Intrusion Detection Architecture with a neat diagram.



Consists of three main components. The components are:
• **Host agent module**: audit collection module operating as a background process on a monitored system
• **LAN monitor agent module**: like a host agent module except it analyzes LAN traffic
• **Central manager module**: Receives reports from LAN monitor and host agents and processes and correlates these reports to detect intrusion.

14. Explain how agent is implemented in Distributed Intrusion Detection system.

1.All traffic from inside to outside, and vice versa, must pass through the firewall. This is achieved by physically blocking all access to the local network except via the firewall. Various configurations are used.
2.Only authorized traffic, as defined by the local security policy, will be allowed to pass. Various types of firewalls are used, which implement various types of security policies.
3.The firewall itself is immune to penetration. This implies that use of a trusted system with a secure operating system.

10. Define the general techniques that firewalls use to control access and enforce the site's security policy.

There are four techniques:
1. Service control: Determines the types of Internet services that can be accessed, inbound or outbound. The firewall may filter traffic on the basis of IP address and TCP port number; may provide proxy software that receives and interprets each service request before passing it on; or may host the server software itself, such as a Web or mail service.
2. **Direction control:** Determines the direction in which particular service requests may be initiated and allowed to flow through the firewall.
3. **User control:** Controls access to a service according to which user is attempting to access it
4. **Behavior control:** Controls how particular services are used. For example, the firewall may filter e-mail to eliminate spam, or it may enable external access to only a portion of the information on a local Web server.

11. Define the various limitations of firewalls:

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

Firewalls have their **limitations**, including that they:

1. cannot protect against attacks that bypass the firewall, e.g. PCs with dial-out capability to an ISP, or dial-in modem pool use
2. Do not protect against internal threats, e.g. disgruntled employee or one who cooperates with an attacker
3. Cannot protect against the transfer of virus-infected programs or files, given wide variety of O/S & applications supported

12. Describe the various techniques 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** (those of one to three characters).
3. Try words in the system's **online dictionary** or a list of likely passwords-available on hacker bulletin boards.
4.Collect information about users, such as their full names, the names of their spouse and children, pictures in their office, and books in their office that are related to hobbies.
5. Try users' phone numbers, Social Security numbers, and room numbers.