

MT5103: Network Security 2001

Question 5:

(a) A firewall is generally a networked device that is used to control access to resources on the network and enforce the site's security policy.

- Packet filtering firewalls.

A packet filtering firewall operates at the network and transport layer of the OSI framework. It is used to apply rules to each incoming IP packet and then forwards or discards the packet.

It is typically configured to filter packets going in both directions. Filtering rules are based on fields in the IP and transport header, including source and destination IP address, IP protocol field (which defines the transport protocol) and TCP or UDP port number (which defines the application).

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

The default rule can either be to discard the packet or to allow the packet. Which default policy to configure is usually a choice between convenience (default allow) and more custom based configuration (default discard). The latter is usually a pain to the user. In order for the latter to work effectively for the user, the administrator must spend more time on configuring the device. So there is a tradeoff between ease-of-use and security.

Packet filtering can only enforce coarse grain policies, thus reduced flexibility of what applications are supported properly.

- Stateful packet filter.

This is the same as the packet filtering firewall but it provides with the added capability to remember connection states. Initial packets are remembered and replies are automatically allowed. This is useful in supporting a greater range of protocols and policies are easier to configure.

- Application-level gateways.

Application-level gateways, also called a proxy, acts as a relay of application level traffic. For each application there is a complete client-server implementation in the same device. Typically a connection is established twice.

1. The user connects to the proxy via the desired application
2. The proxy validates the request
3. The proxy connects to the specified server
4. The request comes back to the user, but is also processed by the client/server on the proxy

The proxy basically relays TCP segments containing the application data. Further the gateway can be configure to support a limited set of features for the application.

Proxies tend to be more secure than packet-filters. The proxy needs only to scrutinize the application data for the services that are supported. No need for complex rule-sets to meet the desired effect. In addition it is easy to log and audit all incoming traffic at the application level.

A major disadvantage of this type is the additional processing overhead that on each connection. The gateway examines and forwards all traffic in both directions.

- Circuit-level gateway

This can be a standalone system or it can be a special function performed by an application-level gateway. A circuit level gateway will typically set up two connections. One between the user and the gateway and one between the gateway and the server. Once the connection is established the TCP segments are relayed without being processed by the gateway. A typical use of a circuit level gateway is to implement an application level gateway for all incoming connections and a circuit level gateway for outbound connections. This assumes that the users on the internal network are trusted.

With such an approach the processing overhead on the proxy is reduced considerably.

(b) However firewalls cannot prevent every attack. Packet-filtering firewalls do not check the content of a connection. Thus although only e-mail is allowed, this will not prevent a virus that is attached to the e-mail. Application-level gateways can protect to some extent from viruses. Since the content is checked on every connection. However some type of viruses cannot be prevented (Nimda: HTTP request). However firewalls cannot scrutinize encrypted content. IP spoofing is a common attack, which can be prevented by having incoming connections, bound to a physical interface and outbound connections to a different one. Specifying the appropriate policy on the firewall can prevent source routing and tiny fragment attacks.

Firewalls must be set up properly to function correctly and to protect the network. A typical configuration that allows for more security is to use a bastion host between the firewall and the internal network. The bastion host is typically a proxy or a circuit level gateway, and even if the firewall is compromised the attacker will have to gain access to the bastion host to attack the network directly. The bastion host usually runs a trusted OS for enhanced security.