

MULTIPURPOSE INTERNET MAIL EXTENSIONS (MIME)

MIME transforms non-ASCII data at the sender's site to Network Virtual Terminal (NVT) ASCII data and delivers it to client's Simple Mail Transfer Protocol (SMTP) to be sent through the Internet.[4] The server SMTP at the receiver's side receives the NVT ASCII data and delivers it to MIME to be transformed back to the original non-ASCII data.

Message Authentication Code

A Message Authentication Code is a cryptography method that uses a secret key to encrypt a message. This method outputs a MAC value that can be decrypted by the receiver, using the same secret key used by the sender. The Message Authentication Code protects both a message's data integrity as well as its authenticity.

Firewalls

A firewall controls access between networks. It generally consists of gateways and filters which vary from one firewall to another. Firewalls also screen network traffic and are able to block traffic that is dangerous. Firewalls act as the intermediate server between SMTP and HTTP connections.

Role of firewalls in Internet security and web security

Firewalls impose restrictions on incoming and outgoing packets to and from private networks. All the traffic, whether incoming or outgoing, must pass through the firewall; only authorized traffic is allowed to pass through it. Firewalls create checkpoints between an internal private network and the public Internet, also known as choke points. Firewalls can create choke points based on IP source and TCP port number. They can also serve as the platform for IPsec. Using tunnel mode capability, firewall can be used to implement VPNs. Firewalls can also limit network exposure by hiding the internal network system and information from the public Internet.

TYPES OF FIREWALLS

Packet filters

Packet filters are one of several different types of firewalls that process network traffic on a packet-by-packet basis. Their main job is to filter traffic from a remote IP host, so a router is needed to connect the internal network to the Internet. The router is known as a screening router, which screens packets leaving and entering the network.

Circuit level gateways

The circuit level gateway is a proxy server that statically defines what traffic will be allowed. Circuit proxies always forward packets containing a given port number, provided the port number is permitted by the rules set. This gateway operates at the network level of an OSI model. The main advantage of a proxy server is its ability to provide Network Address Translation (NAT), which can hide the user's IP address from the Internet, effectively protecting all internal information from the Internet.

Application level gateways

An application level gateway is a proxy server operating at the TCP/IP application level. A packet is forwarded only if a connection is established using a known protocol. Application level gateways are notable for analyzing entire messages rather than individual packets of data when the data are being sent or received.