**Network Firewalls**

Your network's first line of defense is a firewall.

A firewall is used to prevent unauthorized users from accessing your network.

usually placed near the perimeter of the network to serve as a gatekeeper for both incoming and outgoing traffic.

By creating a virtual wall between your network or computer and the Internet, it protects your PC from online dangers.

**How Does a Firewall Work?**

Examines the traffic sent between two networks.

e.g., examines the traffic being sent between your network and the Internet.

Data is examined to see if it appears legitimate:

* if so, the data is allowed to pass through.
* If not, the data is blocked.

You may set rules with a firewall to control what traffic is allowed into and out of your private network.

**Creating Rules**

Traffic blocking rules can be based upon:

Words or phrases

Domain names

IP addresses

Ports

Protocols (e.g. FTP)

While firewalls are essential, they can block legitimate transmission of data and programs.

**Common Firewall Types**

In general, there are software firewalls and hardware firewalls

* Even in-home networks

Usually found in routers, which distribute incoming data from an Internet connection to computers, are hardware firewalls.

Software firewalls are installed on each individual computer.

A network should have both.

**Software Firewall**

Protect only the computer on which they are installed.

Provide excellent protection against threats (viruses, worms, etc.)

Have a user-friendly interface.

Have flexible configuration.

**Router Firewall**

Protect your entire network or part of a network.

Located on your router.

Protect network hardware which cannot have a software firewall installed on it.

Allows the creation of network-wide rules that govern all computers on the network.

**Firewall Operation**

Can be divided into three main methods:

* Packet filters (see last topic)
* Application gateways
* Packet inspection

Individual vendors of firewalls may provide additional features

* You should look at their products for details

**Application Gateways**

Application-layer firewalls are able to understand the traffic that passes through them and decide whether to allow or deny it based on the content.

Application-layer firewalls include host-based firewalls that are intended to prevent challenging Web material based on keywords.

To be sure a request isn't actually an attack in disguise, application-layer firewalls can examine packets headed for an internal Web server.

**Advantage of Application Gateways**

Offer protection against application attacks and port scans.

In order to attack devices protected by the firewall, an attacker must first pass the application or proxy firewall if they discover a weakness in an application.

Able to be quickly patched should a vulnerability be found.

If every internal device is patched, this might not be the case.

**Disadvantage**

Must be able to manage traffic going to and coming from your particular application.

It's possible that your application layer firewall won't support a unique application unless it undergoes a number of significant modifications.

In general, packet-filtering or packet-inspection firewalls operate far more quickly than application firewalls.

They execute programs, keep the client and server's states up to date, and examine traffic.

**Packet inspection Firewalls**

Examine the session information between devices:

Protocol

New or existing connection

Source IP address

Destination IP address

Port numbers

IP checksum

Sequence numbers

Application-specific information

**Outbound Internet Traffic**

The client initiates a connection to the web server's IP address that is intended for port 80 (HTTP).

Based on the present rule-set, the firewall decides whether to allow that packet through.

Firewall examines the IP packet's data section to determine if the communication is legitimate HTTP traffic.

If everything checks out, the session data is used to generate a flow entry in the firewall, allowing the packet to pass through.

**Inbound Internet Traffic**

Web server receives the packet and responds.

Return traffic is received by the firewall.

Firewall compares the session information with the data in the local translation table to determine if return traffic is permitted.

The payload is looked at to confirm that the HTTP protocol is appropriate if the return traffic matches previous requirements.

Then it is forwarded to the client.

**Advantages**

Generally, much faster than application firewalls.

They are not required to host client applications.

Most of the packet-inspection firewalls today also offer deep-packet inspection.

The firewall can dig into the data portion of the packet and also:

* Match on protocol compliance.
* Scan for viruses
* Still operate very quickly.

**Disadvantage**

Open to certain denial-of-service attacks.

These can be used to fill the connection tables with illegitimate connections.

**Firewall Architecture**

Network perimeters as well as the perimeters of subnetworks are protected by firewalls.

Where firewalls should be placed is one of a network administrator's most important questions.

The firewall architecture describes how firewalls are positioned relative to other network components.

We will simply examine how firewalls are positioned and the implications of this;

additional security devices need to be used as well.

**Firewall Architecture**

The following are common firewall architectures:

Screening router

Screened host

Dual homed host

Screened subnet

Screened subnet with multiple DMZs

Dual firewall

**Screening router**

Simplest of firewall architectures

Traffic is screened by a router

* Packet filtering
* Using ACLs

Traffic is screened according to:

* Source or destination IP address
* Transport layer protocol
* Services requested

**Screening Router**

Usually deployed at the perimeter of the network.

May be used to control access to a Demilitarized Zone (DMZ).

More often used in conjunction with other firewall technologies.

**Advantages and Disadvantages**

Advantages

* Simple
* Cheap

Disadvantages

* No logging
* No user authentication
* Difficult to hide internal network structure

**Demilitarized Zones (DMZ)**

Although it is a part of the internal network, a DMZ is kept separate from the rest of the network.

The firewall still filters traffic going through it that is traveling between the DMZ and other interfaces on the firewall's protected side.

Firewall protection policies are in place for this traffic.

Common to put public-facing servers on the DMZ:

* Web Servers
* Email Servers

**Screened Host Firewall**

Adds an extra layer of security over a screening router.

Across networks is a Bastion Host/Firewall.

There are two NICs on Bastion Host/Firewall.

The trusted network and the untrusted network are connected via Bastion Host/Firewall.

Traffic up to the application layer is filtered using stateful and proxy technologies.

**Bastion Host**

A specialized computer that has been set up and intended to withstand attacks.

The first line of defense is the router.

The router is where access control and packet filtering are done.

The server that uses the router to connect to the insecure network is known as the bastion host.

**Advantages & Disadvantages**

Advantages

* Security is distributed between two points
* Greater security than screening router
* Transparent outbound access/restricted inbound access

Disadvantages

* Difficult to hide internal structure
* There is a single point of failure in the network

**Dual-Homed Host**

A Bastion Host/Firewall is surrounded with packet filtering routers.

* Dual-homed - outside world and protected network.
* Multi-homed - outside world and multiple protected networks.

Routers filter traffic to the Bastion Host.

Bastion Host adds additional filtering capabilities.

Bastion Host has no routing capabilities.

**Advantage and Disadvantage**

Advantages

* Hides internal network structure

Disadvantages

* Requires users to log onto bastion host or the use of proxy servers

**Screened Subnet DMZ**

Packet filtering routers surround Bastion Host.

They control data entering and leaving the trusted and untrusted network segments.

Features a DMZ, adding another level of usefulness.

The packet filtering router and Bastion Host are required to handle traffic from the DMZ to the trusted network.

**Advantages and Disadvantages**

Advantages

* Provides services to outside without compromising inside
* Internal network hidden

Disadvantages

* Single point of failure

**Screened subnet multiple DMZs**

Allows configuration of varying levels of security between:

* DMZs and the untrusted network
* Different DMZs
* DMZs and the trusted network

**Dual Firewall Architecture**

Using two or more firewalls enhances security.

Cab be used to create DMZs.

Using technology from multiple vendors can enhance security.