Introduction to Information Technology

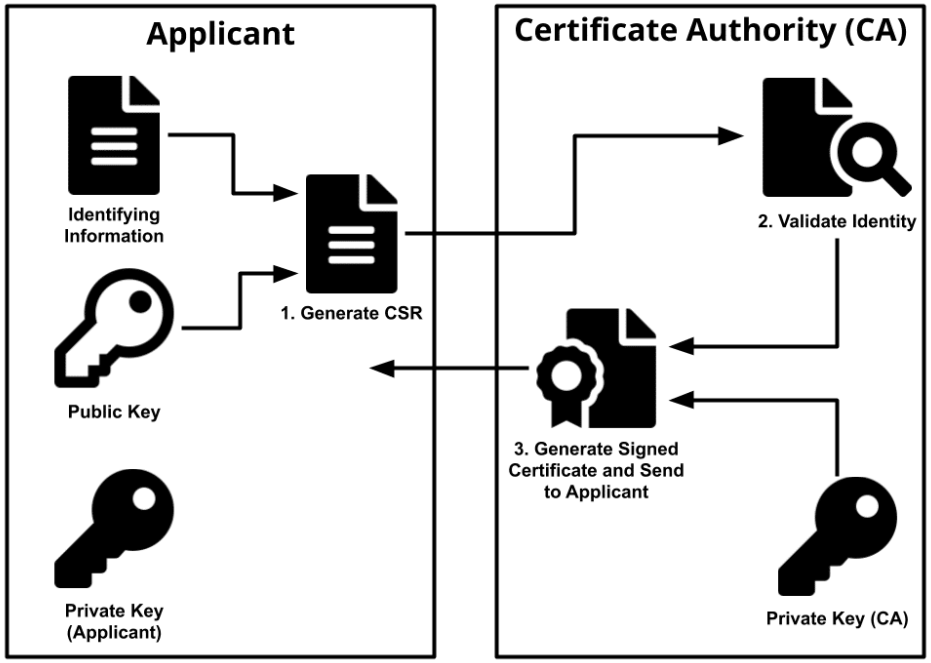
CSC109

2020

By: Rajiv Raman Parajuli

Certificate Authority (CA)

- A **certificate authority (CA)** is a company or organization that acts to validate the identities of entities (such as websites, email addresses, companies, or individual persons)
- It bind them to cryptographic keys through the issuance of electronic documents known as **digital certificates**.



- CA issues digital certificates which contains a public key, a name, an expiration date, the name of authority that issued the certificate, a serial number, any policies describing how the certificate was issued, how the certificate may be used, the digital signature of the certificate issuer, and any other information..

DIGITAL SIGNATURE

- A digital signature is used to sign a computerized document
- This is the primary method of identification in use on the Internet
- The protocols securing your browsing session when visiting a webpage of HTTPS make heavy use of Digital Certificates (SSL/TLS).
- A digital certificate is issued by a Certification Authority (CA)
- Digital signatures are easy for a user to produce, but difficult for anyone else to forge
- Digital signatures can be permanently tied to the content of the message being signed and then cannot be moved from one document to another, as such an attempt will be detectable.
- Inside a digital certificate is a very important piece of information: a Public Key of an Asymmetric Key Pair. This key is used to verify that the entity who presents the certificate is the true owner of the certificate. Much like your picture or signature on your driver's license.

Digital signature scheme is a type of asymmetric key pair cryptography;

The digital signature scheme typically consists of three algorithms:

- **Key generation algorithm** —The algorithm outputs private key and a corresponding public key.
- **Signing algorithm** —It takes, message + private key, as input, and, outputs a digital signature.
- **Signature verifying algorithm** —It takes, message + public key + digital signature, as input, and, accepts or rejects digital signature.

Digital signature creation and Digital signature verification are two process involved.

1. Generate Key-pair

2. User-A requests CA Certificate

3. CA responds with its CA Certificate including its Public Key

4. Gather information

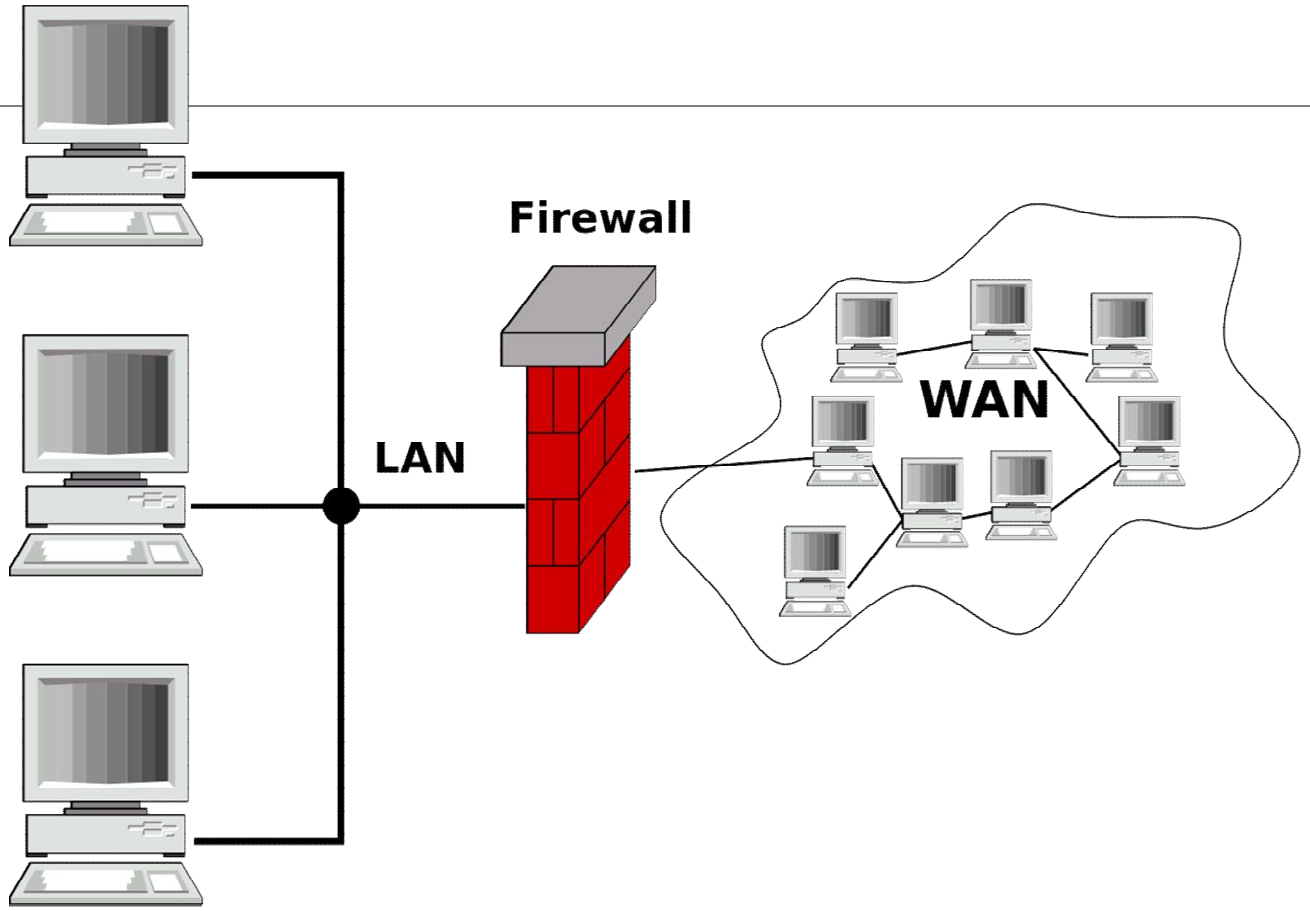
5. Request the Certificate which has User-A's identity and Public Key

6. CA verifies the identity of User-A

7. Issue the Certificate for User-A

FIREWALL

- A firewall is a security mechanism to protect a local network from the threats it may face while interacting with other networks (Internet).
- A firewall can be a hardware component, a software component, or a combination of both。
- It prevents computers in one network domain from communicating directly with other network domains。
- All communication takes place through the firewall, which examines all incoming data before allowing it to enter the local network。
- It Interconnects networks with differing trust
- Imposes restrictions on network services; only authorized traffic is allowed。
- Auditing and controlling access； implement alarms for abnormal behavior
- Itself immune to penetration


Firewall
LAN
WAN

Working of Firewall

The working of firewall is based on a filtering mechanism.

The filtering mechanism keeps track of source address of data, destination address of data and contents of data.

The filtering mechanism allows information to be passed to the Internet from a local network without any authentication.

It makes sure that the downloading of information from the Internet to a local network happens based only on a request by an authorized user.

Firewall Related Terminology:

1. Gateway
2. Proxy Server
3. Screening Routers

Types of Firewall

The type of firewall used varies from network to network

1. **Packet Filter Firewall**
2. **Circuit Filter Firewall**
3. **Application-Level Gateway/ Proxy server**

Packet Filter Firewall

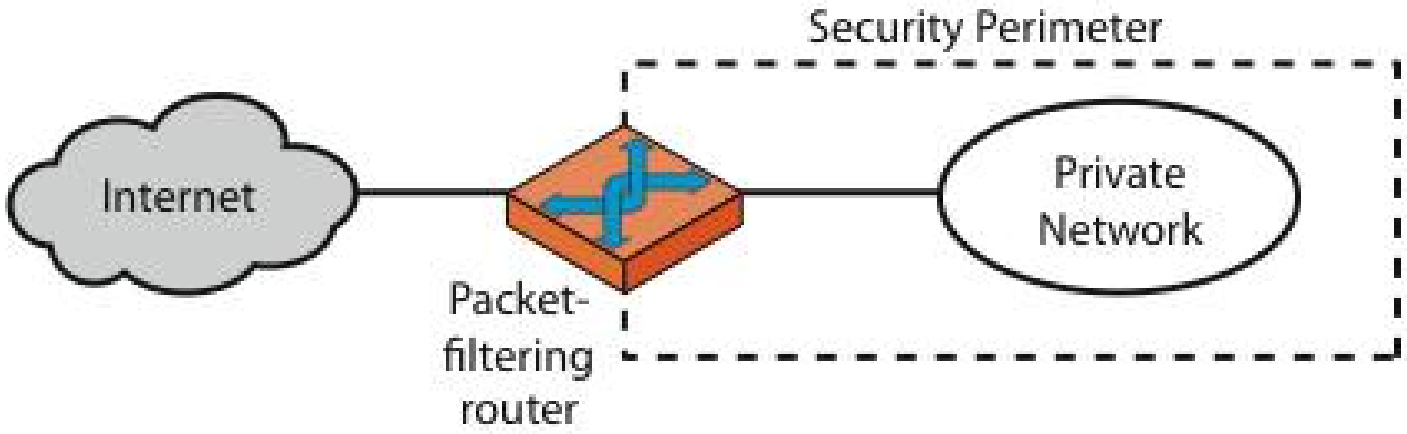
Simplest of components, use in routers
Implemented at Physical and Network Layer of OSI Model

- check incoming and outgoing packets
- filtering rules are applied to the data packets for filtering
- If the packet is found valid, then it is allowed to enter or exit the local network

Packet filtering is fast, easy to use, simple and cost effective.

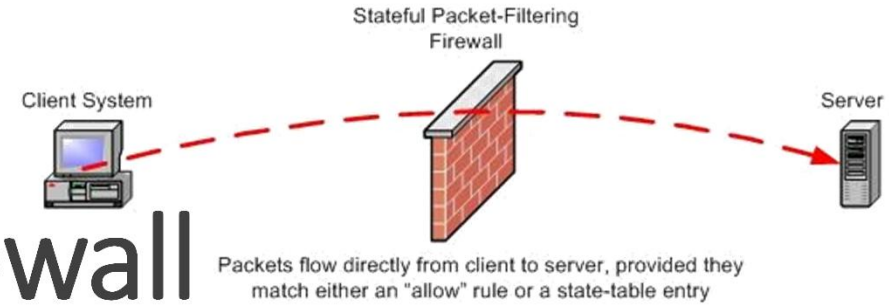
Packet filter firewall alone is not a complete solution

Packet Filter Firewall



(a) Packet-filtering router

Circuit Filter Firewall



More Secure over Packet Filter; “stateful inspection”

Traditional packet filters do not examine transport layer context

- ie matching return packets with outgoing flow

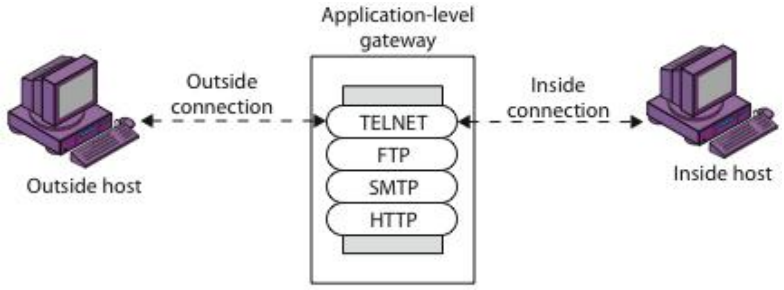
Stateful packet filters address this need

They examine each IP packet in context

- Keep track of client-server sessions
- Check each packet validly belongs to one

Hence are better able to detect bogus packets out of context

Application-Level Gateway



An application-level gateway protects all the client applications running on a local network from the Internet by using the firewall itself as the gateway

- Proxy firewall operates on the application layer. direct connection from an external computer to local network never takes place.
- The proxy automatically segregates all the packets depending upon the protocols used for them. A proxy server must support various protocols. It checks each application or service.
- A proxy server is easy to implement on a local network.
- Application level gateways or proxy server tend to be more secure than packet filters.

Instead of checking the TCP, UDP and IP combinations that are to be allowed, it checks the allowable applications.