CRYPTOGRAPHY AND INFORMATION SECURITY

IT 3203

LECTURE 28

By

Varsha Himthani

Assistant Professor (Selection Grade)

Manipal University Jaipur

Password Protection

Password protection refers to the practice of securing access to a system, application, or data with a password—a secret string of characters known only to the authorized user.

Effective password protection involves not only choosing a strong, hard-to-guess password but also implementing measures and policies to ensure the secure use, storage, and management of passwords.

Password Protection Schemes

1.Hashing and Salting:

1. **Hashing:** Passwords should never be stored in plaintext form. Instead, they should be hashed using a strong cryptographic hash function (e.g., SHA-256, bcrypt, scrypt) to create a fixed-length, irreversible representation of the password.

2. **Salting:** A unique, random salt should be added to each password before hashing to protect against dictionary and rainbow table attacks. This ensures that even if two users have the same password, their hashed passwords will be different.

Password Protection Schemes

2. Encryption:

Passwords may be encrypted when stored or transmitted over the network to protect them from interception. Decryption keys must be securely managed.

3. Secure Transmission:

Passwords should be transmitted securely using encrypted protocols such as HTTPS, SSH, or TLS to prevent eavesdropping or man-in-the-middle attacks.

4. Two-Factor Authentication (2FA):

2FA adds an additional layer of security by requiring the user to provide a second form of authentication (e.g., a code sent to their phone or a biometric factor) in addition to their password.

Password Protection Policies

By implementing these schemes and policies, organizations can enhance password protection and improve overall security for their systems and data.

1.Password Complexity:

- Encourage or require users to choose strong passwords that include a mix of uppercase and lowercase letters, numbers, and special characters.
- Avoid common or easily guessable passwords (e.g., "password123").

2.Password Length:

Require passwords to be a minimum length, such as 8-12 characters, to increase resistance to brute-force attacks.

3.Password Expiration:

Regularly require users to change their passwords to limit the impact of potential breaches. However, frequent changes can be inconvenient and may lead to weaker passwords being chosen.

Password Protection Policies

4. Account Lockout:

Implement an account lockout policy that temporarily disables accounts after a certain number of failed login attempts to prevent brute-force attacks.

5. Password Reuse:

Discourage or prohibit users from reusing old passwords or using the same password across multiple accounts.

6. Password Storage:

Store passwords securely using hashing and salting techniques. Never store passwords in plaintext.

7. User Education:

Educate users about password best practices and the importance of keeping their passwords confidential.

Firewalls

A firewall is a network security device or software application that monitors and controls incoming and outgoing network traffic based on predetermined security rules. Firewalls serve as a barrier between trusted and untrusted networks, such as the internet and a private network, to protect against unauthorized access and potential attacks.

Definition:

A firewall is a security measure that filters network traffic according to defined rules and policies. It inspects data packets as they enter or leave a network, allowing or blocking them based on specified criteria such as source and destination IP addresses, port numbers, protocols, or application-level content.

Firewall

- Firewalls play a crucial role in network security by acting as a gatekeeper for network traffic.
- By implementing security rules and filtering traffic, firewalls help protect networks from unauthorized access, attacks, and data breaches.
- Next-generation firewalls extend traditional functionality with advanced threat detection and response capabilities.

Firewall: Construction and Operation

1.Rules and Policies: Firewalls operate based on a set of security rules and policies defined by the network administrator. These rules specify which types of traffic are allowed and which are blocked.

2.Monitoring Traffic: Firewalls monitor all incoming and outgoing network traffic, inspecting packets for adherence to the security rules.

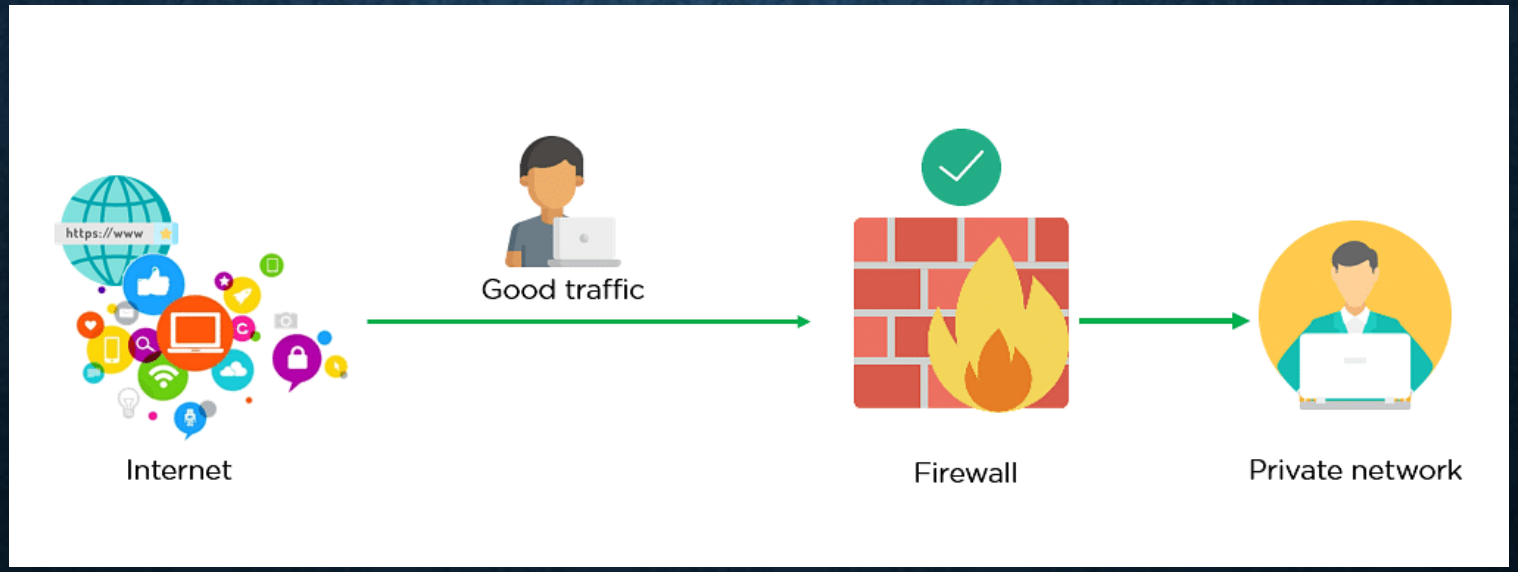
3.Filtering Traffic: Firewalls filter traffic based on the defined rules. They can allow or deny traffic based on various criteria such as IP addresses, port numbers, protocols, or application data.

4.Logging and Alerts: Firewalls often log traffic and generate alerts for suspicious or unauthorized access attempts. This information can be used for threat detection and analysis.

5.Placement: Firewalls are typically placed at network boundaries, such as between a private network and the internet, to provide a layer of protection against external threats.

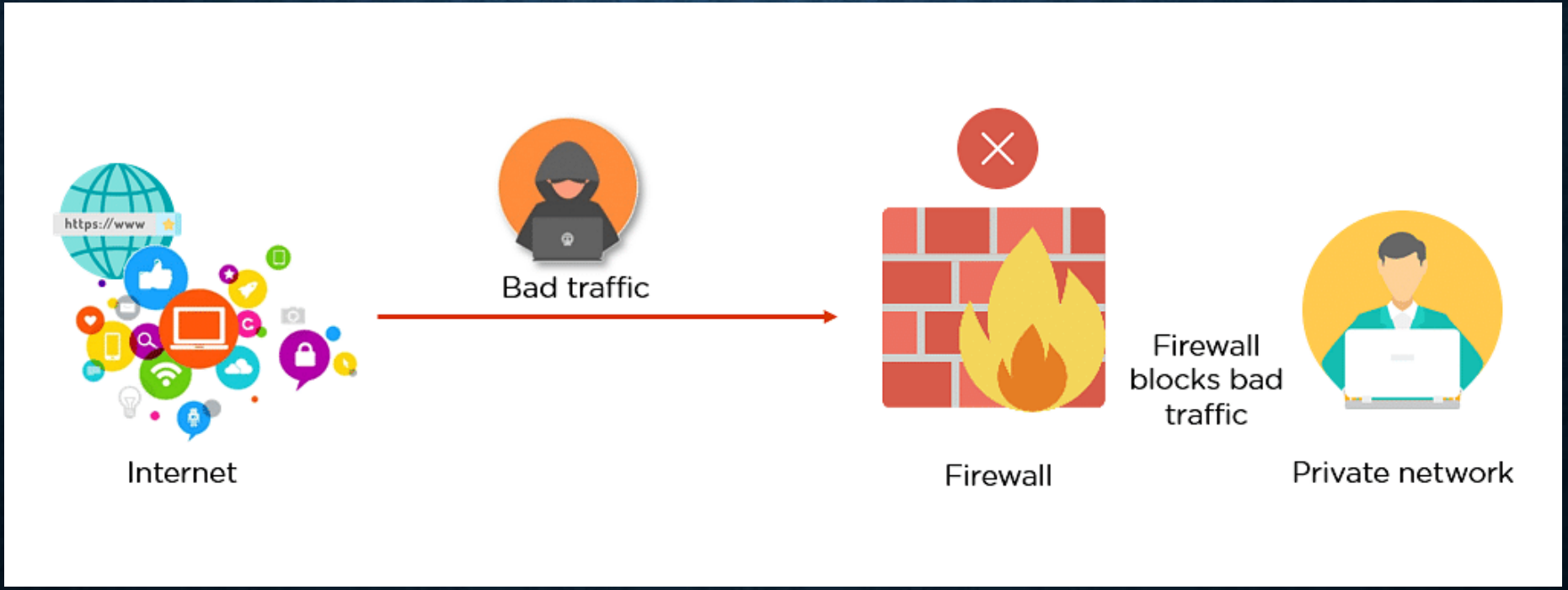
Working of Firewall

A firewall welcomes only those incoming traffic that has been configured to accept. It distinguishes between good and malicious traffic and either allows or blocks specific data packets on pre-established security rules. These rules are based on several aspects indicated by the packet data, like their source, destination, content, and so on. They block traffic coming from suspicious sources to prevent cyberattacks. For example, the image depicted below shows how a firewall allows good traffic to pass to the user's private network.



Working of Firewall

In the example below, the firewall blocks malicious traffic from entering the private network, thereby protecting the user's network from being susceptible to a cyberattack.



Thank you