CHAPTER 6

Firewalls and Intrusion Detection

TESTOUT NETWORK PRO

Firewalls

Section Skill Overview

- Configure Windows Firewall
- Configure Linux iptables
- Configure a host firewall

Key Terms

- Firewall
- Access control list (ACL)

Key Definitions

- **Firewall**: A firewall is a software- or hardware-based network security system that allows or denies network traffic according to a set of rules.
- **Access control list (ACL)**: Firewalls use filtering rules, which are sometimes called access control lists (ACLs), to identify allowed and blocked traffic.

Firewalls

Firewall

- Network security system
- Allows network traffic
- Denies network traffic

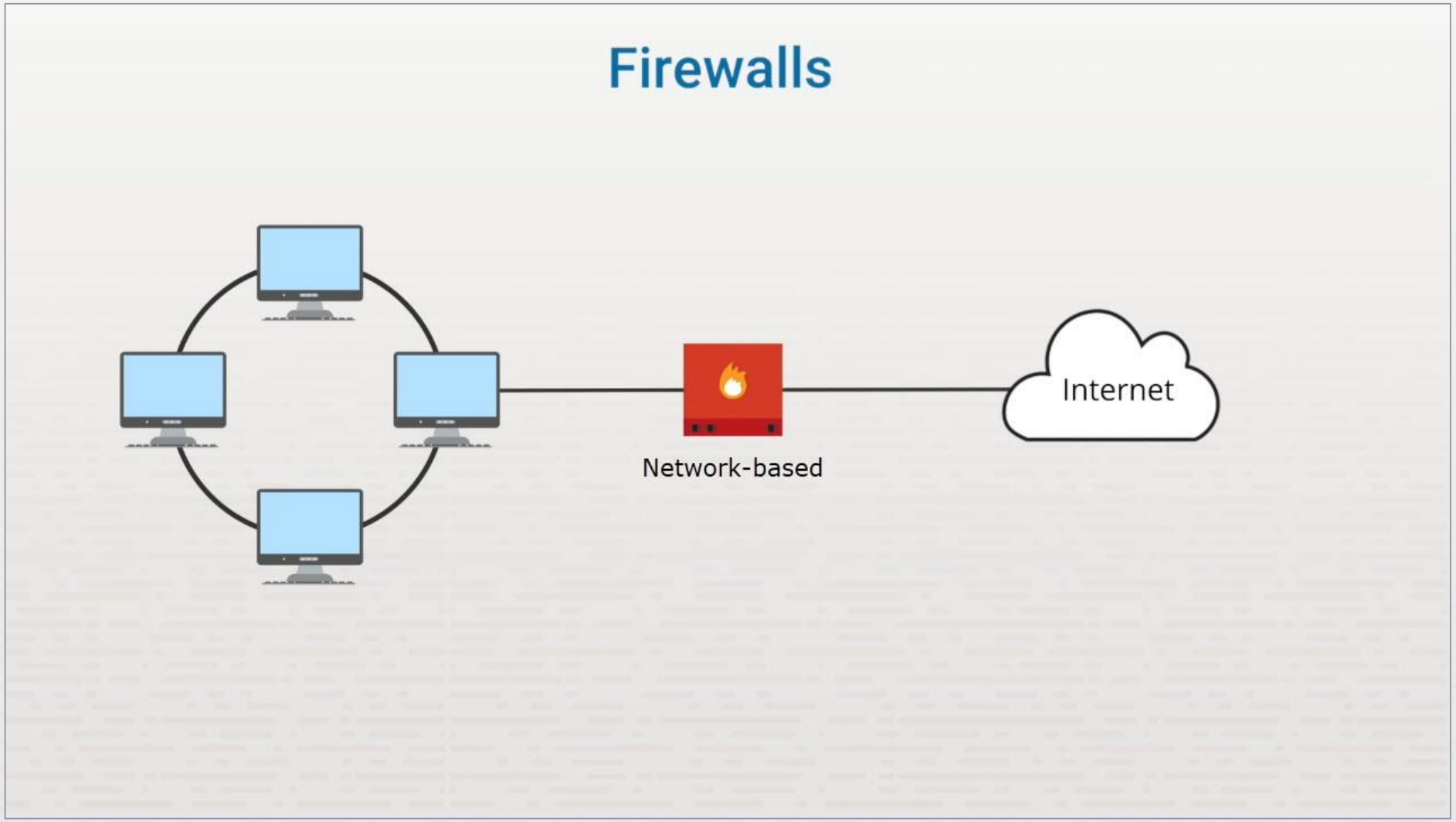
Hardware Firewall

- Protects entire network
- Protects a network segment
- Dedicated hardware
- More expensive
- Best performance

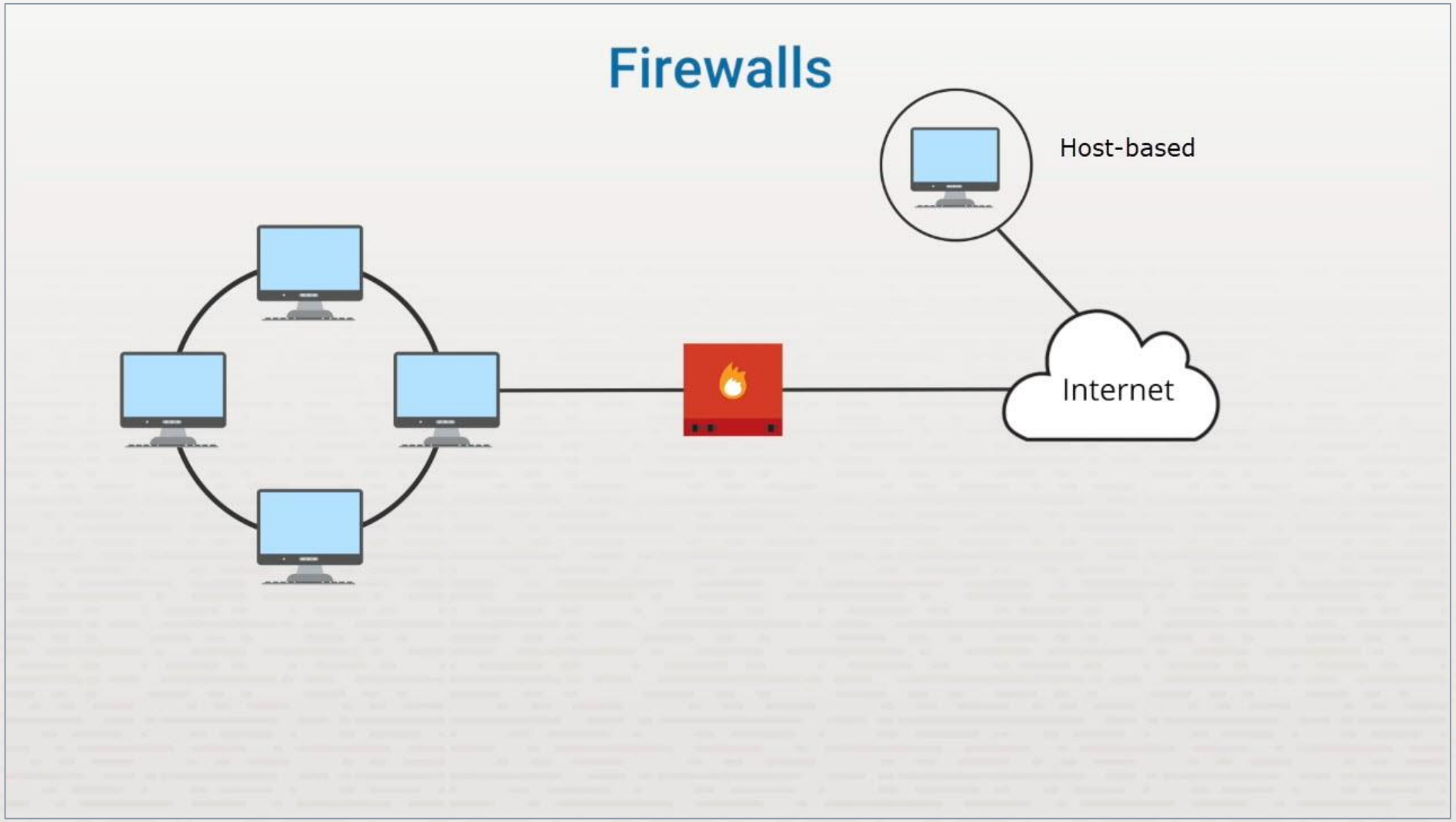
Software Firewall

- Protects a single device
- Less expensive
- Less robust

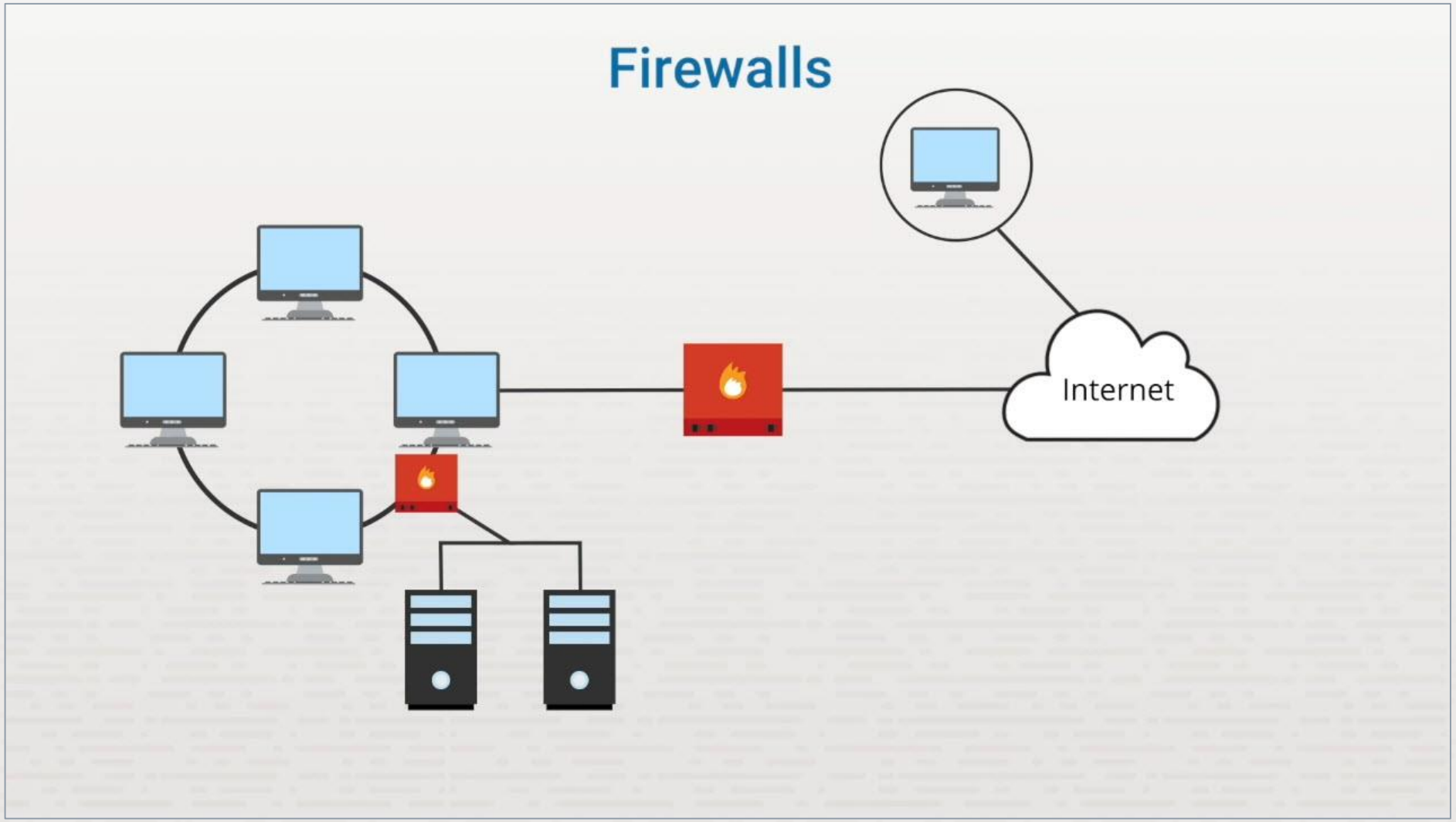
Firewalls



Firewalls



Firewalls



Implicit Deny

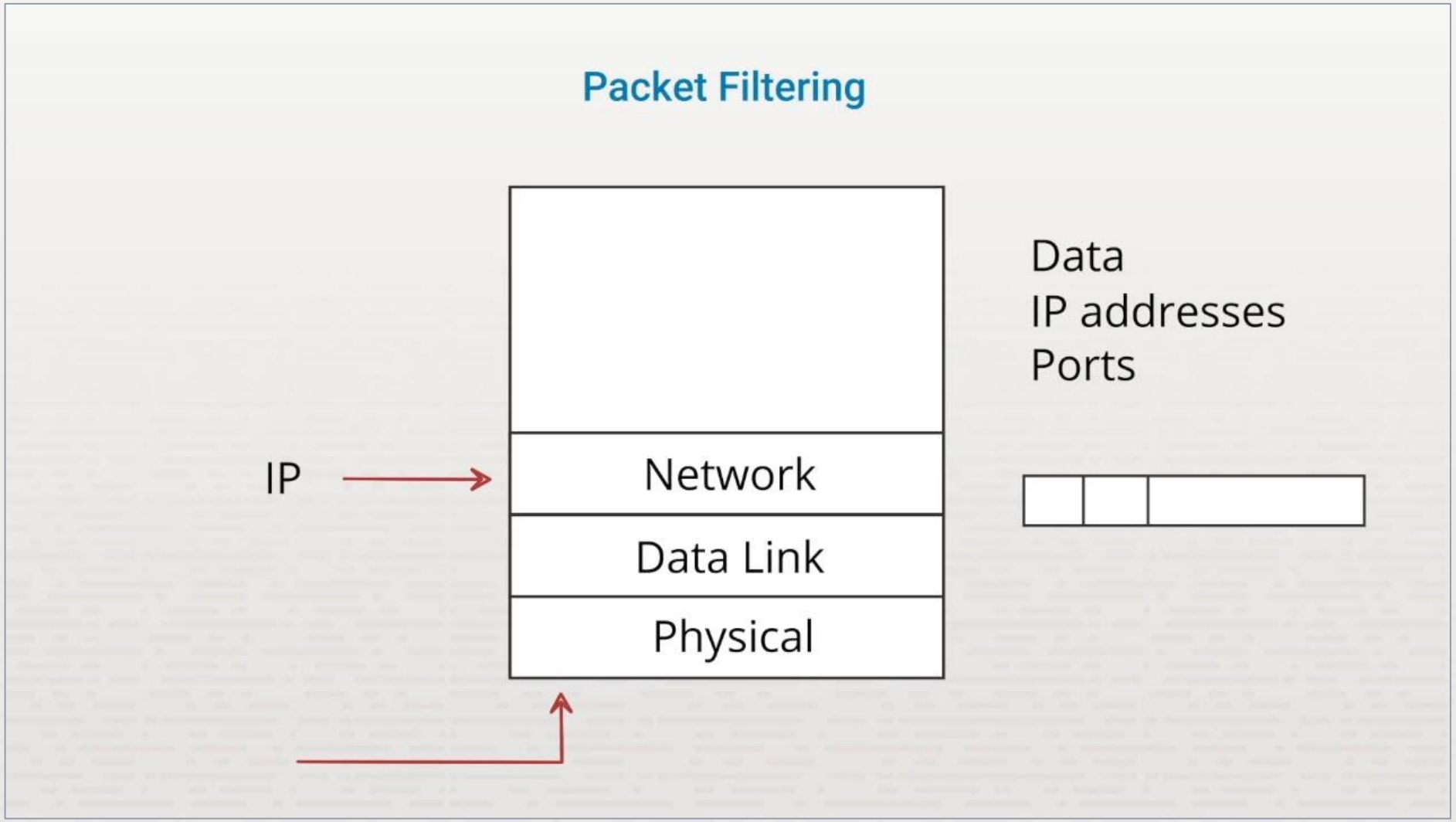
- Blocks non-ACL traffic
- Good security practice

Summary

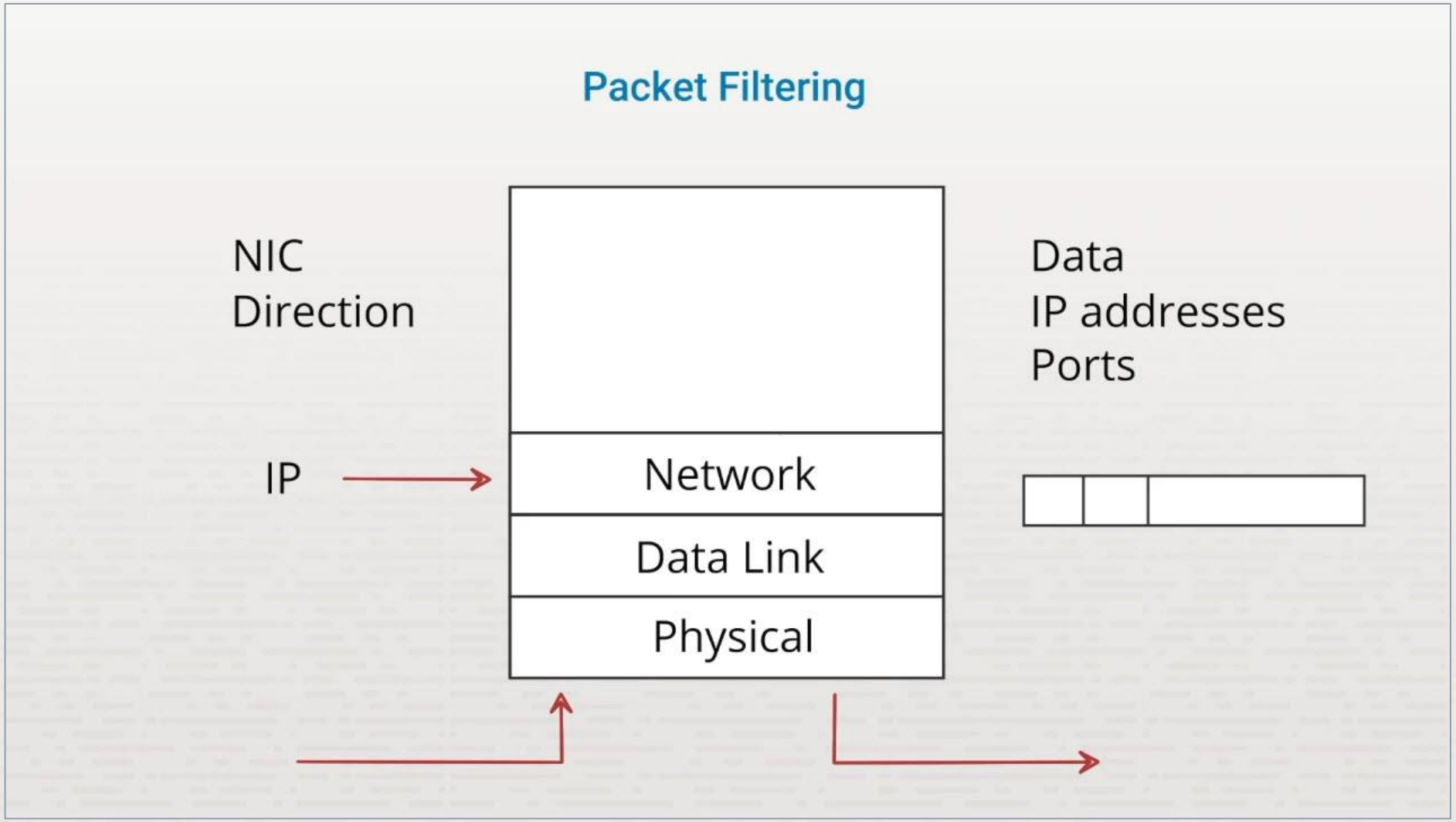
- The importance of firewalls

Firewall Types

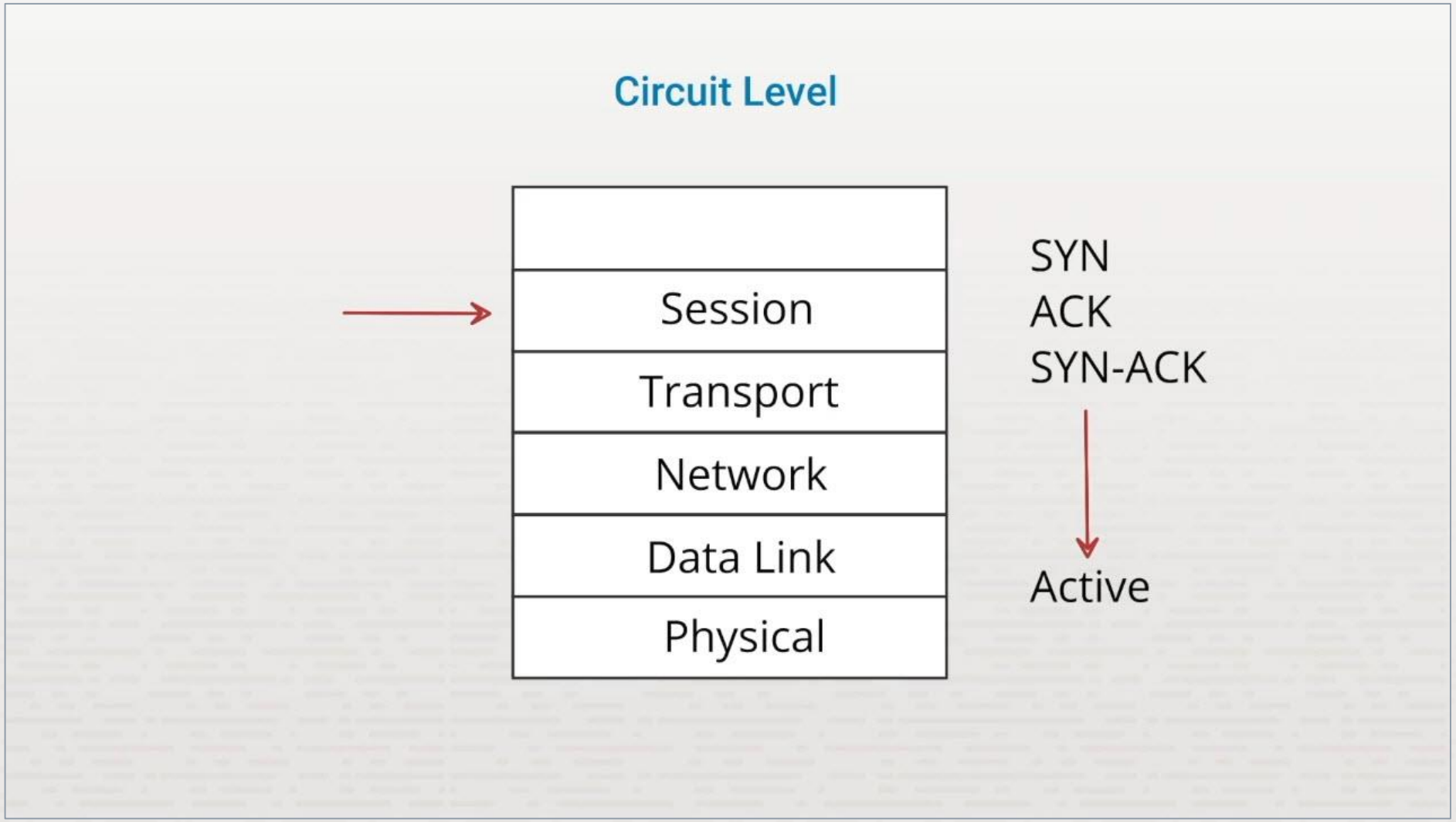
Firewall Types



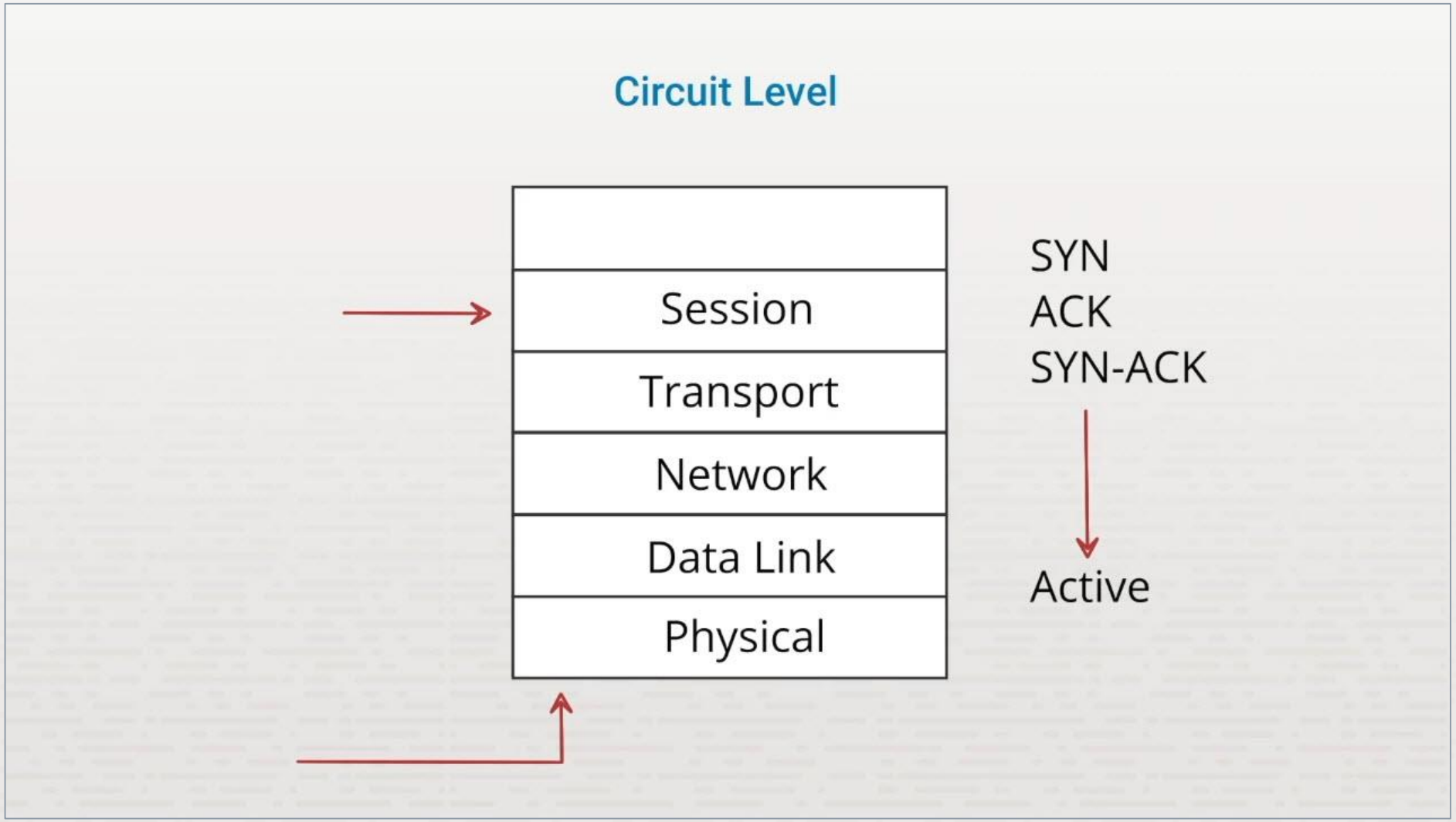
Firewall Types



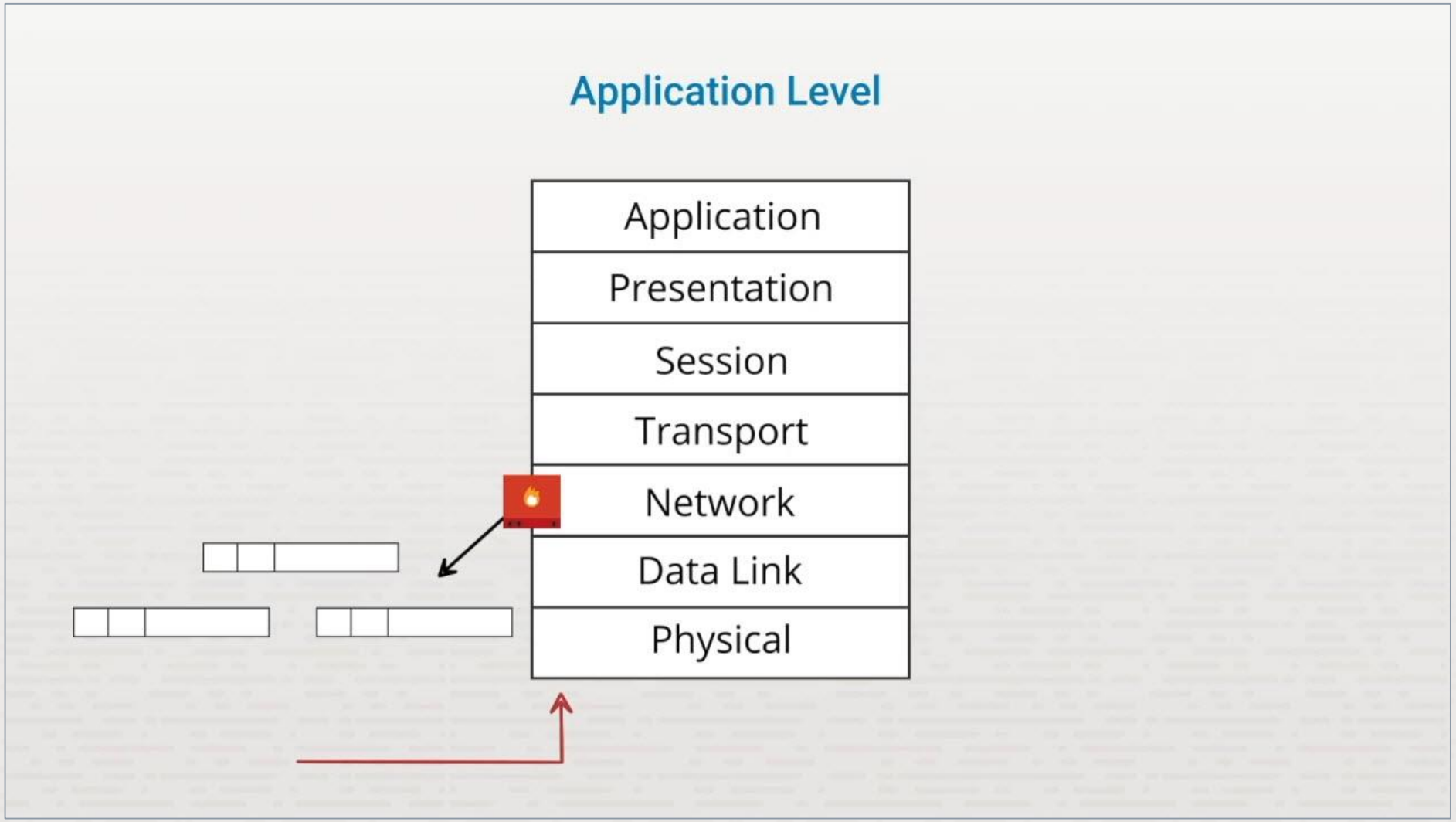
Firewall Types



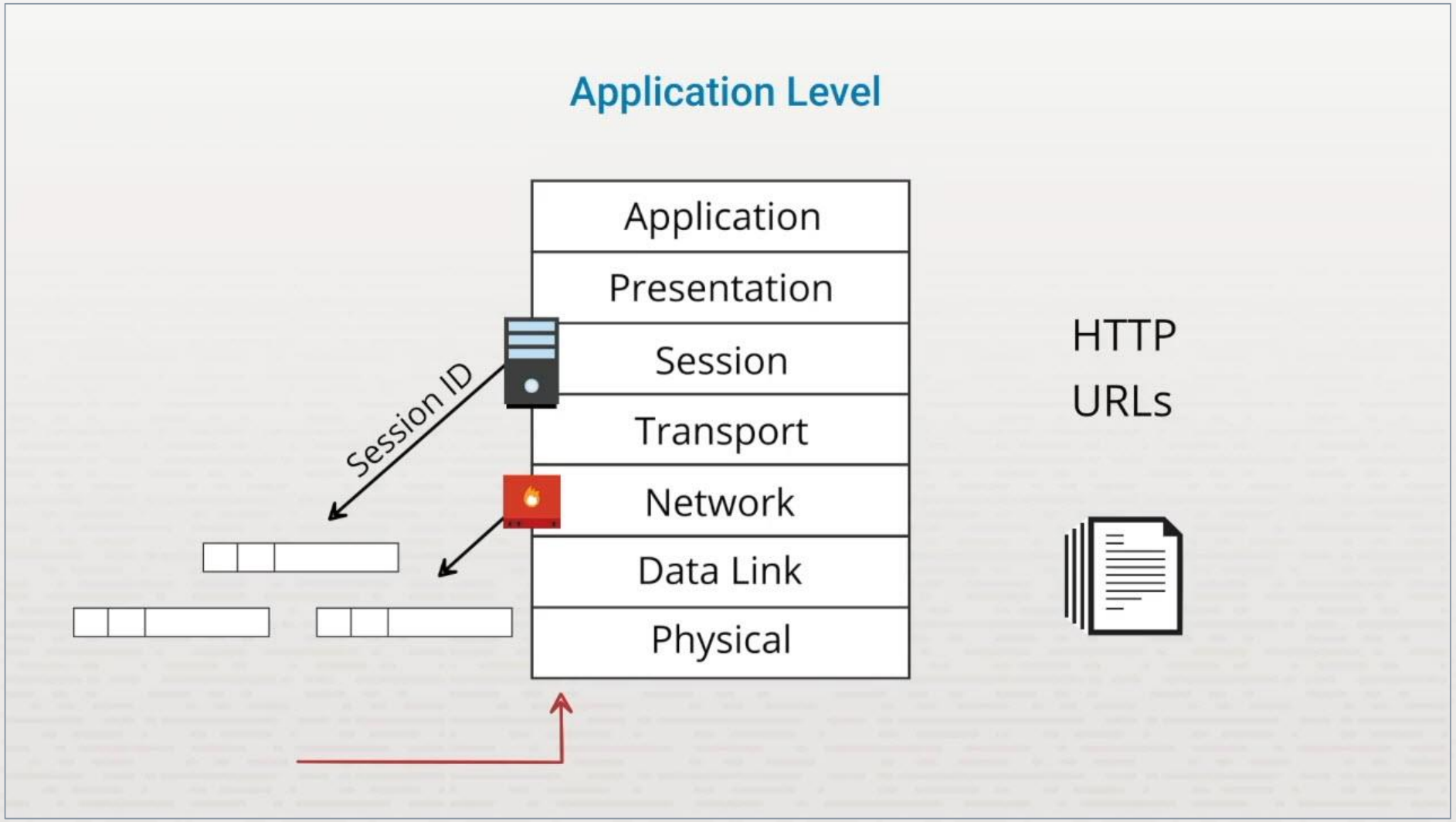
Firewall Types



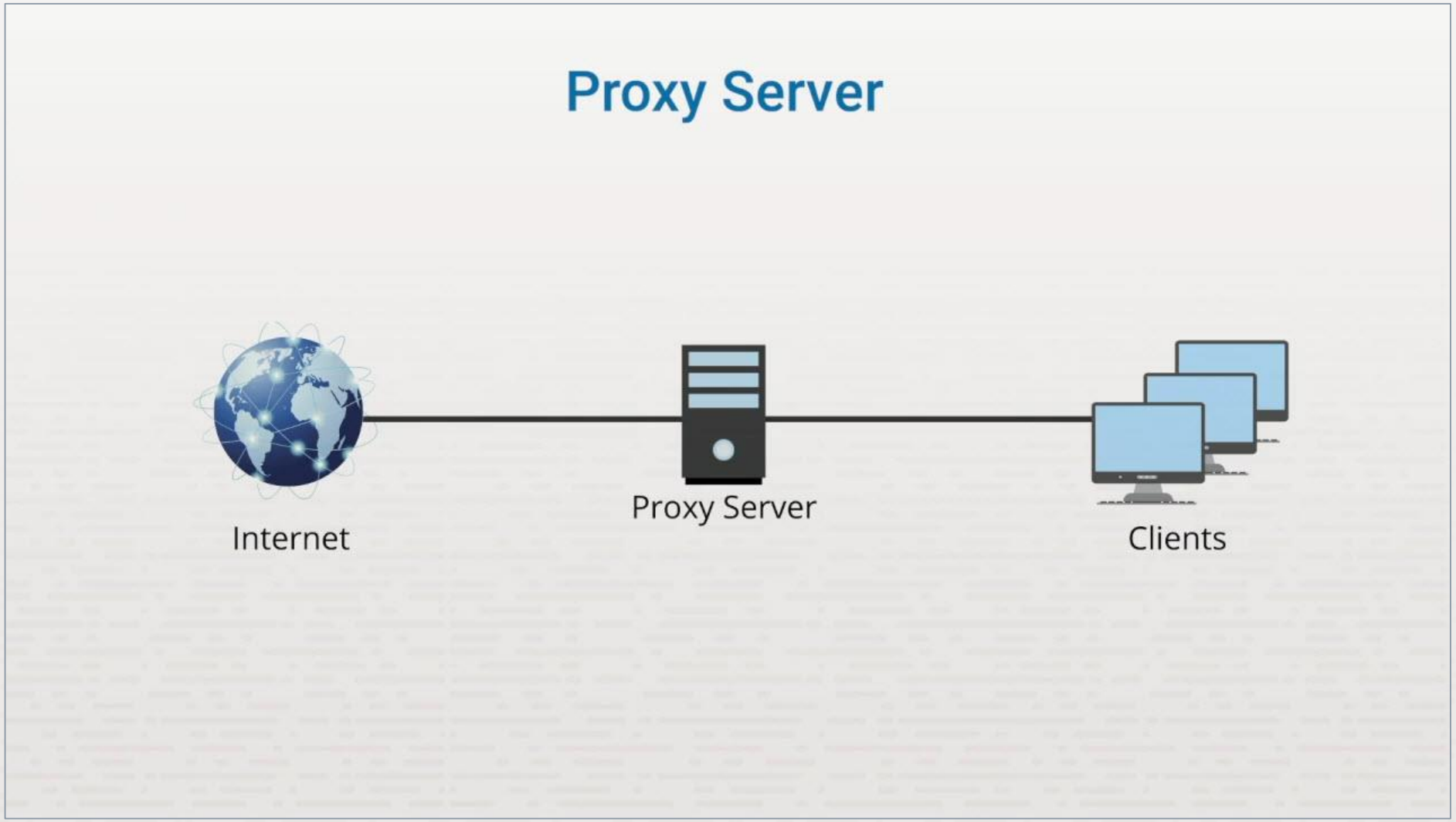
Firewall Types



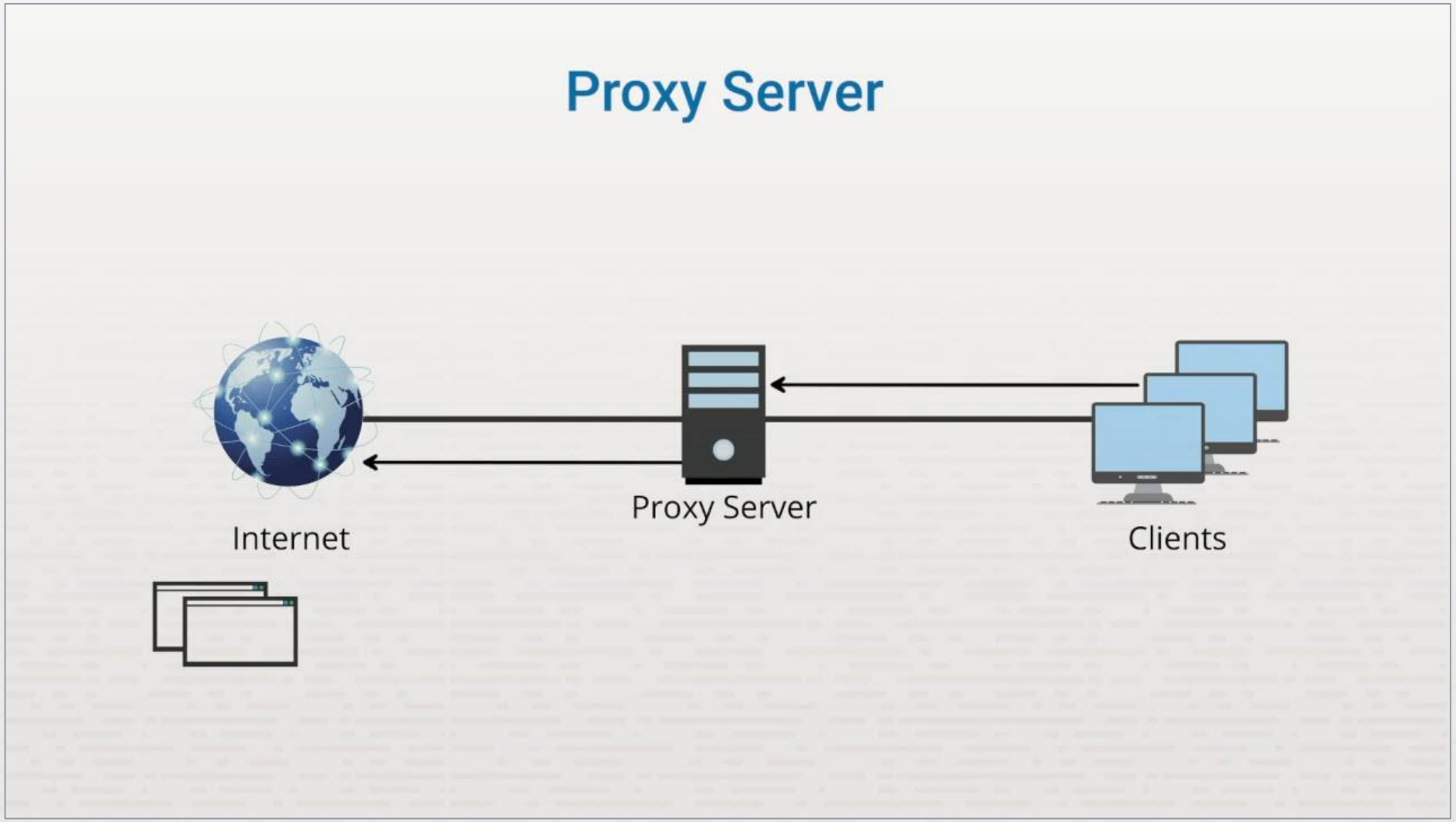
Firewall Types



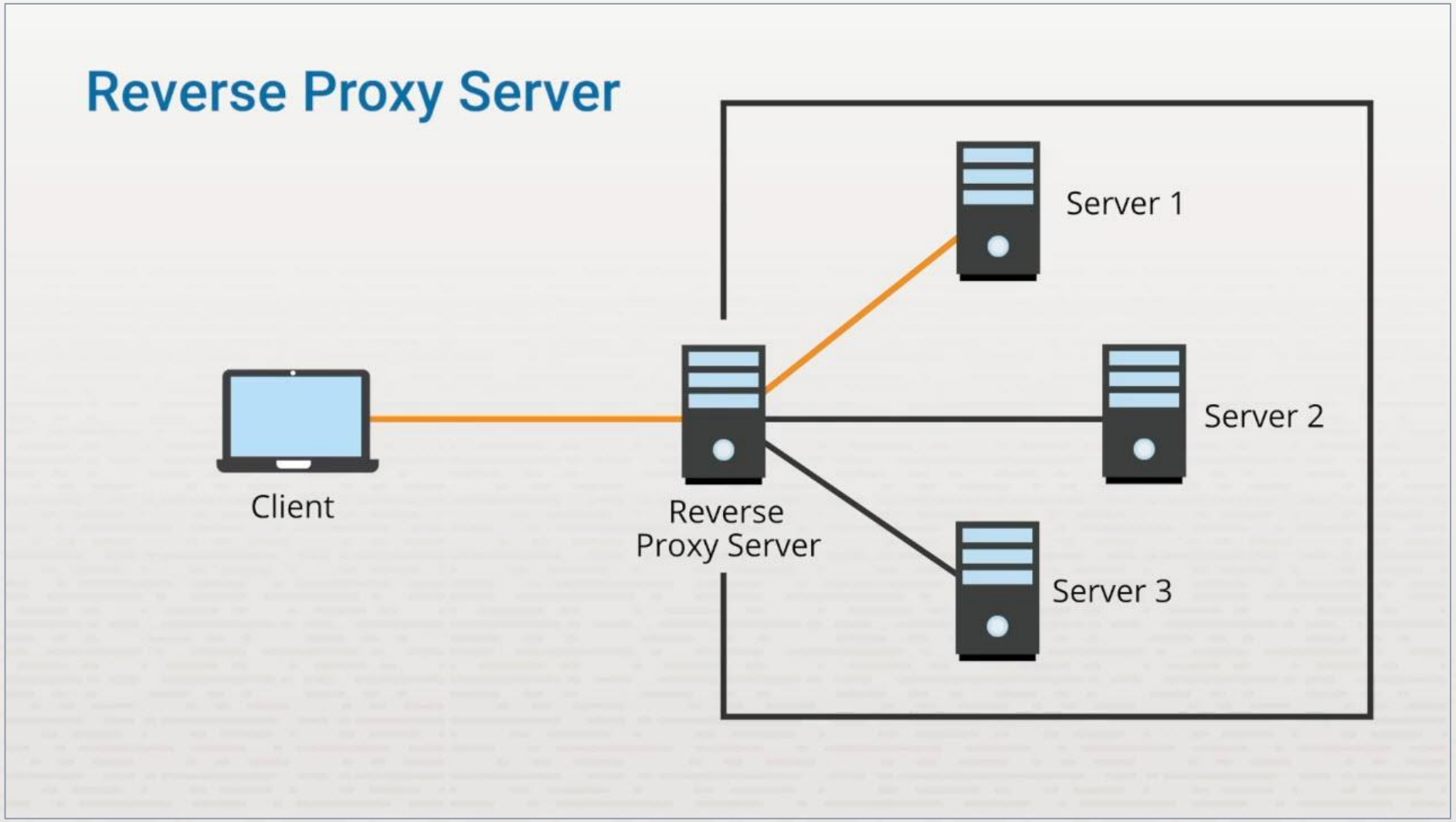
Firewall Types



Firewall Types



Firewall Types



UTM

- Combines security services
- Makes management easier
- Single point of failure

Summary

- Firewall types
- Ways to implement firewalls

In-Class Practice

Do the following labs:

- 6.1.7 Configure a Host Firewall

Class Discussion

- How is a packet-filtering firewall different from a circuit-level gateway?
- Why is a packet-filtering firewall a stateless device?
- Which types of criteria can an Application layer gateway use for filtering?
- What is the difference between a proxy and a reverse proxy?

6.2 FIREWALLS AND INTRUSION DETECTION

Firewall Design and Implementation

TESTOUT NETWORK PRO

Section Skill Overview

- Configure network security appliance access
- Configure a security appliance
- Configure a perimeter firewall
- Create firewall ACLs

Key Terms

- Unified threat management (UTM)
- Screened subnet
- Access control list (ACL)

Key Definitions

- **Unified threat management (UTM):** A UTM appliance, combines several layers of security and networking services into one solution. It is also known as an all-in-one appliance.
- **Screened subnet:** A buffer network (or subnet) that sits between the private network and an untrusted network (such as the internet.) Also known as an all-in-one appliance.
- **Access control list (ACL):** ACLs are filtering rules firewalls use to identify which traffic to allow and which to block.

Unified Threat Management (UTM) Appliances

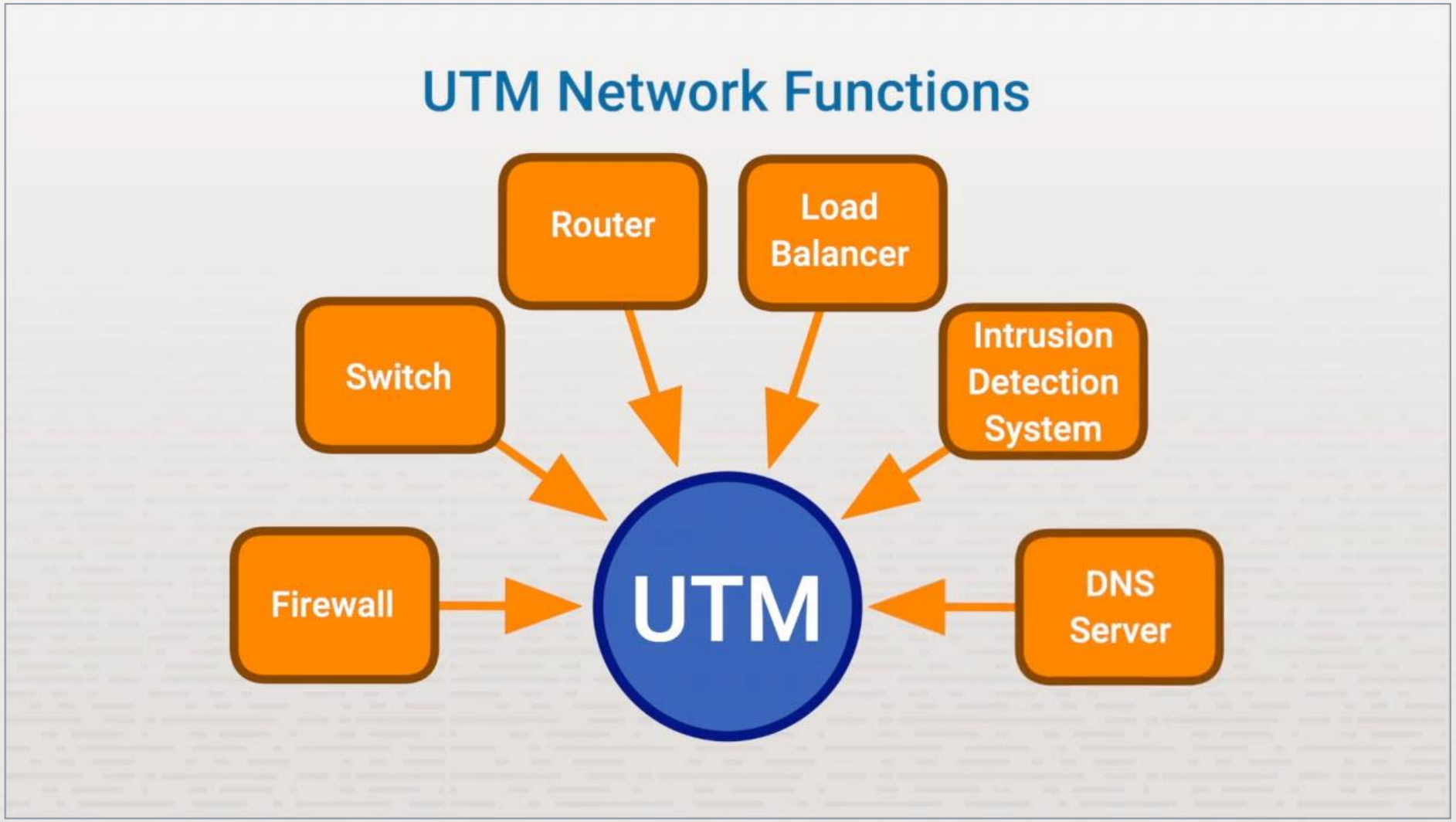
UTM Benefits

- Small to mid-sized
- Startup companies
- Limited budgets
- Limited office space
- Remote branch

UTM Firewall

- Proxy-based inspection
  - Buffers incoming traffic
  - Holds data for inspection
  - Used for high data integrity
- Flow-based inspection
  - No buffering
  - Examines each packet
  - High processing speed

Unified Threat Management (UTM) Appliances



Security Functions

- Web filters
- Email filters
- VPN
- Application control
- DNS filters
- DDoS mitigation
- Data leak prevention

Summary

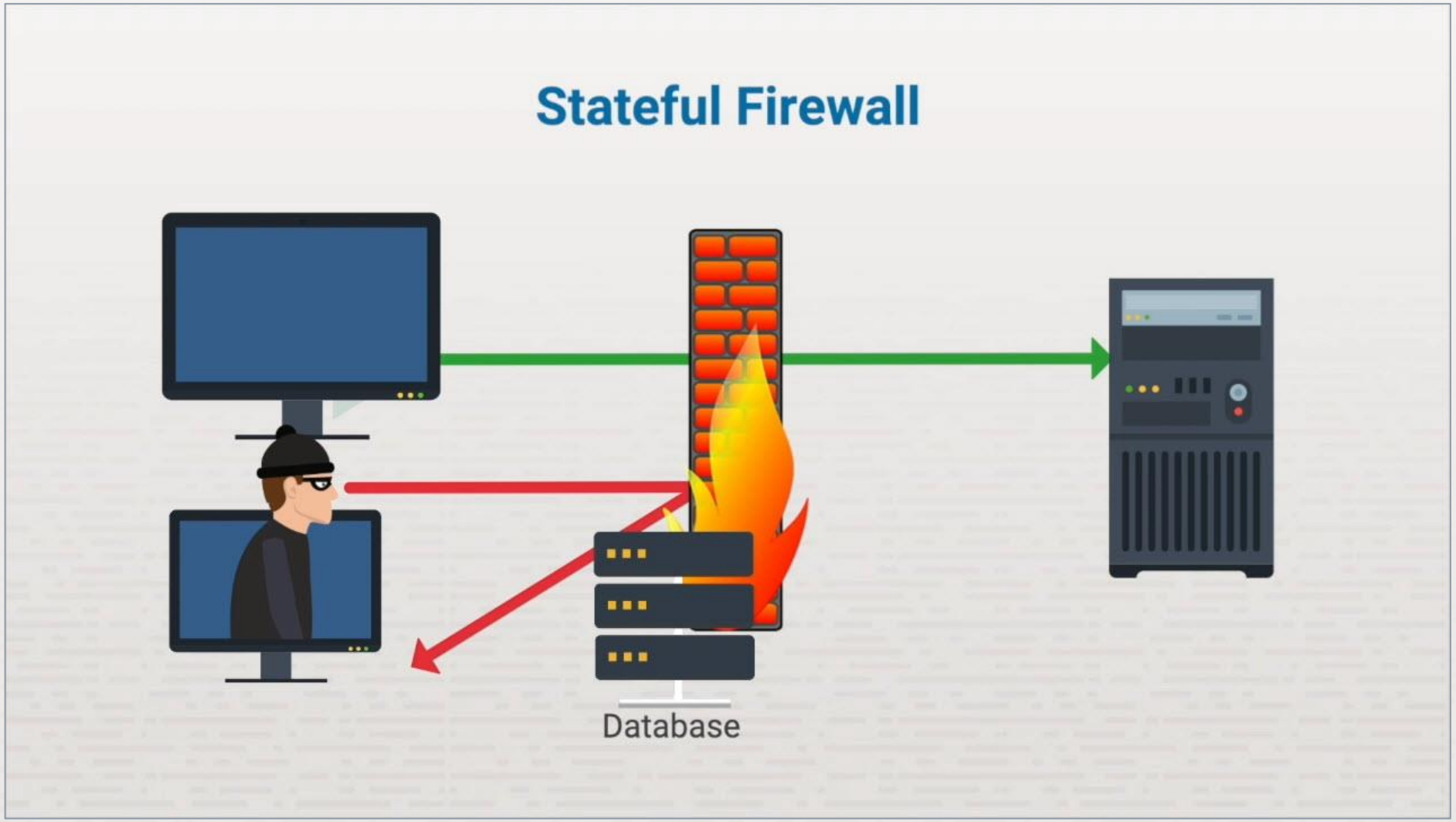
- UTM benefits
- UTM functions
- UTM network security

Firewall Network Design Principles

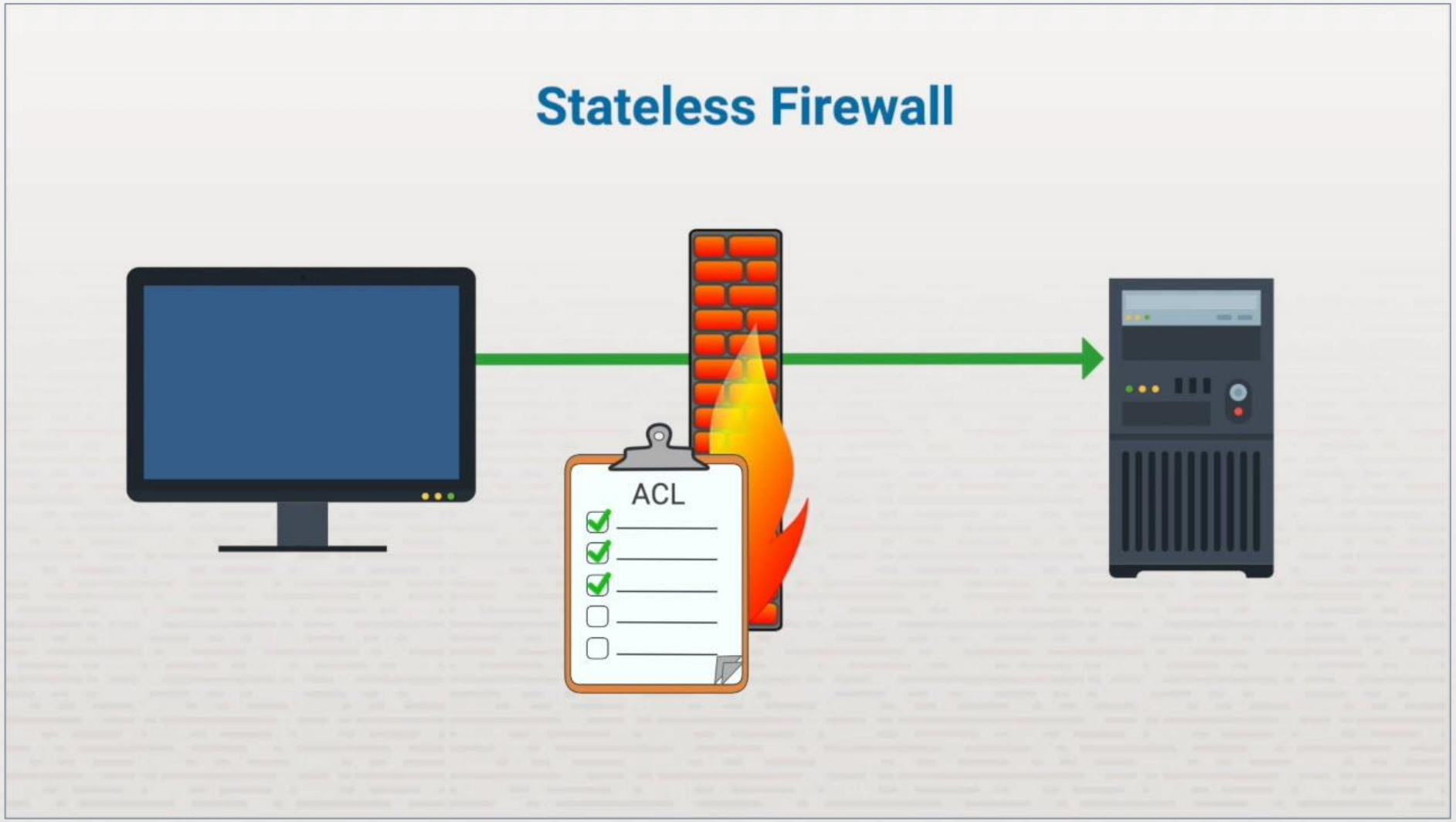
Firewall Features

- Encryption
- User authentication
- Filtering at higher layers
- Intrusion detection system
- Stateful or stateless

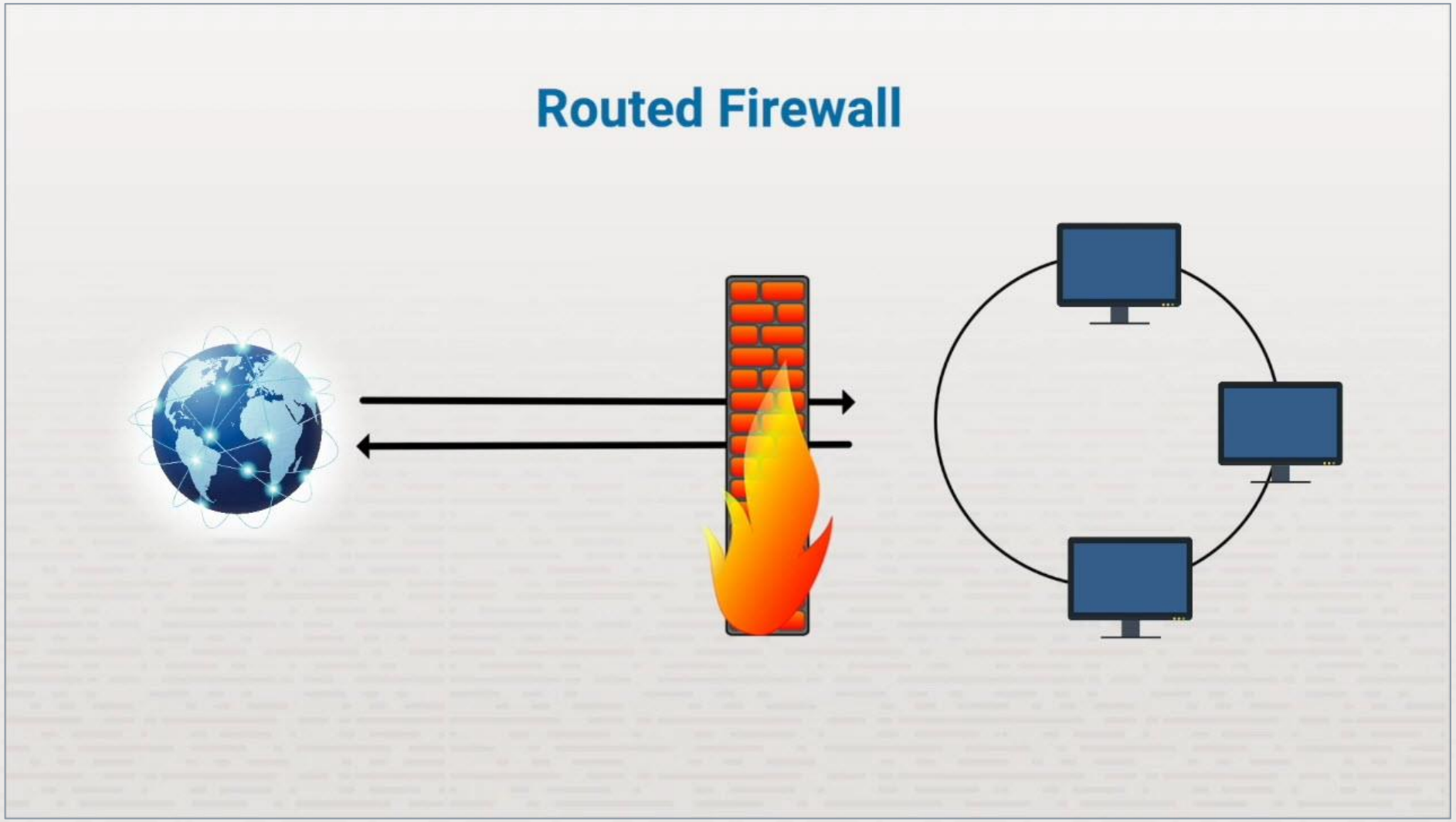
Firewall Network Design Principles



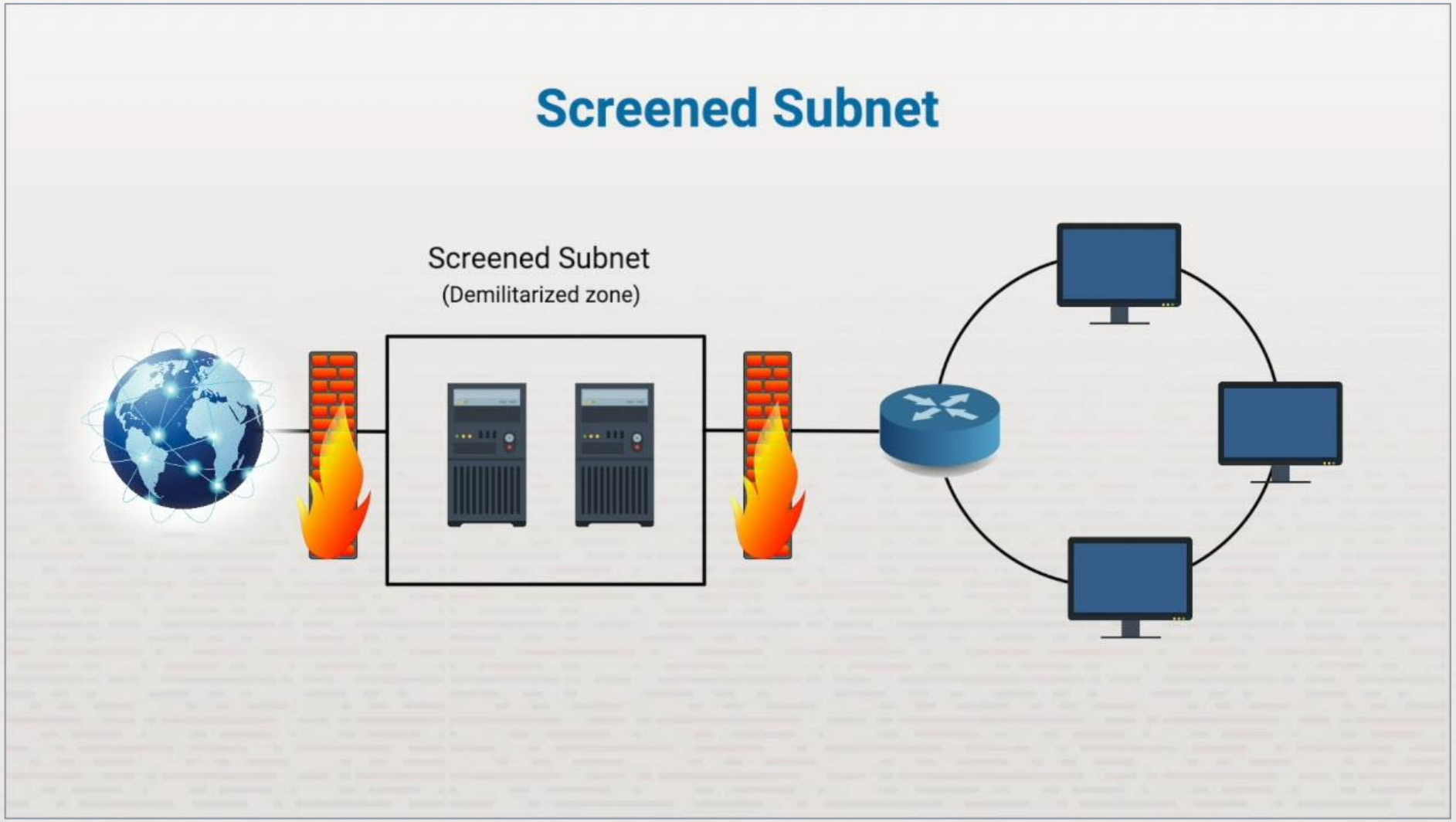
Firewall Network Design Principles



Firewall Network Design Principles



Firewall Network Design Principles



Firewall Configuration

- Change username, password
  - Use complex passwords
- Not too restrictive
- Not too lenient

Summary

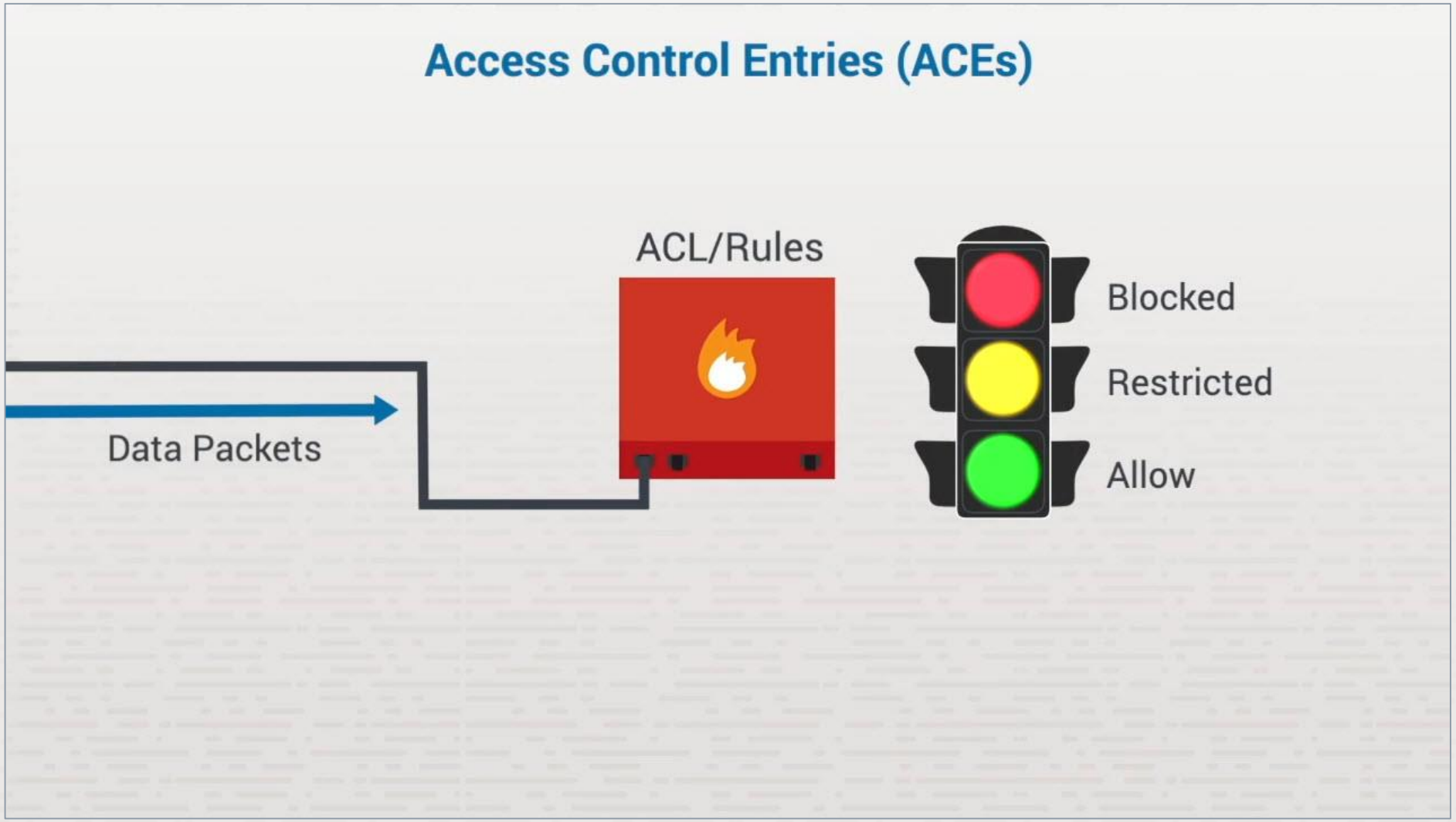
- Firewall features
- Firewall placement
- Firewall configuration

Firewall ACLs

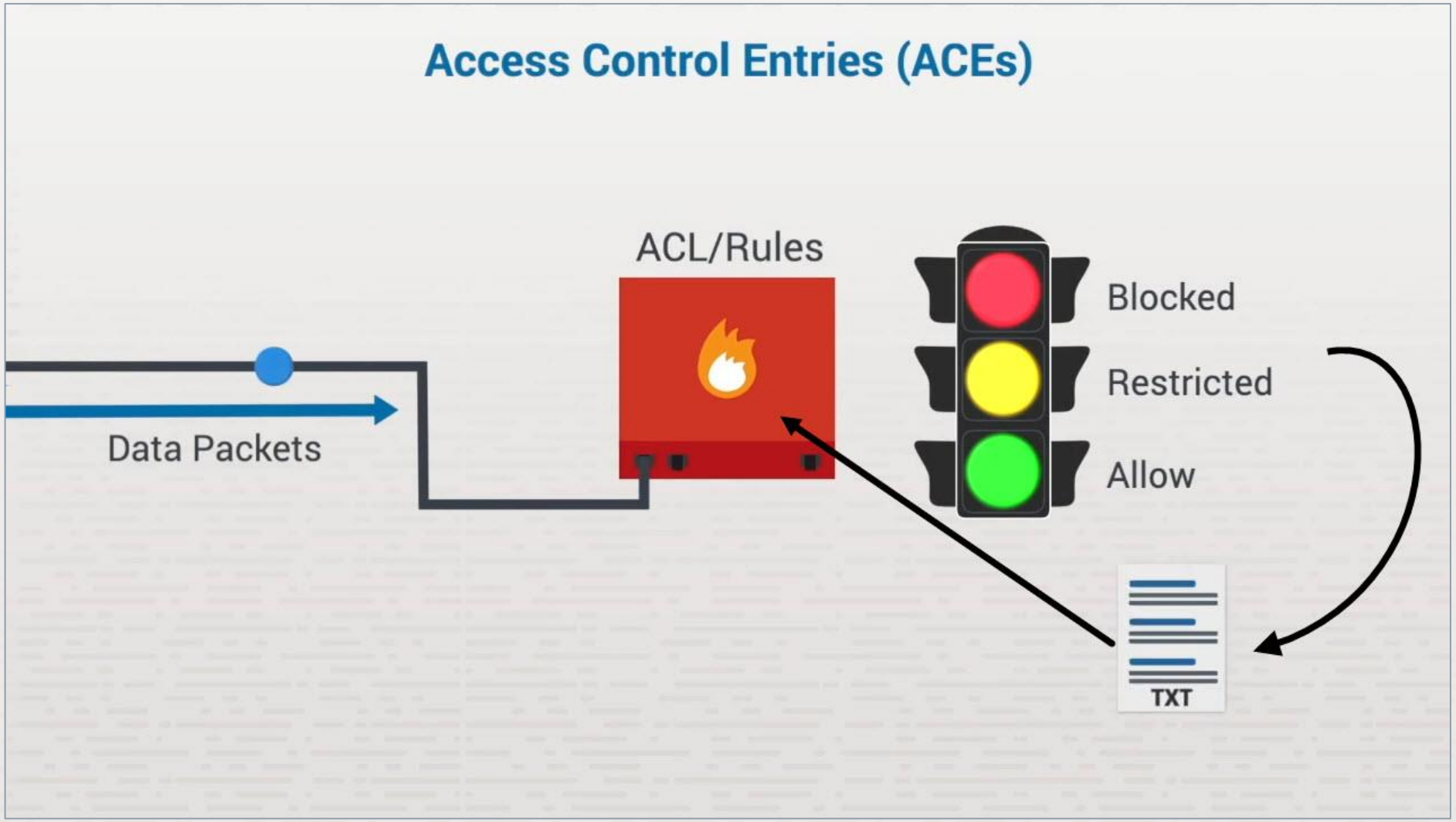
ACL Benefits

- Security
- Traffic control
- Network performance

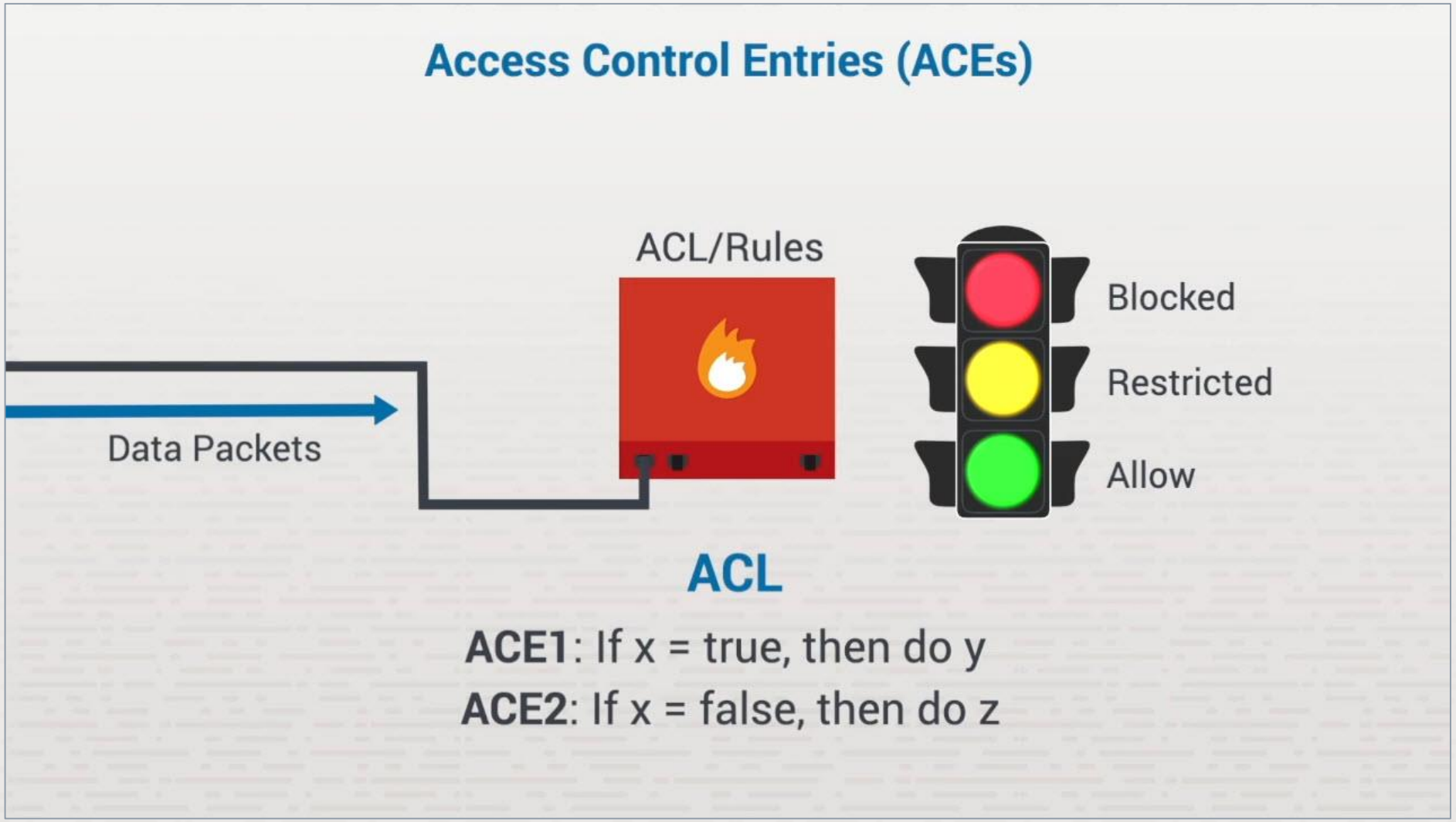
Firewall ACLs



Firewall ACLs



Firewall ACLs



Extended ACL Filters

- Source address
- Destination address
- Protocol type
- Ports

Deny Any

- Place at end of ACL
- Prevents unwanted traffic
- Built into Cisco devices

Summary

- ACL benefits
- Access control entries (ACEs)

In-Class Practice

Do the following labs:

- 6.2.5 Configure Network Security Appliance Access
- 6.2.6 Configure a Security Appliance
- 6.2.8 Configure a Perimeter Firewall

Class Discussion

- What are the benefits of a UTM?
- What is the difference between a stateful and a stateless firewall?
- What is the difference between a standard ACL and an extended ACL?
- Filtering rules firewalls use to identify which traffic to allow and which to block.

Screened Subnets

Section Skill Overview

- Configure a screened subnet

Key Terms

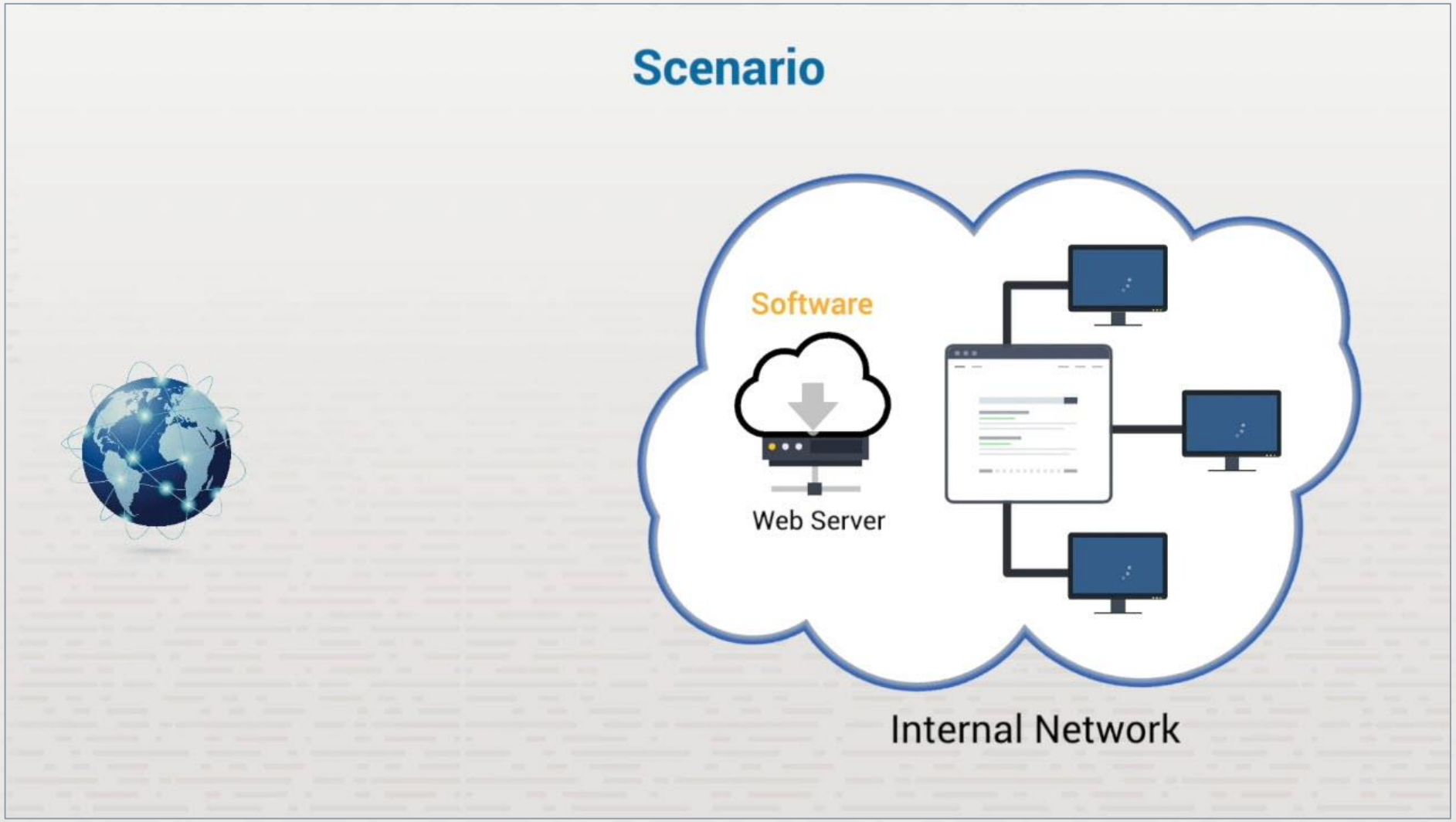
- Screened subnet

Key Definitions

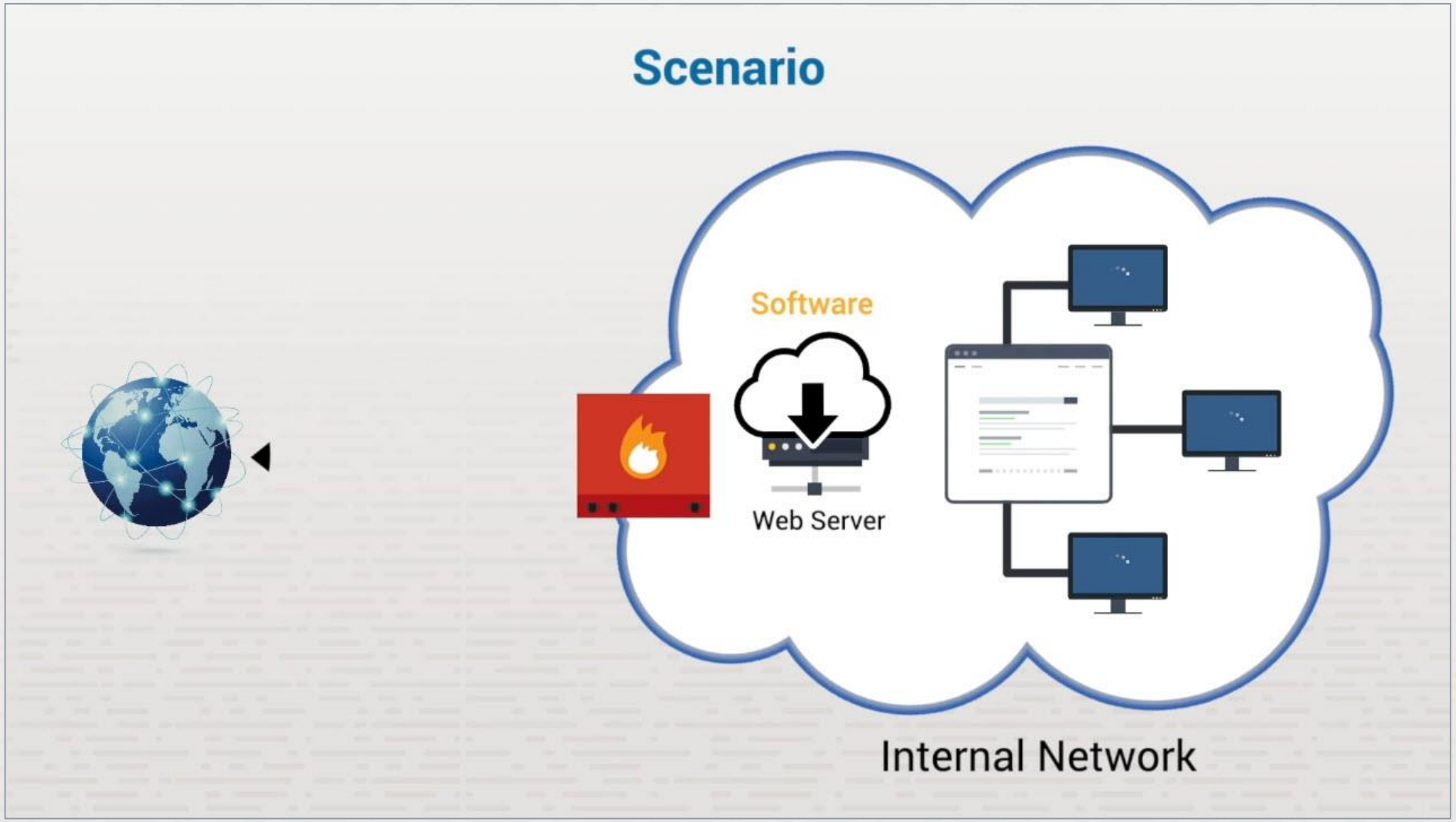
- **Screened subnet:** A buffer network (or subnet) that is located between a private network and an untrusted network, such as the internet.

Screened Subnets

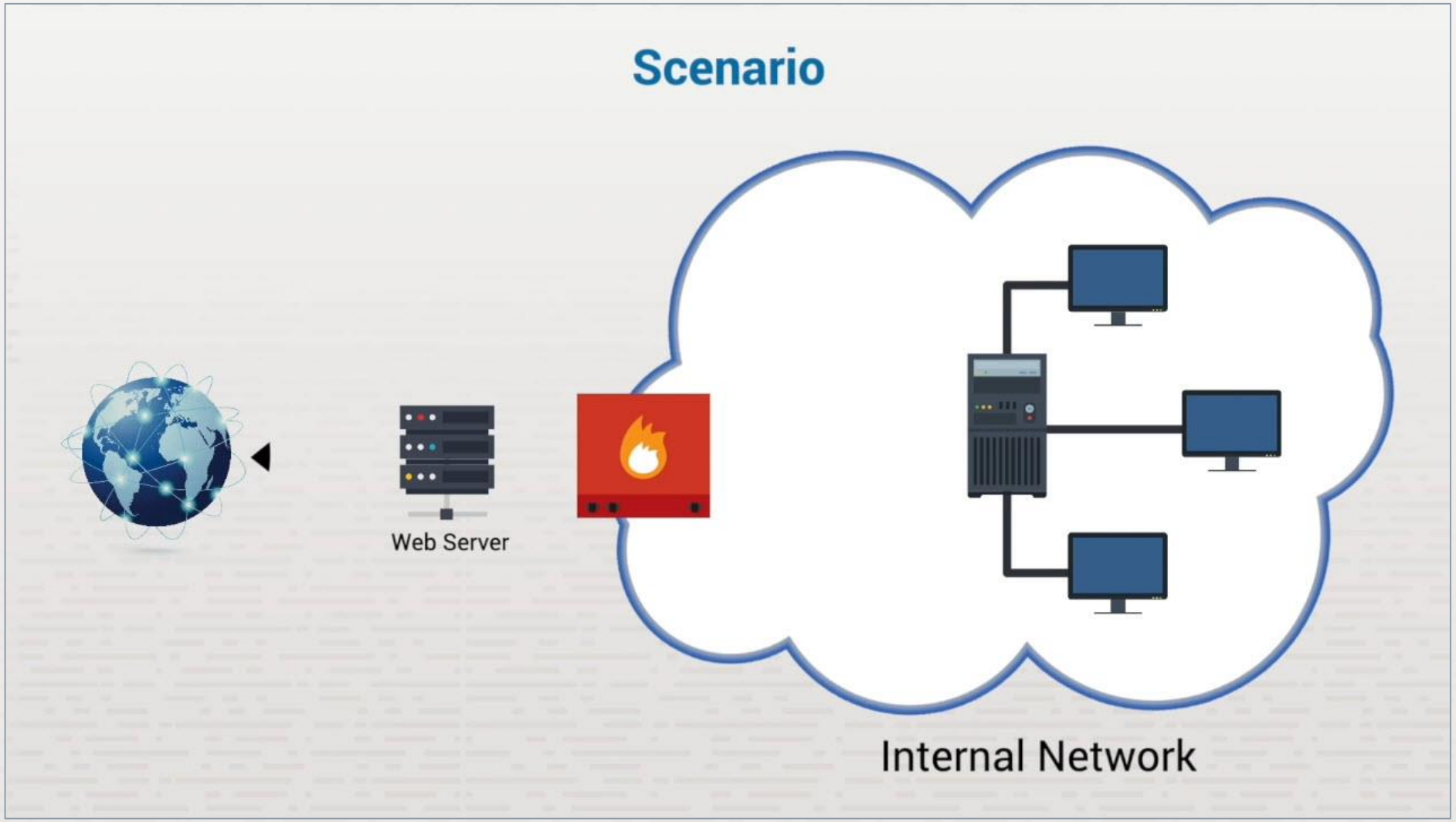
Screened Subnets



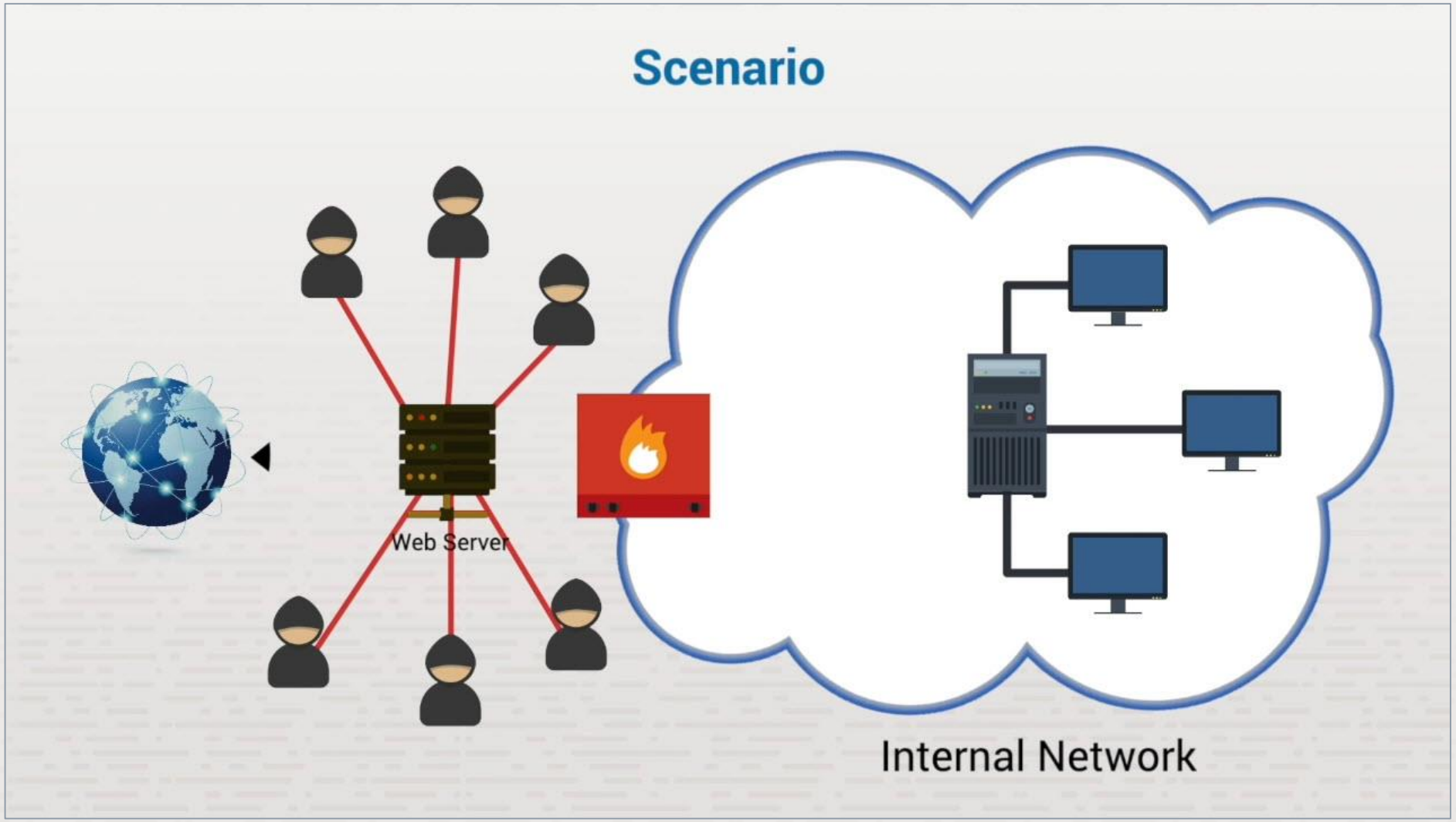
Screened Subnets



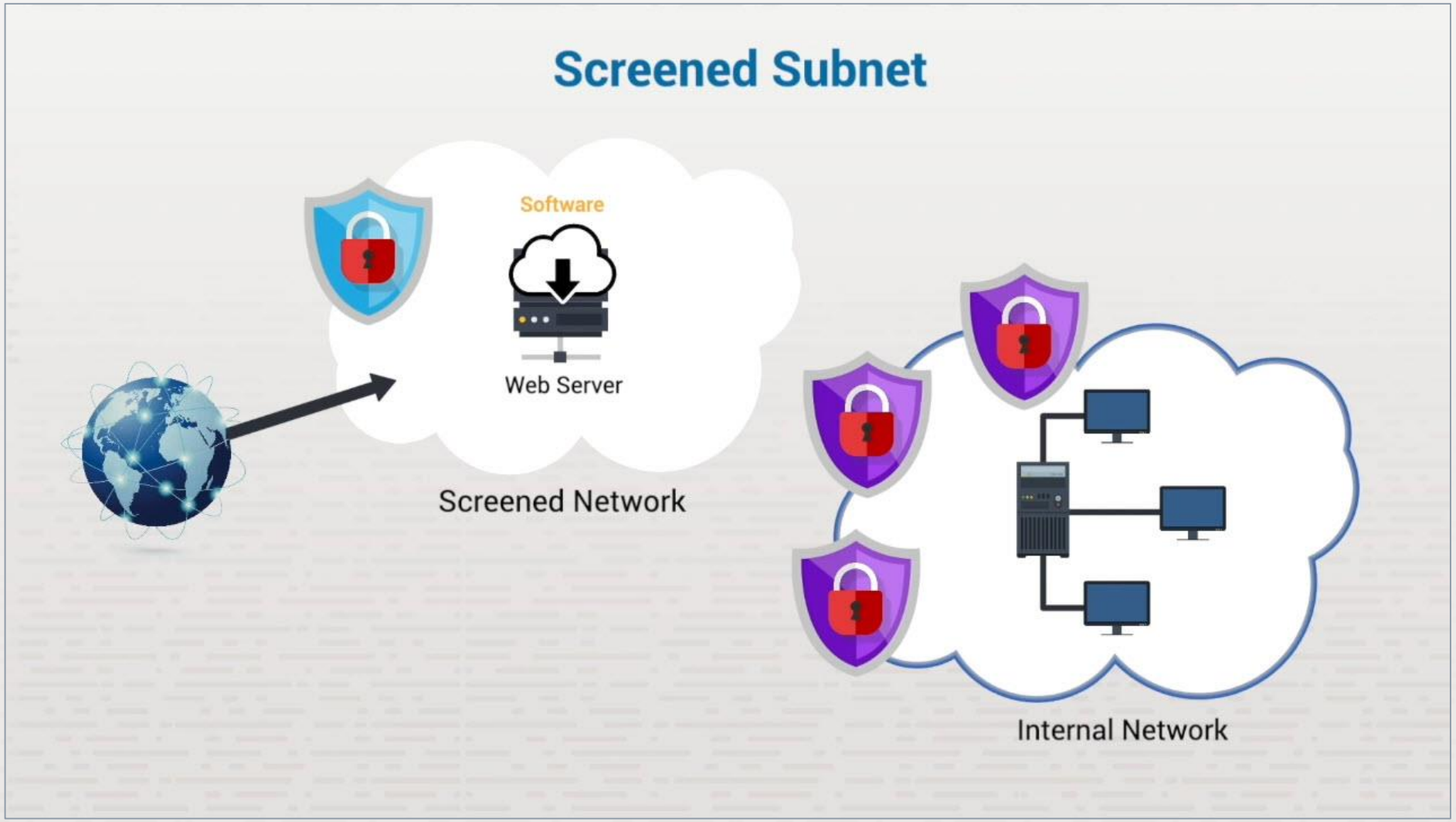
Screened Subnets



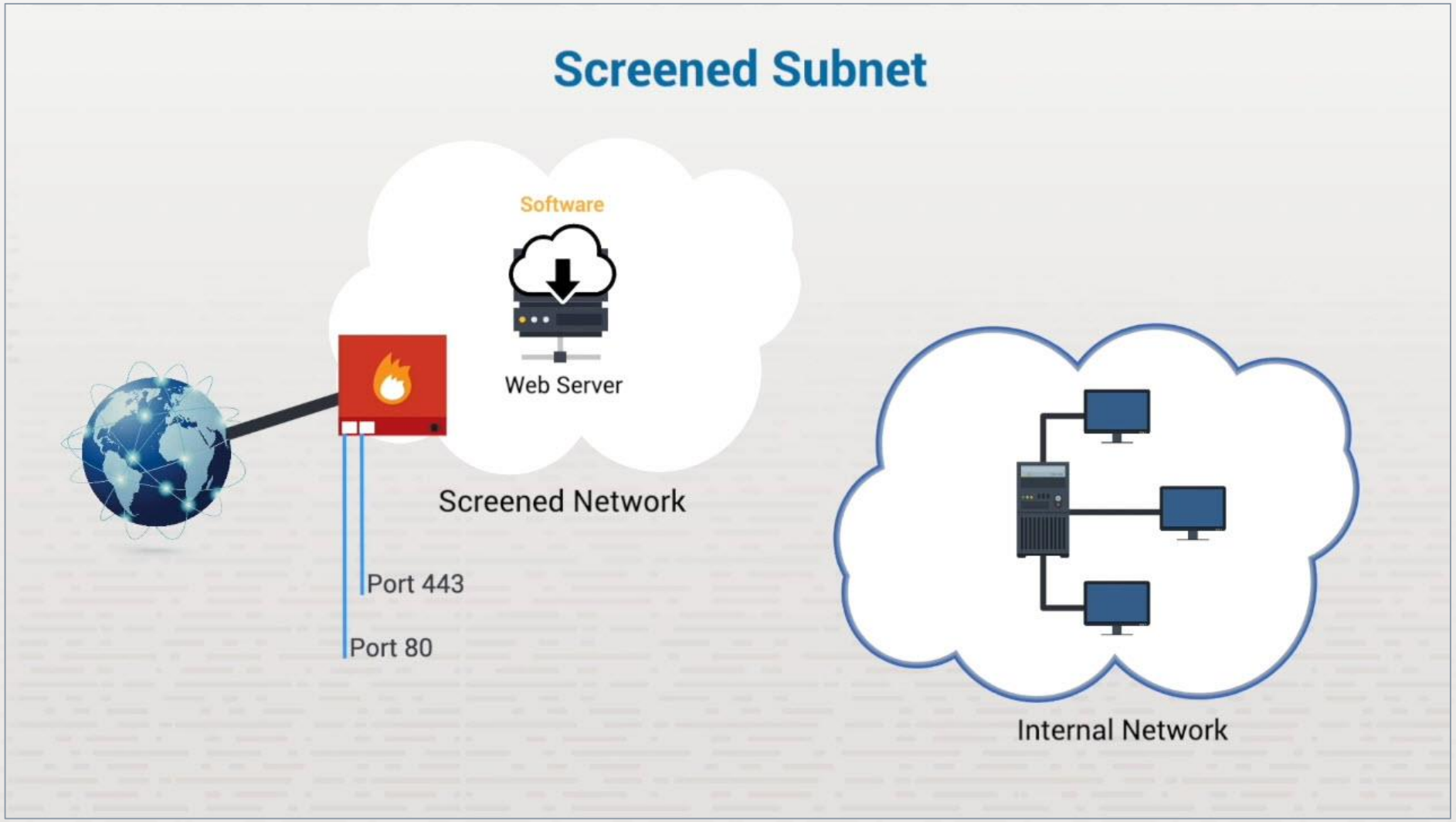
Screened Subnets



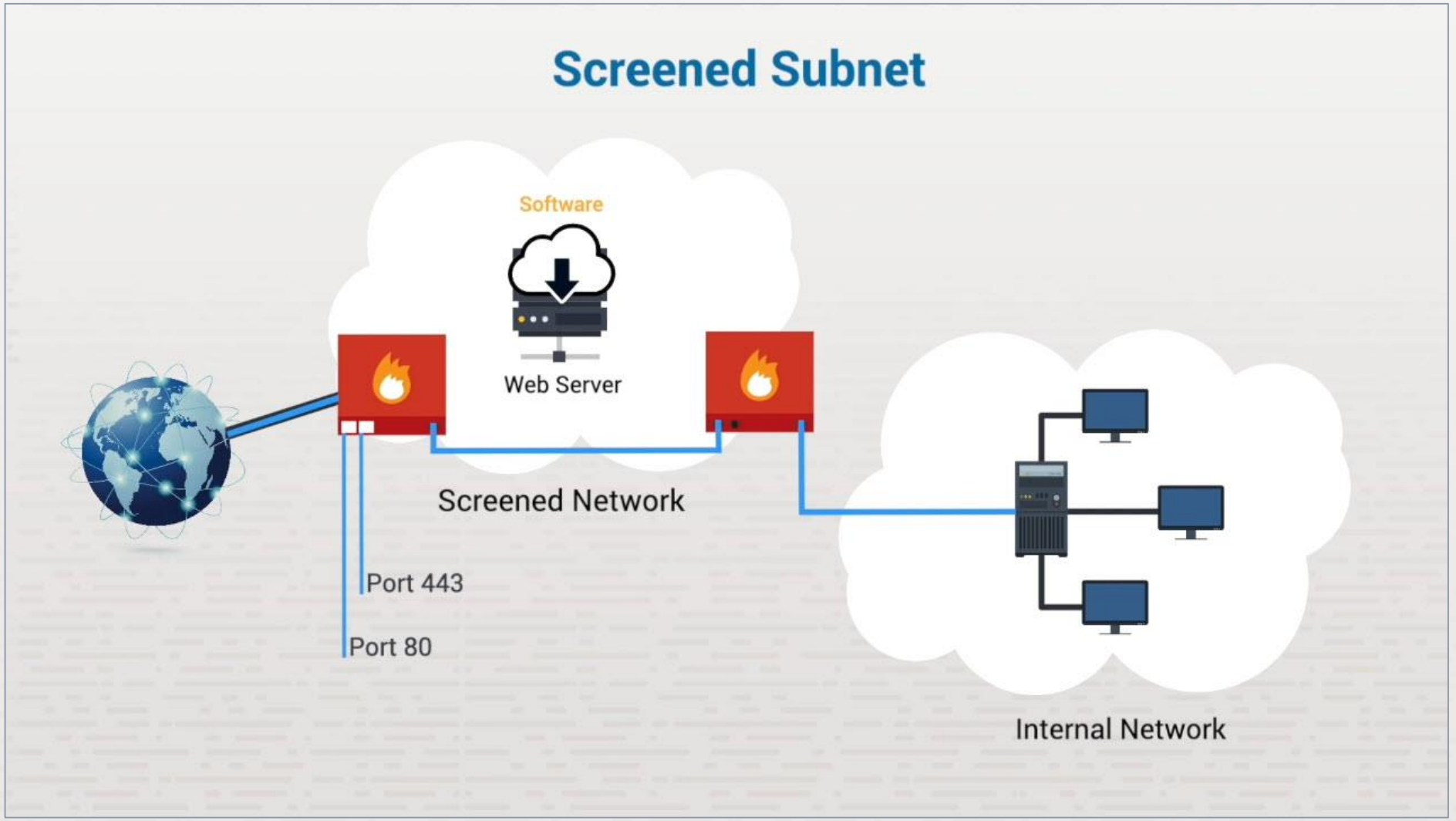
Screened Subnets



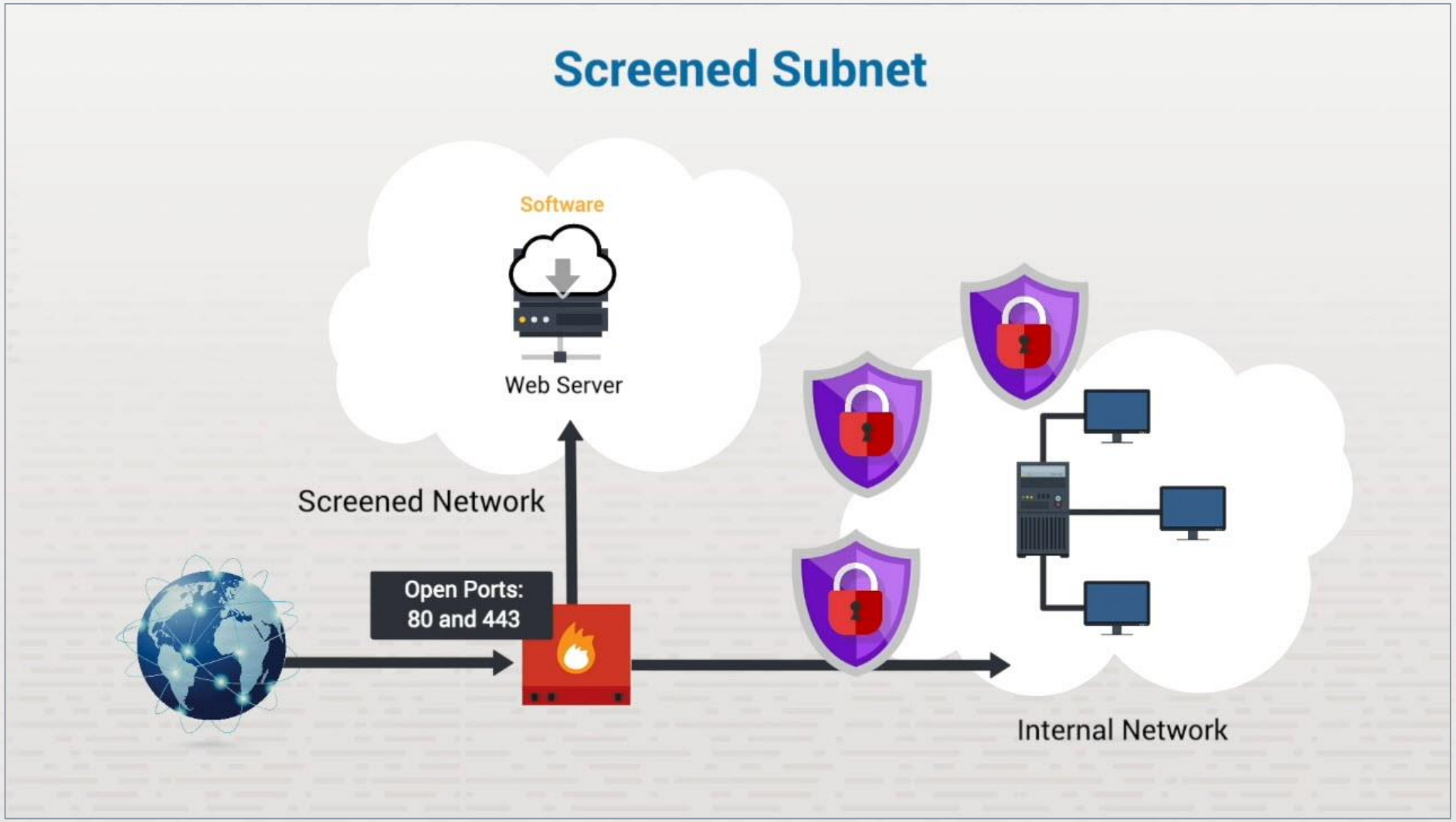
Screened Subnets



Screened Subnets



Screened Subnets



Summary

- Screened subnet
  - Two firewall solution
  - Single firewall solution

In-Class Practice

Do the following labs:

- 6.3.4 Configure a Screened Subnet (DMZ)

Class Discussion

- What is the typical configuration for a screened subnet implemented as a dual-homed gateway?
- What are the functions of the two firewalls in a screened subnet?
- Which type of computer might exist inside a screened subnet?

Intrusion Detection and Prevention

Section Skill Overview

- Implement intrusion detection
- Implement intrusion prevention

Key Terms

- Intrusion detection system (IDS)
- Intrusion prevention system (IPS)

Key Definitions

- **Intrusion detection system (IDS)**: A device or software that monitors, logs, and detects security breaches but takes no action to stop or prevent the attack.
- **Intrusion prevention system (IPS)**: A device that monitors, logs, detects, and reacts to stop or prevent security breaches.

Intrusion Detection and Prevention

Signature-Based Detection

- Uses known signatures
- Updated by IDS vendors
- Detects identified attacks

Anomaly-Based Detection

- Establishes thresholds
- Generates threshold alerts
- Detects without a signature

IDS Implementation

- Host-based IDS
- Network-based IDS
- VM-based IDS
- Perimeter IDS

Intrusion Detection and Prevention

Summary

- Intrusion detection system (IDS)
- IDS detection
- IDS implementation
- Intrusion protection system (IPS)
- IDS/IPS benefits

In-Class Practice

Do the following labs:

- 6.4.4 Implement Intrusion Prevention

Class Discussion

- What is an intrusion detection system?
- How is an intrusion detection system different from an intrusion prevention system?
- What is the difference between anomaly-based and signature-based monitoring?