Diploma in Infocomm & Security

IT2654: Systems Administration & Security

TOPIC 12:
PATCH MANAGEMENT

Objectives

- Understand importance of patch management
- Learn about Microsoft Windows Software Update Services (WSUS)

Patch Management

- **What is patch management?**
  - It is the process of managing and deploying patches across the network.
  - A patch contains code that fixes software bugs and vulnerabilities.
  - It can also contain code that upgrades an application.
- **Why is patch management important?**
  - Protect against zero-day threats
  - Obtain latest upgrades – improves functionality

Types of Patches

- Microsoft has made popular the following types of patches which refer to their size and function.
  - **Hotfixes** – Updates created to address a particular issue. Usually not tested thoroughly due to urgency of update. eg. address **zero-day** attack
  - **Roll-ups or Patches** – Collection of hotfixes and tested thoroughly for mass roll out.
  - **Service Packs** – Collection of many patches which constitute a significant upgrade.

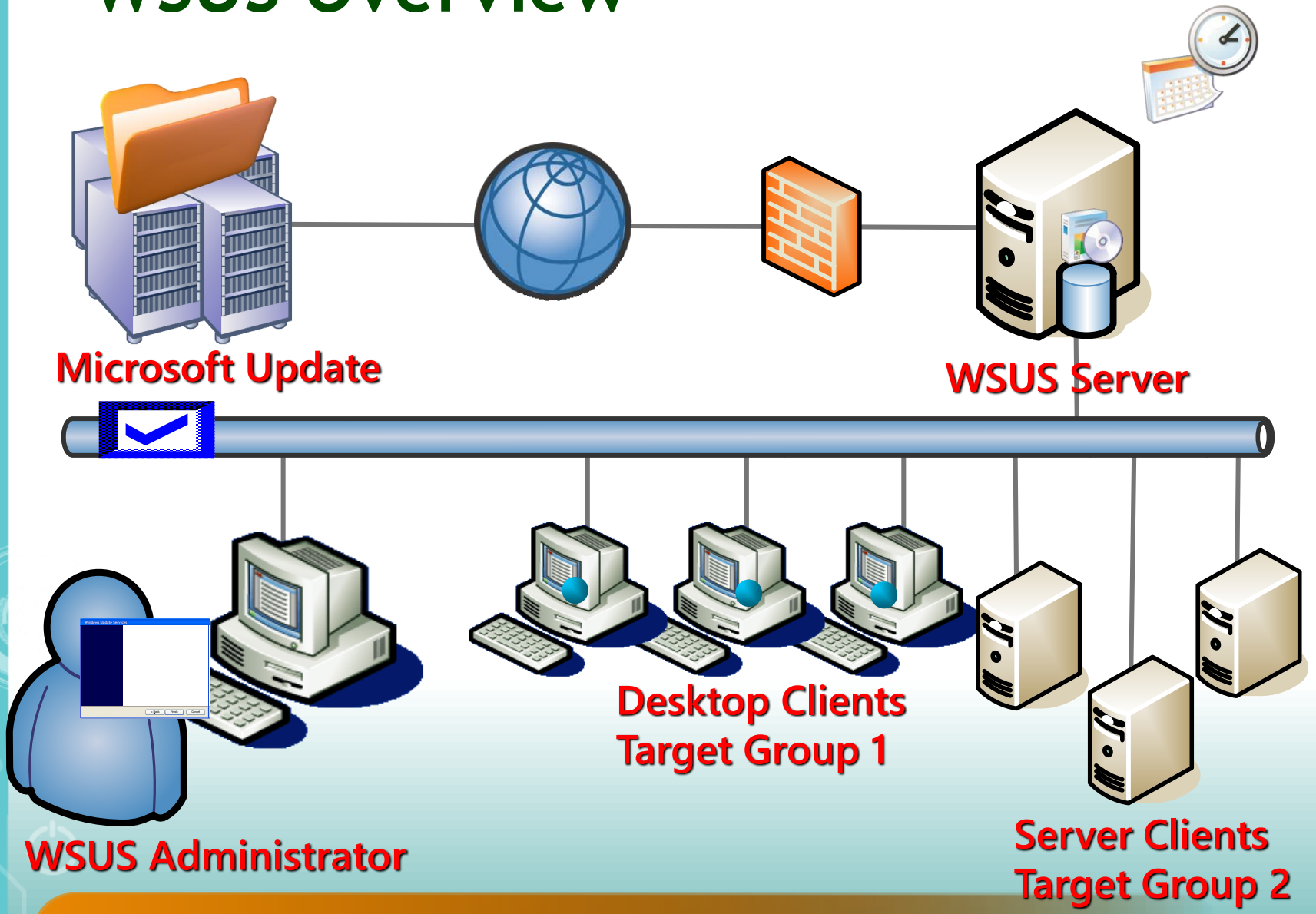
Windows Server Update Services (WSUS)

- System that enables administrators to manage the distribution of updates and hotfixes released for Microsoft products to computers in a corporate environment.

WSUS Benefits

- Centralized update management
  - Administrators can review, test, and approve updates before deployment
- Update management automation
  - Updates to computers in the network can be automated
- Easy to implement
- Free tool from Microsoft

WSUS Overview



Agents install administrator approved updates

WSUS Components

WSUS provides a management infrastructure that consists of the following components:

- **Microsoft Update**
  The Microsoft Web site that distributes updates for Microsoft products.
- **Windows Server Update Services (WSUS) server**

  The server that is installed on the Windows Server 2016, which can be used to manage and distribute security updates through administrative console. It can obtain updates from Microsoft Update or from another WSUS server.

WSUS Components cont..

- **WSUS Administration Console**
  The WSUS Administration Console is automatically installed on the WSUS server, and it can also be installed on any computer that runs on a supported operating system. You can use the WSUS Administration Console to manage any WSUS server in any domain with which it has a trust relationship.

- **Client Component - Automatic Updates**
  The client computer software component that is built into Windows operating systems. Automatic Updates enables the server and client computers to receive updates from Microsoft Update or from a WSUS server.

WSUS – Server Component

- The server component of WSUS is Windows Server Update Services (WSUS):
  - Can synchronize updates from Microsoft Update on a schedule
  - Provides a Web-based administrative GUI
  - Has several built-in default security features
  - Provides synchronization and update reports
  - Uses MSDE or SQL Server database to store update metadata, events, and settings
  - Interface is localized in many languages

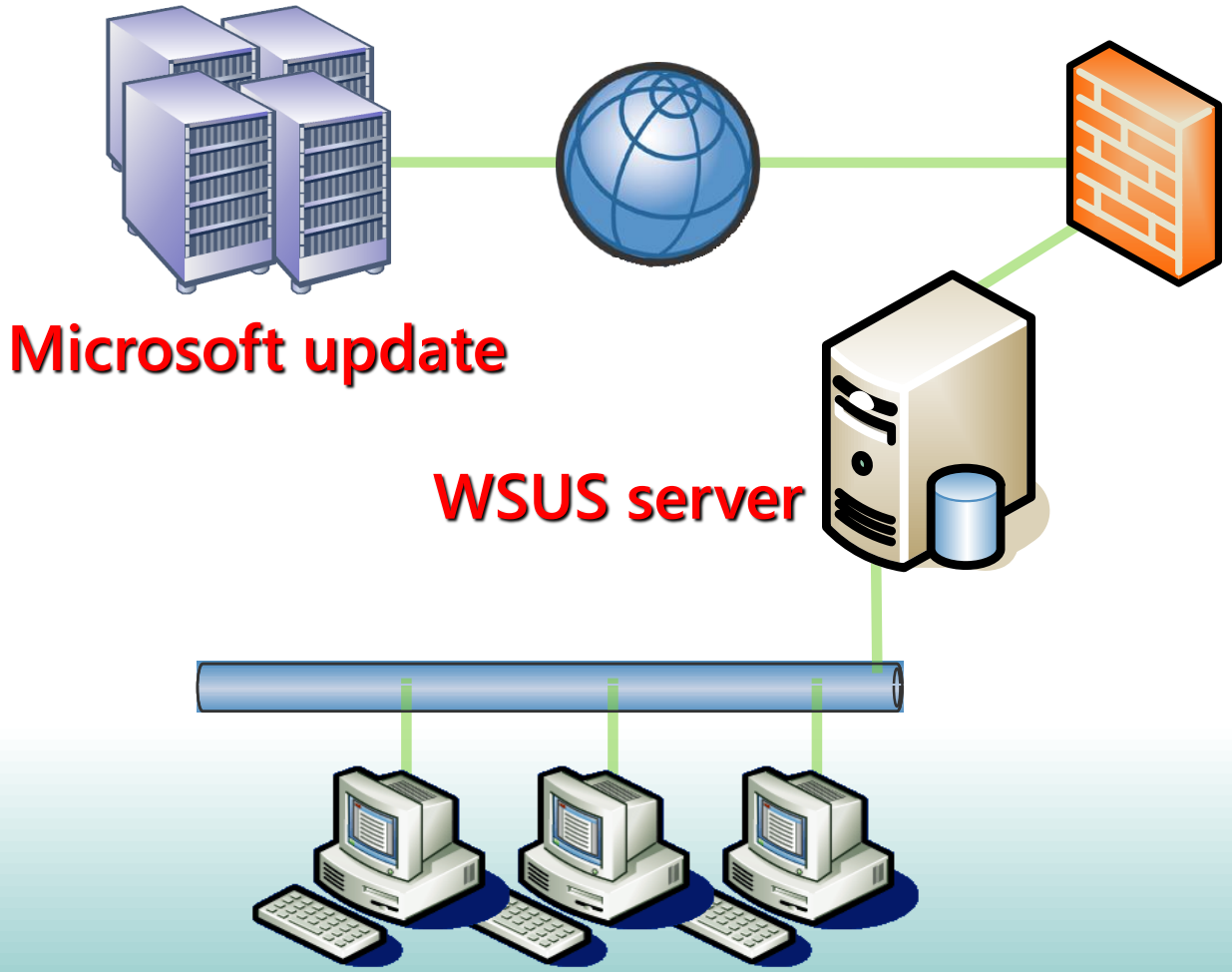
WSUS – Client Component

- The client component of WSUS is Automatic Updates:
  - Can be configured to pull updates either from corporate WSUS server or from Microsoft Update
  - Three ways to configure Automatic Updates:
    - Centrally, by using Group Policy
    - Manually configure clients
    - Use scripts to configure clients
  - WSUS requires a compatible Automatic Updates client

Deployment Options

- Server deployment options
  1) Single server
  2) Multiple servers
  3) Disconnected servers

Single Server

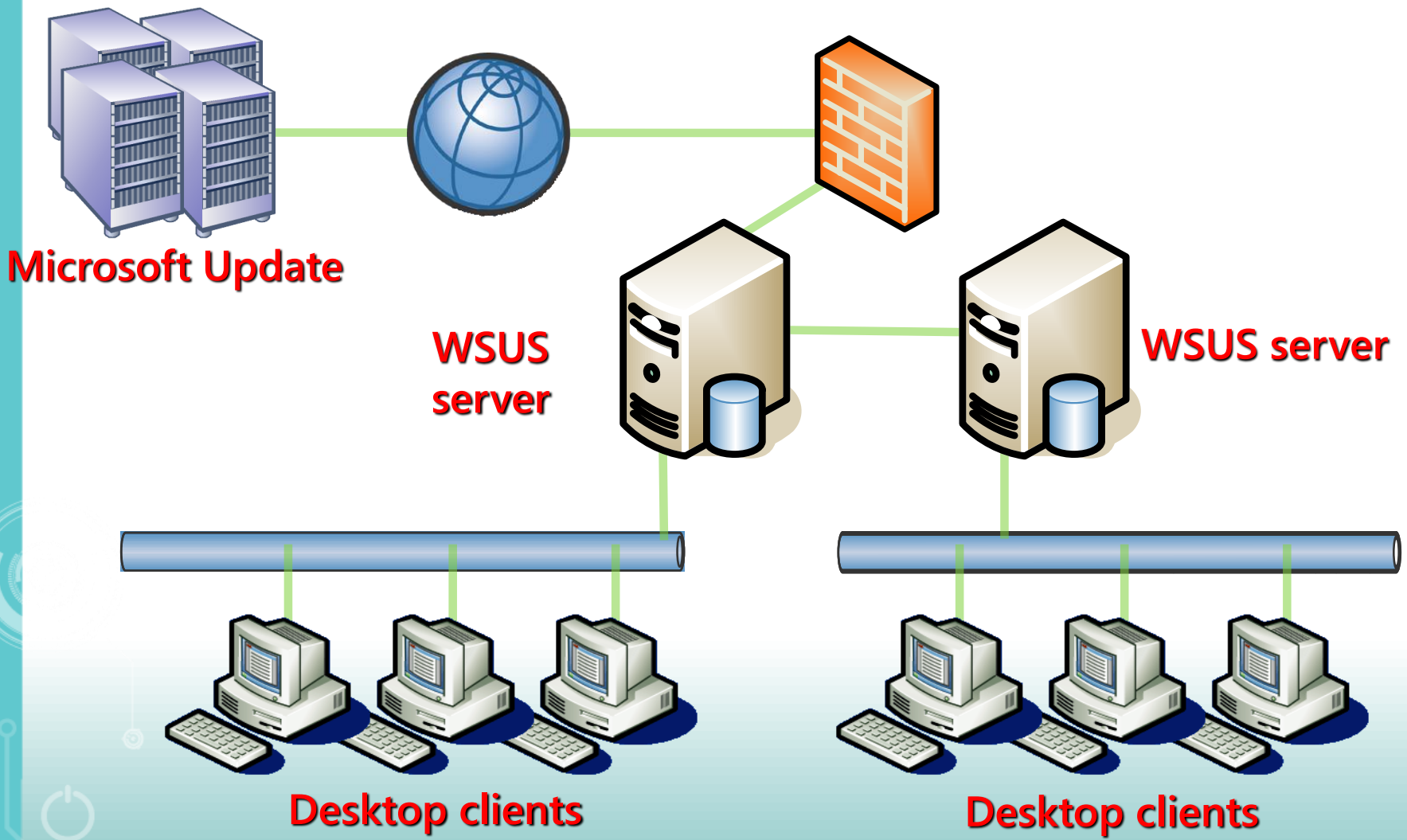


Single Server

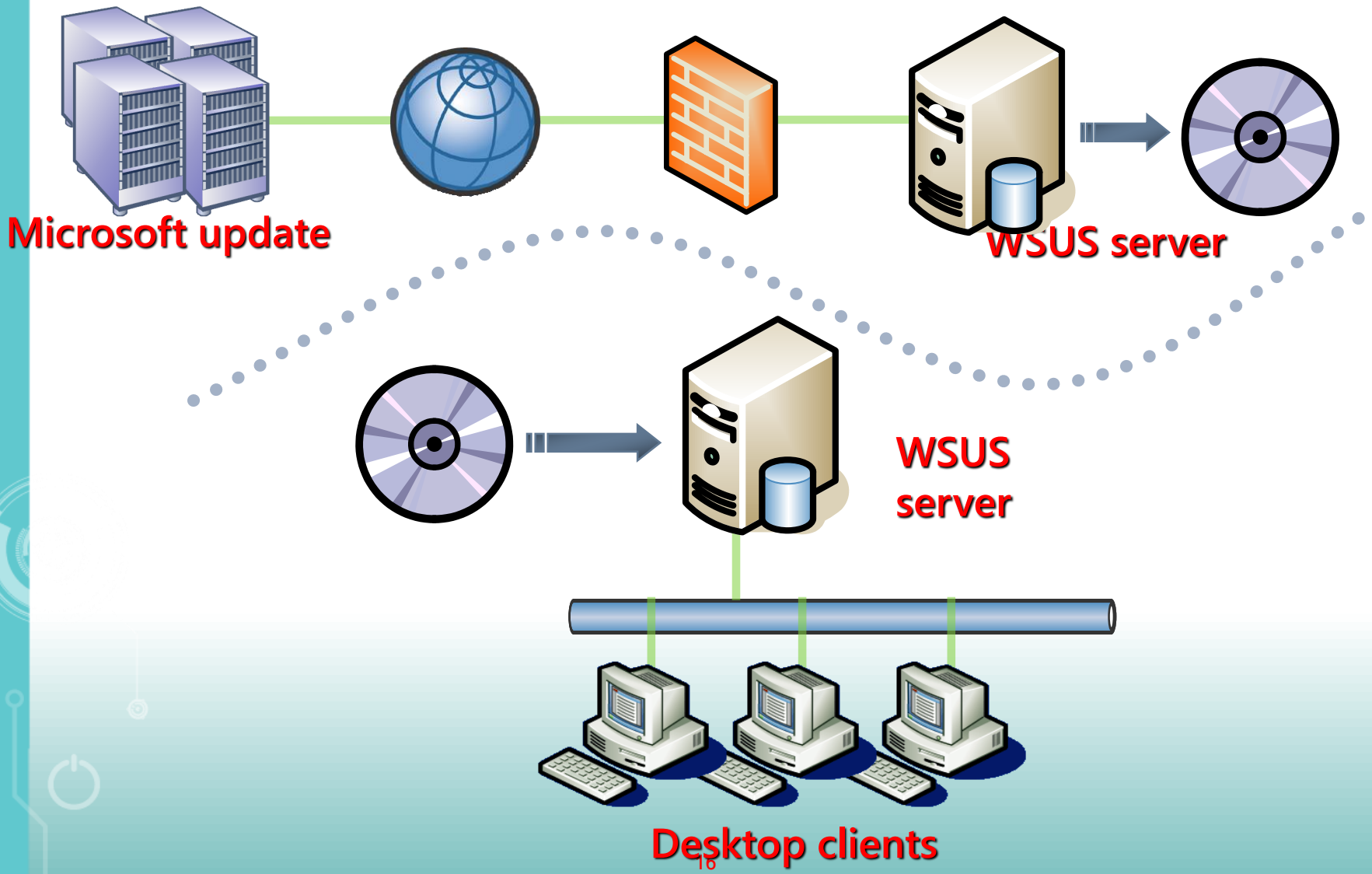
Small organization or simple network

- Configure single server to talk to MU (Microsoft Update)
- Synchronize all relevant updates
- Configure clients to point to the WSUS server
- Optionally:
  - Create target groups for different groups of machines
  - Configure clients to be members of a target group
  - Configure auto approval rules to approve updates for install automatically

Multiple Servers



Disconnected Servers



Disconnected Server

- Setup an external server to talk to MU (Microsoft Update)
- Synchronize all relevant updates
- Export update data and content to media
- Import update data and content to WSUS server on disconnected network
  - Server will validate Microsoft certificates on content and data relationships integrity
- Configure clients to point to respective WSUS servers

How to Use WSUS

- On the WSUS server:
  1. Administer the WSUS server at http://<*server name*>/WSUSAdmin
  1. Configure the WSUS server synchronization schedule and settings
  2. Create client computer groups and assign computers
  3. Review, test, and approve updates
- On each WSUS client:
  - Configure Automatic Updates on the client to use the WSUS server

Summary

- Patch management is important to the security of the entire system.
- Microsoft provides WSUS to implement patch management.
- WSUS components
- 3 deployment options of WSUS