WAN Network Devices..2

Lecture 9

Proxy

- A **Proxy** is a server that acts as an intermediary for requests from clients seeking resources from other servers.
- A client connects to the proxy, requesting some service, *such as a file, connection, web page, or other resource available from a different server,* then the proxy sends the request to the server. The proxy server then obtains the file and sends it to the requesting computer.
- Today, most proxies are **web proxies (web gateway)**, facilitating access to content on the World Wide Web, providing anonymity and may be used to bypass IP address blocking.

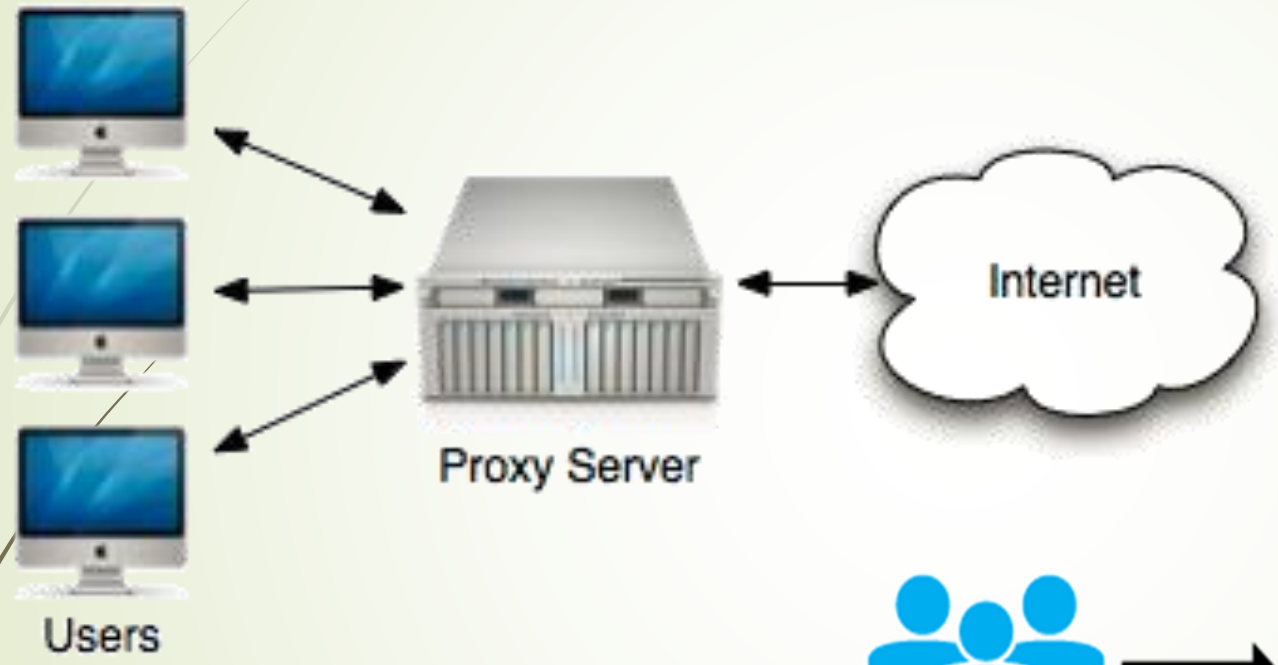
Uses of proxy

- To share Internet connection on a LAN.
- speed up Internet surfing(caching proxy)
- Security (hiding the IP address of the client computers)
- Bypassing filters and censorship
- Translation
- Internet access control:
  - Monitoring and filtering
  - Filtering of encrypted data
  - Logging and eavesdropping

Reverse proxies

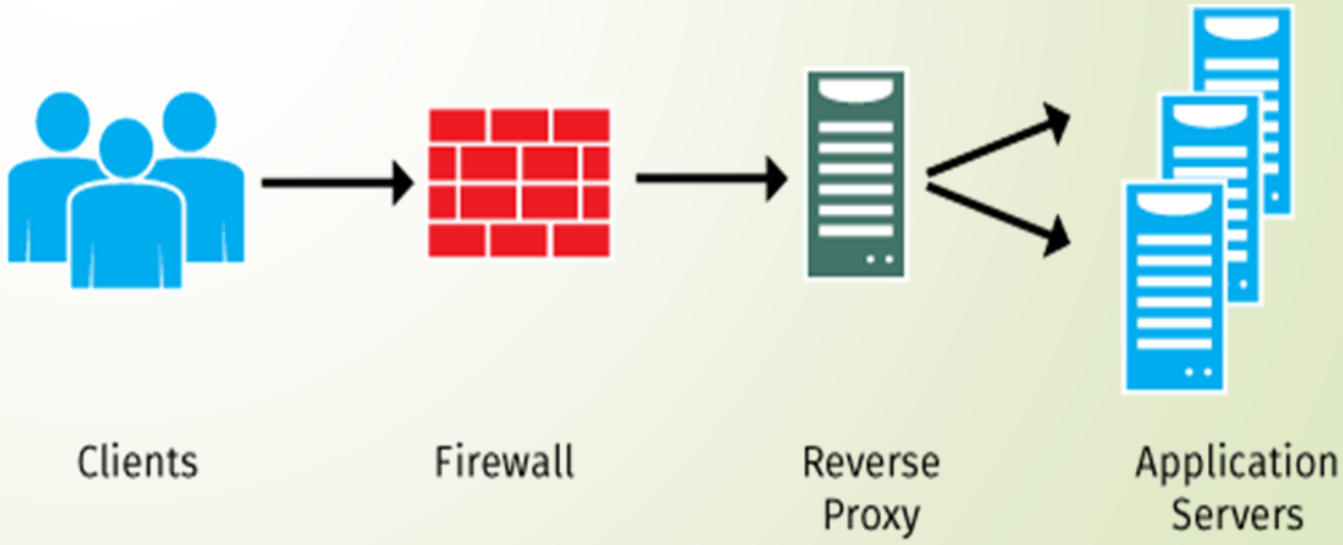
- A **reverse proxy**: is a proxy server that appears to clients to be an ordinary server. Reverse proxies
  - forward requests to one or more ordinary servers which handle the request.
  - The response from the proxy server is returned as if it came directly from the original server, leaving the client with no knowledge of the origin servers.
  - installed in the neighborhood of one or more web servers. All traffic coming from the Internet and with a destination of one of the neighborhood's web servers goes through the proxy server.
  - The use of "reverse" originates in its counterpart "forward proxy" since the reverse proxy sits closer to the web server and serves only a restricted set of websites.

Proxy deployments



Some Vendors of web proxies

- Blue Coat
- Barracuda Networks
- Cisco
- Websense
- Intel Security (McAfee)
- Sophos
- Symantec



Content filtering

- Designed to **restrict or control the content** a user is authorized to access, especially when utilized to restrict material delivered over the Internet via the Web, e-mail, or other means.

Bypassing filters

- Content filtering in general can "be bypassed entirely by tech-savvy individuals." Blocking content on a device "[will not]...guarantee that users won't eventually be able to find a way around the filter.

Types of filtering

- Browser based filters
- E-mail filters
- Client-side filters
- Network-based filtering
- DNS-based filtering
- Search-engine filters

Packet shaper / Bandwidth shaper

- PacketShaper is the **BW management solution** that brings efficient performance to applications running over WAN and the Internet.
- With PacketShaper, you can control performance to suit applications' characteristics, business requirements, and users' needs.

Packet shaper illustration

- https://www.youtube.com/watch?v=pl5eQisvpaA
- https://www.youtube.com/watch?v=k_8_c33HDs0

- View at home: https://www.youtube.com/watch?v=kn1I6LgTItc

Packet shaper vendors

- Bluecoat
- Symantec
- Citrix Netscalar

Network Intrusion Detection System (NIDS)

- A device or software application that **monitors** a network or systems **for malicious activity** or policy violations.
- Any malicious activity or violation is typically reported either to an administrator or collected centrally using a security information and event management (SIEM) system.
- Can work in Stealth mode; just observing and never sending data.

Detection approaches

1. **Signature-based** detection (recognizing bad patterns, such as malware)
2. **Anomaly-based** detection (detecting deviations from a model of "good" traffic, which often relies on **machine learning**).

- **Intrusion prevention system:** Some IDS having the ability to **respond to detected intrusions**.

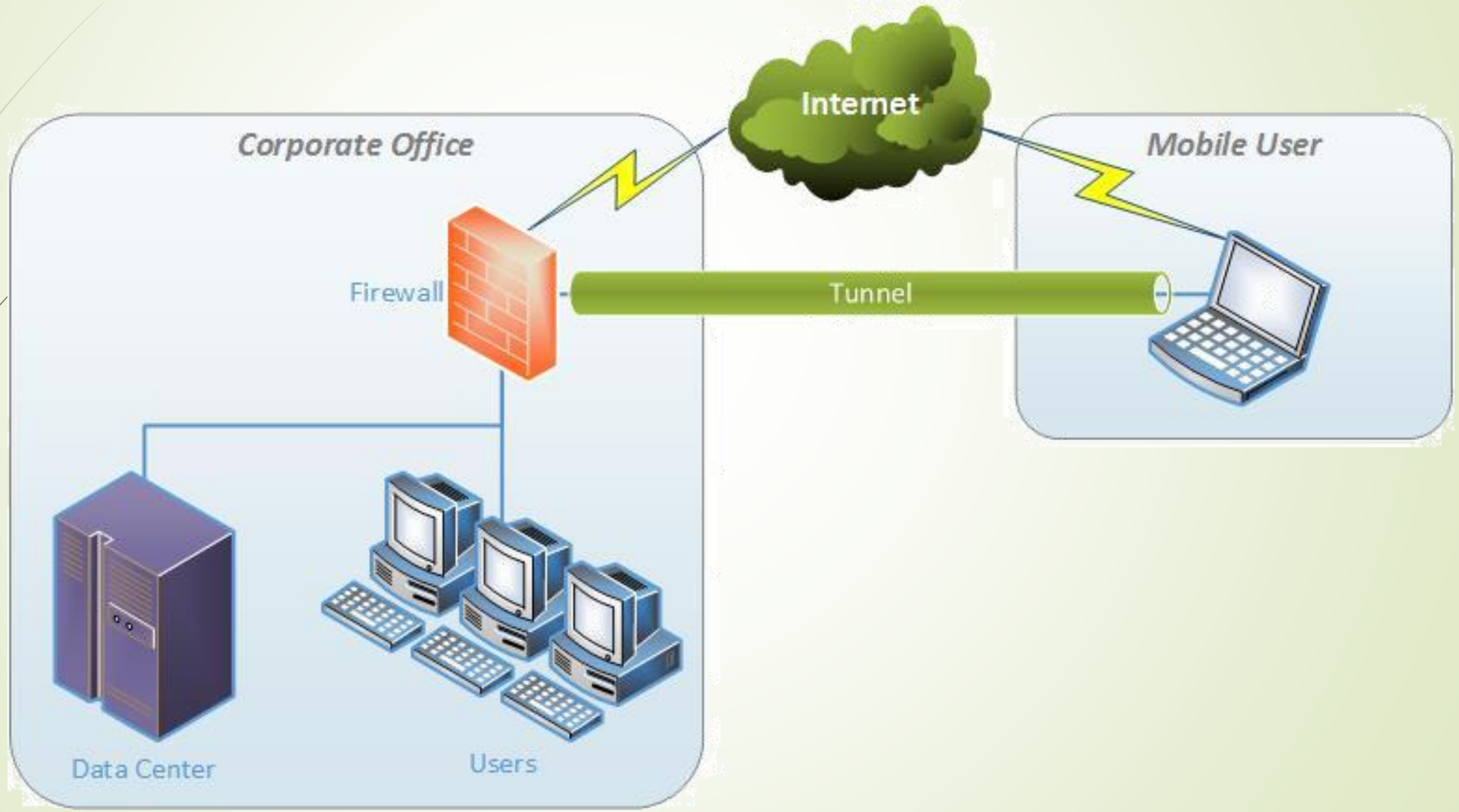
A host-based intrusion detection system (HIDS)

- An intrusion detection system that is capable of monitoring and analyzing **the internals** of a computing system **as well as the network packets** on its network interfaces.
- Its goal is to **protect one machine** and its data.
- Monitors important operating system files.

Virtual Private Network (VPN)

- A VPN :
  - Extends a private network across a public network
  - enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network.
  - Applications running across the VPN may therefore benefit from the functionality, security, and management of the private network

VPN concept


Internet
Corporate Office
Mobile User
Firewall
Tunnel
Data Center
Users

VPN concentrator

- A **VPN concentrator** is a type of networking device that provides secure creation of VPN connections and delivery of messages between VPN nodes.

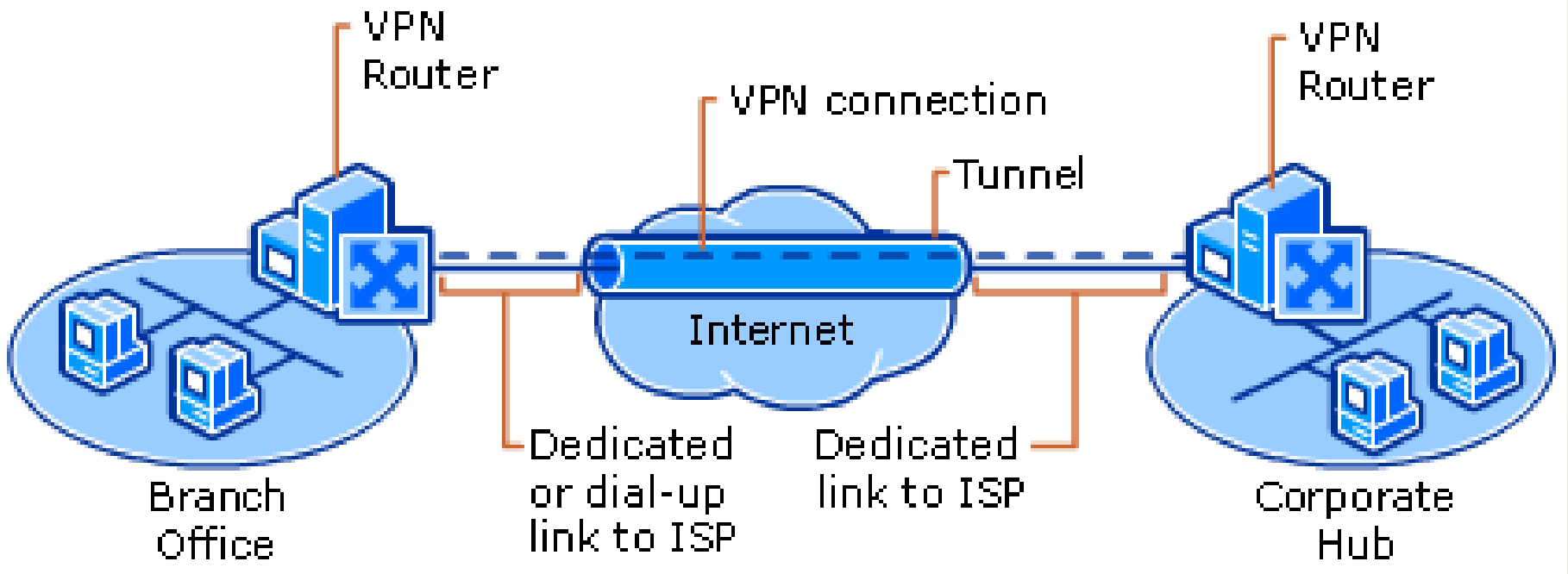
- It is a type of **router device**, **built specifically** for creating and managing VPN communication infrastructures.

VPN concentrator

- Adds the capabilities of a VPN router by adding advanced data and network security to the communications. It has the ability to create and manage a large quantity of VPN tunnels.

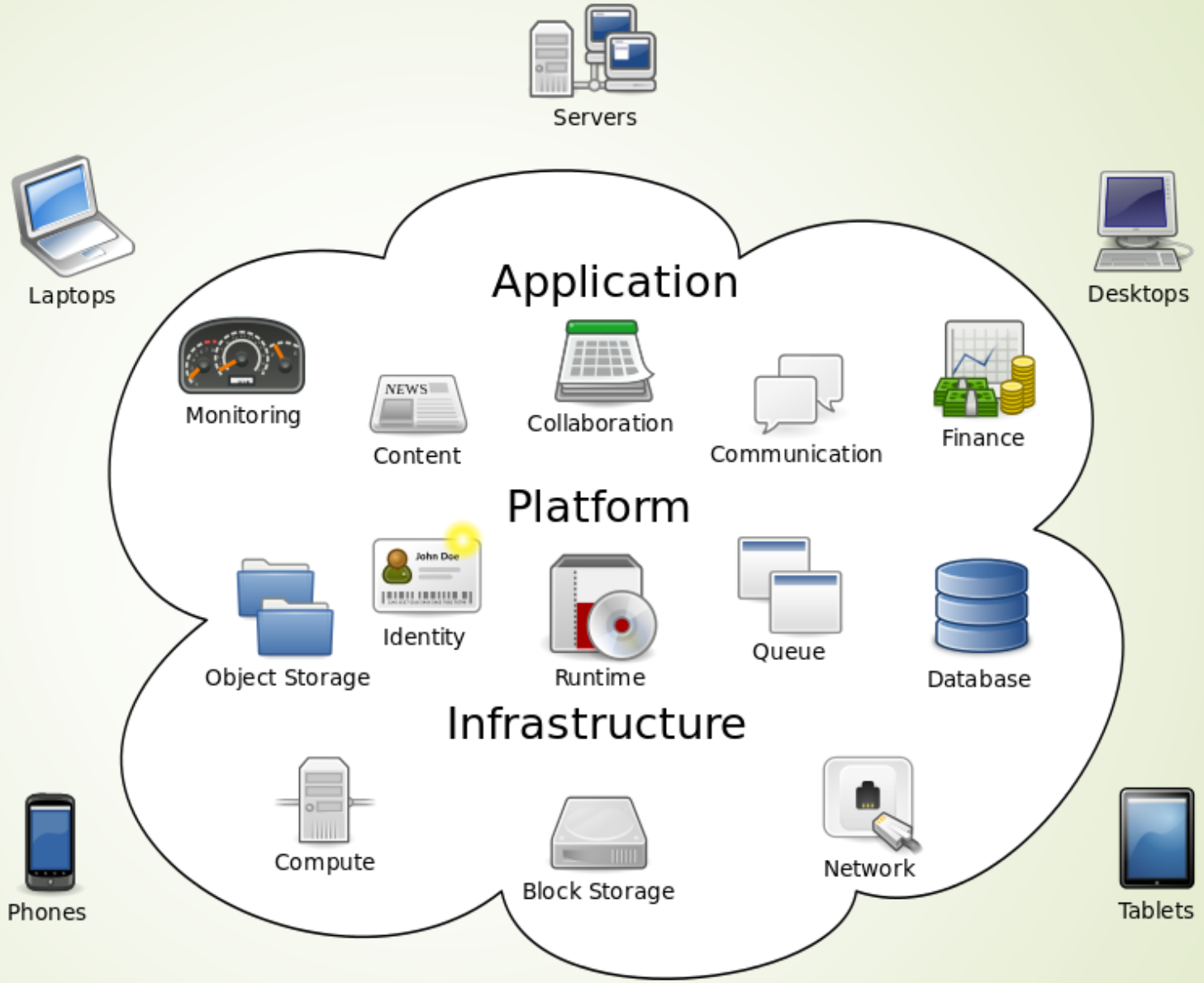
- Typically used for creating **site-to-site VPN architectures**. It can:
  - Establish and configure tunnels
  - Authenticate users
  - Assign tunnel/IP addresses to users
  - Encrypt and decrypt data
  - Ensure end-to-end delivery of data

VPN concept


VPN
Router
VPN connection
Tunnel
VPN
Router
Internet
Dedicated
or dial-up
link to ISP
Dedicated
link to ISP
Branch
Office
Corporate
Hub

What about cluster, cloud,virtualised?

- A **computer cluster** is a set of loosely or tightly connected computers that work together so that, in many respects, they can be viewed as a single system.
- **Cloud network** is referred to a computer network that exists within or is part of a cloud computing infrastructure. It is a computer network that provides network interconnectivity between cloud based or cloud enabled application, services and solutions.
- **Network virtualization** is a method of combining the **available resources** in a network by **splitting up the available bandwidth** into channels, each of which is **independent from the others**, and each of which can be assigned (or reassigned) to a particular server or device in real time.



Cloud computing

Questions?