Hiding the Private Network

Professor: David A. Cass & Kevin McKenzie

Chapter 20

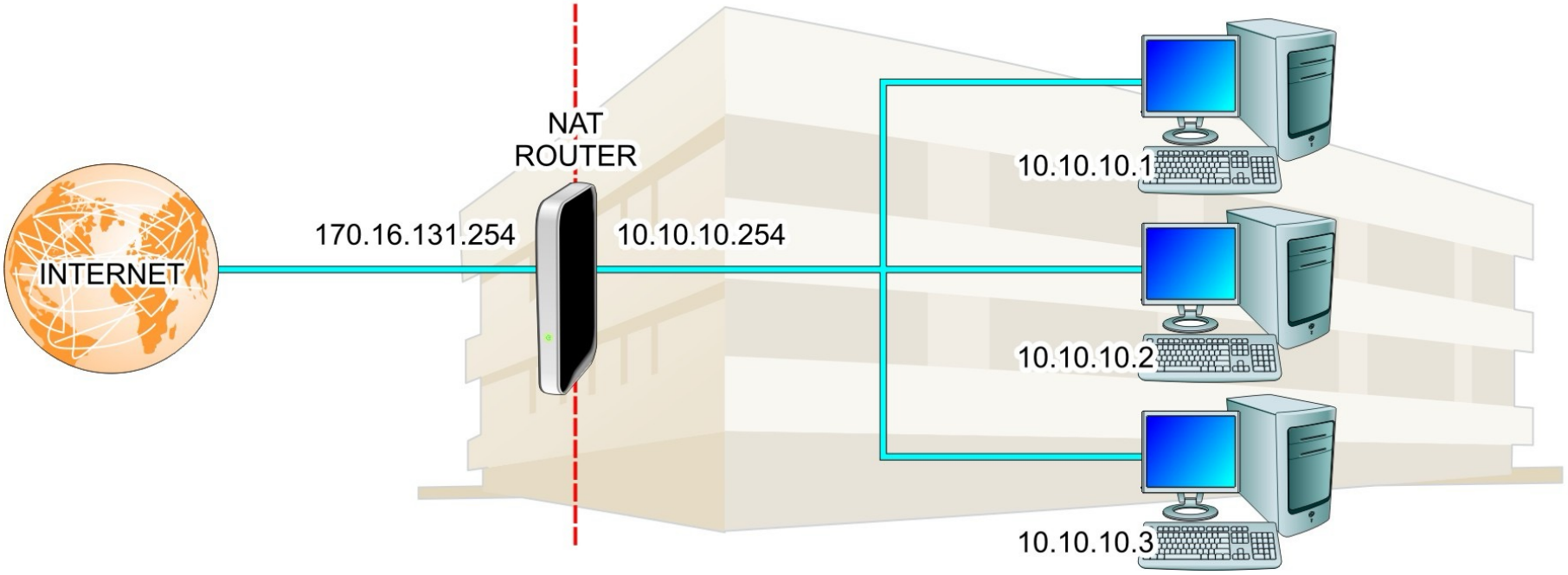
In this chapter, you'll learn to:

- Discuss the advantages and disadvantages of implementing Network Address Translation (NAT) and Port Address Translation (PAT) for network security.

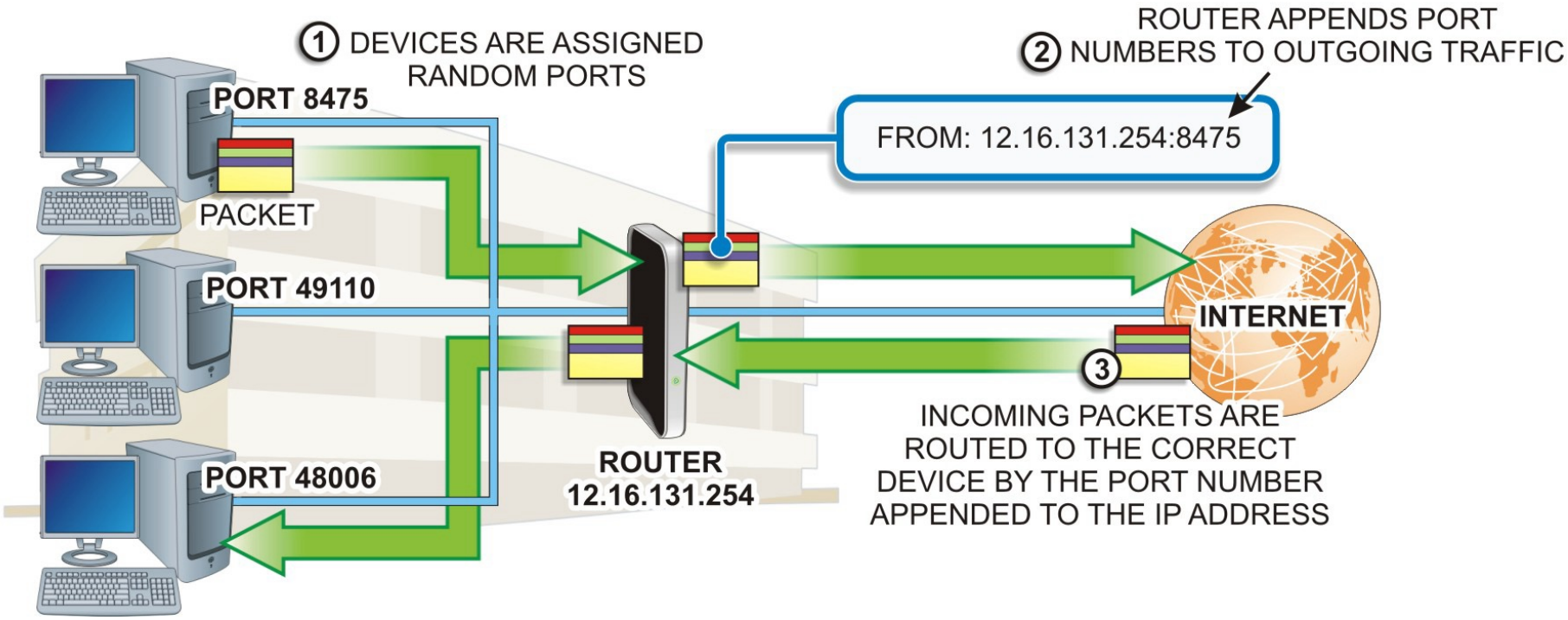
In this chapter, you'll learn to:

- Define and describe network segmentation and security zones
- Use NAT to create security segments in the network
- Use VLANs to implement security zoning

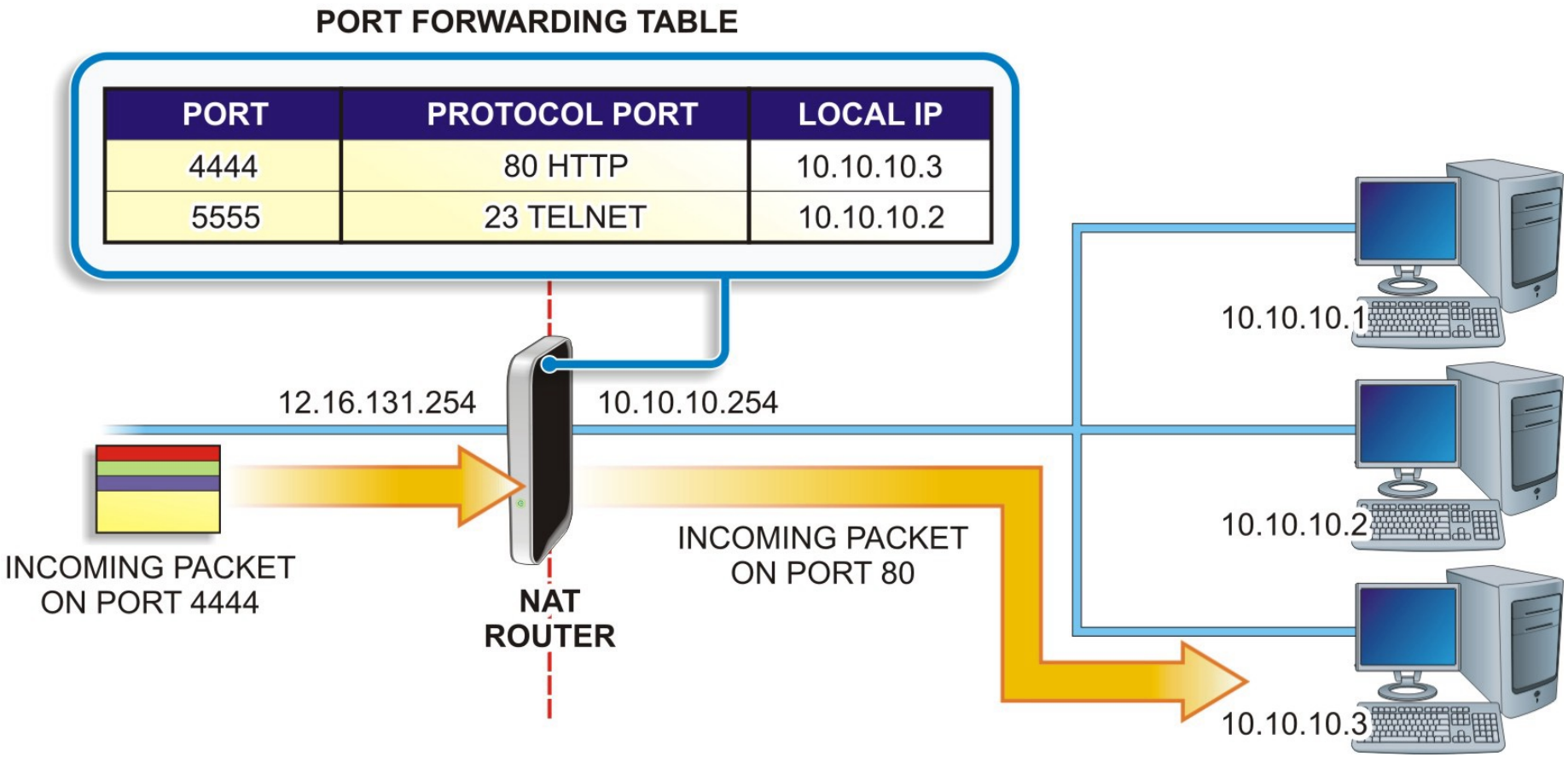
NAT Configuration



PAT Configurations

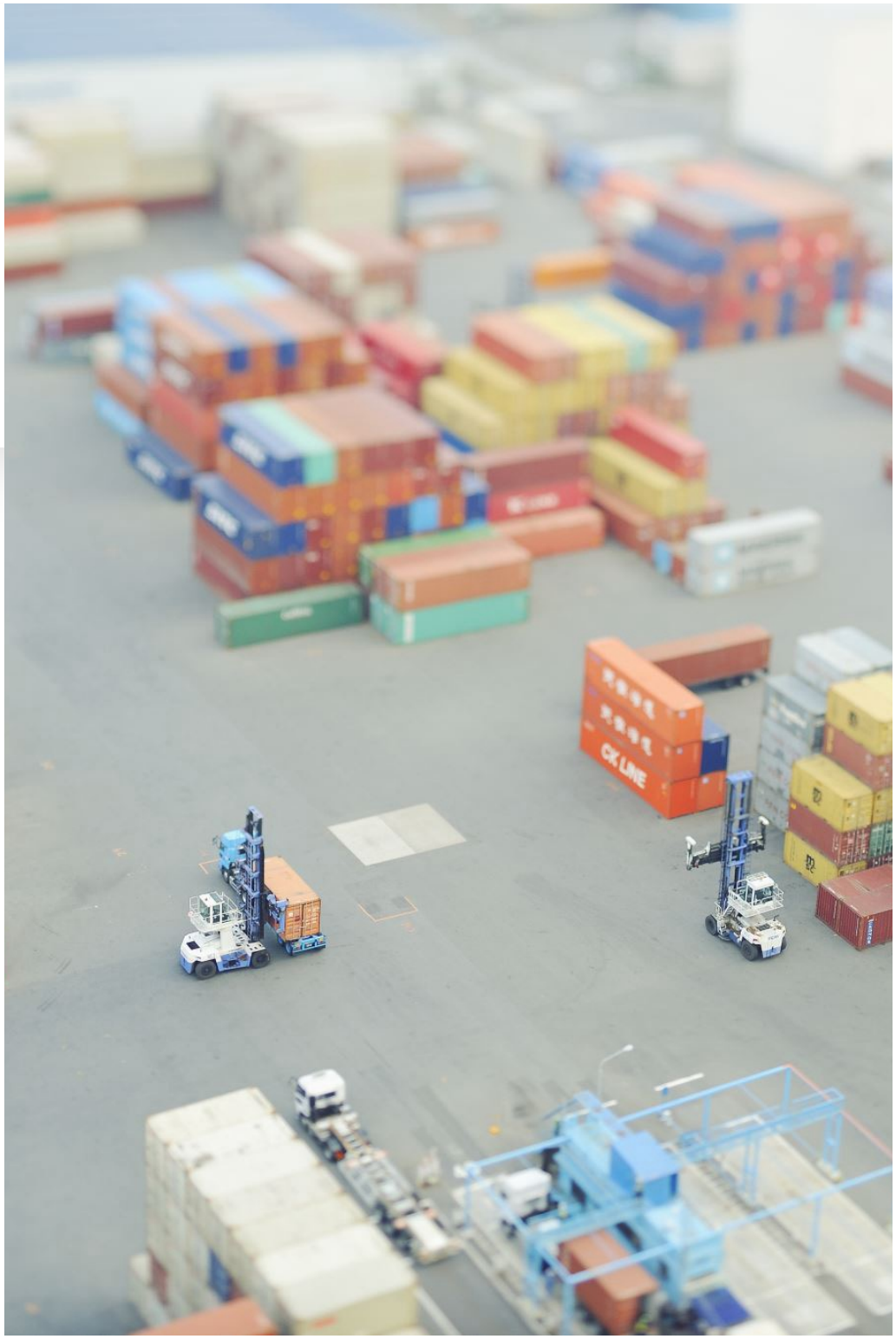


Port Forwarding



Security Through Obscurity

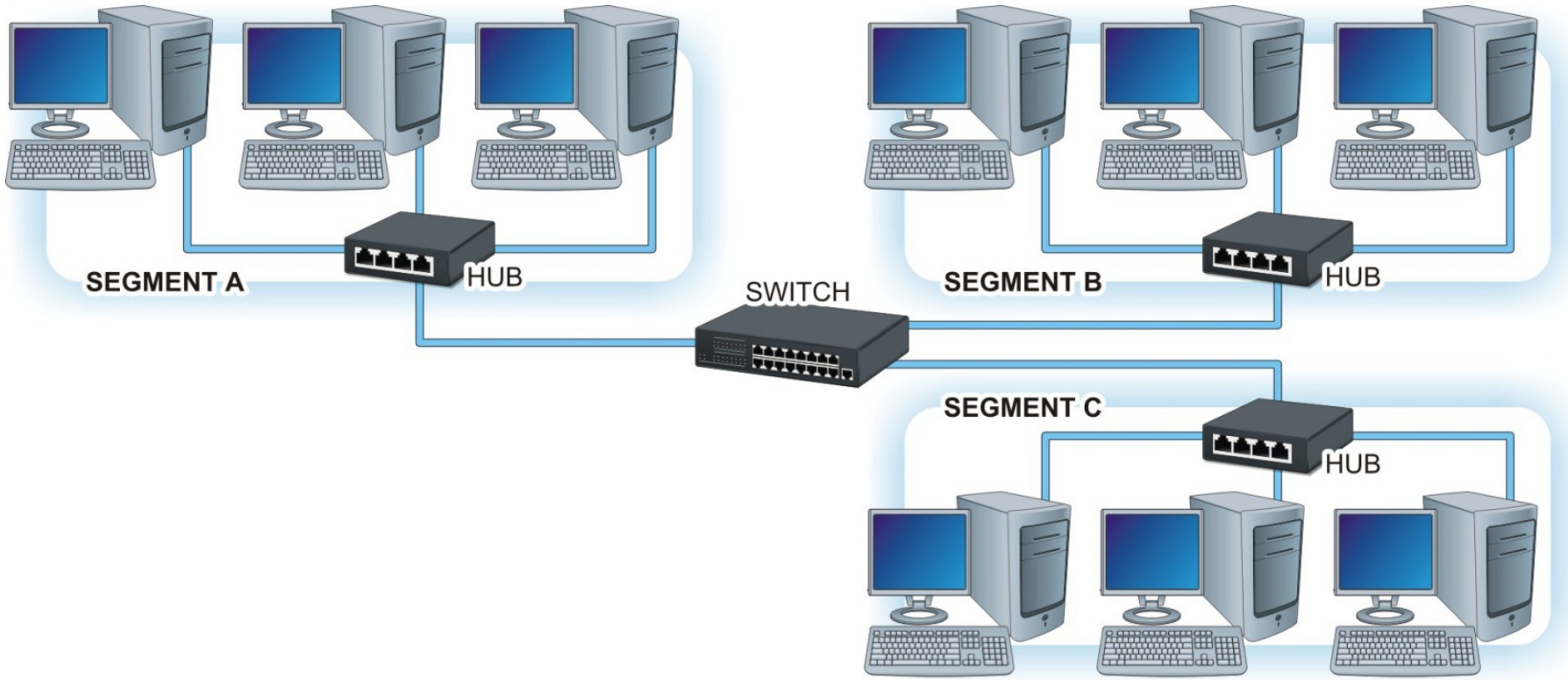
- Most port scans are vanilla and will look at every potential port – all 65,535 of them – but a hacker might be looking for specific open ports in a strobe scan. Mapping unusual ports to those services, you could potentially discourage those attackers, but then clients would need to append a nonstandard port to their requests. Security through obscurity will not provide a successful security plan.



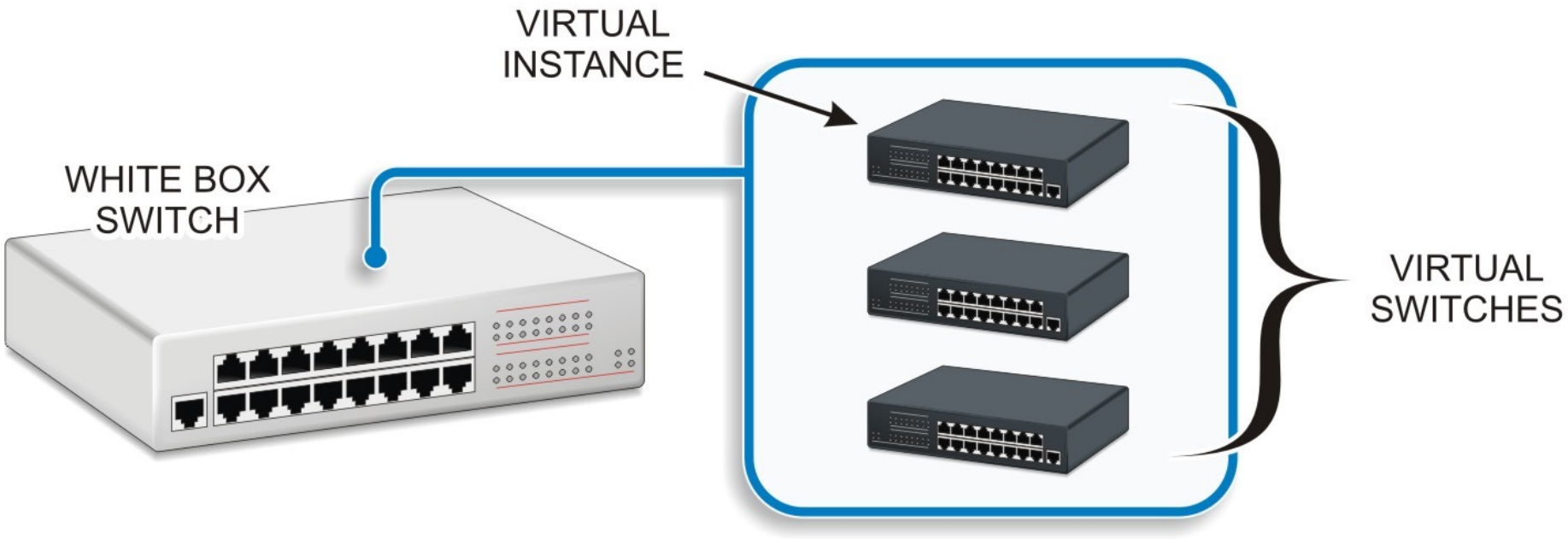
A Word about Port Forwarding

- Previously, some standard port numbers were discussed, and every hacker knows these common ports well. Any time you can easily map nonstandard ports, rather than use common ports, you should. However, serious hackers will still find these open ports, so port forwarding alone can’t be thought of as a security technique.

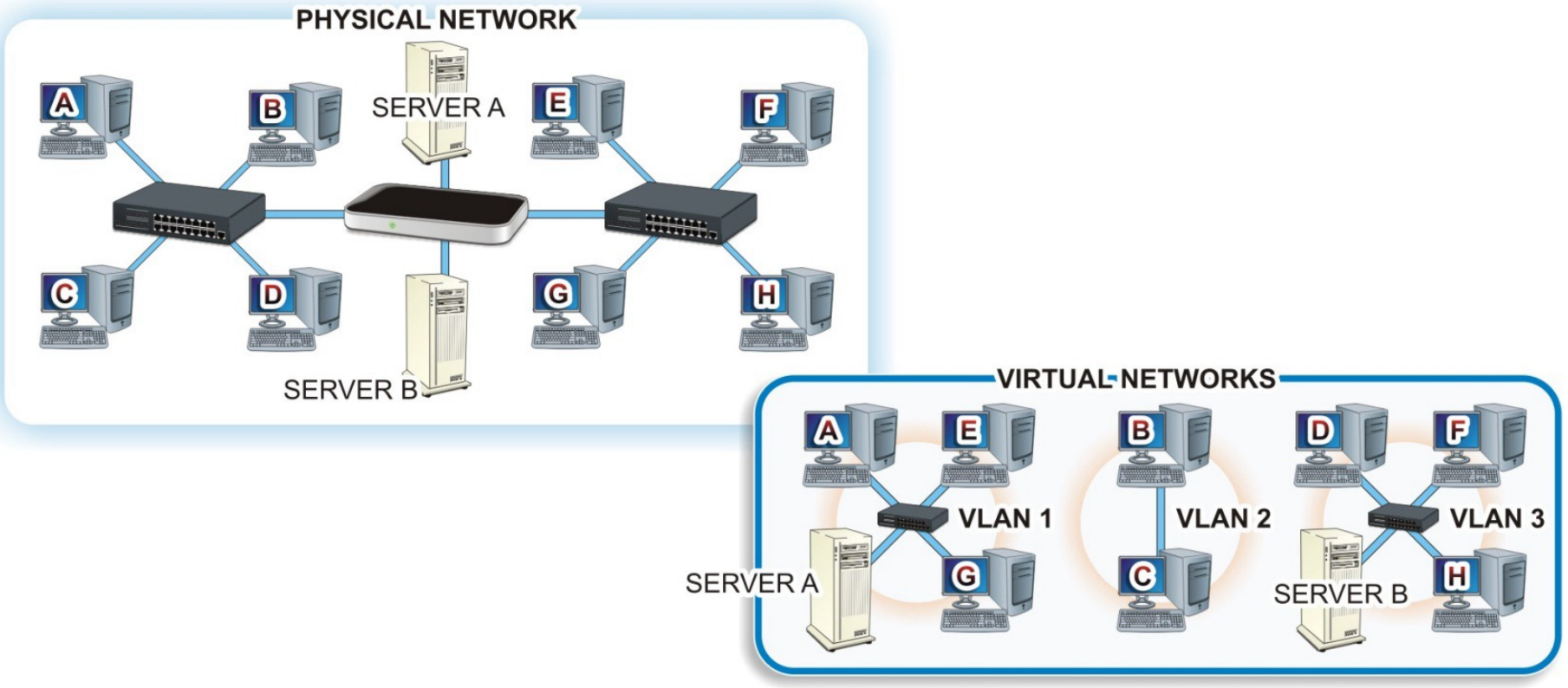
A Segmented Network



Virtual Instances

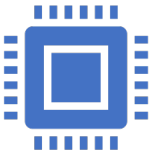


VLAN


PHYSICAL NETWORK
A
B
SERVER A
E
F
C
D
SERVER B
G
H
VIRTUAL NETWORKS
A
E
VLAN 1
G
SERVER A
B
VLAN 2
C
D
F
VLAN 3
SERVER B
H

Hands-On Exercises Objectives

Check system for compatibility with Hyper-V.



Enable Hyper-V on a Windows 10 Professional computer.

Install and explore a virtual switch Hyper-V Manager.

Install a virtual machine.

Protecting the Perimeter

Chapter 21

In this chapter, you'll learn to:

01

Implement firewalls and other intrusion-prevention devices and structures

02

Describe common enterprise-network structures, including intranets, extranets, DMZs, and honeypots

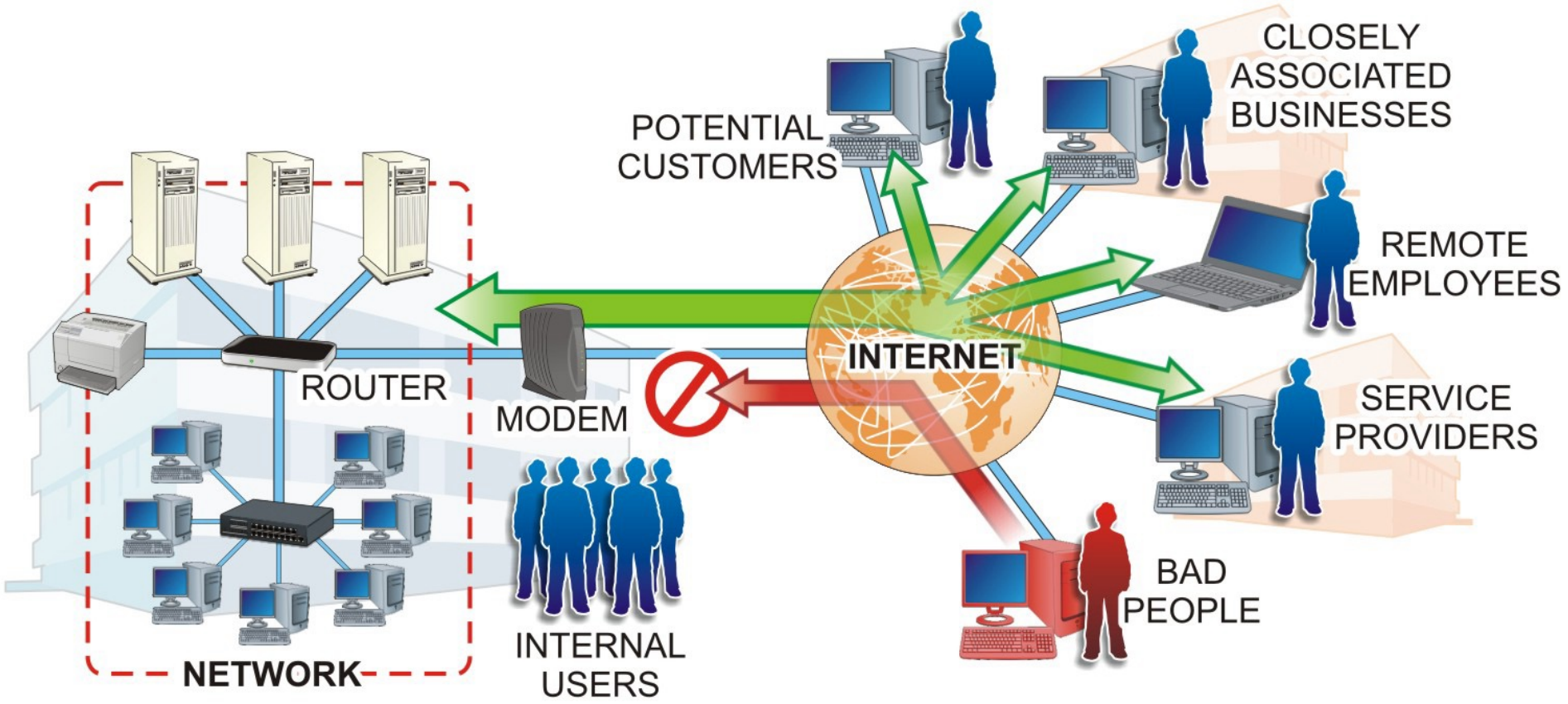
03

Describe the purpose and limitations of firewalls

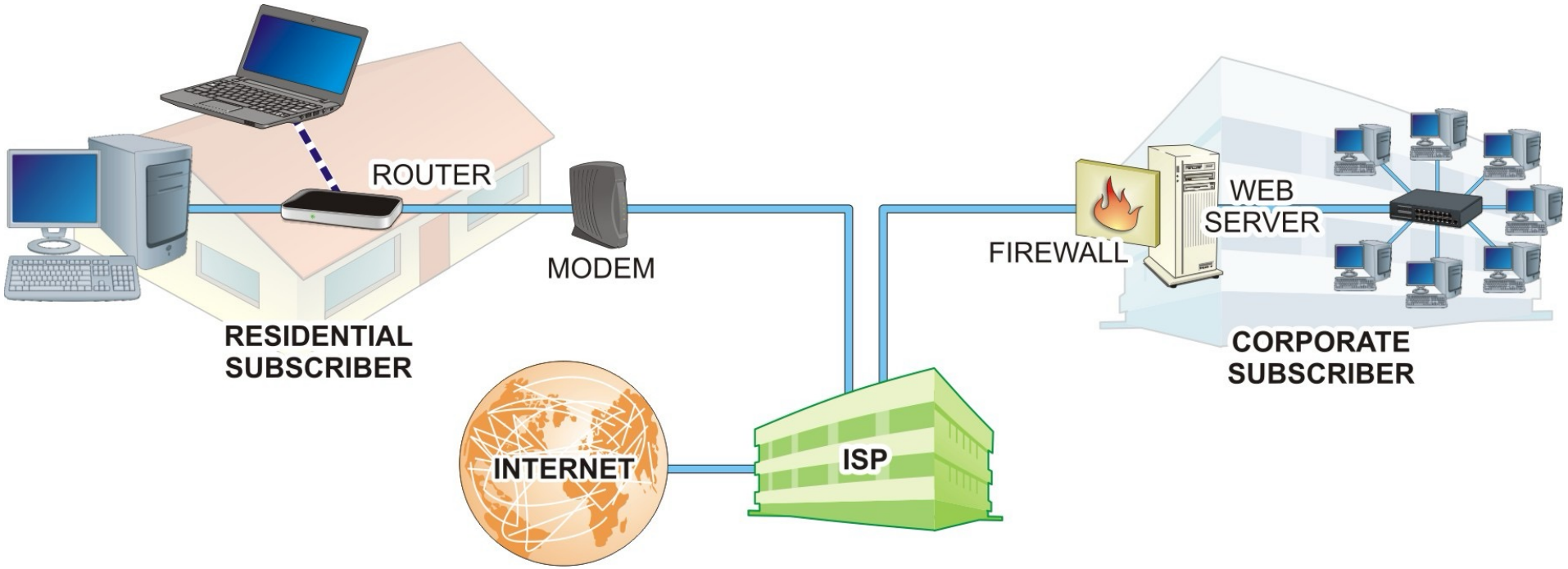
In this chapter, you'll learn to:

Describe	Understand	Explain
Describe the use of honeypots as an intrusion-prevention technique	Understand the role of DMZs (demilitarized zones) in cybersecurity topologies	Explain the configuration and operation of a demilitarized zone (DMZ) host, including the key services contained within the zone

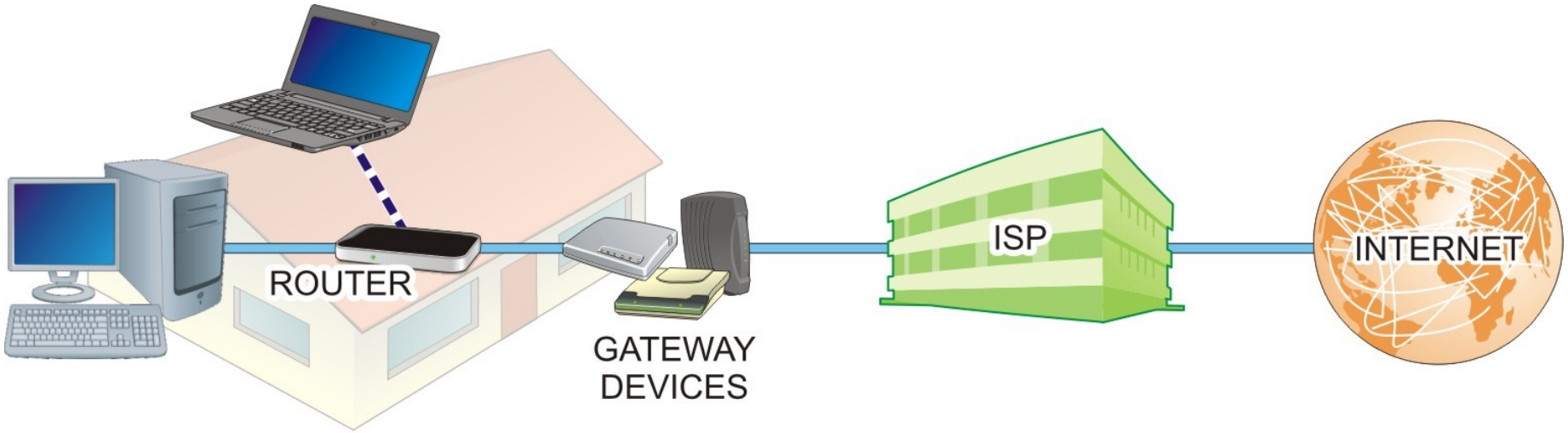
The Perimeter



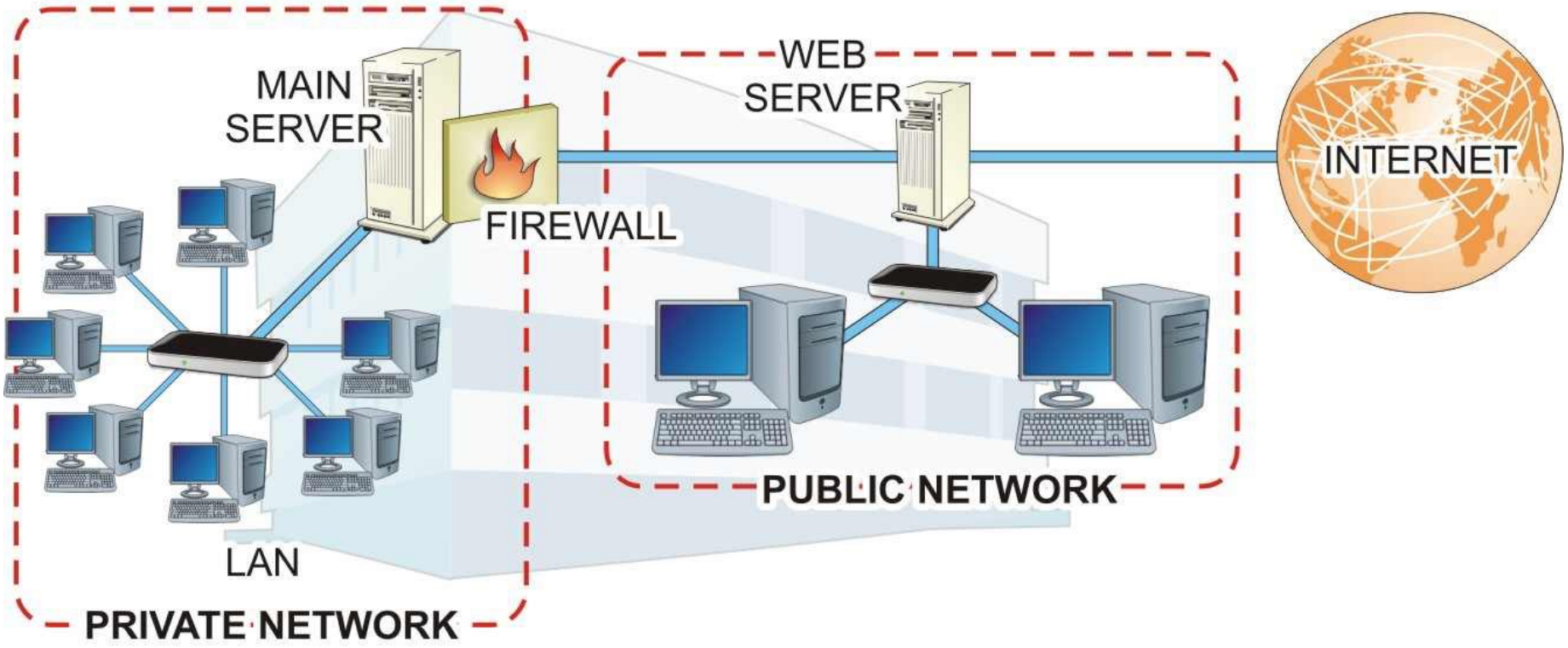
Internet Connectivity



Gateway Connection Options



Private and Public Networks



Important Questions

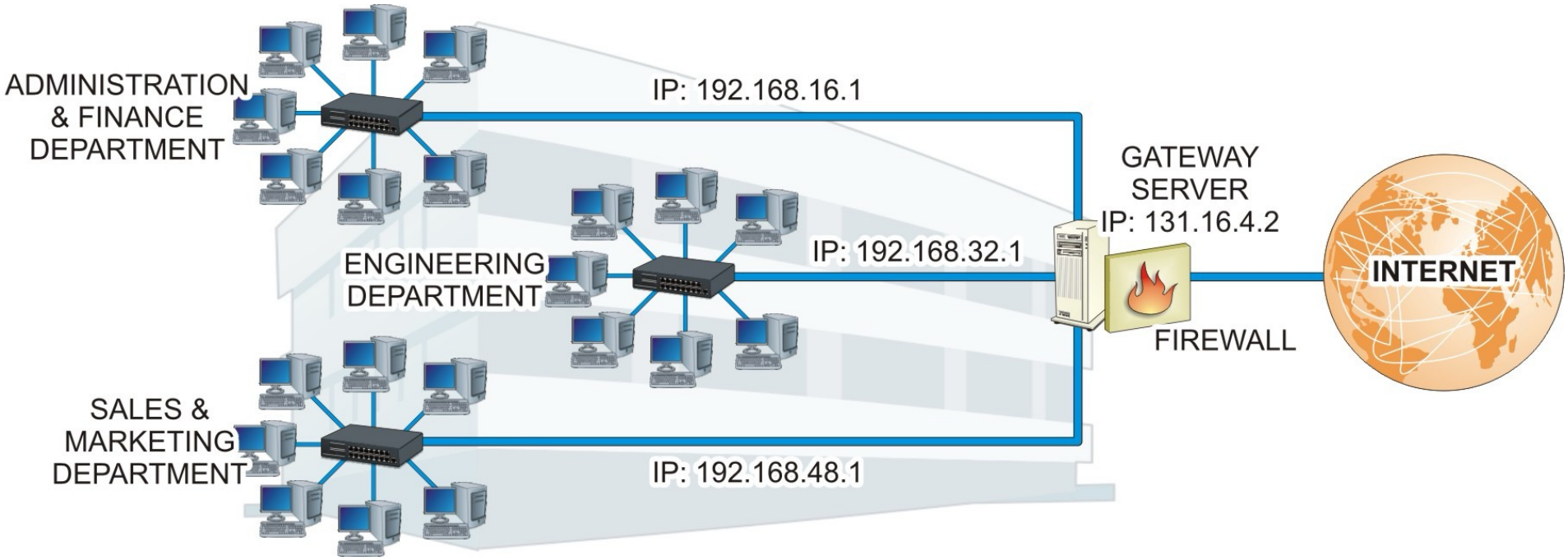
- How important is what you are protecting?
- What is the worst-case scenario?
- How much will it hurt you or your company if the network is compromised?

Important Questions

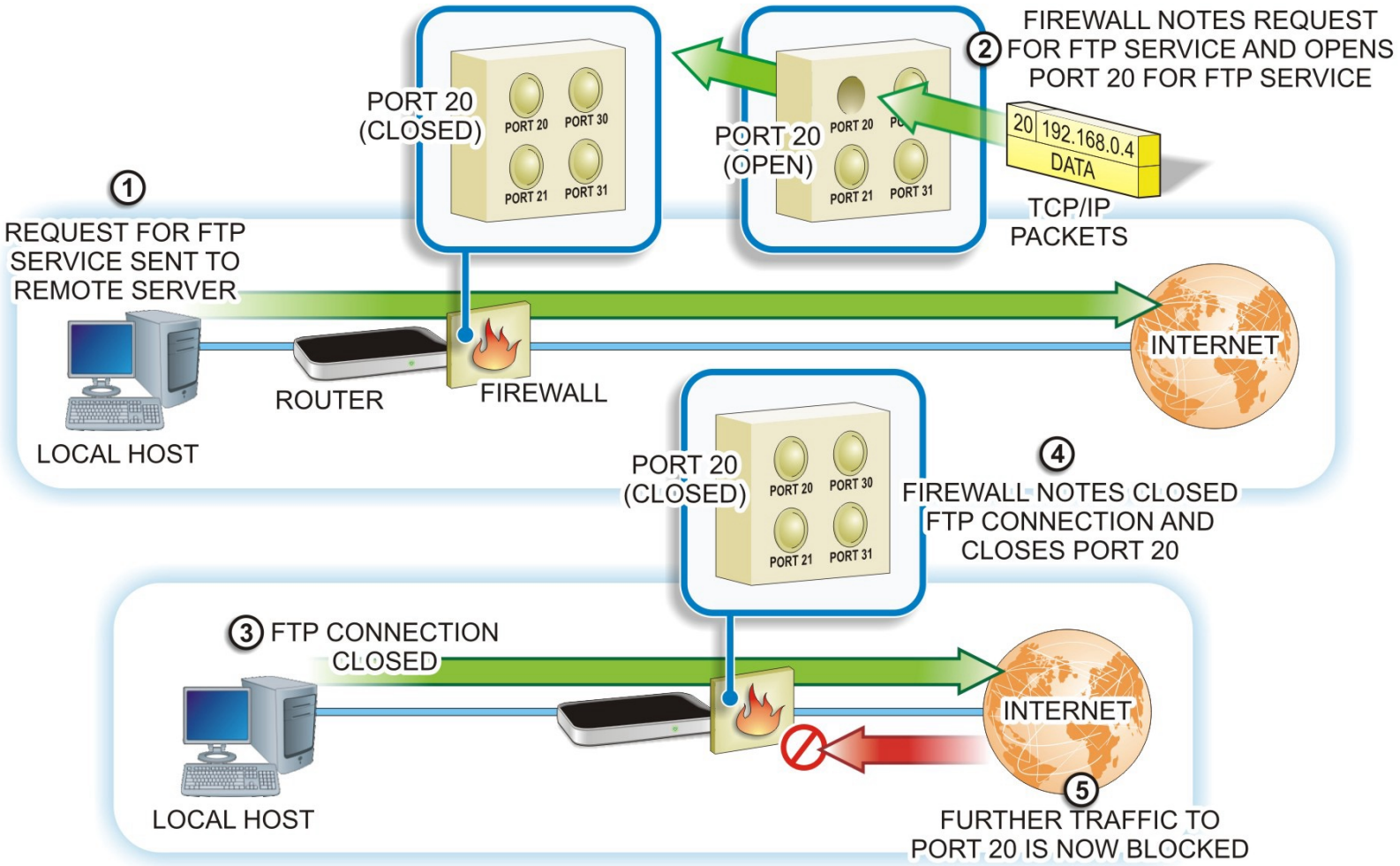
Do you have private data that must be protected or are there any liability concerns if data is obtained by outside users?

Are there regulations or laws requiring you to protect your data?

Network Firewall

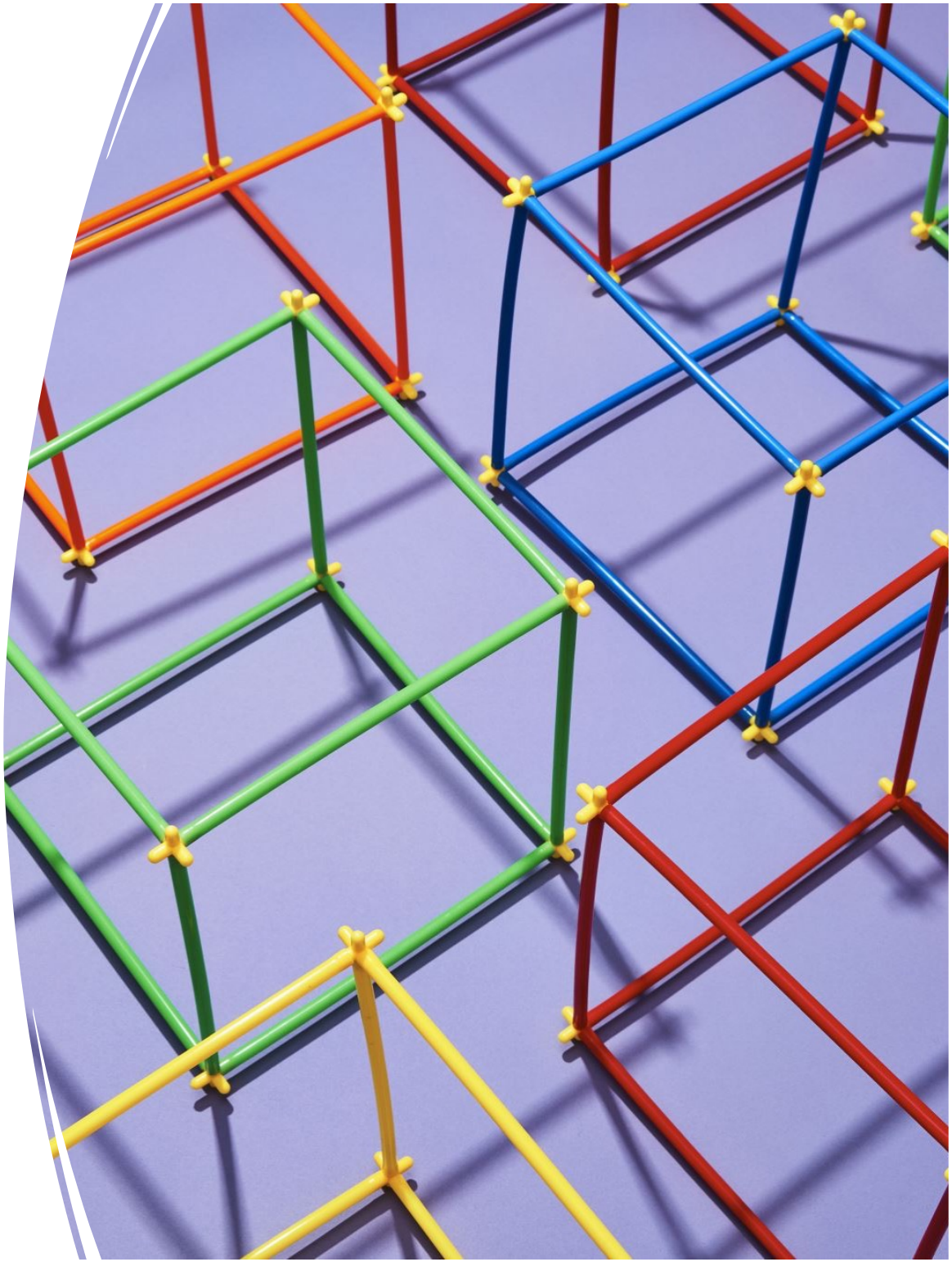


Stateful Firewall Operations



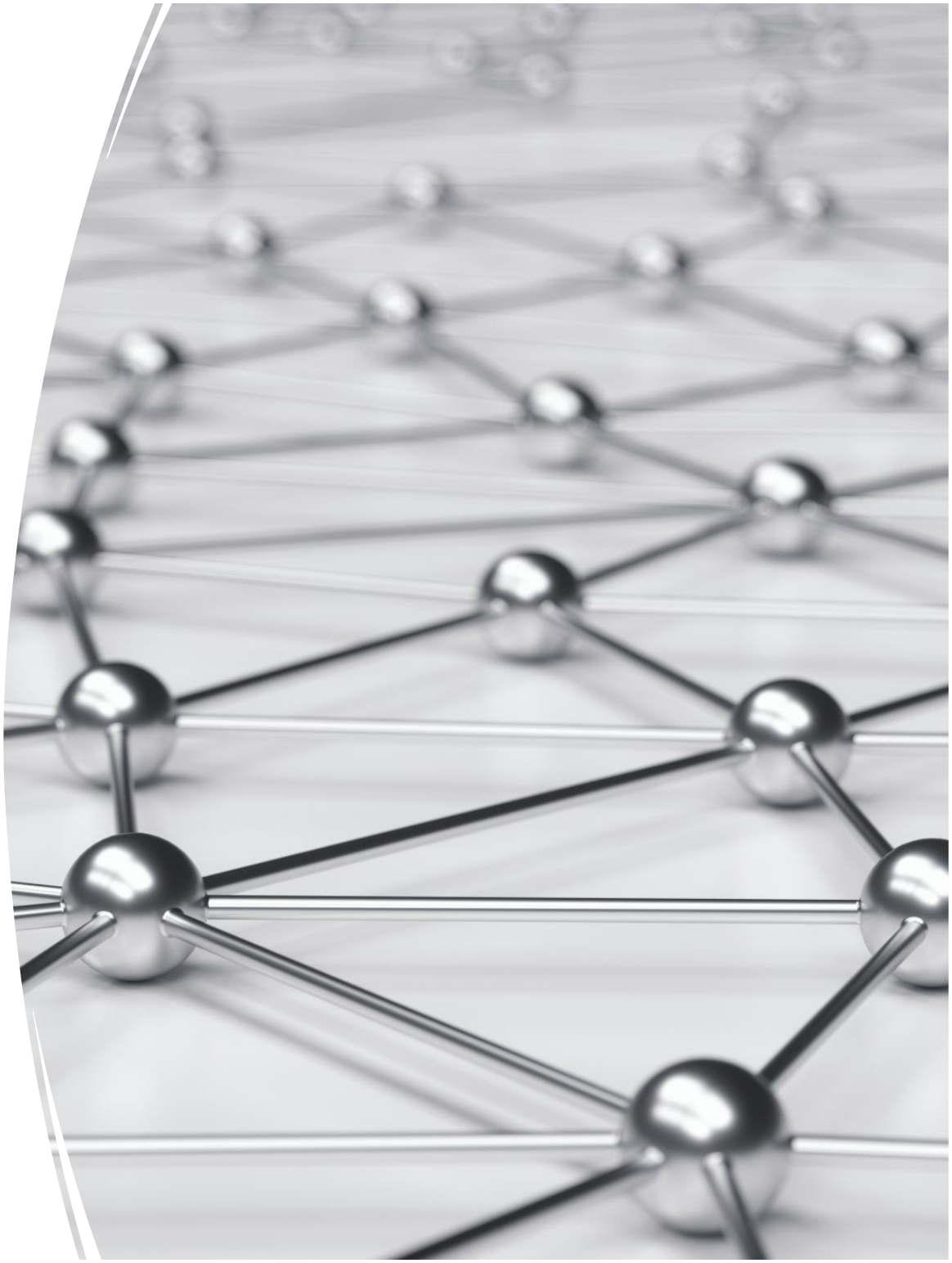
Firewall Considerations

- What applications do outside users need access to?
- Will outside users be using a VPN or not?



Network Considerations

- Resources:
  - What are the available network resources?
  - How many users will be sharing those resources?
  - If you are working with limited bandwidth, you will need to consider traffic management and QoS features.



Network Considerations

What are the most critical network services?

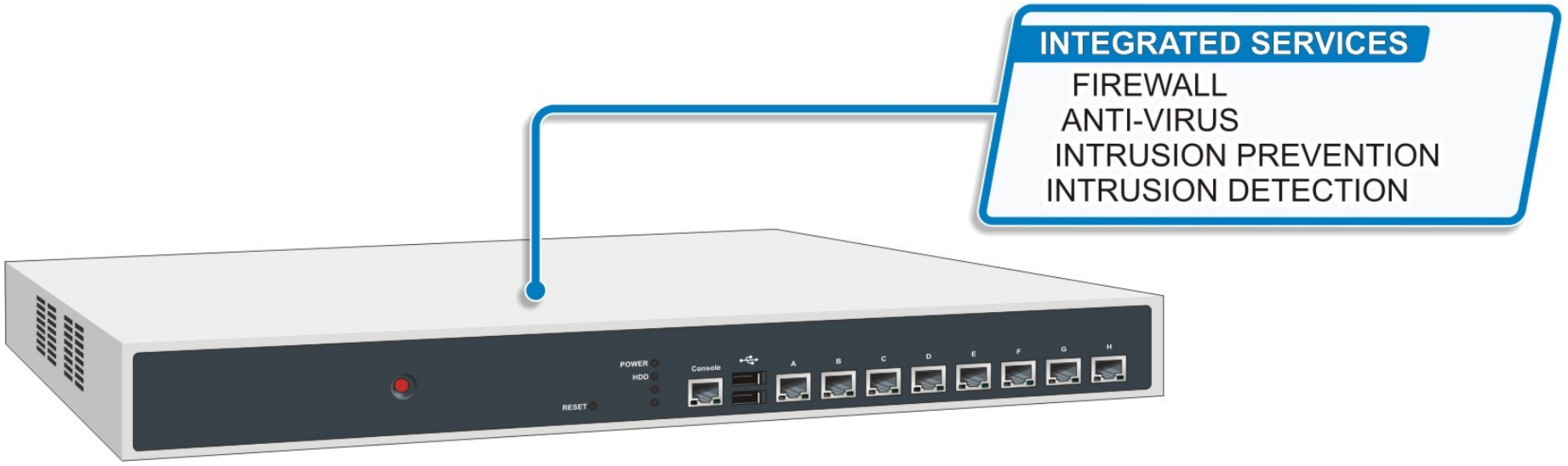
- Configure QoS to prioritize those services.

What is considered acceptable use to management?

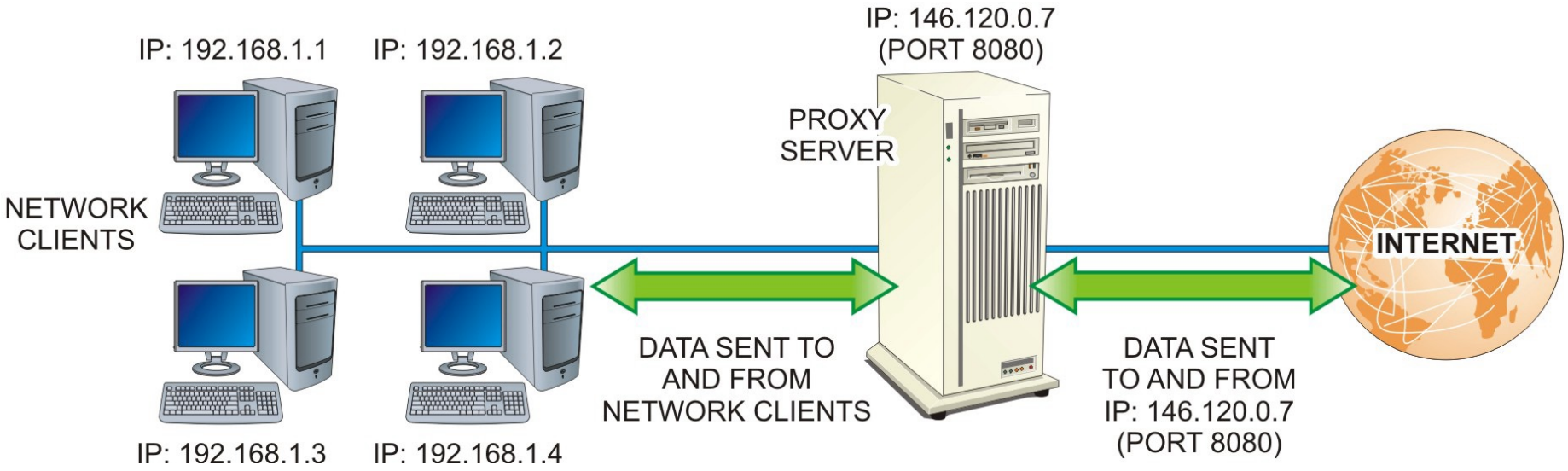
Hardware Procurement

- What remote access needs to be supported?
  - VPN support will depend on the network hardware.
  - Do you need to run an email server behind the firewall that can also be accessed by Internet users who aren't connecting through a VPN?
- How will you segment the network to minimize risks?

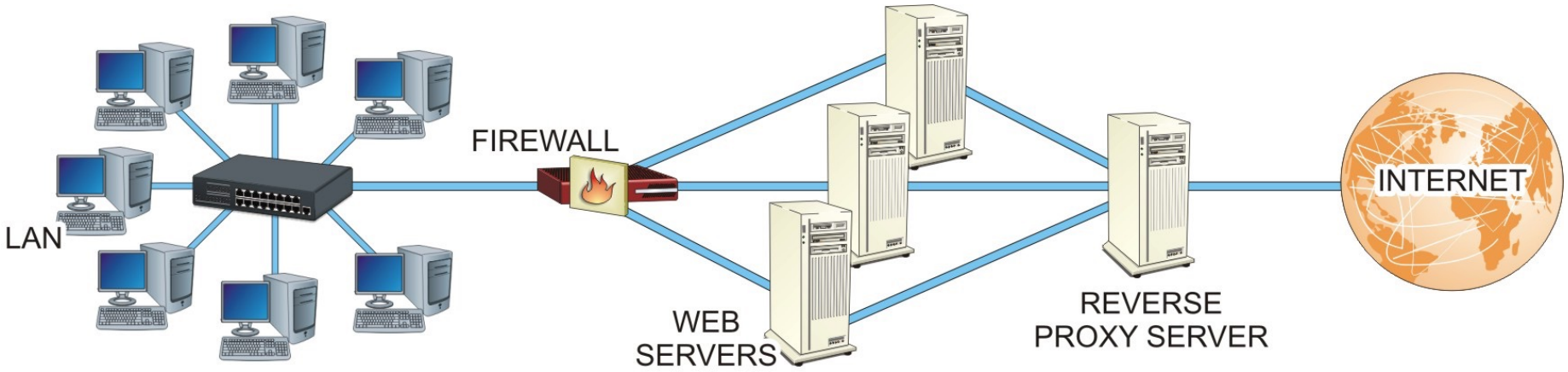
A UTM Device


INTEGRATED SERVICES
FIREWALL
ANTI-VIRUS
INTRUSION PREVENTION
INTRUSION DETECTION
POWER
HDD
RESET
Console
A
B
C
D
E
F
G
H

Operation of a Proxy Server



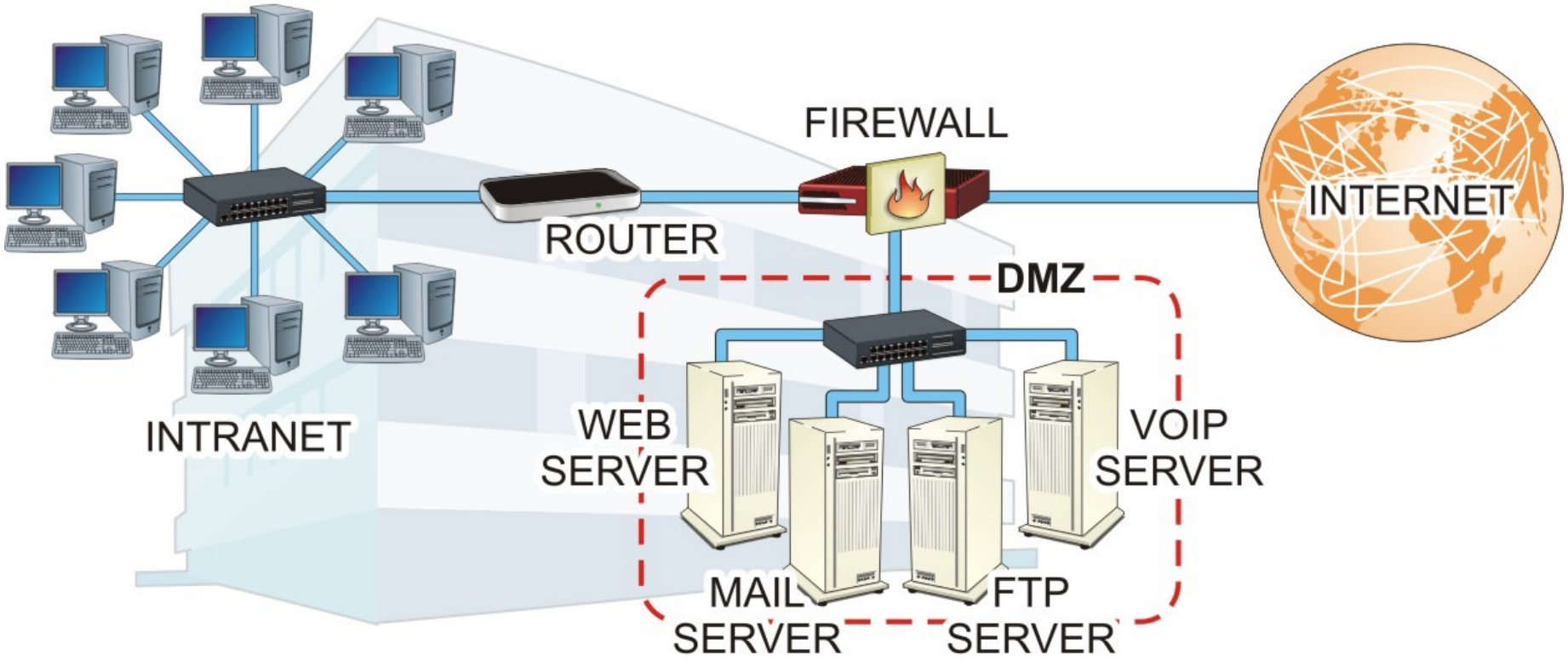
Reverse Proxy Operations



Public Access Services

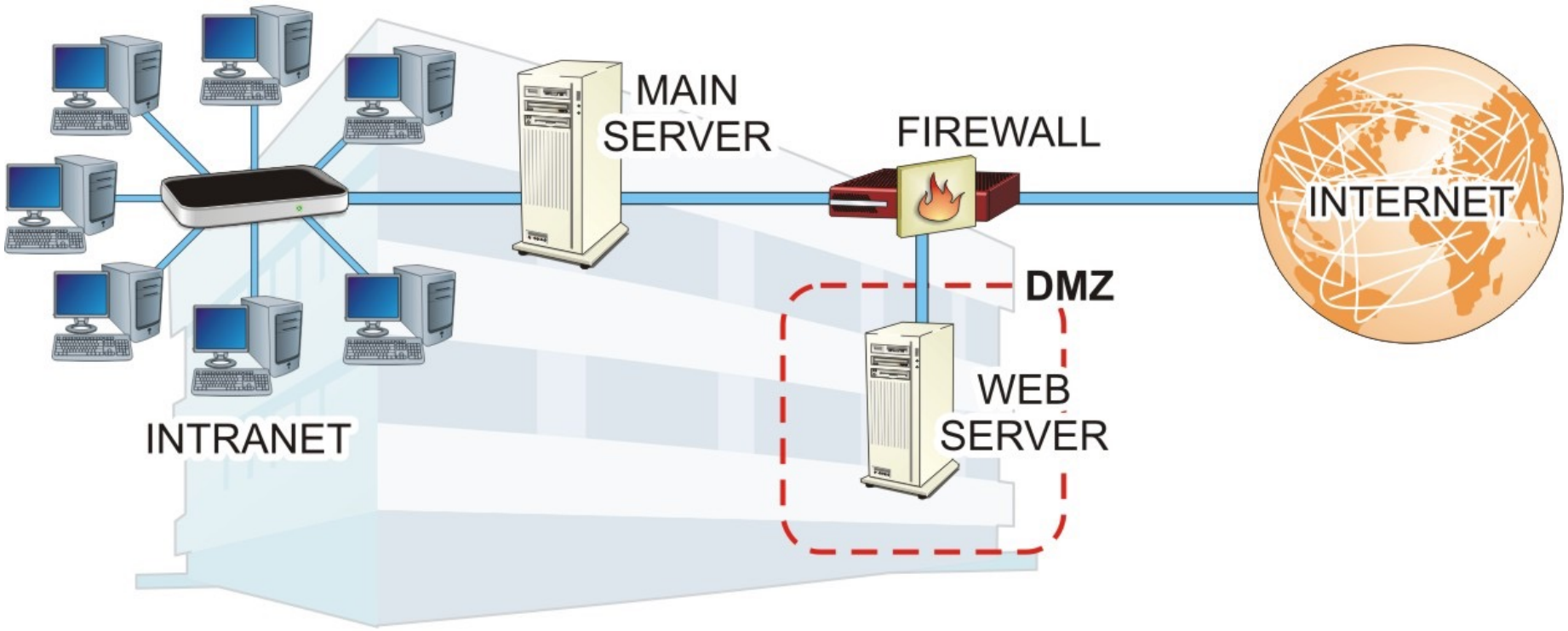
- Web servers
- Mail servers
- FTP servers
- VoIP servers

A DMZ


FIREWALL
INTERNET
ROUTER
DMZ
INTRANET
WEB
SERVER
VOIP
SERVER
MAIL
SERVER
FTP
SERVER

Single-Firewall DMZs

- One interface for the Internet (external, uncontrolled network)
- One interface for the intranet (internal, controlled network)
- One interface for the DMZ network (external, controlled network)

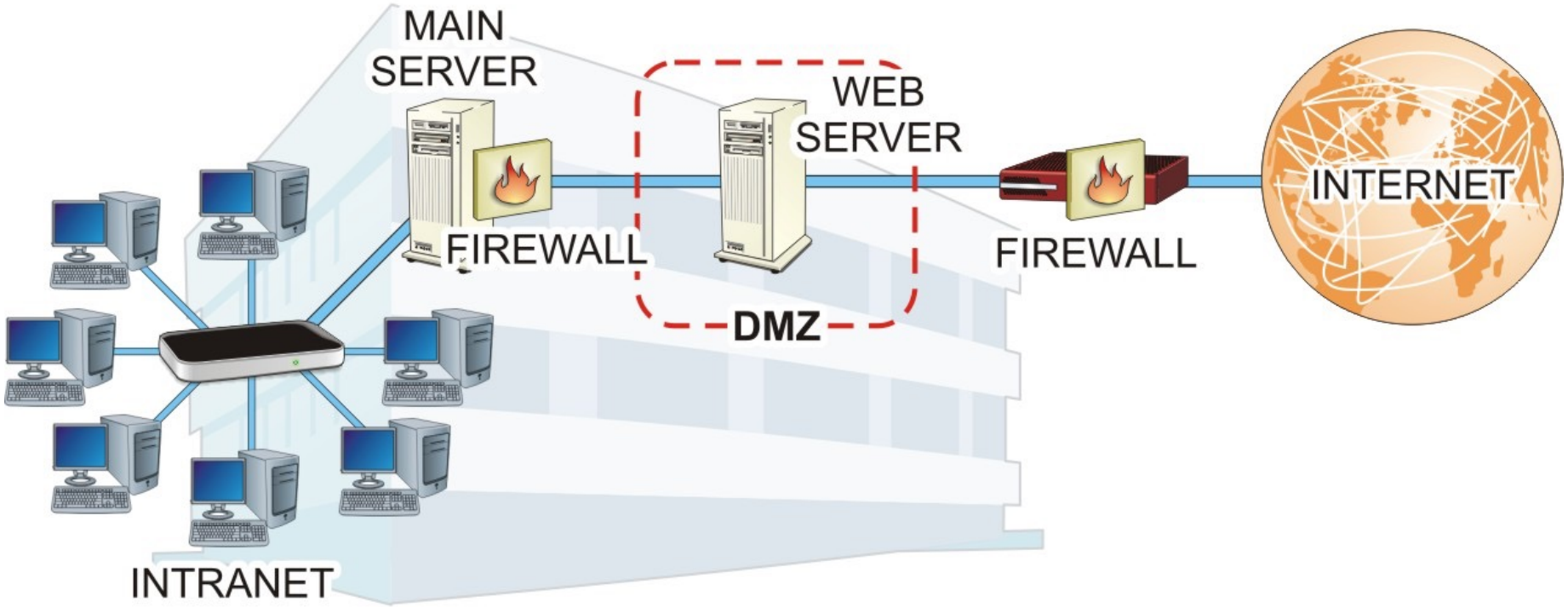


A Single-Firewall DMZ

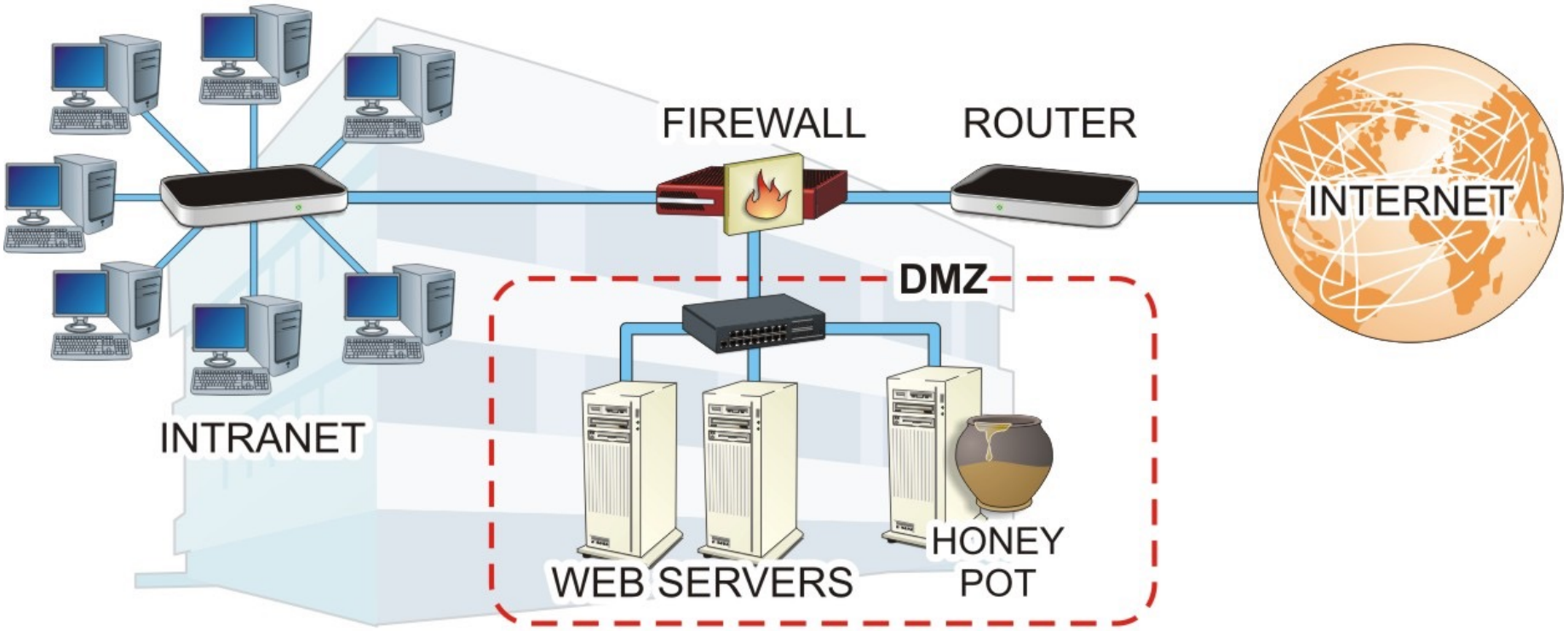
DMZ Examines All Outgoing Traffic to Determine whether it should be

- Passed from the intranet to the DMZ network to service internal requests for Web and mail services
- Passed to the intranet from the DMZ network as the response to requests from there
- Passed to the Internet

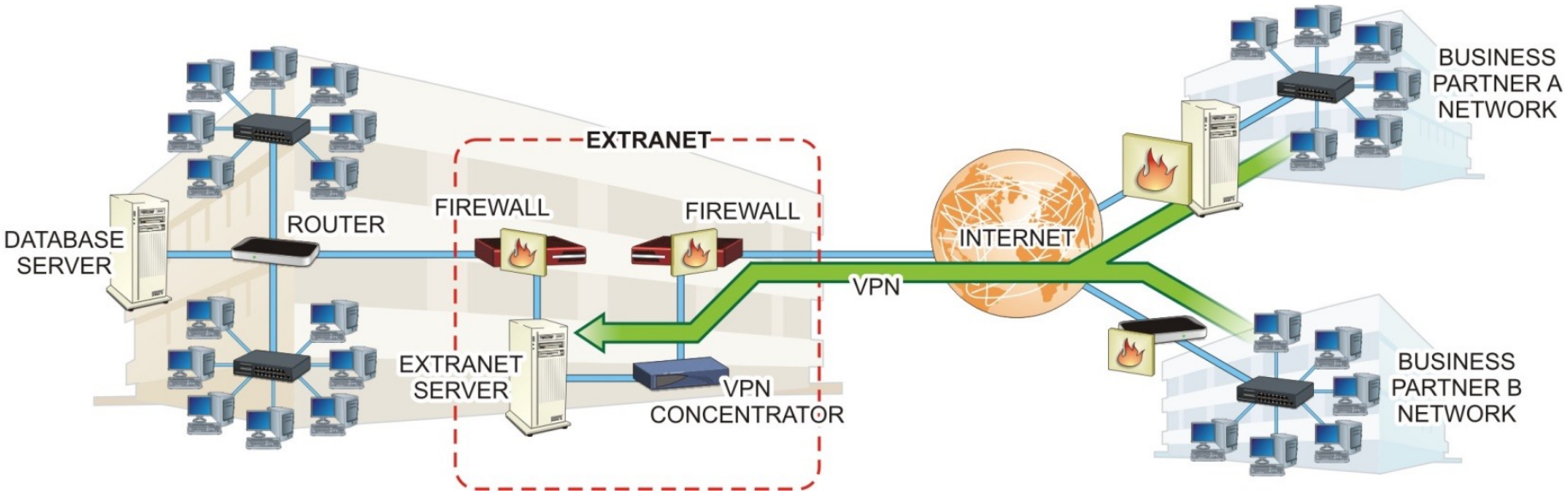
A Dual Firewall DMZ



Honey Pot Implementation



An Extranet


EXTRANET
FIREWALL
FIREWALL
ROUTER
DATABASE SERVER
INTERNET
VPN
BUSINESS PARTNER A NETWORK
BUSINESS PARTNER B NETWORK
EXTRANET SERVER
VPN CONCENTRATOR

Hands-On Exercises Objectives

- The purpose of this lab is to set up a VPN and confirm that the VPN is working. You will download and install software, configure the software, and examine the difference before using a VPN and after using a VPN.

Questions