CALIFORNIA STATE UNIVERSITY
LONG BEACH
College of Engineering

CECS 303: Networks and Network Security

VLANs and Firewalls

Chris Samayoa

Week 7 – 1st Lecture
3/1/2022

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

- Vulnerability Discussion
- VLANs
- Firewalls (cont’d)

Log4j Wrap-up

- Fix essentially revolves around disabling LDAP protocol calls from JNDI
  - Only Java protocol allowed from JNDI
- https://logging.apache.org/log4j/2.x/security.html#Fixed_in_Log4j_2.15.0
  - Review this link for more detail on fix for primary and follow-up CVEs

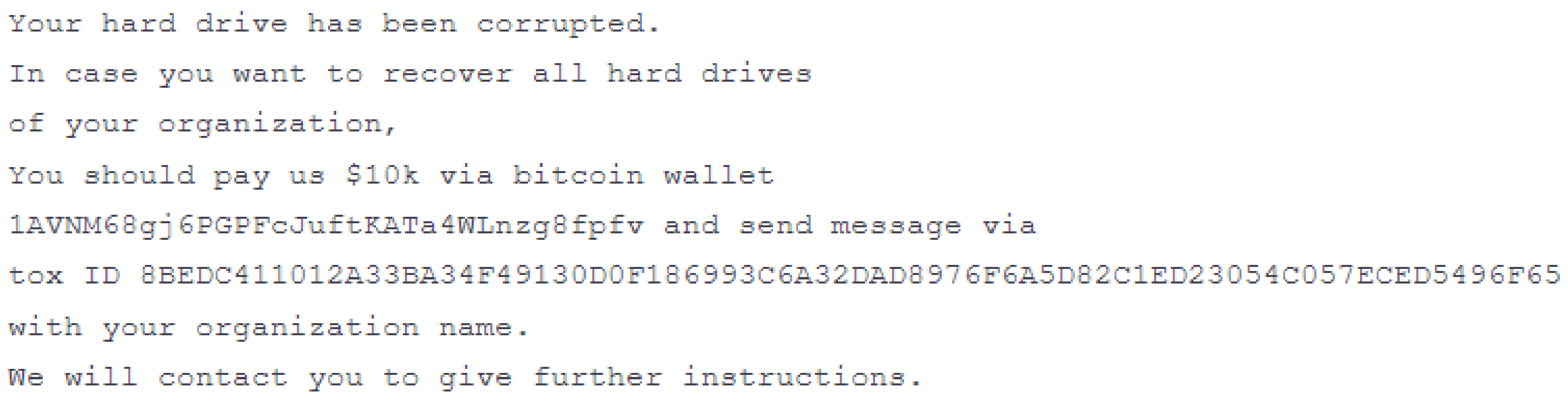
Wiper Malware Overview

- WhisperGate
  - Identified by Microsoft Threat Intelligence Center (MSTIC)
    - Tracked as DEC-0586
    - https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/
  - First seen on January 13,2022 (Ukraine systems)
    - Reported on January 15, 2022
  - Targeted government, non-profit, and information technology organizations
- HermeticWiper
  - Discovered by Symantec or ESET research centers
  - First seen on February 23, 2022
  - Targeting organizations in Ukraine
  - https://www.sentinelone.com/labs/hermetic-wiper-ukraine-under-attack/

WhisperGate

- Observed activity
  - Overwriting Master Boot Record (MBR)
    - Part of hard drive that tells computer how to load its operating system
  - Malware often named stage.exe
    - Common directories used: C:\PerfLogs, C:\ProgramData, C:\, and C:\temp
- Stage 1
  - Overwrites MBR with a ransom note
    - Ransom note is a ruse
    - No mechanism for recovery
  - Malware executes when the device is powered down

WhisperGate Ransom Note

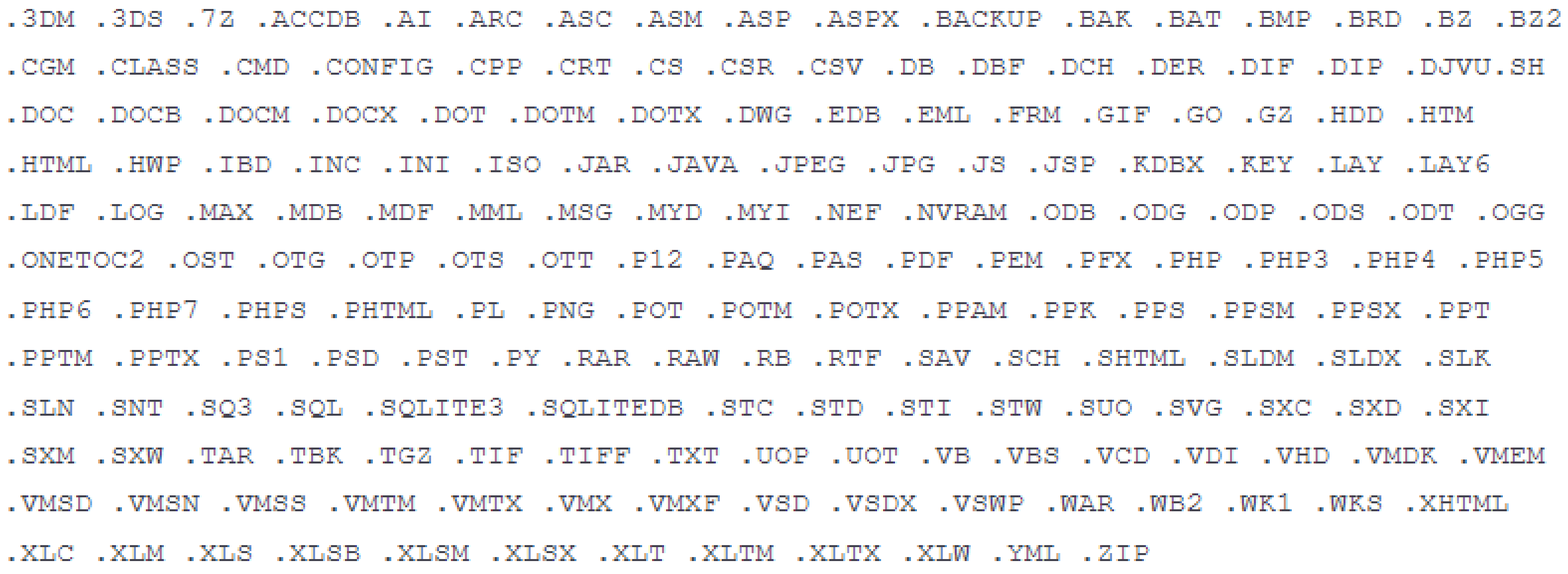


```
Your hard drive has been corrupted.
In case you want to recover all hard drives
of your organization,
You should pay us $10k via bitcoin wallet
1AVNM68gj6PGPFcJuftKATa4WLnzg8fpfv and send message via
tox ID 8BEDC411012A33BA34F49130D0F186993C6A32DAD8976F6A5D82C1ED23054C057ECED5496F65
with your organization name.
We will contact you to give further instructions.
```

Source: https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/

WhisperGate (cont’d)

- Stage 2
  - Stage2.exe downloads additional malware
  - Corrupter locates files with specific extensions and overwrites content



```
.3DM .3DS .7Z .ACCDB .AI .ARC .ASC .ASM .ASP .ASPX .BACKUP .BAK .BAT .BMP .BRD .BZ .BZ2
.CGM .CLASS .CMD .CONFIG .CPP .CRT .CS .CSR .CSV .DB .DBF .DCH .DER .DIF .DIP .DJVU.SH
.DOC .DOCB .DOCM .DOCX .DOT .DOTM .DOTX .DWG .EDB .EML .FRM .GIF .GO .GZ .HDD .HTM
.HTML .HWP .IBD .INC .INI .ISO .JAR .JAVA .JPEG .JPG .JS .JSP .KDBX .KEY .LAY .LAY6
.LDF .LOG .MAX .MDB .MDF .MML .MSG .MYD .MYI .NEF .NVRAM .ODB .ODG .ODP .ODS .ODT .OGG
.ONETOC2 .OST .OTG .OTP .OTS .OTT .P12 .PAQ .PAS .PDF .PEM .PFX .PHP .PHP3 .PHP4 .PHP5
.PHP6 .PHP7 .PHPS .PHTML .PL .PNG .POT .POTM .POTX .PPAM .PPK .PPS .PPSM .PPSX .PPT
.PPTM .PPTX .PS1 .PSD .PST .PY .RAR .RAW .RB .RTF .SAV .SCH .SHTML .SLDM .SLDX .SLK
.SLN .SNT .SQ3 .SQL .SQLITE3 .SQLITEDB .STC .STD .STI .STW .SUO .SVG .SXC .SXD .SXI
.SXM .SXW .TAR .TBK .TGZ .TIF .TIFF .TXT .UOP .UOT .VB .VBS .VCD .VDI .VHD .VMDK .VMEM
.VMSD .VMSN .VMSS .VMTM .VMTX .VMX .VMXF .VSD .VSDX .VSWP .WAR .WB2 .WK1 .WKS .XHTML
.XLC .XLM .XLS .XLSB .XLSM .XLSX .XLT .XLTM .XLTX .XLW .YML .ZIP
```

HermeticWiper

- Additional information
  - Digital certificate used to sign malware issued under company name "Hermetica Digital Ltd" (valid as of 2021)
    - Not currently associated with any legitimate files
- Observed activity
  - Attacks Windows machines
  - Uses driver 'empntdrv.sys' to entry point for attack
  - Goal is to execute wiper malware
    - Also targets MBR for every physical drive connected to affected system (focuses on first 512 bytes)
  - Randomizes partitions as well (differentiates between FAT and NTFS partitions for behavior)

CISA Alert

- Cybersecurity & Infrastructure Security Agency (CISA)
  - https://www.cisa.gov/uscert/ncas/alerts/aa22-057a
  - TLP: White
- Recommended mitigation
  - Scan for indicators of compromise (IOCs) using network defense tools
  - Proper network segmentation to minimize propagation
  - Principle of least privilege (ACLs and local/domain authorization)

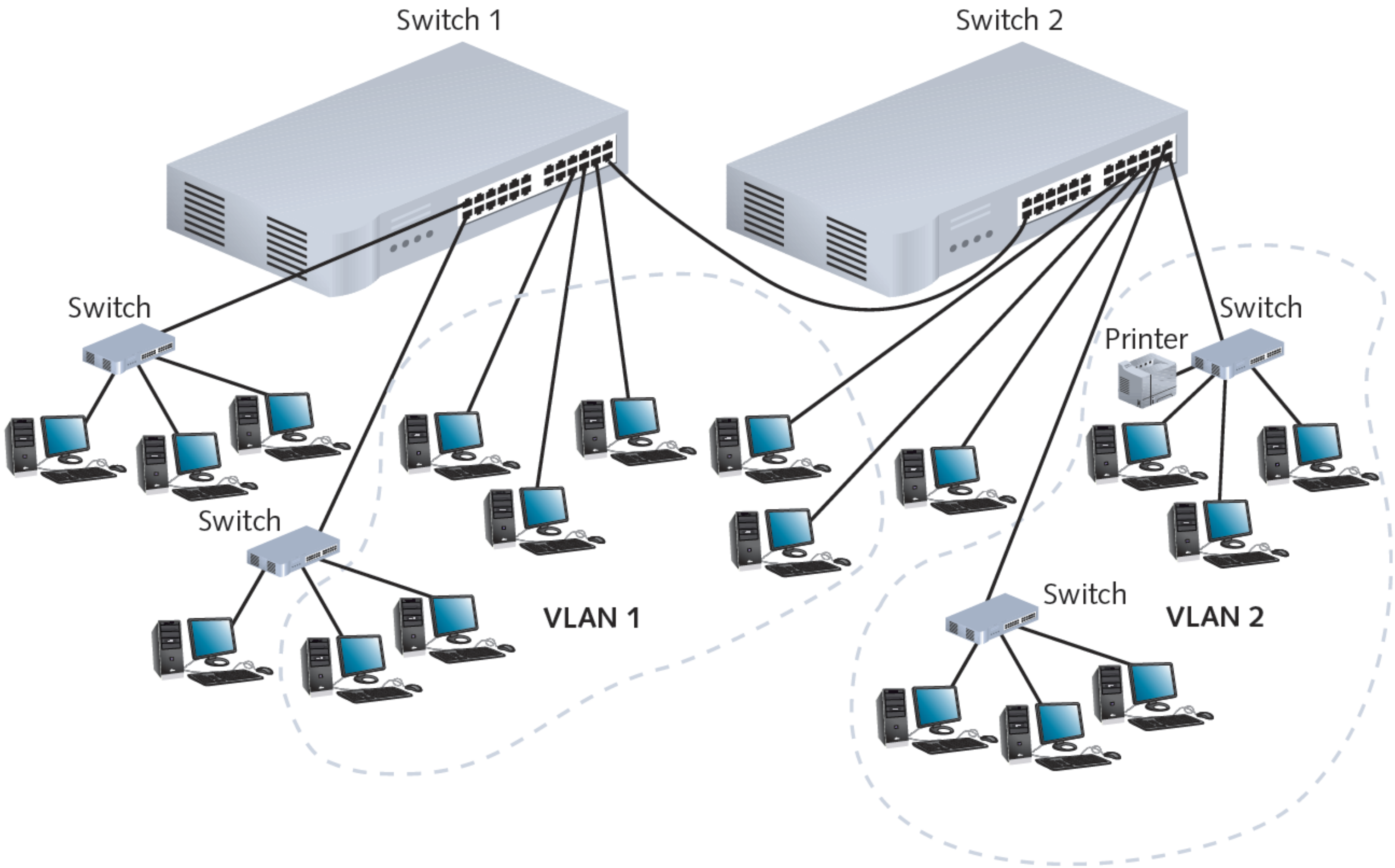
Objectives

- Vulnerability Discussion
- 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

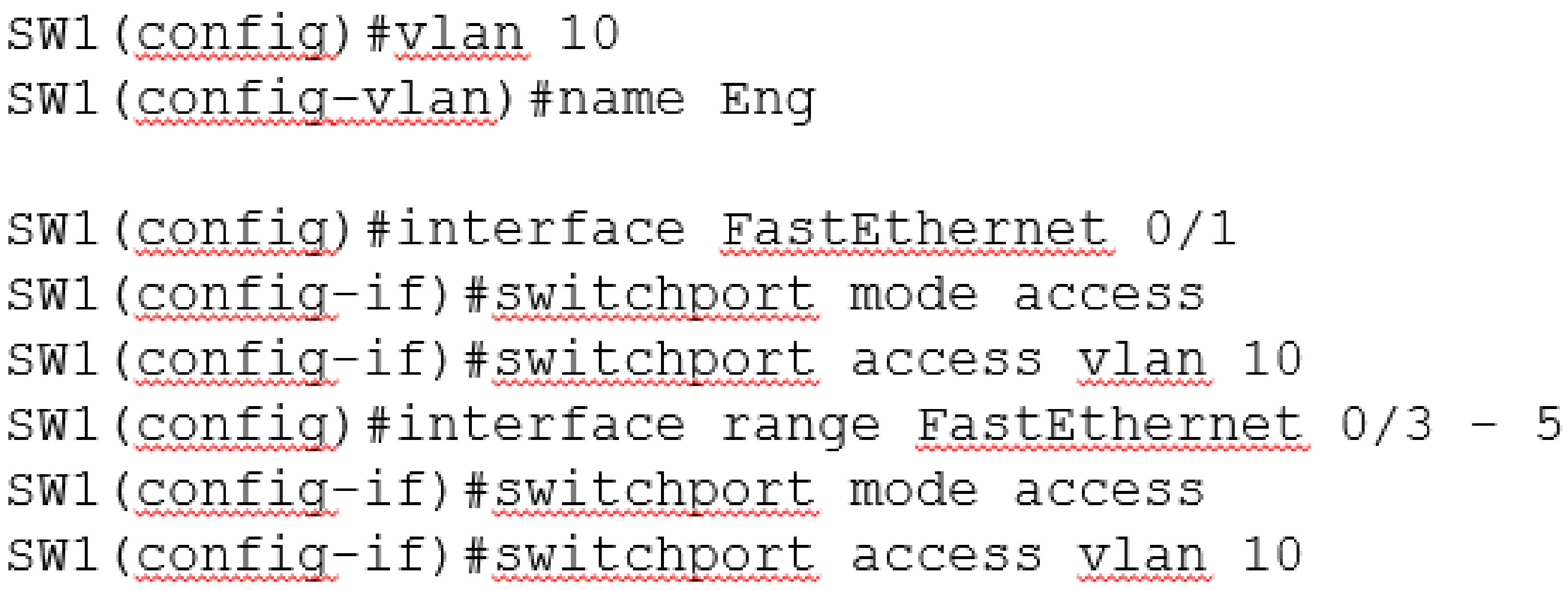
VLANs (cont’d)

- 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

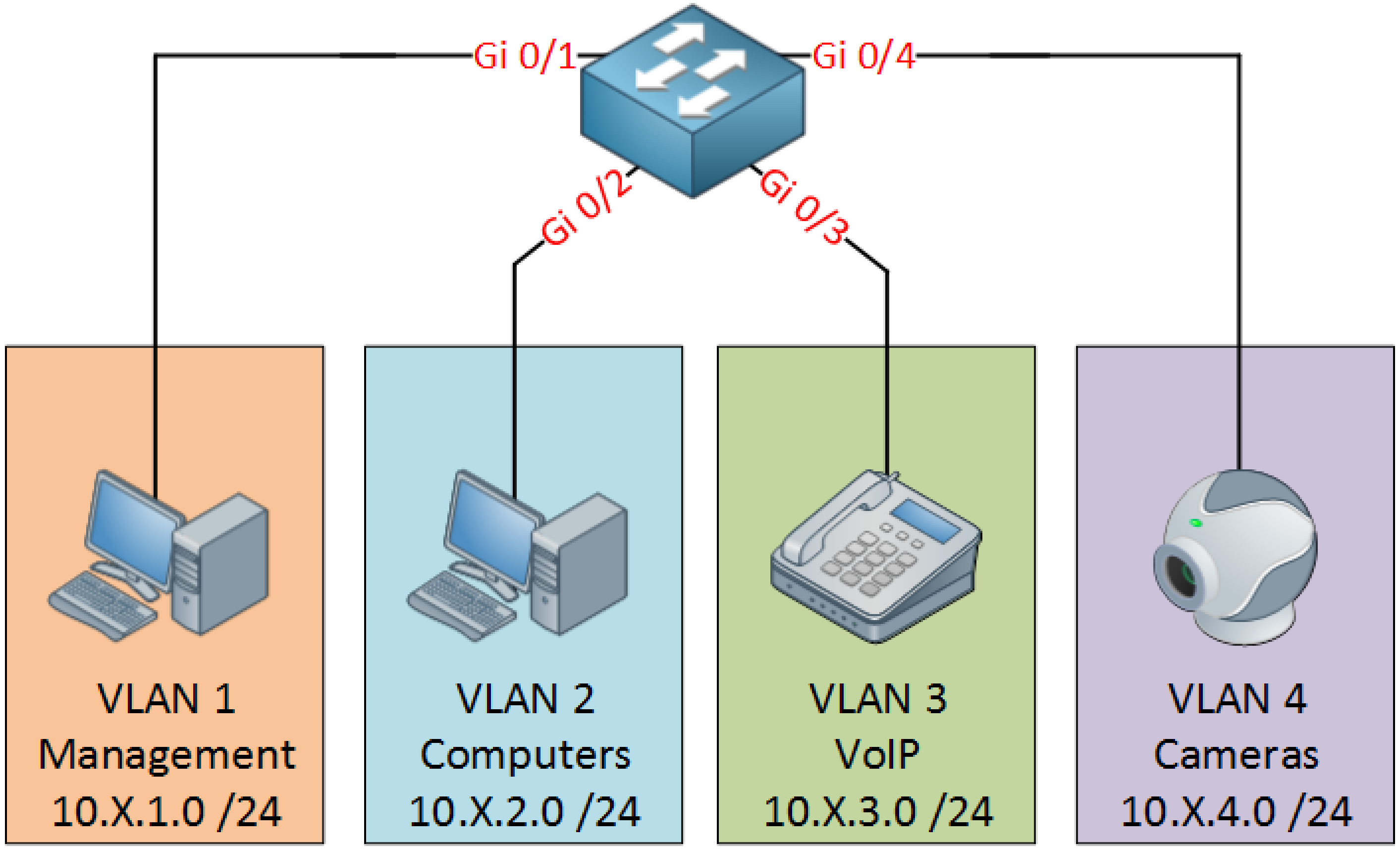


```
SW1(config)#vlan 10
SW1(config-vlan)#name Eng

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

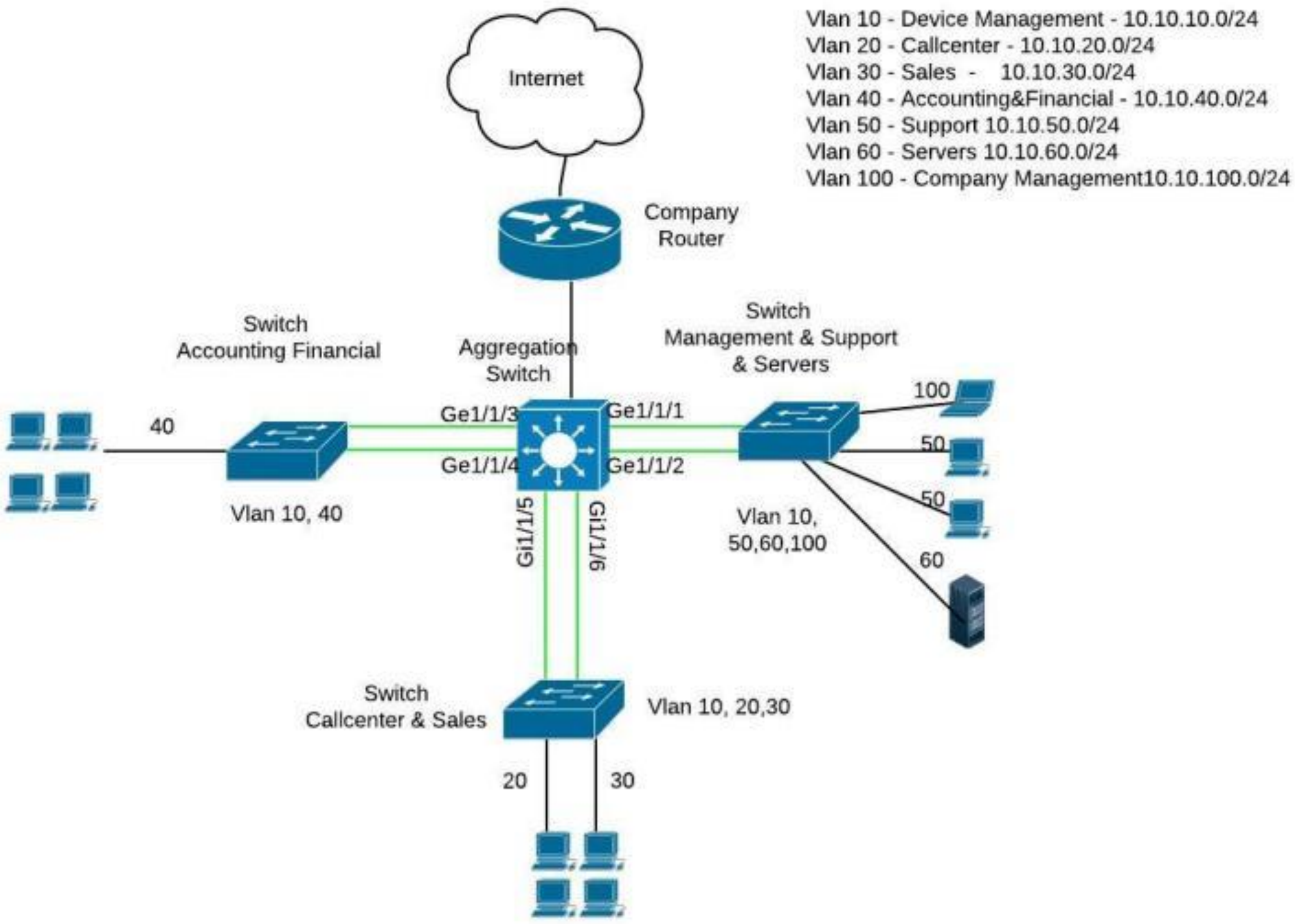


Source: https://networklessons.com/switching/cisco-small-business-switch-vlan-configuration

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

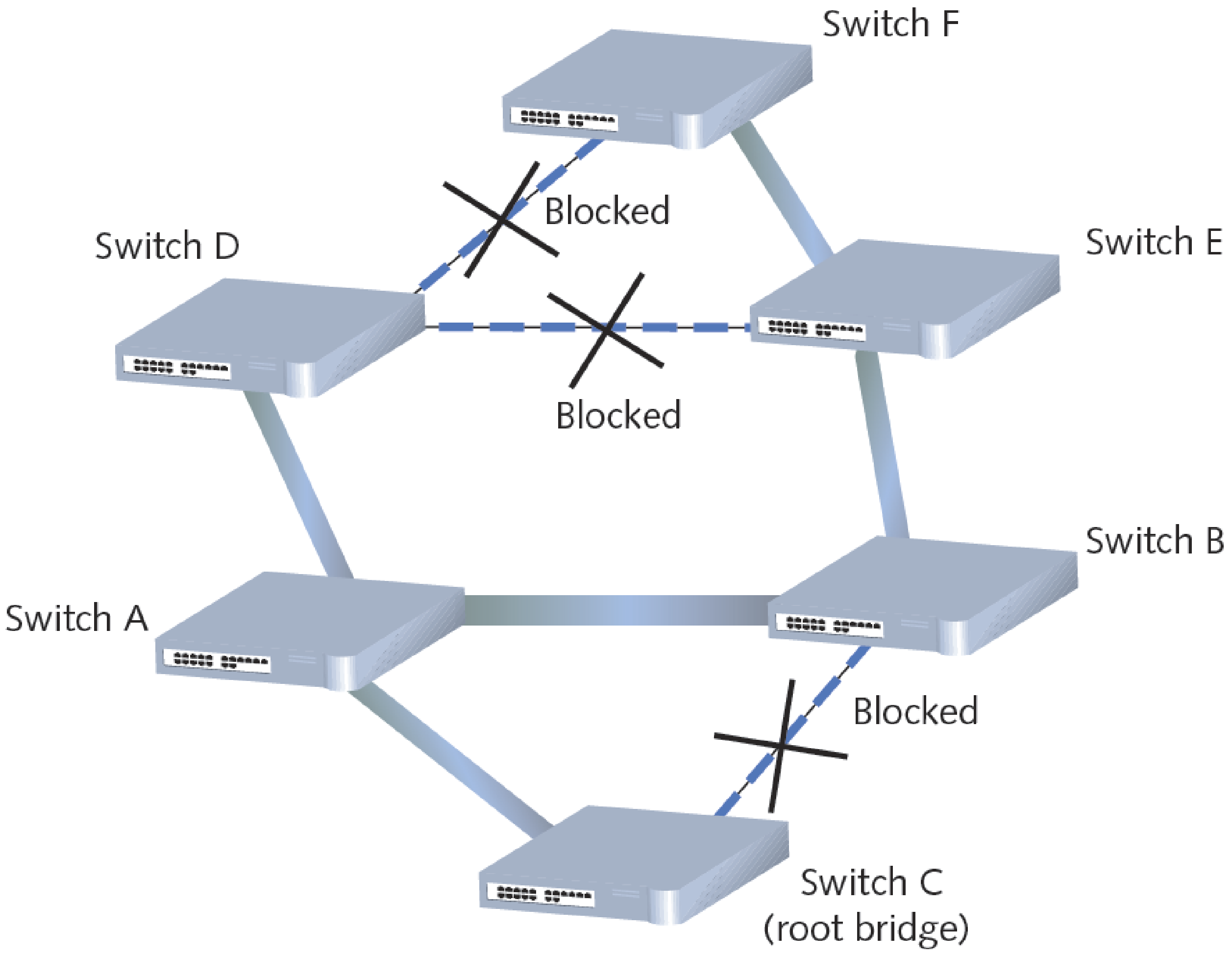
```
interface GigabitEthernet0/3
 description  Server
 switchport access vlan 60
 switchport mode access
 spanning-tree portfast  <—— allows immediate transition of the
                             port into forwarding state
 spanning-tree bpduguard enable <——- if a BPDU is received on the
         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

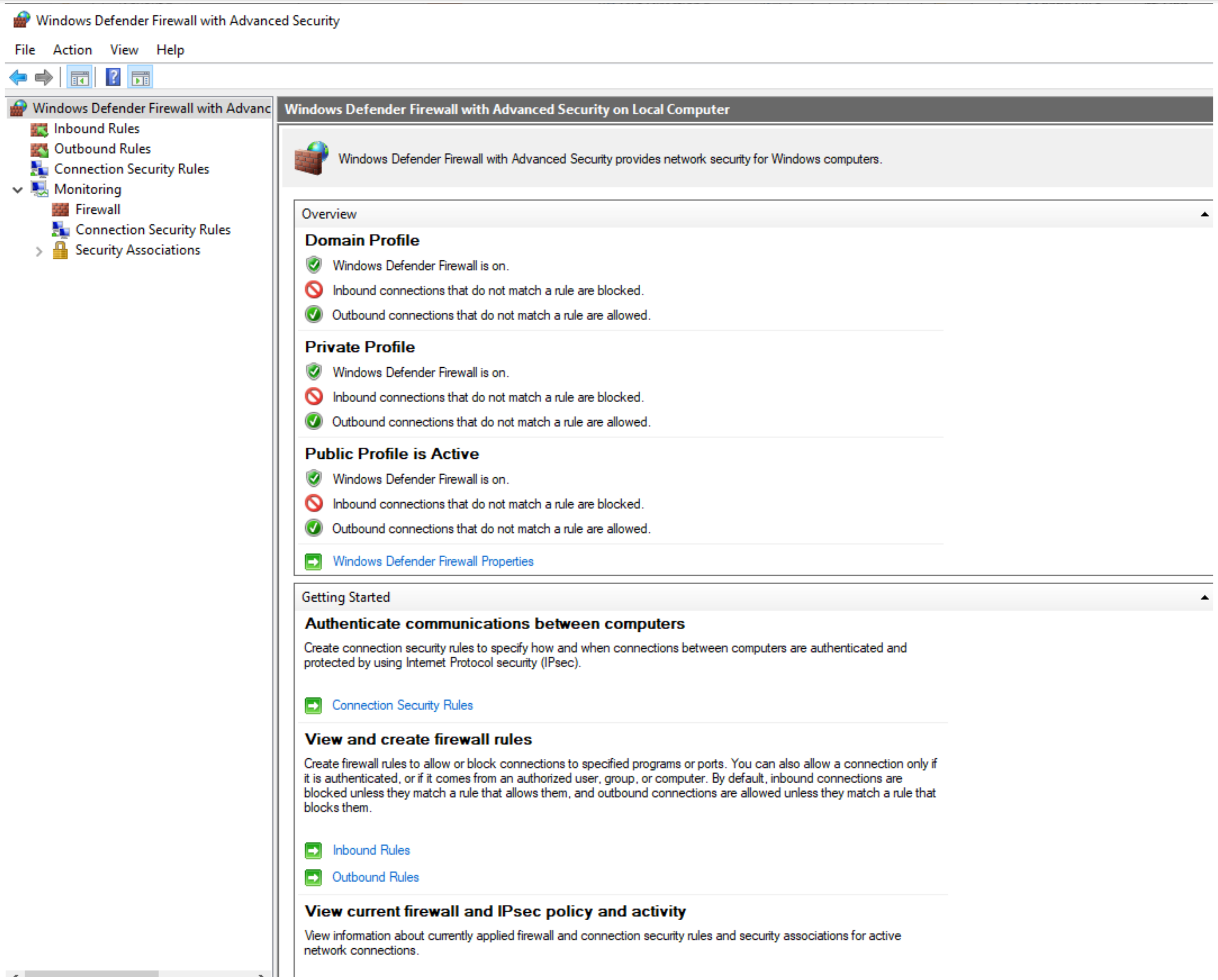
Objectives

- Vulnerability Discussion
- 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
Overview
Getting Started

Windows Defender Firewall with Advanced Security on Local Computer

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

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

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.

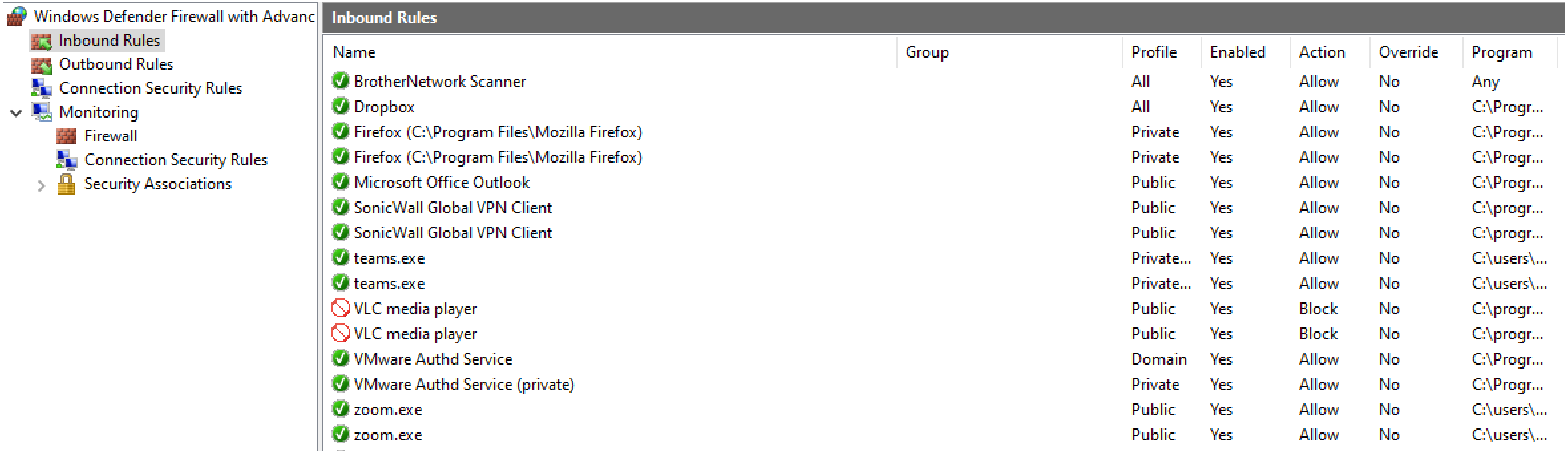
Inbound Rules

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

- 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