

Secure Network Administration Principles

Christopher Rees

<https://www.linkedin.com/in/cdrees>

@cdrees

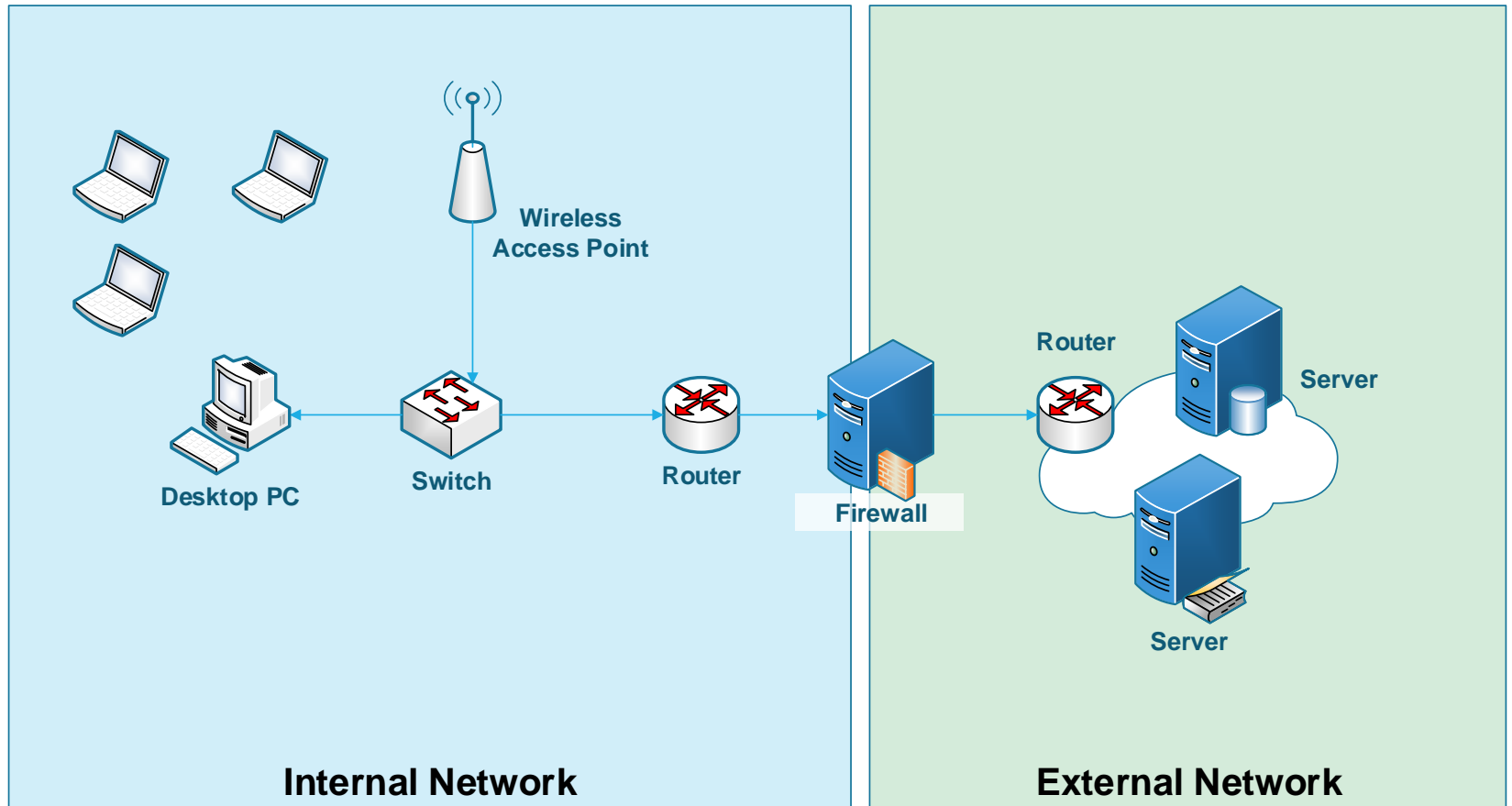


pluralsight 
hardcore dev and IT training


Module Overview

- Rule-Based Management
 - Firewall Rules
 - Implicit Deny
 - Secure Router Configuration
 - Access Control Lists (ACLs)
 - VLAN Management
 - Network Separation
 - Port Security
 - 802.1x
 - Flood Guards
 - Loop Protection
 - Log Analysis
 - UTM
- Securing Flow of Traffic**
- Securing and Separating Network Segments**
- Securing Physical Access to the Network**
- Ensuring Availability**
- Proactive Review/Analysis of Security Logs**
-

Scenario for Module Concepts



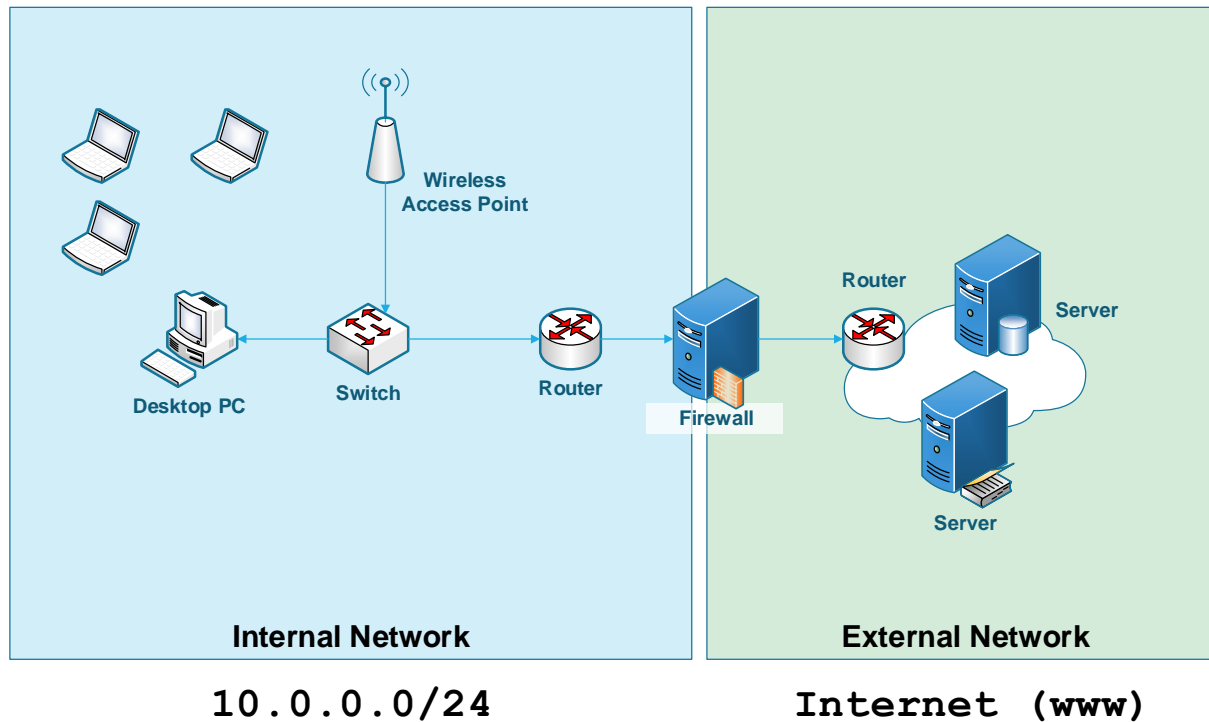
Module Overview

- Rule-Based Management
 - Firewall Rules
 - Implicit Deny
 - Secure Router Configuration
 - Access Control Lists (ACLs)
 - VLAN Management
 - Network Separation
 - Port Security
 - 802.1x
 - Flood Guards
 - Loop Protection
 - Log Analysis
 - UTM
- 
- Securing Flow of Traffic**

Rule/Role-Based Access Control

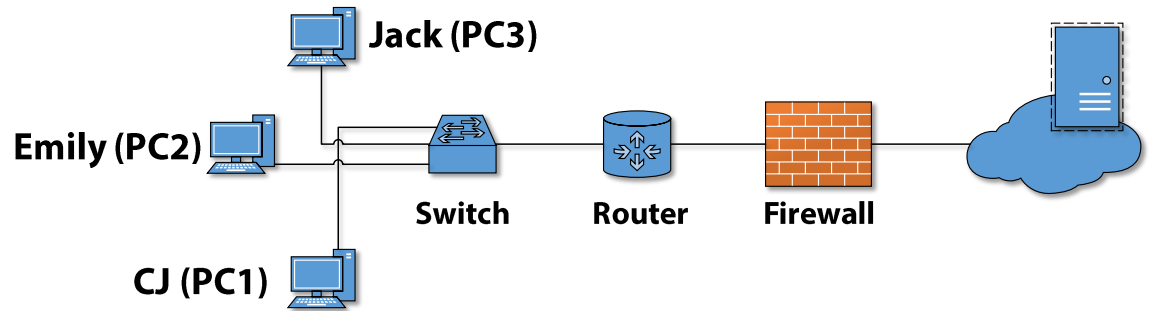
■ RBAC

- Popular method of enable access to a resource and is based on pre-defined policies set by an administrator



Access Control List

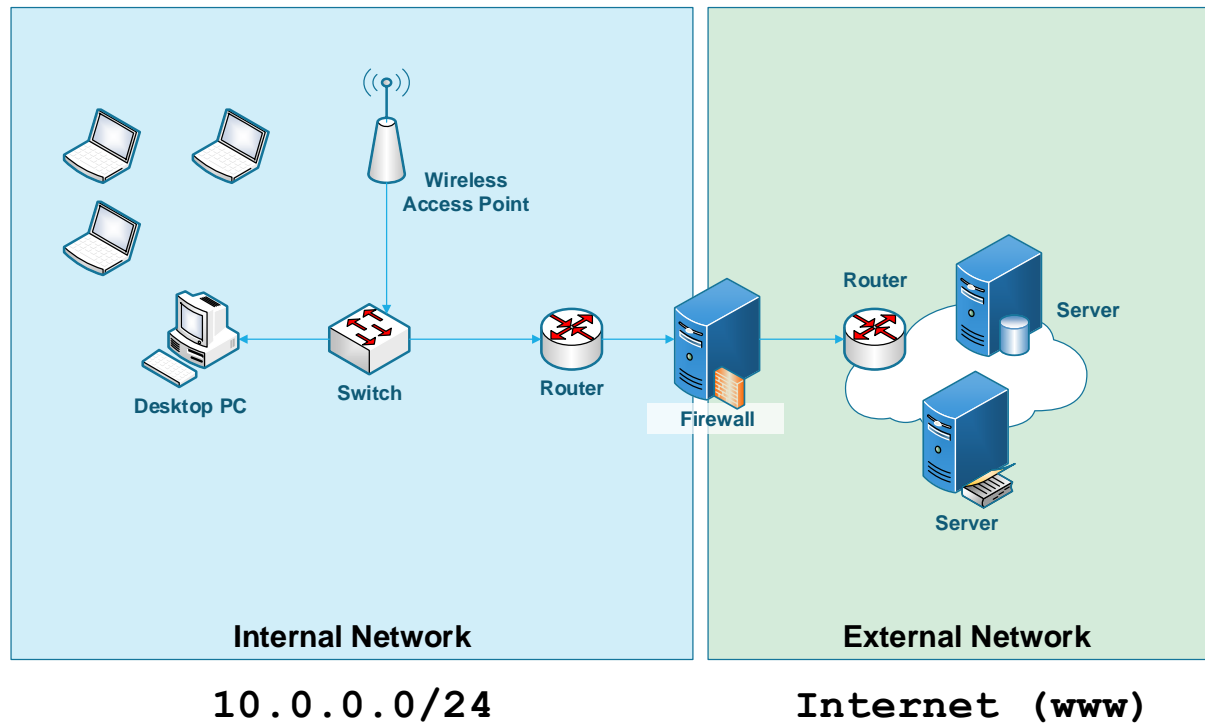
- Designed to explicitly permit certain IP address, IP ranges or protocols
 - Implicitly denying the rest
- Permit the following protocols
 - HTTP (80)
 - HTTPS (443)
 - SSH (22)
 - RDP (3389)
- Implicitly deny the rest
 - FTP (21)
 - Telnet (23)



Access Control List Example

```
Firewall(config)#  
Firewall(config)#  
Firewall(config)#  
Firewall(config)#  
Firewall(config)#  
Firewall(config)#  
Firewall(config)#  
Firewall(config)#  
Firewall(config)#  
Firewall(config)#
```

	Action	Network	Mask	Destination
access-list 150 permit TCP 10.0.0.0	permit	10.0.0.0	255.255.255.0	any eq 80
access-list 150 permit TCP 10.0.0.0	permit	10.0.0.0	255.255.255.0	any eq 443



Secure Network Administration

- Rule-Based Management
- Firewall Rules
- Implicit Deny
- Secure Router Configuration
- Access Control Lists (ACLs)

- VLAN Management

- Network Separation



Securing and Separating Network Segments

- Port Security
- 802.1x
- Flood Guards
- Loop Protection
- Log Analysis
- UTM

VLANs and Network Separation

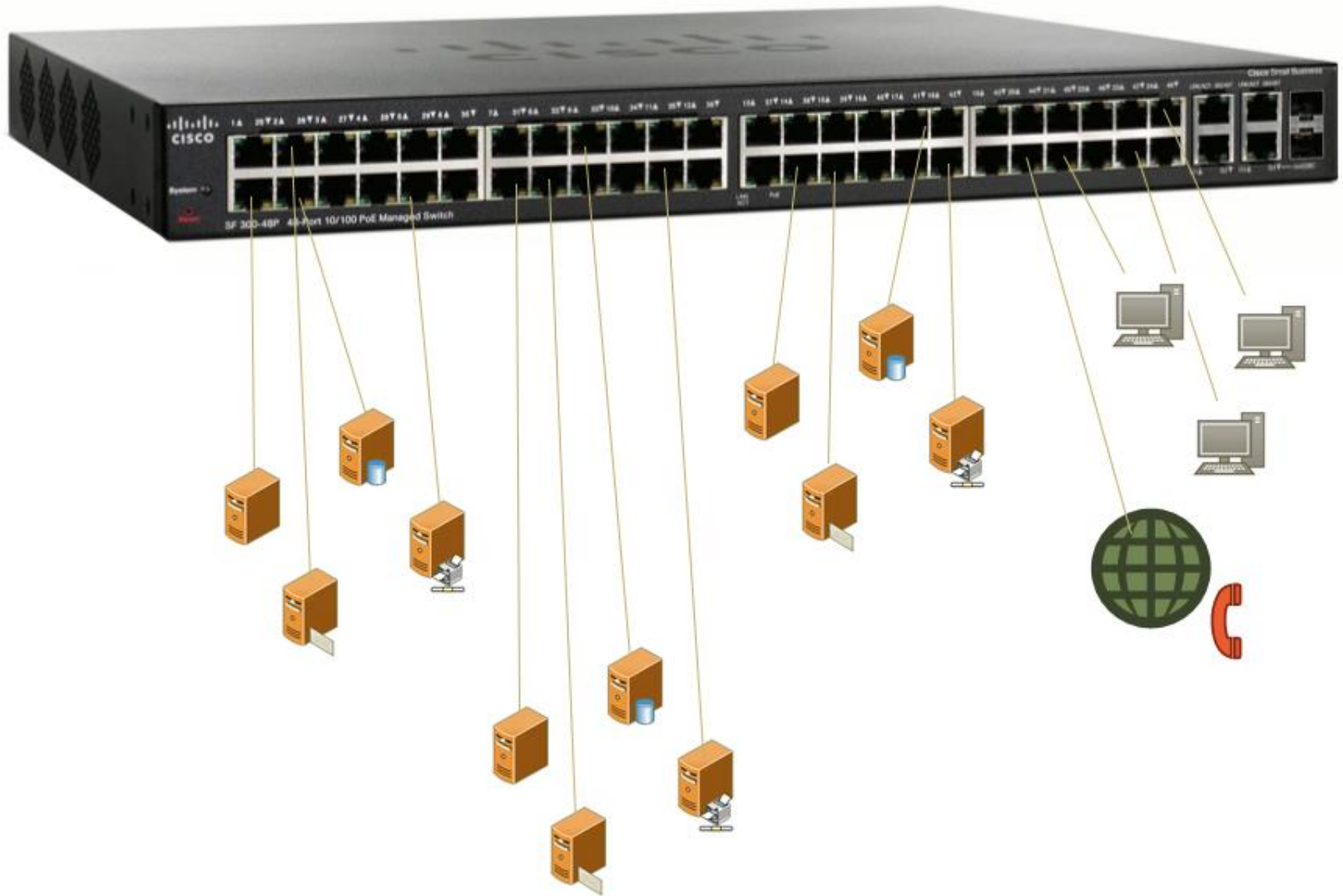
- Virtual Local Area Network (VLAN)
 - Creates separate “Broadcast Domains”
 - Separates traffic, reduces collisions
 - Increases security



VLANs and Network Separation



VLANs and Network Separation

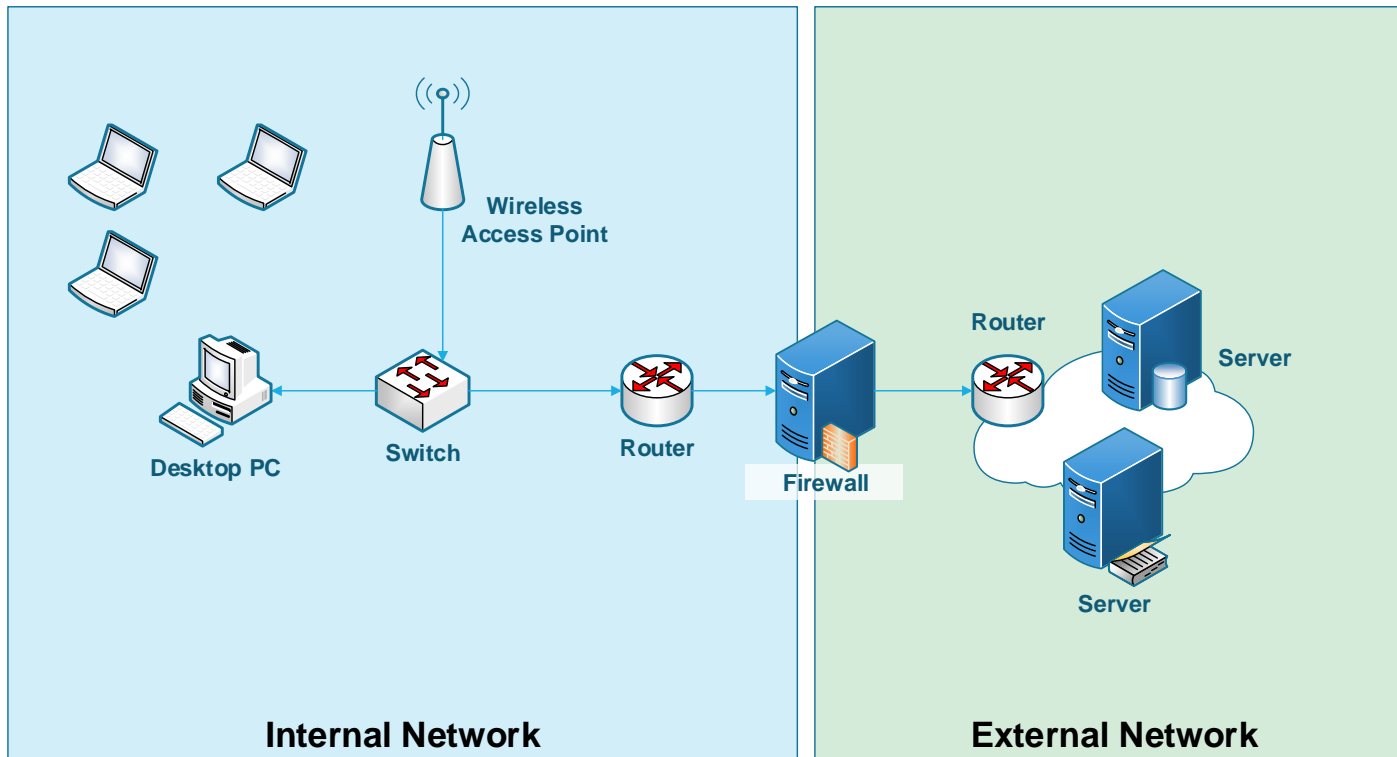


VLANs and Network Separation



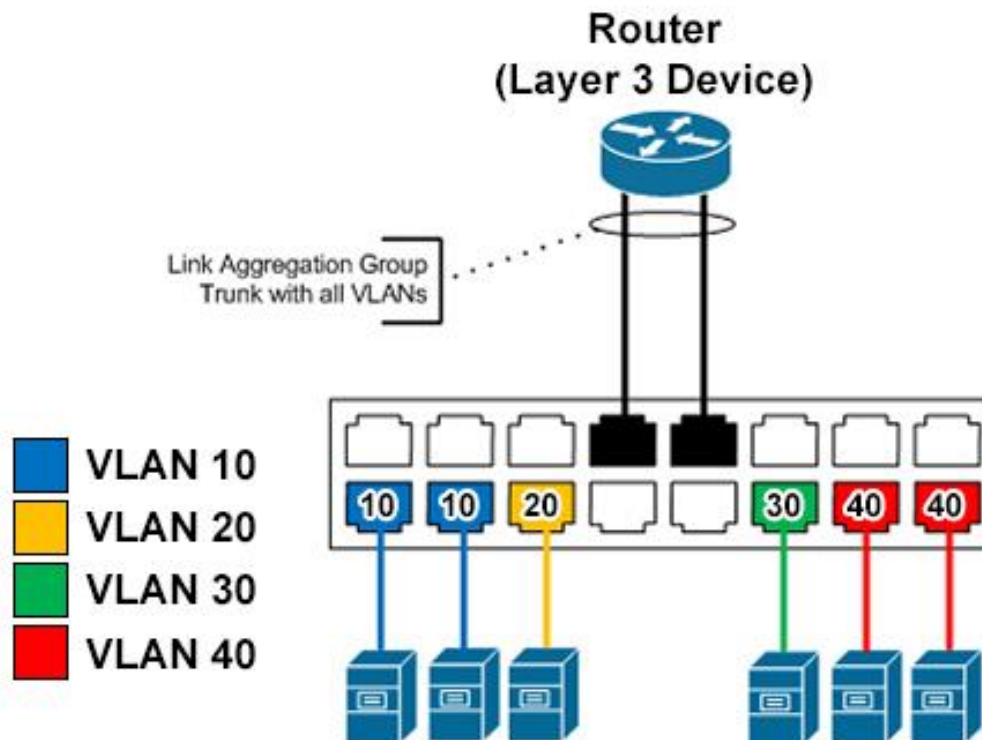
VLAN Management

- Create Security by Segmentation
 - Separate VLANs need layer 3 routing to access other VLANs
 - Can use **802.1q** (VLAN tagging) on the router interface



802.1q (VLAN Tagging)

- **Router interface can be configured with subinterfaces**
 - Aggregate links to increase bandwidth
 - Enable trunk ports to carry all VLAN traffic
 - Separated (tagged) – Router knows which subinterface to pass traffic



802.1q

Configuring subinterface on a Cisco Router

```
GigabitEthernet1/0/0.10
```

```
Description Subinterface for VLAN 10
```

```
ip address 10.0.10.1 255.255.255.0
```

```
encapsulation dot1q 10
```

```
GigabitEthernet1/0/0.20
```

```
Description Subinterface for VLAN 20
```

```
ip address 10.0.20.1 255.255.255.0
```

```
encapsulation dot1q 20
```

Secure Network Administration

- Rule-Based Management
 - Firewall Rules
 - Implicit Deny
 - Secure Router Configuration
 - Access Control Lists (ACLs)
 - VLAN Management
 - Network Separation
 - Port Security
 - 802.1x
 - Flood Guards
 - Loop Protection
 - Log Analysis
 - UTM
- } **Securing Physical Access to the Network**

Port Security

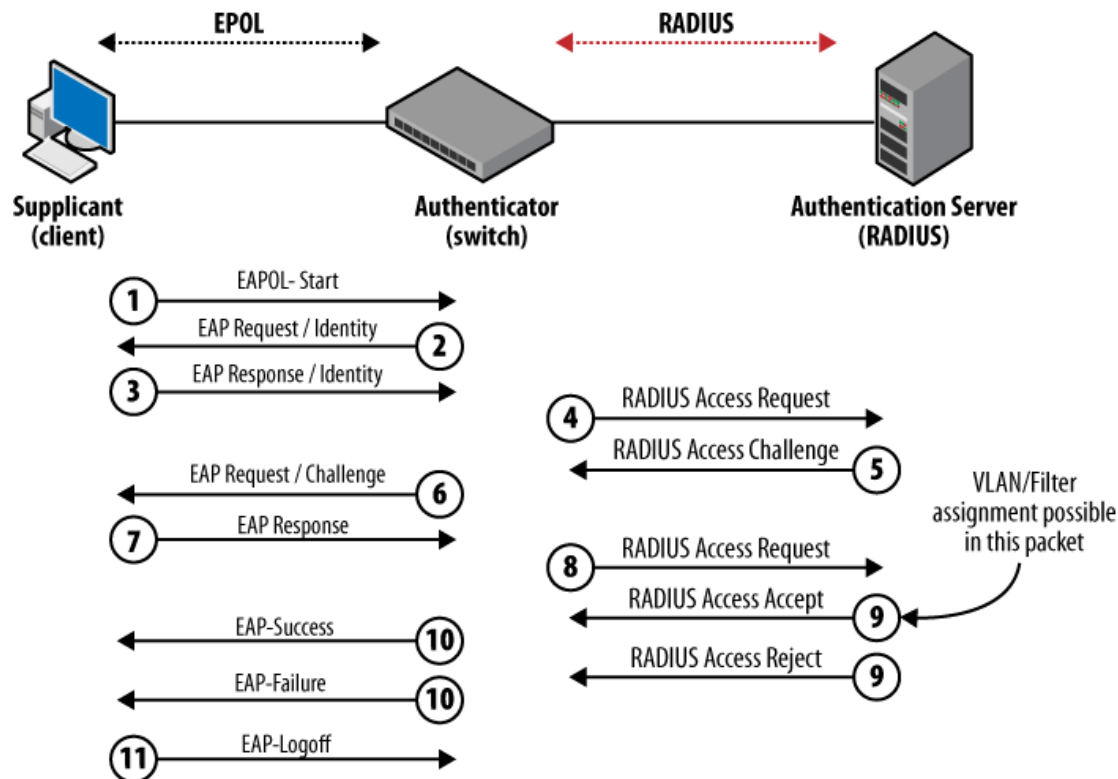
- **Configure a switch so that it only learns one MAC address per port**
 - Keeps attackers from sending multiple fake MAC addresses
 - Can be set to trigger alert
 - MAC address can be hard-coded to a particular port
- **Can be used in conjunction with 802.1x to strengthen security at the wall jack**



802.1x Authentication

■ 802.1x – EAPOL

- (Extensible Authentication Access Protocol over LAN)
- Allows only EAPOL traffic over port until client authenticates with a RADIUS or authentication server



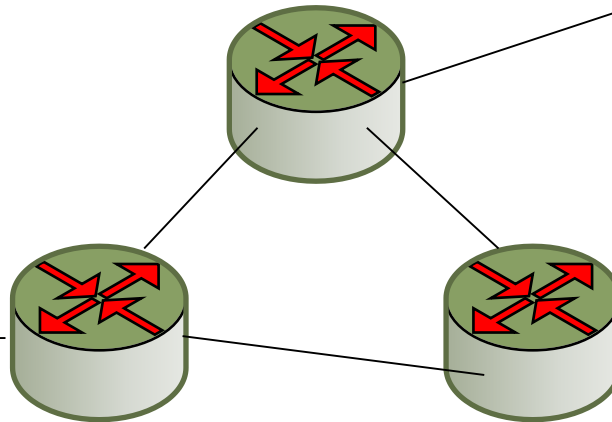
Secure Network Administration

- Rule-Based Management
 - Firewall Rules
 - Implicit Deny
 - Secure Router Configuration
 - Access Control Lists (ACLs)
 - VLAN Management
 - Network Separation
 - Port Security
 - 802.1x
 - Flood Guards
 - Loop Protection
 - Log Analysis
 - UTM
- } Ensuring Availability

Loop Protection and Flood Guards

- **Loop Protection**

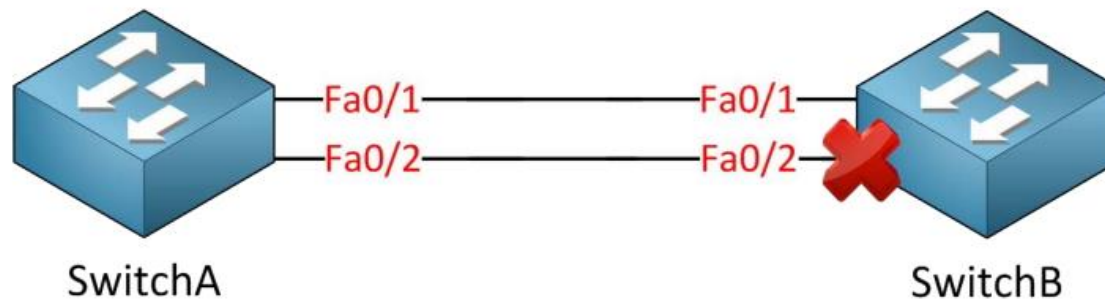
- Layer 3 Routers implement Time to Live (TTL)
 - Each router hop decrements the TTL
 - Packet dropped once TTL expires



Spanning Tree Protocol (STP)

■ Layer 2 protection

- Spanning Tree Protocol (STP) is typically enabled to prevent layer 2 loops
- Switches can also prevent ports from flooding the network by “clamping down” once broadcasts hits a certain percentage



Root Bridge

The elected center of the network

Designated Bridge

Forwarder that sends data to the Root Bridge

Root Port

Port that sends data toward to the root bridge

Secure Network Administration

- Rule-Based Management
 - Firewall Rules
 - Implicit Deny
 - Secure Router Configuration
 - Access Control Lists (ACLs)
 - VLAN Management
 - Network Separation
 - Port Security
 - 802.1x
 - Flood Guards
 - Loop Protection
 - Log Analysis
 - UTM
- } **Proactive Review/Analysis of Security Logs**

Log Analysis

- **Logs are generated by a number of devices**
 - Firewalls
 - Routers
 - Switches
 - IDS/IPS Systems
- **Typically sent to some type of SYSLOG Server**
 - Splunk>
 - IBM QRadar
 - NetIQ
 - Tripwire
 - Symantec



Log Aggregators

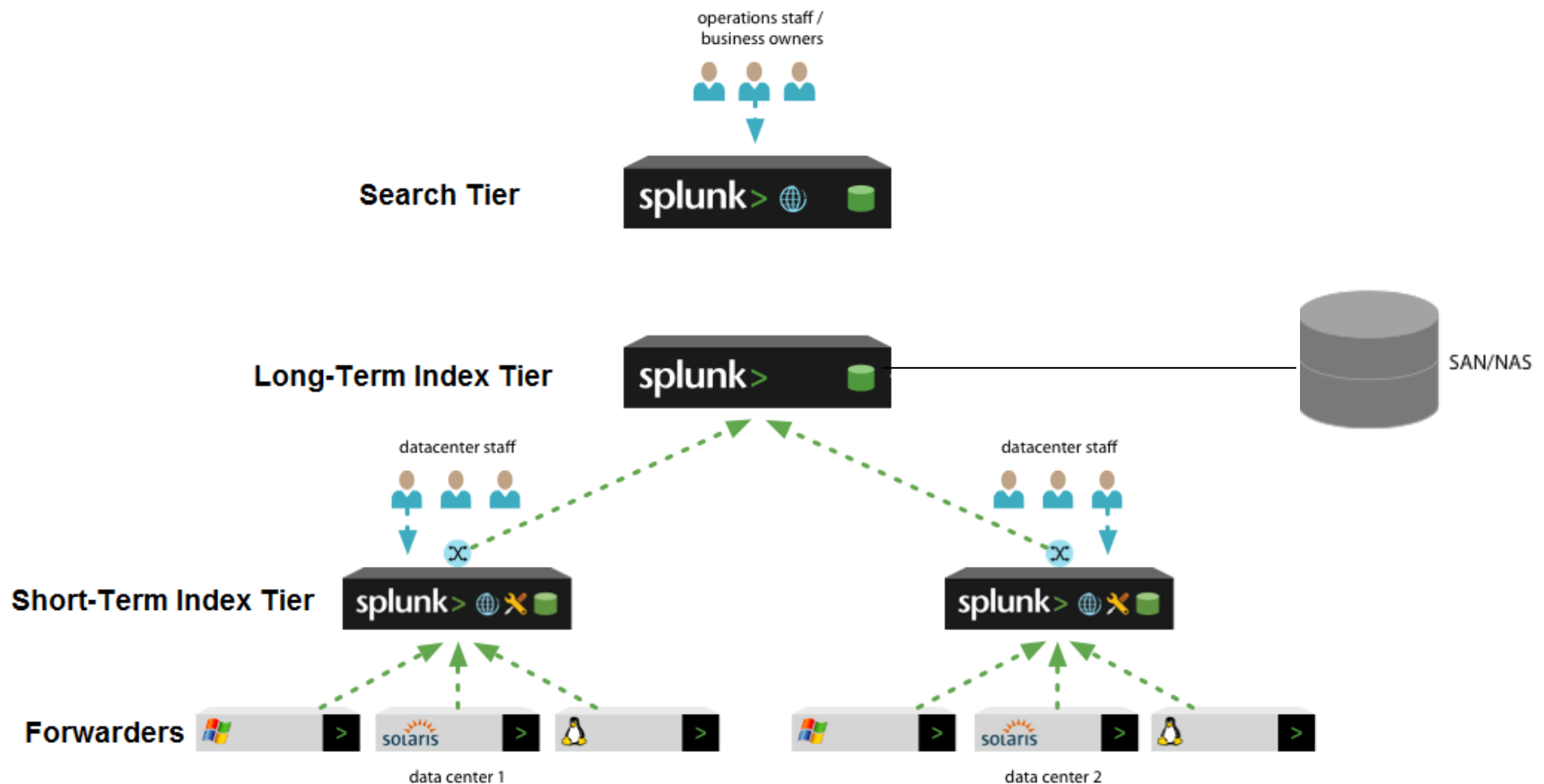
■ Splunk

- Takes inputs from various devices, applications, machine data
- Allows for event correlation across the entire enterprise



Log Aggregator at Scale

- For larger enterprise environments the log analysis tools should be deployed in a **distributed** architecture



Module Summary

- Rule-Based Management
 - Firewall Rules
 - Implicit Deny
 - Secure Router Configuration
 - Access Control Lists (ACLs)
 - VLAN Management
 - Network Separation
 - Port Security
 - 802.1x
 - Flood Guards
 - Loop Protection
 - Log Analysis
 - UTM
-
- The diagram groups the topics into five categories, each represented by a curly brace on the right side of the list:
- Securing Flow of Traffic** (includes Rule-Based Management, Firewall Rules, Implicit Deny, Secure Router Configuration, and Access Control Lists (ACLs))
 - Securing and Separating Network Segments** (includes VLAN Management and Network Separation)
 - Securing Physical Access to the Network** (includes Port Security and 802.1x)
 - Ensuring Availability** (includes Flood Guards and Loop Protection)
 - Proactive Review/Analysis of Security Logs** (includes Log Analysis and UTM)