



# Secure Architecture Design

[ine.com](https://ine.com)



# Brian Olliff

Defensive Engineering Instructor

---



[bolliff@ine.com](mailto:bolliff@ine.com)



[@CybeardSec](https://twitter.com/CybeardSec)



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

# Topics

**Secure Architecture  
Principles**

**User-level Design**

**Infrastructure Design**

**Architecture Planning**

**Logging**

**Backup & DR**

**Documentation**

# Learning Objectives

- Understand basic principles of a secure infrastructure
- Understand the goals behind proper infrastructure design
- Be familiar with design techniques for authentication & authorization systems
- Explain proper methods to securely design a network infrastructure
- Understand the various threat modeling techniques and how to use them
- Know the importance of proper architecture planning, before implementing
- Be familiar with how logging systems fit into overall secure architecture
- Understand various backup & recovery methods for disaster recovery
- Know different methods of documentation and when/how to use them

# Basic Security Principles



# CIA Triad

---

- Confidentiality
  - Private data stays private
  - Encryption, access control
- Integrity
  - Data is free from unauthorized changes
  - Digital certificates, file hashes
- Availability
  - Maintain timely and reliable access to all systems
  - Redundancy, protection from security controls

# Basic Principles

---

- Trust but verify
  - Applies to all aspects of security
  - Check controls, settings to ensure they are set as they should be
- Zero Trust
  - Model where nothing is trusted, until it is verified
- Defense in depth
  - Multiple layers of security controls
  - Overlap of systems
  - Try to use different vendors
- Security through obscurity
  - Attempting to secure assets by making them “difficult” to detect
  - Ex: hidden SSIDs on wireless, using non-standard ports for public access
- Asset & inventory management and control

# Security Techniques

---

- Minimizing the attack surface
  - Reducing services, open ports, etc on devices/systems
  - Less for attackers to potentially compromise
- Secure defaults
  - New devices & systems configured in secure manner prior to deployment
  - Server images secure
  - No default passwords, ports, services, etc
- Privacy by design
  - All private data should be secured at all times
- Fail secure
  - If/when a system fails, should not increase security concerns
  - Predictable and uncompromising behavior



# Authentication & Authorization

---

- Least Privilege
  - Grant access for what is needed to perform job, nothing more
- Separation of duties
  - Begin to introduce roles in authorization
  - Access given based on job roles
- RBAC
  - Role Based Access Control
  - Roles and groups created - permissions assigned to groups, not users
- Auth creep
  - More and more access granted over time
  - Department or job transfers
  - Remove old access and assign new roles (RBAC)

# What is Secure Architecture?



# Secure Architecture

---

- Designing and configuring infrastructure with security in mind
  - Starts with proper design
  - Documentation and asset management
  - Hardened servers, workstations, and other endpoints
  - Secure network infrastructure design and implementation
  - Policies, procedures, standards, and baselines
- Starting with secure design helps eliminate future issues
  - Security considered from the beginning and throughout
    - Results in stronger controls, better adaptation
    - Policies to support
    - Buy-in from executive leadership
  - Security as an afterthought = more potential incidents

# Threat Modeling

---

- Used to help determine possible impacts to infrastructure
- Process to identify assets, threats, and impacts
- Similar to risk assessment process
  - Start with list of all assets
  - Identify possible threats against those assets
  - List possible impacts those threats could have
  - Identify how to defend against them
- Multiple frameworks and models to use
  - Lockheed Martin Cyber Kill Chain
  - MITRE ATT&CK Framework
  - STRIDE

# Frameworks

---

- Designed to make entire process easier
- Baselines and guidelines to help streamline
  - Customizable to specific organizational requirements
- NIST CSF
  - Guides for cybersecurity activities
  - Based on established practices, standards
- NIST SP 800-53
  - Guides for more specific security controls
- ISO 27000 series
  - Multiple standards, best practices for security programs
- CIS Controls and Hardened Images

## Risks

---

- Secure architecture from the start helps avoid excessive incidents
- Without comprehensive design
  - Maintenance and documentation suffer
  - Vulnerabilities can go unpatched
  - Attackers can remain on network for extended periods
- Some risks of not implementing:
  - More threats coming in through email
    - Insufficient email security controls (filtering, URL sandboxing, etc)
  - Easier for attackers to move laterally in network
    - Improper network segmentation
  - Increased ransomware occurrences
    - Insufficient controls across environment
- Lost revenue, lawsuits, public image, fines, other penalties

# General Principles of Secure Architecture



# Zero Trust

---

- Attacks can come from anywhere on the network
- Some attackers take their time
  - Can be inactive on network for days, weeks, months
- Malicious (or careless) insiders
- Assume everything in network is malicious, unless proven otherwise
- Near impossible to implement full zero trust model
  - Environment would be too locked down for real productivity
- Where implemented - targeted approach
  - Specific systems or areas
  - Usually more critical systems



# Trust But Verify

---

- Even when something is trusted, still verify settings/behaviors
- Often implemented with zero trust models
  - Can be used completely independently
- Auditing and processes are key
  - Verifying requires auditing systems and settings
  - Must have processes in place to facilitate this
  - Processes should place proper emphasis on tiers of systems
- Automation and baselines can make this process easier

# Security Through Obscurity

---

- Using secrecy as primary method of security
- Does not provide any real security
  - Only (possibly) slows down attackers
- Do not rely on this alone for proper security controls
  - Used with other more security controls - can be successful
- Examples:
  - Hidden WiFi SSIDs
  - Using non-standard ports on public sites that should not be public
  - Encoding sensitive data that should be encrypted

# Asset Management

---

- Critical for any proper security program
- Impossible to properly secure assets if unaware of their existence
- Should consist of process handled by multiple areas
  - Procurement - initial purchase and licensing
  - IT - documentation of location, use, infrastructure information, etc
  - Security - control/countermeasure information, vulnerability status, etc
- At a minimum, anything connected to network should be recorded
- Direct ties into
  - Vulnerability management
  - Patch management
  - Risk assessment program
  - Audits

# Secure Architecture Goals



# Minimize the Attack Surface

---

- Attack surface
  - What is available to an attacker to compromise
  - Any server, endpoint, network device, etc
  - Attack vector
- Reducing attack surface shrinks available attack vectors
- Multiple methods to accomplish this
  - Device hardening (servers, workstations, devices)
  - Minimize what is publicly accessible
  - Implement MFA
  - Vulnerability/risk management programs
  - Security controls and countermeasures

## Secure Defaults

---

- By default, most systems not secure when brand new
  - Default passwords
  - Unnecessary services enabled
  - More user friendly for deployments, but not secure
- Secure defaults - all systems start in extremely secure configuration
- Restrictions are loosened as needed for functionality
  - Part of a risk management and change control process
- Overall goal
  - Start in extremely secure manner, most access/functionality is blocked
  - Intentionally release restrictions to point of usefulness

# System Hardening

---

- Most systems do not start out with strict security
- Instead, more functionality and user friendliness out of the box
- Tools, techniques, best practices to reduce vulnerability
  - Goal: Reduce security risk by minimizing attack surface
- Remove extra functions and applications
  - Disable unnecessary services
  - Change default passwords/accounts
  - Tighten firewalls
- Systems should be as secure as possible, while still maintaining functionality

# Defense in Depth

---

- Using multiple layered security controls in a coordinated manner
- Has commonly been used for physical security
  - Fences, lighting, locked doors, cameras, guards
  - All another layer to physically protect assets
- Typically is addressed from perimeter in, using multiple types of controls
  - Firewall
  - IPS
  - Network segmentation
  - Access controls and authentication
  - EDR/AV
  - System hardening
  - Encryption



# Secure The Users



# Authentication & Authorization

---

- Authentication
  - Begins with identification - “I am Bob”
  - Verifying that identity using some sort of credentials
  - Proving you are who you say you are
  - Username/password
  - Addition of MFA
- Authorization
  - Permission to access a resource or asset or perform an action
  - Implemented with access controls
  - Ideally using role based access controls (RBAC)

## Separation of Duties

---

- Organizations place some level of trust in their employees
  - Normally for a specific role - their job duties
- Their access should reflect that specific role
  - Access levels determined by their job and duties
- No one person has all of the responsibility
  - No one should have all of the access rights
- Users should only have access to what they need to do their job
  - Least Privilege
  - Roles and groups
    - RBAC

# Least Privilege

---

- Much easier to grant more access than is needed
  - Reduces support calls, eases administration
- Grant access based only on what is needed for job, nothing more
- Need-to-know
  - What does an employee need to know to perform their responsibilities?
  - What access do they need in order to accomplish this?
- John works in facilities management
  - Responsible for ensuring generators are operating properly
  - Certain reporting requirements and documentation
  - John only needs access to a specific folder that contains these documents
  - Does NOT need full access to all facilities files

## Role Based Access Control (RBAC)

---

- Assigning permissions and access controls based on role, not individual
- Requires roles to be carefully defined
- Assigning permissions
  - Groups are created in authentication/authorization system
  - Permissions assigned to the groups
  - Individual users placed into those groups
- John in facilities management
  - Added to “Generator Reporting” role
    - Grants edit access to appropriate folder
  - Director of department added to “Facilities Management” role
    - Grants full permission to entire department folder

# Authorization Creep

---

- Employees can change departments, promotions, etc
  - As these change, so do their access requirements
- Access needs change, but granted access does not
  - New access given, but old permissions not removed
- Similar to least privilege - easier to give more access than needed
- RBAC can help prevent authorization creep
  - Removing and adding new roles is much easier
- Requires proper IAM (Identity & Access Management)
  - Provisioning systems and automation
  - Coupled with RBAC can significantly ease administrative burden

# Privacy by Design

---

- Organizations are responsible for properly safeguarding data
- Privacy as an afterthought makes this incredibly difficult
- Privacy built in to systems/applications from the start
- GDPR based on this principle
- Embed privacy into design
  - Server configurations
  - File storage systems (encrypt data)
  - Access controls (least privilege & separation of duties)
  - Application development
  - Publicly accessible systems (websites)

# Secure Infrastructure





# Infrastructure

---

- What makes up our infrastructure?
  - Servers (AD, file, web, database, application, etc)
  - Workstations (Windows, Linux, Mac)
  - Network devices (firewall, router, switch, etc)
  - IoT devices (thermostats, media devices, cameras)
  - Cloud (SaaS, IaaS, PaaS)
  - Virtualization (servers, desktops, network)
- Securing each part requires different steps
  - Basic guidelines are the same
- Protect company data and assets, while ensuring continued operation
- CIA triad

# Basics

---

- Before any systems can be **properly** secured, planning is required
- Defense in depth strategy
  - Layer controls to fill gaps and provide redundancies
- Proper network segmentation
  - Split the network into sections based on purpose and access rights
- IAM process and infrastructure
  - Proper authorization and authentication controls
  - Least privilege and separation of duties
  - Avoid auth creep
- Documentation
  - All security infrastructure and controls
  - Policies, procedures
  - Change management

# Encryption

---

- Part of a defense in depth strategy
- Used with access controls, permissions
- Best practices
  - Encrypt all mobile devices
  - Sensitive data encrypted at rest and in transit
    - Databases, file servers, email databases, etc
  - Desktops
  - Configuration records
  - Backups
- Many different technologies available

# Email Security

---

- SPF - Sender Policy Framework
  - Attempts to prevent email spoofing
  - Specifies what hosts are allowed to send email as a domain
- DKIM - DomainKeys Identified Mail
  - Designed to validate origin & integrity of messages
  - Email servers digitally sign messages as they are sent
- DMARC - Domain-based Message Authentication, Reporting, Conformance
  - Combines SPF and DKIM for email traffic
  - Adds reporting features
- Data privacy
  - Email is not encrypted by default

## Fail Secure

---

- Closely related to secure defaults
  - Instead of new configs, what happens when something fails?
- When failure occurs
  - Devices should behave securely and predictably
- Firewall reboots or power cycles unexpectedly
  - Block all traffic until administrator analyzes
- If AV/EDR software encounters critical errors
  - Locks down system until checked
- Unverified certificates for websites
  - Connection blocked

# Threat Modeling



# Threat Modeling Basics

---

- Similar to risk analysis
- Method to identify where to focus efforts
- Important to use realistic threats - what is likely to happen
- What would the impact be if they did happen?
  - Business processes
  - Other assets
  - Revenue
- Where do the threats originate from?
  - Knowing the source helps identify countermeasures
  - Better understanding of capabilities and motivations
  - Not the same as attribution

# Mapping

---

- Attack tree - method to visualize a threat and it's steps
- Multiple different methods attackers use to accomplish the same goal
  - Attack tree helps to identify and trace the steps
- Example:
  - Attacker's goal - steal organizational trade secrets
  - Methods - gain access to server, trick employee to providing
    - Access server - use credentials, steal access token, hack into server
      - Credential use - brute force, steal access token, phishing
    - Trick employee - social engineering



# Cyber Kill Chain

---

- Developed by Lockheed Martin
- Model that lays out seven specific stages of an attack
  1. Reconnaissance
  2. Weaponization
  3. Delivery
  4. Exploitation
  5. Installation
  6. Command & Control
  7. Actions on Objective
- Allows for development of countermeasures at each stage
- Goal is to stop an attack early in the chain

# MITRE ATT&CK

---

- Developed by MITRE Corporation
- Adversarial Tactics, Techniques, and Common Knowledge = ATT&CK
- Much more detailed than Cyber Kill Chain
- Breaks down attacks into small sections
  - Tactics
    - 14 tactics
  - Techniques
  - Sub-techniques (procedures)
- Mapping tool available - <https://attack.mitre.org/>

## MITRE ATT&CK Tactics

---

- Reconnaissance
- Resource Development
- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Command & Control
- Exfiltration
- Impact

# Secure Architecture Planning



# Planning

---

- Multiple steps go into proper planning
- Importance and criticality of systems involved
  - Group systems by tiers
- Types of systems and technologies in organization
- Risk assessment & threat modeling
  - Identify threats and determine controls & countermeasures
- Budget decisions
- Organizational requirements
  - Expansions, acquisitions, mergers, etc
  - Compliance or regulatory requirements
- End goal - balance security with usability

# Inventory and Prioritize

---

- Proper inventory is required to know what controls are needed
- Identify various systems
  - Vendors
  - Operating systems
  - Software versions
- Prioritization of systems (tiering)
  - Tier 1 - Most critical systems, business processes depend
  - Tier 2 - Important systems, small business impact
  - Tier 3 - Supporting systems, inconvenient to go down but no major impact
    - Unless offline long-term
- Feeds into assessments

# Threat Modeling & Risk Assessment

---

- Once assets are identified, start assessing for threats and risks
- Risk assessment & analysis processes
  - Identifies all risks posed
  - Assists in identifying priorities and controls
- Threat modeling
  - More specific to cyber security threats
  - Couple with risk assessment to fine-tune where efforts should be focused
- Compliance & regulatory requirements
  - May not always be part of risk assessment
  - Specific requirements will impact control options & selection

## Budget & Organizational Decisions

---

- Security requirements and associated controls identified
- Almost all controls require purchase & licensing
  - Some open source, no-cost options as well
  - Important to not discount just because they're free
- Budget decisions based tightly on risk assessments
  - Especially cost/benefit analysis (quantitative analysis)
- Other organizational decisions will affect selection of controls
  - Available funds & revenue
  - Risk appetite of organization
  - Other business activities



## Documentation & Communication

---

- Important that entire process is team-based
  - Multiple areas of organization need to be involved
  - Security & IT
  - Any area of business that may be impacted
- Document all steps
  - Needed for reference & collaboration
  - Audit requirements
  - Used to build policies
  - Change management programs

# Creating a Secure Network



# Network Design

---

- Secure network takes careful consideration and design
  - DNS
  - Encryption
  - Segmentation
  - Number of switches/routers/firewalls
  - Device authentication & management
  - Types of protocols used/allowed
  - Network scanning points (tap, span, decryption, etc)
- Networks should be designed with network engineers and security

# Network Segmentation

---

- VLANs most commonly used
  - Virtual local area network
- Allows logical separation of devices
- Can still be physically connected to same switches
  - Physical separation is another form of network segmentation
- Can prevent lateral movement
  - Ex: attackers compromise workstation on Sales network, cannot pivot to Finance server network
- Limits spread of ransomware (or other wormable malware)
  - Worm: malware than can self-replicate and self-propagate without any interaction from users

# Encryption

---

- End-to-end encryption
  - Not all pieces of traffic are encrypted - header information still clear
- Link encryption
  - Encryption happens at layer 1 or 2 - all header information encrypted
- TLS (Transport Layer Security)
  - Replaced SSL - no longer secure
  - Newer versions reduced number of cipher suites
- Malicious traffic can be encrypted
  - Decryption options exist to scan traffic
  - Can be harder to detect
    - Source/destination information can be helpful

# Secure Protocols

---

- Applies to normal traffic and network management
  - HTTPS vs HTTP
  - SSH vs telnet
  - SFTP (or SCP) vs FTP
- Secure protocols encrypt authentication
- Monitor network for use of insecure or outdated protocols
  - Centralized logging systems help with this
- DNS commonly used in attacks
  - Randomly generated DNS names used by malware
  - Traffic other than DNS on port 53

# Configuration Backups

---

- Integrity and Availability (parts of CIA triad)
- Known good backups can be used as baselines
  - Can help identify changes to network devices (Integrity)
    - Malicious or accidental
- Equipment failures happen
  - Backups can significantly shorten downtimes (Availability)
- Secure Backups
  - Backups kept in secure location and encrypted
  - Minimal access via network

# Logging





## Scott Michaels Paper Company

---

- Company manufactures and sells paper products
- Competitor appears with very similar products
  - Company is based in another country
  - Much cheaper prices
- Organization suspects that other company broke into network
- Did not have proper logging set up
  - Cannot see account activity from more than 24 hours ago
  - No network logs older than 6 hours
  - File access information not recorded anywhere
- Company has no proof that IP was stolen
- Try to lower prices to undercut, but eventually go out of business

## What To Log

---

- Whatever is critical to your organization
- Account and group activity
  - Creation, deletion, modification
  - Log on/off - including source information
- Network traffic
  - Firewall traffic - inbound and outbound
  - Internal network traffic as needed
- File access
  - Especially any sensitive, proprietary information
- Email systems
  - Any email filtering
  - Inbound and outbound mail

# What To Log

---

- Server event logs
  - Specific events depend on server purpose
  - Windows servers - PowerShell, system, application
- Applications
  - Any specific application logs that may be relevant to security
- Any public facing interfaces
  - Web servers
  - Remote access gateways
  - Email portals
  - Customer interface
  - APIs

## Centralized Logging

---

- Single (or multiple) destinations for all logs in environment
- Typically, one dashboard to view all logs and analysis
- All systems that generate logs, send to centralized destination(s)
- Capabilities & Benefits
  - One place to go for all logs
  - Ability to introduce automation and alerting
  - Analysis of all correlated logs
- Increases difficulty for attackers altering/deleting logs
  - Attackers frequently delete logs to cover tracks
  - Offloaded logs are protected from that

# Log Analysis & Retention

---

- Automated or manual analysis
  - Automated can provide alerting for certain events, behaviors
    - Usually requires central logging set up
  - Manual allows deep-dive, human insight into logs
  - Good practice to employ both techniques
- Alerts require attention and tuning to prevent “alert fatigue”
- Keep logs for as long as necessary
  - Based on organizational and/or regulatory requirements
  - Longer retention requires more storage
  - Retention periods will vary across systems

## Scott Michaels Paper Company (with logging)

---

- Company has central logging systems in place
  - Account activity
  - File access (especially on critical data)
  - Network traffic (including inbound & outbound at firewall)
  - Email traffic
  - Public web server
  - Endpoint security
- Logs indicate multiple possible phishing emails - Block IP and URLs
- Logs show attempts to scan firewall - Block IPs
- Logs report multiple attempts to brute force remote access
- All attempts to breach network fail
- No new, suspicious company appears

# Disaster Recovery



# Disaster Recovery & Business Continuity

---

- Business Continuity
  - How to maintain business functions during disruptions
  - Plans for how processes continue during a disaster
  - Includes plans for responding to and recovering from disasters
- Disaster Recovery
  - Minimize the effects of major disruptions
  - Plans for how to specifically prepare for, respond, and recover from disasters
    - How are systems restored?
    - How is data backed up?
    - How will that data be restored?
    - How will the organization return to “normal”?



# Backups

---

- Data is important to any organization
  - Data will inevitably be corrupted or deleted
- Policies and procedures are required
  - What data is backed up
  - How often backups occur
  - How that data is restored when needed
- System tiering is often used
  - Most critical systems have priority, may be backed up more often
- Backup considerations
  - Type of backup
  - Destination
  - Frequency
  - Retention

# Backup Types

---

- Full backup
  - All in-scope data is backed up
  - Usually first step of any backup
  - Takes most of amount of time to perform
  - One step restore
- Differential backup
  - Any files that have changed since last full backup
  - Faster than full backup
  - Two step restore
- Incremental backup
  - Files that have changed since last full *OR* last incremental
  - Fastest backup to perform
  - Multiple step restore

# Backup Schedules

---

- Annual backup
  - Usually for archiving purpose - rarely used for production restore
- Monthly backup
  - Usually a full backup
  - Often used as starting point for incremental or differential
- Weekly
  - Can be a full, usually differential or incremental
  - Frequently used for full restores
- Daily/Nightly
  - Usually incremental
  - Useful if small restores are needed

# Backup Storage

---

- Direct-attached
  - Internal or external drives
  - Easiest, but not most secure
- Network-attached
  - Good for central management
  - If site or network fails, may be inaccessible
- Cloud
  - Combines easy storage and offsite storage
  - Requires internet connectivity for backup and restores
- Offline
  - Most time consuming, but most secure
  - Used for most critical data

## Hot, Warm, & Cold

---

- Refers to additional networks or data centers used for DR
- Sites should be geographically distant from each other
- Hot site
  - Full replica of production systems, online and ready for use immediately
  - Requires regular maintenance and patching
- Warm site
  - Equipment present on site, requires time to set up
  - Data might need to be copied over
- Cold site
  - Building ready for use
  - No equipment ready

# Documenting the Secure Architecture



# Documentation Basics

---

- Documentation makes implementation easier and clearer
  - Properly documented layouts and configurations
  - Responsibilities for who performs what steps
- Reference material
  - Can be used as baseline guides
  - Answer questions about architecture
  - Help prepare for new additions & expansions
- Audits often require documentation
- Available on need-to-know basis
  - Architecture documentation often contains sensitive information
- Backups!

# What to Document

---

- Network layout
  - How systems fit in to the architecture as a whole
  - What devices can talk to
- Device Information
  - IP/subnet information
  - Hostnames
  - Vendor information (name, contact/support info, warranty information)
  - Software versions
- Backup schedules
- Administration and management responsibilities
  - Who maintains vs who manages

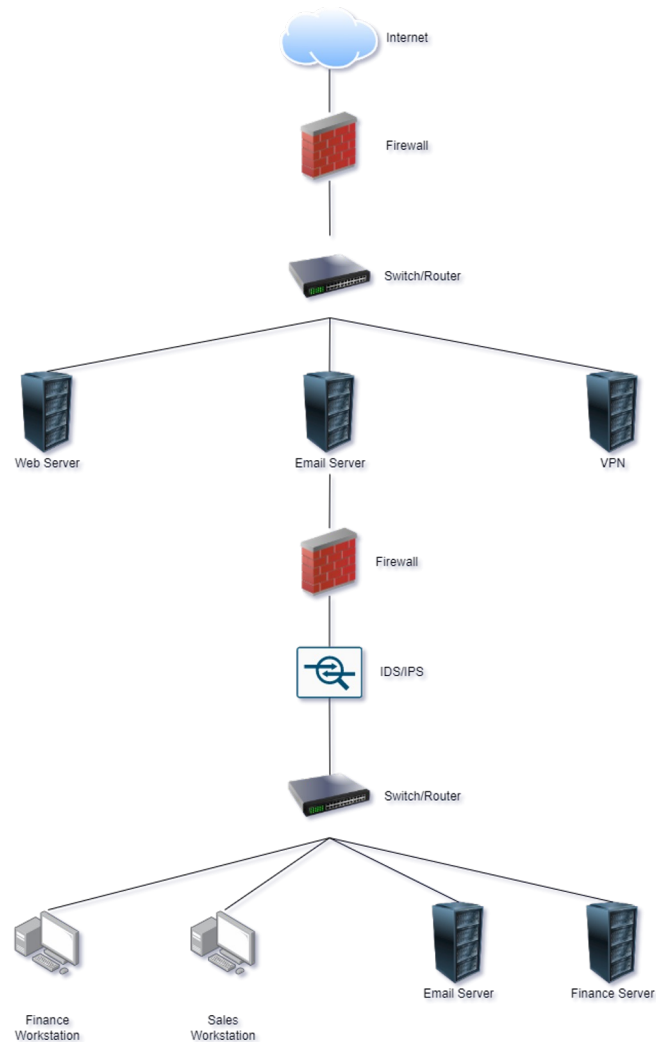


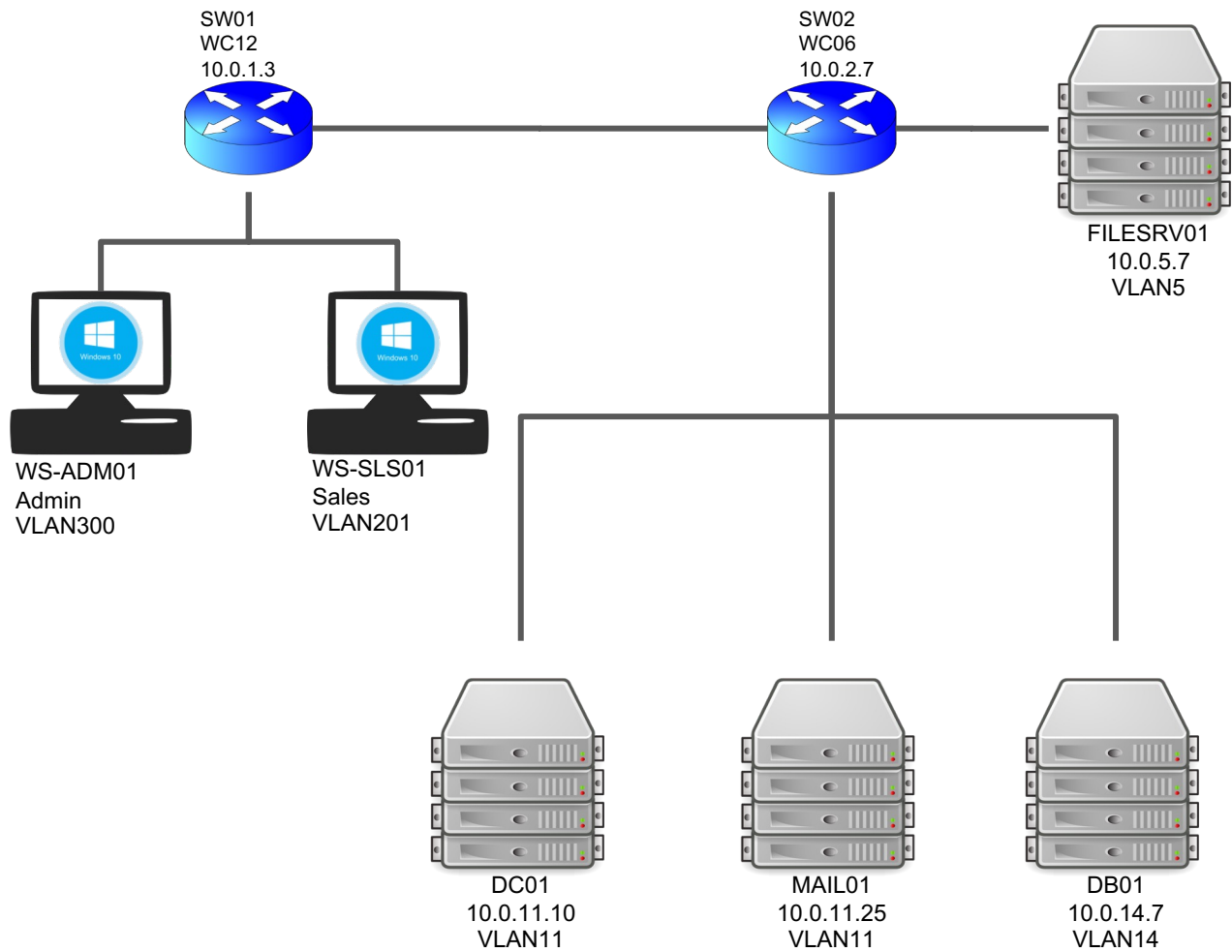
# Types of Diagrams and Designs

---

- Network Diagram
  - Shows logical locations of all networked devices
    - Network devices
    - Servers (usually by subnet or VLAN)
    - Security controls
  - Typically shows host/network information
  - Can include physical information
- Inventory database
  - Lists all assets in environment
  - System information (hostname, IP, manufacturer, vendor, software, etc)
  - Department responsible

# Network Diagram Example





# Architecture Documentation Tools

---

- Layout diagram
  - MS Visio
  - Presentation/slide software
  - Multiple free utilities available online
- Spreadsheet programs
- Word processing software
- Managed inventory programs
  - Solarwinds
  - Lansweeper

# Brian Olliff

Defensive Engineering Instructor

---



[bolliff@ine.com](mailto:bolliff@ine.com)



[@CybeardSec](https://twitter.com/CybeardSec)



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