MITCHELL
SYSTEMS

# NETWORK REDESIGN

# 2026

# REGIONAL INSURANCE


Prepared by:
**Brayden Mitchell**

Presented by:
**Mitchell Systems**



braydenatroberts.org

## Executive Summary

This report presents the findings and recommendations resulting from a comprehensive evaluation of the Regional Insurance Group's network infrastructure and security posture. The assessment identified several areas of concern, including limited network segmentation, insufficient monitoring capabilities, and a lack of secure remote access solutions. These gaps increase the organization's exposure to cybersecurity threats and reduce its ability to effectively detect, respond to, and mitigate potential incidents.

To address these risks, a redesigned network architecture is recommended, emphasizing improved segmentation, scalability, and layered security controls. The proposed structure incorporates the use of Virtual Local Area Networks (VLANs) and subnetting to isolate critical systems and sensitive data, thereby reducing the overall attack surface. Enhanced routing and switching configurations further support improved network performance, reliability, and manageability.

A key recommendation within this report is the implementation of a Security Information and Event Management (SIEM) solution. This system provides centralized logging, real time monitoring, and correlation of network events, enabling more efficient identification of suspicious activity. By improving visibility across the environment, the SIEM strengthens incident detection and response capabilities while also supporting compliance and audit readiness.

In addition, the report recommends the deployment of a Virtual Private Network (VPN) to enable secure remote access for employees and authorized users. The VPN ensures that data transmitted over external networks is encrypted and protected, while authentication controls verify user access. This capability is essential for supporting remote work without compromising the security of internal systems and sensitive information.

The adoption of these recommendations is expected to deliver significant business benefits. Improved network segmentation and monitoring will reduce the likelihood and impact of security incidents, while enhanced infrastructure design will support future growth and operational efficiency. The  implementation of secure remote access will enable greater flexibility for the workforce while maintaining strong data protection standards.

In summary, this report outlines a strategic approach to strengthening the organization's network infrastructure and cybersecurity posture. By addressing current vulnerabilities and aligning with industry best practices, the Regional Insurance Group will be better positioned to protect its assets, maintain business continuity, and respond effectively to an evolving threat landscape.

## Regional Insurance Group Current Network Report

The current network infrastructure of Regional Insurance Group supports both internal business operations as well as customer access. The network provides internet connectivity, internal communication between the different systems, and access to the critical services of the business such as customer management, database storage, and file sharing. The network is protected by a single perimeter firewall and relies on a single managed switch, using IPv4 addressing to connect internal devices.

The company hosts a public facing web server that allows customers to access the company's online portal. This server is operated using a linux system and an apache web server platform. This server has also been placed in a demilitarized zone or a DMZ. This provides controlled external access from the internet. The DMZ separates publicly accessible services from the internal corporate network to reduce the risk of unauthorized access to the sensitive data held within the internal systems.

Behind the firewall, the internal network supports several different servers that provide different services for the company. Two servers each are assigned to customer management, database storage and file storage. The customer management systems process requests from internal workstations and communicate with the database systems to retrieve and also store information.

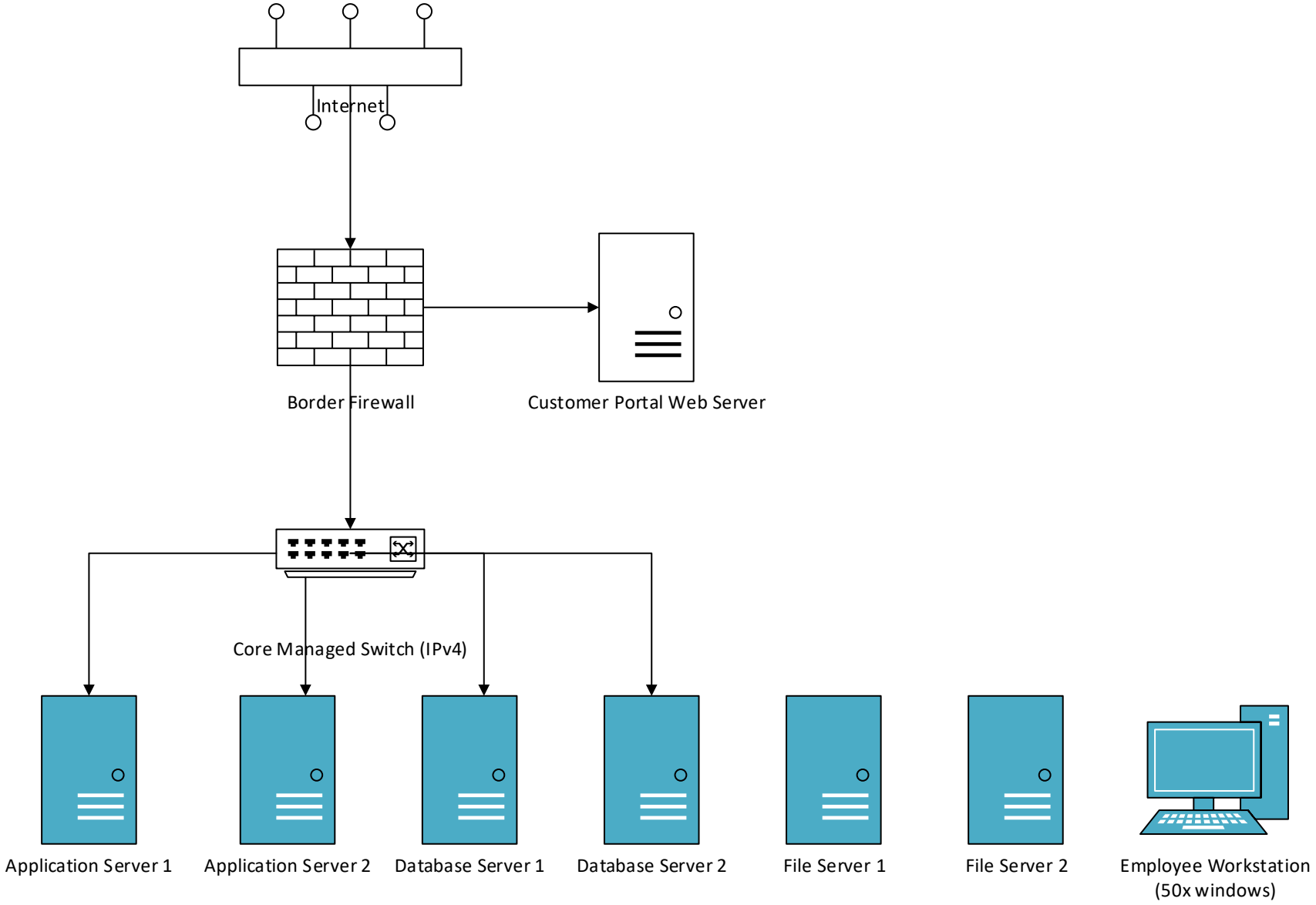
The windows database servers are responsible for storing sensitive customer information and organizational data. The last two servers, the file and print servers provide file storage and print capabilities for employees throughout the organization.

The last component of the network includes 50 windows workstations for employee access which are also connected to the internet through the managed switch. The switch serves as the main connectivity point that links all the workstations and servers within the local area

network. The switch manages the traffic flow between all of the devices and ensures reliable communication using IPv4 network addressing.

All the systems are connected through a hierarchical structure where the firewall serves as the entry point between the internet and the internal systems. The firewall filters incoming and outgoing traffic, according to its configured rules, which helps to prevent unauthorized access to internal systems. From the firewall traffic is routed to either the DMZ web server or to the internal network through the managed switch infrastructure.

Although the network does support the essential services and connectivity, the current setup presents potential security limitations. The organization relies on a single border firewall for protection and it lacks deeper internal segmentation between the critical systems. As a result, if an attacker were to gain access to the internal network. Sensitive systems would be reached quite easily. Improving segmentation and implementing additional security controls would greatly strengthen the overall network security.


Internet
Border Firewall
Customer Portal Web Server
Core Managed Switch (IPv4)
Application Server 1
Application Server 2
Database Server 1
Database Server 2
File Server 1
File Server 2
Employee Workstation
(50x windows)

## Regional Insurance Group Network Redesign Report

Regional Insurance Group's original network architecture relied on a single firewall at the perimter of the network, and lacked internal network segmentation. The design created several security risks because sensitive systems and basic departmental resources were being housed on the same network segment. The new and improved, redesigned network improves the organization's security position by introducing network segmentation between departments, layered firewall protection, and a new system for authentication. These improvements follow network design principles such as defense in depth, diversity of defense, segmentation and least privilege access.

### Segmentation

Logical network separation between the accounting and sales departments was implemented using Virtual Local Area Networks or VLANs. VLANs allow multiple "logical" networks to exist on the same physical network. This keeps traffic isolated between departments.

The Accounting department is assigned VLAN 10, while the Sales department is assigned VLAN 20. Each department's workstations connect to switch ports configured for their respective VLAN. This prevents direct communication between departments.

A switch performs inter-VLAN routing when communication between departments or networks is needed. Firewall rules also further restrict access to any sensitive resources, ensuring that only authroized systems have the ability to communicate across VLANs. This design is intentional to prevent lateral movement within the network which protects each individual VLAN network from being compromised if one of them becomes compromised.

**Firewall Selection and Placement need sources**

The redesigned network uses a layered firewall design to protect different parts of the network infrastructure. The perimeter firewall remains in use. A perimeter firewall is not a bad thing, it was just not enough for this organization. The perimeter firewall is a pfsense firewall. This firewall supports packet filtering, network address translation, VPNs, and intrusion detection features.

A second firewall has been introduced between the DMZ and the internet network in order to restrict communication between the publicly available services within the DMZ and the private systems within the internal network. This segmentation firewall ensures that only specific, and necessary traffic is allowed to reach and access internal systems. For this firewall I decided to go with an OPNsense firewall. This firewall option provides all of the same great features but introduces the practice of diversity of defense

In addition to our network firewalls, each Windows system uses Windows Defender Firewall. This provides one more security layer which also controls incoming and outgoing traffic, but at the device level. This multied layer approach follows defense in depth practices when building a network.

**DMZ Implementation**

A demilitarized zone or a DMZ has been implemented in order to isolate publicly accessible systems from the local network. The organization's public facing web server which houses the customer portal is placed within this DMZ network which is now a segment of the original network.

The DMZ network has been connected to the perimeter firewall and completely separated from the internal network thanks to the new internal firewall. Only specific services required for customer access like HTTP and HTTPS traffic are allowed into the DMZ.

Communication is also strictly controlled between the DMZ and the internal systems through the firewall rules.

The implementation of a DMZ provides security by limiting the exposure of internal systems to external attacks and threats. If the public facing web server were to become compromised, attackers would be stuck inside the DMZ and unable to directly access any of the internal systems including the sensitive ones. This design follows the best practice for protecting networks with a LAN to WAN domain.

**Network Authentication need sources**

The new redesigned network now includes authentication services that secure access to internal resources. Most of the systems are windows so the authentication services are provided by and managed with Microsoft Active Directory running on a windows server.

An active directory domain controller was placed within a dedicated authentication VLAN so that it was completely isolated. When users log in to their workstatuions, their credentials are verified by the domain controller before access to network resources like any servers or files can be granted.

In addition to active directory, strong password policies, account lockout policies and role based access rules are also implemented to stregthen physical security. The principle of least privilege has also been enforced by allowing users access to only what they need for their job description.

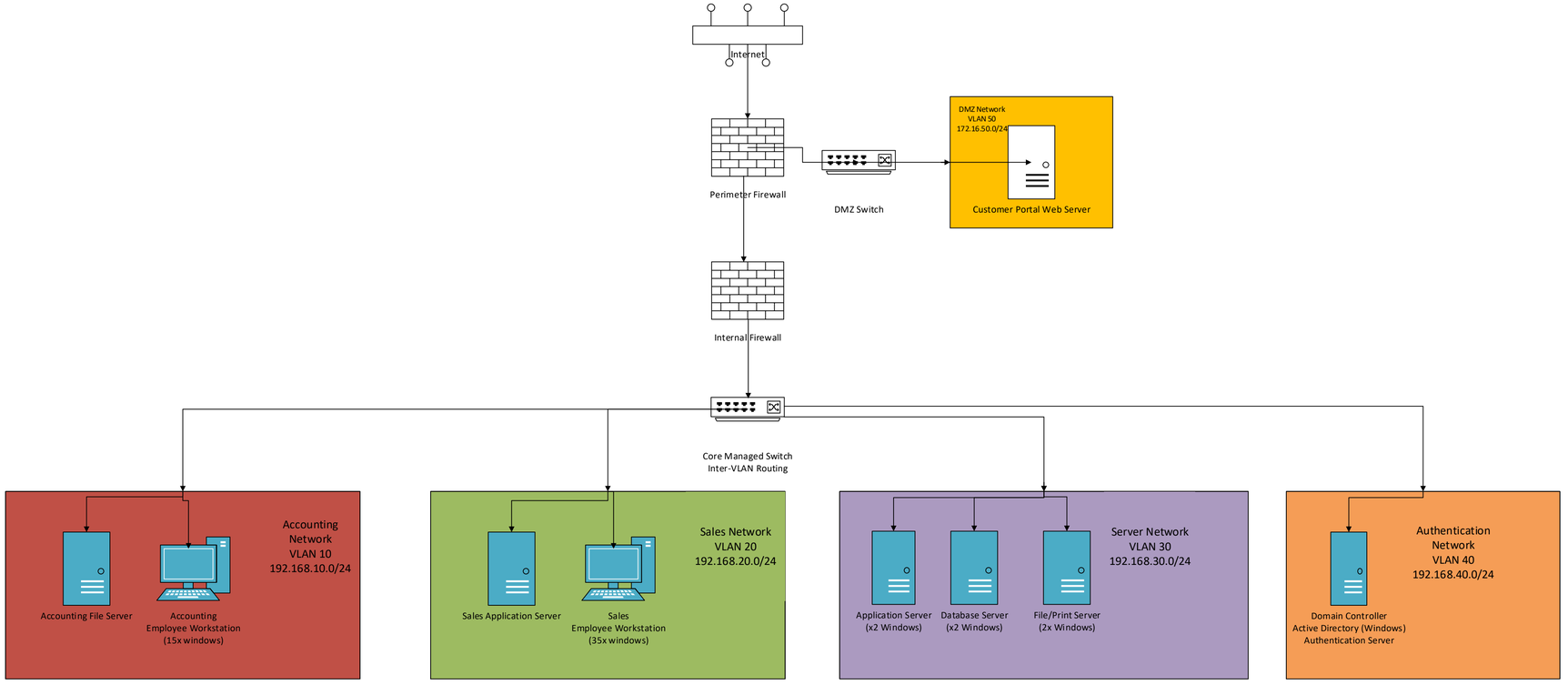
**Summary of Network Configuration Changes**

Several major changes were made to the network in order to strengthen the security of the system before changes to how Regional Insurance Group runs their business can actually work. First, VLAN segmentation was introduced which logically divided the accounting and sales departments as well as isolated a server VLAN and a new authentication VLAN.

Second, an additional firewall was deployed which provided an internal and external network segmentation and improved overall security for all internal systems.

Third, a DMZ network was implemented which isolated the public web server from all of the internal systems which reduces exposure threats to the internal network. Last, authentication services were deployed using Active Directpory which prodives identity management and access control.

Together all of these changes become a huge improvement for Regional Insurance Group, and sets them up for expansion and success as a more secure and flexible company.


Internet
Perimeter Firewall
DMZ Switch
DMZ Network
VLAN 50
172.16.50.0/24
Customer Portal Web Server
Internal Firewall
Core Managed Switch
Inter-VLAN Routing
Accounting
Network
VLAN 10
192.168.10.0/24
Accounting File Server
Accounting
Employee Workstation
(15x windows)
Sales Network
VLAN 20
192.168.20.0/24
Sales Application Server
Sales
Employee Workstation
(35x windows)
Server Network
VLAN 30
192.168.30.0/24
Application Server
(x2 Windows)
Database Server
(x2 Windows)
File/Print Server
(2x Windows)
Authentication
Network
VLAN 40
192.168.40.0/24
Domain Controller
Active Directory (Windows)
Authentication Server

## Regional Insurance Group VPN Deployment

### VPN Recommendation

For Regional Insurance Group, an SSL/TLS VPN is the most appropriate option for a remote access solution. An SSL/TLS VPN uses web browsers to operate and uses Transport Layer Security to encrypt the communication between remote and internal users. This makes it suitable for a worskforce that is distributed, like workers are at home, and for anyone using personal devices and home networks.

Compared to IPSec VPN's, SSL/TLS provide ease of use, firewall compatibility, granular access control and scalability. No VPN client is needed, users can connect using a web browser. When it comes to firewall compatibility SSL/TLS use HTTPS which is rarely blocked. Granular access control allows administrators to allow access to specific segments of the network, and certai applications rather than full network access. Finally, SSL/TLS VPNs leave room for growth in the company and do not pose a long term scalability problem.

TLS protocol combines both symmetric and asymmetric encryption types to ensure both confidentiality and integrity for all data being transported. This provides a safe connection, key exchange and bulk data transfer.

SSL/TLS VPN inherently encapsulates traffic securely without requiring tunnel configuartio complezit, making it more suitable for end users.

To strengthen remote access security, multifactor authentication, Zero trust network access, and endpoint security controls should be implemented. MFA will prevent the misuse of credentials, ZTNA will block everyone and everything until the user can prove they are allowed into the network. Devices should also be checked for compliance which includes antivirus, and patching. Unsafe devices can pose a risk to the network.

**Additional Remote Access Options**

While a SSL/TLS VPN can serve as Regional Insurance Group's primary remote access solution, additional complementary systems can and should also be in place to strengthen security, increase usability and align with best practices for an always available remote network.

RDP, or Remote desktop protocol is a very popular option. It is built in to all windows machines and lets users access their desktop from another device. This option does require specific configuration and security measures in order to alleviate any potential threats. This would not be recommended for all of the remote workers due to the configuration and security concerns, but it is a great backup option.

There are also several remote access softwares available including one from chrome. Again this provides a lightweight, semi-secure option but should not be the first option to use. Using outside software introduces the chance that the connection could be interrupted, or compromised by any bugs, or security issues with the software. This can be a short term solution if absolutely necessary but should not be used for the day to day operations of a remote worker. What this would be great for is temporary connections that the IT team may need to make, but the Remote Desktop protocol built in to windows would even be a better option.

## Regional Insurance Group SIEM Implementation

### SIEM Tool Selection

Reginal Insurance Group should implement Splunk enterprise security as your SIEM solution. It has a proven effectiveness when it comes to logs. Including log aggregation and real time analysis. Splunk includes a strong correlation engine and advanced threat detection tools and capabilities. It is compatible with both firewall and VPN log formats. Splunk is a long trm solution that fits with any size business and is scalable to future growth as a company. Splunk is also a great choice because it is a well documented system which provides support for the security team.

Other tools that were considered include IBM QRadar, Microsoft Sentinel, and DataDog. While these tools are viable options, Splunk offers the  best balance of usability, and scalability. Splunk also comes with a MITRE ATT&CK Matrix that allows security analysts to build situational awareness about incidents. Having that built in is a great added bonus and just another reason to go with splunk.

### Network Security Objectives

Implementing a Splunk SIEM system will support all of the following network security objectives:

- Centralized Log Management
- Threat Detection and Response
- Secure Remote Access Monitoring: Very important considering a VPN is being implemented for all remote workers which will make up most of the company
- Regulatory Compliance
- Incident Investigation
- Reduced Response Time: Automatic alerts for security incidents, time is so important when it comes to responding to potential security breaches or issues.

**Data Sources Integrated**

Many data sources will be integrated into the SIEM system in order to best keep track of any security incidents across the network. This includes:

1. Firewall Logs
2. VPN Logs
3. Server Logs
4. Enpoint Security Logs
5. Router logs
6. SWitch Logs
7. Active Directory Logs
8. Web server Logs

This may seem like a lot but splunk will be able to help the security team keep tabs and respond to any security incidents as needed.

**Proposed SIEM Rules**

The following rules are what make the SIEM system work. These rules will tell Splunk when to generate alerts so that the security team can give the issue immediate attention.

Authentication-Based Rules

- Detect multiple failed login attempts (brute force attacks)
- Identify login attempts outside normal working hours
- Alert on privileged account misuse

Network Activity Rules

- Detect unusual outbound traffic patterns
- Identify communication with known malicious IP addresses
- Detect port scanning behavior

VPN-Specific Rules

- Multiple failed VPN login attempts
- Simultaneous logins from different geographic locations
- Connections from blacklisted or suspicious IP addresses

Firewall-Based Rules

- Repeated denied connections from a single source
- Detection of unusual port or protocol usage
- IDS/IPS alert correlation

Data Exfiltration Rules

- Large or abnormal data transfers
- Unusual file access patterns

**Alert Configurations**

While the rules tell Splunk when to send alerts, alert cnfigurations tell whoever is responding to the alerts what the severity of the issue is which tells the security professional how much immediate attention should be given to the issue. For example if you were working on a low level alert and a critical alert comes in, attention should be given to the critical alert until the issue is resolved. All alerts should be

given attention and all the issues should be fixed in a timely manner but the following configurations show which issues should be addressed first:

Critical Level Alerts

- Confirmed intrusion attempts
- Malware detected on critical systems
- Unauthorized privileged access

High Level  Alerts

- Brute force login attempts
- Suspicious VPN activity
- Communication with malicious IP addresses

Medium Level Alerts

- Policy violations
- Unusual but non-critical traffic patterns

Low Level Alerts

- Informational events for auditing purposes

Alerts should be delivered in a safe and secure, and reliable manner. For most cases an email notification to the security team, push notifications on a specific system and for the most critical alerts a text message alert. The alerts should be regularly reviewed to limit the number of false positives.

## Implementation Roadmap

The recommended improvements should be implemented in a phased approach to minimize operational disruption and ensure proper validation at each stage. The first phase focuses on planning and preparation, including finalizing network design specifications, selecting appropriate SIEM and VPN solutions, and allocating necessary resources. During this stage, stakeholder alignment and risk assessment are critical to ensure a smooth transition.

The second phase involves the deployment of the redesigned network architecture. This includes implementing VLANs, subnetting, and updated routing and switching configurations. Changes should be introduced incrementally, with testing conducted after each step to confirm stability and performance. Proper documentation and configuration backups should be maintained throughout this process.

The third phase centers on the implementation of the SIEM solution. This includes configuring log sources, establishing event correlation rules, and tuning alerts to reduce false positives. Initial monitoring should be closely supervised to ensure the system is functioning as intended and providing meaningful insights.

The fourth phase includes the deployment of the VPN solution to enable secure remote access. This involves configuring encryption protocols, authentication mechanisms, and user access controls. End-user testing and training should be conducted to ensure usability and compliance with security policies.

The final phase focuses on validation and continuous improvement. This includes conducting security testing, reviewing system performance, and refining configurations as needed. Ongoing monitoring, regular audits, and periodic updates will ensure the long-term effectiveness of the implemented solutions.

## Success Metrics

The success of the implemented recommendations can be measured through a combination of technical performance indicators and business outcomes. One key metric is the reduction in detected security incidents and response times. With the SIEM solution in place, the organization should observe faster identification and resolution of potential threats.

Network performance and reliability also serve as important indicators. Improvements in uptime, reduced latency, and more efficient traffic management will demonstrate the effectiveness of the redesigned architecture. Additionally, successful segmentation can be validated through controlled access testing and reduced lateral movement within the network.

User access and security compliance metrics are also critical. The VPN solution should enable secure and reliable remote connectivity, with minimal access-related issues and strong adherence to authentication requirements. Monitoring unauthorized access attempts and failed login rates can provide further insight into security effectiveness.

Finally, audit and compliance readiness should improve as a result of centralized logging and enhanced visibility. The ability to generate detailed reports, track security events, and demonstrate adherence to best practices will indicate a stronger overall security posture.

Together, these metrics provide a clear framework for evaluating the effectiveness of the implementation and ensuring that the organization continues to meet its operational and security objectives.

References

Active Directory Domain Services. (n.d.). Active Directory Domain Services overview. Microsoft. https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview

pfSense. (n.d.). pfSense open source firewall. https://www.pfsense.org/

O'Donnell, J. (2026, February 1). Making Siem alerts smarter: Best practices for real-world detection. Cymulate. https://cymulate.com/blog/smarter-siem-alerts-validation/

OPNsense. (n.d.). OPNsense open source firewall and routing platform. https://opnsense.org/

SentinelOne. (2026, January 8). Top 10 SIEM tools for 2026. https://www.sentinelone.com/cybersecurity-101/data-and-ai/siem-tools/

7 types of remote access and how to pick the right one. RemoteToPC. (2025, December 16). https://remotetopc.com/types-of-remote-access/

SSL VPN vs. IPSec: What are the differences?. Palo Alto Networks. (n.d.). https://www.paloaltonetworks.com/cyberpedia/ipsec-vs-ssl-vpn

Symmetric encryption vs asymmetric encryption: How it works and why it's used. Device Authority. (2024, November 29). https://deviceauthority.com/symmetric-encryption-vs-asymmetric-encryption/

What is splunk? key benefits and features of Splunk. Fortinet. (n.d.). https://www.fortinet.com/resources/cyberglossary/what-is-splunk