Proposed Design for Network Integration

Corey Waldner

School of Technology and Engineering, National University

TIM-7010 v4: Management of Computer Networks

Dr. Carol Cusano

March 14, 2024

Proposed Design for Network Integration

This proposal outlines the network integration plan for the acquisition of a community bank that has 30 locations spread across various states in the Northeastern region of the United States. The current corporate office is located in the Midwestern region of the United States and has The Northeastern company's existing network infrastructure utilizes a wide area network to connect to each branch location. The design is for the integration and expansion of both networks and the integration of the active directory domains and email servers of both. Both networks are outdated and will need to be upgraded and scaled to meet the organization's growing needs, which is expected to grow from 150 employees to 500 employees within the next 18 months. This proposed design also includes an online banking solution, infrastructure redundancies, proactive network monitoring, bring your own device and guest device network, remote worker access, Intranet, unified communications, and Internet of Things best practices. The proposal aims to achieve 99.999 percent uptime, measured through strategic key performance indicators.

Business Requirements

The project's business requirements stem from the acquisition and merger of two banks located in the Midwest and Northeast regions of the United States. Each Bank operates with its own unique set of business processes, applications, and networks. The project's primary goal is to combine the network infrastructure of both banks while enabling customers to access banking services online. Over the next 18 months, employee numbers are expected to increase substantially, growing from the current 150 to over 500.

A business's technical requirements are closely tied to its overall business needs. Factors such as network reliability, security, availability, and ease of troubleshooting are key considerations that shape technical requirements (Pearson Higher Ed, 2024). These factors ensure a business's network infrastructure runs smoothly and without interruption.

Assumptions and Constraints

Identifying and managing assumptions and constraints is crucial to any project, as they are pivotal to its success (Kavirajan, 2021). Throughout the project life cycle, it's essential to continuously monitor and control these factors to minimize any possible obstacles. In this project, assumptions include the need for a data center that can grow as the business expands, as well as reliable internet access and sufficient bandwidth at each site (DTS Labs, 2021)**.** Additionally, it's assumed that the majority of online bank customers will be located in the Midwest and Northeast regions.

Design constraints include legacy AD integration, resource limitations, interoperability, geographical location, and regulation. To overcome these constraints, it's necessary to consolidate AD into a single domain, streamline accounts and group names (Radiant Logic, 2016), and manage resources efficiently. The network infrastructure must facilitate smooth communication and data exchange with third-party systems. Geographical location can pose a challenge regarding network latency and connectivity options, which must be addressed to ensure seamless operations. Finally, compliance with regulations and best practices is critical for any banking network. By staying up-to-date with the latest rules and regulations, the business can generate revenue while remaining compliant and secure (Samuels, 2015).

Technical Requirements

The technical requirements encompass recommendations for a hybrid networking solution. The technical requirements section delves into the network integration, the configuration and locations of the on-premise data center, WAN configuration, AD and email services integration, internet connectivity, scalability, infrastructure redundancies, proactive network monitoring, bring your own device and guest device network, remote worker access, Intranet, unified communications, Internet of Things best practices and online banking infrastructure. These foundational elements form the basis of the consolidated network and services resulting from the merger of banks.

Integrating the Networks

For a smooth and dependable integration of the networks of both banks, it is essential to have an intuitive system (Newman, 2016) that caters to both institutions. The recommendations below are founded on the comprehensive assessment of the processes, procedures, and documentation of both banks' IT infrastructure systems (Burns, 2020), aimed at providing a unified solution for all employees. The proposed solution will enhance the workflows, applications, and network infrastructure (Big Data, 2021), benefiting the banks and their customers.

Data Center

A data center serves as a centralized facility for an organization's IT operations and equipment. Its primary functions include storing, processing, and disseminating data and applications, which are crucial for the continuity of daily operations (What is a Data Center?, 2024). An on-premise solution is recommended for the Bank's data, applications, databases, operating systems, virtualization, physical servers, storage, networks, and the data center (Check Point, 2024). The data center houses critical and proprietary assets, such as the AD server, email server, firewall, router, switches, online bank database, network storage, and online bank application. An on-premise solution allows the Bank to have complete control over data storage and security measures, which is ideal for sensitive or regulated data. Additionally, predictable performance and low-latency access to data are possible because the Bank has complete control over the environment and networking (HPE, 2024).

Data Center Redundancy

In today's highly connected world, the Bank must ensure their services are always available to customers. Network downtime affects its users' finances, and any downtime can lead to significant financial losses for the Bank. To achieve a high level of availability, it is recommended that the Bank adopt a geo-distributed approach for on-premise data centers.

A geo-distributed approach involves setting up two or more data centers in different regions. This approach offers several benefits, such as scalability, data locality, and protection against disasters and failures (Endo & et al., 2017). The system can continue functioning even if one data center goes down by replicating data across multiple data centers. This fault-tolerant approach can achieve 99.999% availability by placing the system and services on at least three geo-locations with an overarching orchestration framework (Han & et al., 2017).

To implement this approach, it is recommended that three data centers be set up in Ohio, Boston, and Kansas City. These locations were chosen because they are thousands of miles apart, which can help safeguard the Bank and its customers against catastrophic events and natural disasters (IBM, 2022). Moreover, these locations support the base of the Bank's customers. By adopting a geographically redundant approach, the Bank can reduce latency and ensure optimal performance (Poole, 2020).

A geo-distributed approach is recommended for the Bank to achieve high availability and protect against disasters and failures. By setting up additional data centers in different locations, the Bank can ensure that its services are always available to customers and can continue functioning even in the face of catastrophic events.

Data Center Data Syncing

The geographically redundant on-premise data center approach ensures seamless handling of unexpected failures and maintains high availability. Redundancy between the data centers can be achieved through active-active or active-standby configurations. For optimal results, active-active mode is recommended as it allows for immediate takeover of customer traffic in case of a failure (Han & et al., 2017). With the geographical approach of the three data centers, a multi-region active-active configuration is established, consisting of the data centers running the same service simultaneously. Load balancing is achieved by distributing workloads across all data centers, preventing any single data center from overloading and improving throughput and response times (Villanueva, 2024). Two primary constraints must be met for this configuration to work: low latency connectivity between the data centers (Portworx, 2024) and consistency between them.

A consistency model for a multi-active availability cluster must be able to handle down data centers. Once the data center is back online, the data must sync between the three locations. An example of how the data will need to be synced between Ohio, Kansa City, and Boston is a write on key xyz of '123' received by Ohio and communicated to Kansa City and Boston. Both cities confirm the receipt of the write. Once Ohio receives the first confirmation, the change is committed. Unfortunately, Ohio fails. Kansa City receives a read of key xyz and returns the result '123'. Boston then receives an update for key xyz to the value '456'. The update is communicated to Kansa City, which confirms receipt of the write. After receiving confirmation, the change is committed. Ohio is restarted and rejoins the cluster, receiving an update that the key xyz now has a value of '456' (Cockroach Labs, 2024). Without consistency depending on which data center you are connected to will have different results.

Data Center Connectivity

To achieve a geo-distributive active-active configuration, a low-latency network is required. To ensure data synchronization between sites, it is recommended that the dedicated fiber line connection between the data centers be ten gigabits per second (Gbps) so the data can be replicated and database mirroring can be established. Going beyond this, the ten Gbps limit may result in hardware limitations, and networking equipment may require an upgrade. Not all switches would have mixed-speed ports, meaning upgrading all servers and the network simultaneously would be necessary to exceed the 10 Gbps limit (Arista, 2024). At ten Gbps, the Bank can handle incoming requests with low latency and provide the necessary level of service to internal users and customers (inSpace, 2013).

Data Center Scalability

The recommended scalability model involves an on-premise scale-out approach, which consists of distributing the processing load across multiple machines. Despite utilizing multiple machines, these machines function as a single server and share the load (YMD Tech, 2015). This approach eliminates the need for hardware swapping and often comes with management software that automates provisioning by leveraging sophisticated computational engines. This additional infrastructure saves time and money and makes incremental changes easy to implement (Network Critical, 2019). As shown in Figure 1, the load balancer, virtualization server, and storage server work together to allow scalability of the required services. The load balancer distributes network traffic equally across a pool of resources that support the banking application (AWS, 2024). The load balancer reduces the number of physical servers the Bank needs to have on-premise, improves resource utilization, allows for dynamic resource allocation, and improves resource prioritization (Karimyar, 2023).

Branch Locations

There are currently 42 Branch locations between the two organizations that have to connect to a data center. The expected growth over the next 18 months will equal roughly 11 employees per location. These are the primary front-line users interacting with customers and the applications. The branch locations have a guest network where guests and employees bring their own devices (BYOD) and can use the Internet.

Branch Location Internet and Redundancy

Internet connectivity is required for each Branch office to connect to the database and cloud applications. The Internet capacity or speed is measured in megabits per second (Mbps), which is the unit of measurement for network bandwidth and throughput (Wright & Scarpati, 2024). For basic online tasks such as emailing and browsing, minimal bandwidth is needed, typically only one Mbps per employee. VoIP calls require .5 Mbps per user while accounting, payroll, and bookkeeping software require three Mbps per employee. For high-definition video teleconferencing, a minimum of six Mbps per person is required, and downloading large files requires at least ten Mbps per employee (CenturyLink, 2024). Each employee must have a minimum capacity of 21 Mbps, and with an average of 11 employees per branch location, a total of 225 Mbps is needed at each location, not including the guest network. For average internet usage, regular access to cloud-based applications, and simultaneous video calls, each branch location should have a 500 Mbps connection (Davis, 2023).

It is also recommended that each Branch location operates with two vendor internet service providers (ISPs), with each ISP option consisting of a dedicated internet connection. This type of connection provides a specific amount of bandwidth that is not shared with other users, ensuring a consistent level of service regardless of the time of day or number of users online in the area. Along with dedicated bandwidth, service-level agreements guarantee performance metrics such as network latency, packet loss, uptime, jitter, and repair timeframes (Verizon Business, 2024).

Guest Network

Ensuring network security is a top priority for any organization that offers guest internet access within the workplace. To maintain the security and administration of the corporate network, it's important to isolate guest and employee BYOD access from the rest of the enterprise network. This can be achieved through physical or virtual network segmentation (Symantec, 2024). Network segmentation involves dividing an organization's computer network into smaller subnets, each forming a smaller network. By doing so, the Bank can better control traffic flow between subnets, improve security policies, and make it more difficult for unauthorized individuals to access sensitive data or critical network components (Sollitto, 2024). Virtual segmentation is recommended for guest and BYOD devices at Branch locations by creating Virtual Local Area Networks (VLAN). VLANs allow devices to be virtually connected as if on the same LAN. This approach improves network performance and prevents cyber threats from spreading beyond a specific network (Zenarmor, 2023).

For guests who require access to internal resources like printers, data storage, internal applications, or Intranet, it is recommended that the user be set up in Active Directory (AD) as a user within a guest container. The guest will need an internal sponsor and will be required to sign an acceptable use policy (AUP) outlining constraints and practices for accessing corporate networks or other resources (Kirvan, 2022). Before granting access to any systems, sponsors must identify which systems the guest will need access to. System access will be managed through group policy in AD, granting granular control (Buenning, 2024). This zero-trust policy ensures that the Bank's guests are authenticated and authorized, keeping its data and systems secure (Tigera, 2024).

Web Content Filtering for Guest Network

Network security is of the utmost importance when bringing guests or BYOD devices. One key aspect of network security is content filtering. Content filtering is a process that manages or screens access to specific emails or web pages. Content filtering aims to block content that contains harmful information (Fortinet, 2024).

Creating the VLAN for the guest devices or BYOD devices on the Bank's enterprise network still utilizes the same networking equipment that is in place, but without web content filtering, the Bank may be liable if someone is doing something illegal on it (Project Vision, 2024). The recommendation for content filtering is to use OpenDNS. OpenDNS is the name of a Domain Name System (DNS) service and the company that provides that service (Rouse, 2015). The OpenDNS service effectively controls access to web content and prevents harmful attacks (Rouse, 2015).

Wide Area Network (WAN)

Establishing a wide area network (WAN) is crucial to achieving seamless connectivity between all Branch locations and the on-premise data centers. The recommended WAN topology is a point-to-point configuration linking each branch location directly to a data center. This configuration simplifies troubleshooting and maintenance, as each site is directly connected to the other (Maggio, 2017).

IPsec VPN technology is recommended for point-to-point WAN. IPsec VPN allows for secure connection of all sites on a private network using the Internet as the data communications network. As shown in Figure 1, this VPN is set up between firewalls at each location, creating a secure IPsec tunnel between sites. The benefits of this recommendation include cost savings and the ability to utilize existing internet connectivity for data transport (Simplify, 2024).

Remote Workforce

Remote work is a method of working that enables employees to complete their tasks without being physically present in a traditional office space. Instead, digital tools facilitate communication and collaboration with colleagues (KissFlow, 2024). The advantages of remote work extend beyond the employee to benefit the entire organization. It is recommended that a remote worker have at least a 50 Mbps internet connection at their remote location, as the minimum required is 21 Mbps, which was stated earlier for the Branch location per employee.

Remote Workforce Training

Working remotely offers benefits for both employers and employees. If a company is planning to transition to a remote work environment on a more long-term or permanent basis, it is important to ensure a smooth transition by implementing excellent remote management plans and a well-defined remote work policy (Peek, 2024). It is recommended that part of the organizational policy for working remotely is a remote work training program, which is essential to provide the same level of safeguards for remote workers as on-site workers. This program should train employees to understand the additional risks of working remotely and the corresponding responsibilities. Security and privacy risks are heightened during times of disaster, such as the coronavirus pandemic, which can lead to poor security decisions and increased susceptibility to phishing attacks (SecurityMentor, 2024). Training should cover phishing attacks, removable media, passwords and authentication, physical security, mobile device security, working remotely, public Wi-Fi, cloud security, social media use, Internet and email use, social engineering, and security at home (Daly, 2024). Employee training reduces remote work risk for data security and uncovers threats before they become significant issues (Freeman, 2023).

Remote Work VPN Access Controls

To further secure the Bank's enterprise network, it is recommended to restrict remote work with approved devices only, thereby disallowing work with personal devices to remote and access critical systems. It is recommended that the approved devices use VPN clients that create a secure connection to another network over the Internet (Barracuda, 2024).

The recommended VPN client type is the Key Exchange/Internet Protocol Security (IKE/IPsec) combination (NSA, 2021). IKE is a key management protocol standard used with the IPsec standard. IPsec is an IP security feature that provides robust authentication and encryption of IP packets. IPsec can be configured without IKE, but IKE enhances IPsec by providing additional features, flexibility, and ease of configuration for the IPsec standard (Cisco, 2024). Approved guests can also utilize the VPN client for internal access through the same process.

Applications and Systems

Seamlessly integrating various applications and systems is crucial for a successful merger. As the Bank navigates through this process, the strategic deployment of technology becomes imperative. This section presents recommendations for critical applications and systems, such as integrating Active Directory and email services, cloud-based intranets, online banking solutions, unified communications, and network storage. By adopting these approaches to application and system implementations, the Bank can unlock greater efficiency, improve collaboration, and enhance its technological infrastructure.

Merging Active Directory and Email Services

It is recommended that an on-premise solution be used for both Active Directory (AD) and email services. The email infrastructure, which consists of hardware and software responsible for sending and receiving email messages (Meyer, 2023), is best managed on-premise for enhanced security and control (Meyer, 2021). AD is a database that stores information on users, devices, and resources, allowing administrators to regulate access to applications and resources (Magnusson, 2022). An on-premise solution is preferred because it provides full control, integrates legacy systems, enhances security, and allows offline authentication (Falak, 2024).

To ensure optimal functionality, the email service necessitates a dedicated server within the data center. Meanwhile, AD operates on a separate server as a module on the domain controller. This recommended infrastructure setup streamlines the most complex business transformations during mergers and acquisitions, reducing the need for troubleshooting and setup (Kapanadze, 2019).

Cloud Based Intranet

The modern business environment demands seamless collaboration and communication among employees, even when geographically dispersed. With the merger, the workforce is spread over different regions of the United States, and now some employees are working remotely. To address this challenge, it is recommended that the Bank implements an intranet, which is a private, secure network that enables communication and collaboration among employees and approved guests.

An intranet is a central website for employees and approved guests to access company information and stay connected with colleagues. The Intranet helps businesses to communicate, be more productive, collaborate, store documents securely, and stay connected (Williamson, 2024). With the Bank having a cloud-first policy, it is recommended that the Intranet be a cloud-based solution.

Traditionally, businesses have relied on on-premises intranet solutions, where the Bank buys and owns the software. The Bank would have to host it at its data centers and maintain all the associated costs and burdens. This includes purchasing and provisioning the hardware and other infrastructure that the software runs on, installing, testing, and deploying the software, maintaining and upgrading it, applying patches and securing it, and expanding capacity as needed as usage grows.

With cloud intranet solutions, these responsibilities fall on the software vendor and cloud services provider. The software is hosted in the cloud, spread across an array of virtualized computing resources typically shared by several customers (Jive, 2024). An intranet is an engagement platform for the Bank to share information, updates, and other needed materials in one place, making it an essential tool for enhancing collaboration and communication in a geographically dispersed workforce.

Unified Communications for Collaboration

An intranet is an excellent tool for disseminating information throughout an organization, but it lacks the real-time communication capabilities necessary for a workforce spread across multiple regions. It is recommended that a cloud-based unified communication as a service (UCaaS) be used as a comprehensive communication system. UCaaS is a system that combines various enterprise communication tools such as Voice over Internet Protocol (VoIP), instant messaging, video conferencing, and business phones into a cohesive application (Sivakrishnan, 2022).

The advantages of UCaaS are numerous, with the main benefit being that this cloud-based communication service allows bank employees to collaborate and communicate virtually wherever and whenever by delivering voice, video calling, document sharing, virtual meetings, and chat with a single platform. Regardless of the team's location, they can communicate and work together seamlessly (Dunham, 2021).

Online Banking

The recommended solution for online banking is an on-premise architecture. With this approach, the Bank can reduce risk, increase customization, ensure compliance, and avoid recurring software fees (Malyshev, 2022). The necessary components for an on-premise solution include an application interface, payment gateway, database, authentication service, notification service, transaction processing service, fraud detection service, and logging and monitoring service (Aaaryana, 2024). As shown in Figure 2, by implementing this infrastructure, the Bank can offer their customers the ability to create bank accounts, transfer money, create payment cards, and make payments directly through their accounts (Pehlivanov, 2021).

Network Storage

A storage system is where data and files can be stored in a central location. The recommended storage type is network-attached storage (NAS). A NAS system is a storage device connected to a network that allows authorized network users and heterogeneous clients to store and retrieve data from a centralized location. NAS systems are flexible and scale out, meaning that as additional storage needs arise, the Bank can add to what it already has (Seagate, 2024). The benefits of a NAS are that it provides a cost-effective method for providing ample storage to multiple individuals or computer systems. Additionally, it offers a user-friendly setup and configuration process, simplifies the process of implementing a Redundant Array of

Independent Disks (RAID) redundancy for a large number of users, and enables users to customize permissions, folder privileges, and access levels to ensure secure document management. Ultimately, it optimizes storage resource utilization to the fullest potential (Hasen, 2024).

To ensure fault tolerance and high availability in an active-active geo-distributed on-premise data center approach, utilizing a NAS system storage at each data center and a Redundant Array of Independent Disks (RAID) is recommended. RAID technology improves an organization's performance and the fidelity of data storage by storing the same data in different locations on multiple hard disk drives or solid-state drives, thus securing the data in the event of a drive failure. There are several RAID levels available, each with different objectives (Piskorz, 2024). For active-active geo-distributed on-premise data centers, it is recommended to have a NAS RAID 10 capacity solution at each data center for both high performance and redundancy.

Monitoring

Network monitoring involves discovering, mapping, and tracking a network's health across its hardware and software layers. A proactive monitoring approach is essential to manage the network effectively. Unlike reactive monitoring, which only detects failures after they occur, proactive monitoring alerts IT administrators to potential issues before they become failures **(Berry, 2022)**. The recommended network tools and processes are categorized into three critical monitoring areas: Network monitoring, device health monitoring, and security monitoring.

Network Monitoring

The proposed design relies on the WAN and data centers to be interconnected. To achieve this, the implementation of Simple Network Management Protocol (SNMP) is proposed. SNMP utilizes a polling methodology to gather data on devices, interfaces, and CPU, among others, to monitor and collect the status of the network infrastructure. Although SNMP provides a foundation for basic working or non-working monitoring, it typically does not offer detailed network information to analyze the root causes of application performance or user experience issues (Preimesberger, 2020).

For additional monitoring of tunnels and performance, sampled flow (sFlow) is recommended because it records statistical and infrastructure metadata about traffic traversing the tunnels. SFlow provides visibility into network and bandwidth usage by applications and users. It also measures the local area network (LAN) and WAN traffic, troubleshooting and diagnosing network problems, detecting anomalous network traffic and illicit network usage, monitoring quality-of-service, and ensuring adherence to service-level agreements (Osowski, 2018). By utilizing both SNMP and sFlow, the Bank can leverage the current status of the SNMP network devices while allowing sFlow to monitor the WAN.

Device Monitoring Tools

While SNMP effectively detects device functionality, it cannot provide a comprehensive overview of a device's history. Log file monitoring is recommended for any network-connected device for a monitoring solution. This involves collecting, analyzing, and acting on log data from multiple sources, including system events, error messages, performance metrics, and user activity generated by various systems and applications (Elastic, 2024). With log file monitoring, the IT team can centrally view a large amount of logs, save time troubleshooting events, and receive alerts for potential future issues.

Security Monitoring

Cybersecurity monitoring tools are crucial to safeguard sensitive data and maintain a secure digital environment (Fibertrain, 2023). The recommended technique is signature-based detection, which utilizes a unique digital footprint from software programs on a protected system. Antivirus programs can scan software, identify the signature, and compare it to known malware signatures. This technique is highly effective against frequent attacks such as phishing, malware, or denial of service, as it relies on regular updates of the signature database from security experts or vendors (RiskXchange, 2024).

Proactive Monitoring

Proactive monitoring attempts to identify potential issues before they create significant impacting failure, performance degradation (Solarwinds, 2024), or problems with the IT infrastructure (Berry, 2022). A cloud-based log analyzer with log intelligence is recommended. A cloud-based log analyzer collects the network monitoring, device health monitoring, and security monitoring logs and applies log intelligence. Log intelligence is a log analysis method powered by artificial intelligence and automation. Intelligence platforms learn normal behavior in the systems and surface performance-impacting issues in the context of alerts and metrics in the same timeframe. This extra intelligence layer analyzes logs automatically, finding the root cause of problems and surfacing anomalies within log data, sometimes even pre-empting trouble before it occurs (LogicMonitor, 2024). This approach goes beyond traditional retrospective analysis by predicting future events based on historical log data patterns. The log analyzer processes and comprehends large amounts of log information, enabling it to recognize trends, correlations, and anomalies. A log analyzer can predict potential issues or security threats before they occur (Gill, 2023), making it a proactive monitoring approach.

Events, Alerts, Notifications and Visualization

An event refers to any discernible alteration or incident within a system, whether it be routine, informational, or indicative of potential problems collected by probes for network monitoring, device health monitoring, and security monitoring. Probes generate logs and regular updates, which are recorded as event data in the cloud-based log analyzer. On the other hand, an alert is a notification prompted by an event that informs stakeholders of a situation requiring immediate attention (Brennen, 2024). It is recommended that these alerts and events be recorded in the IT ticketing system to be addressed based on a tired priority system (see Figure 3). Critical systems and services will generate a notification via user preference. Non-critical events are automatically routed to the responsible individual or team in charge of the corresponding system or service without notification.

Although alerts and events are logged in the system and users receive notifications based on priority, having a comprehensive view of the network's status is still important. To achieve this, a simple yet informative dashboard that all audiences can easily understand, regardless of technical expertise, is recommended. Too many graphs can create visual chaos and detract from the dashboard's value (Lama, 2020). Instead, a widely-used Red-Yellow-Green status dashboard is an effective tool to quickly and simply convey the current state of the network through a visual model that makes it easy to spot patterns (see Figure 4) (Levison, 2021).

Key Performance Indicators (KPIs)

Key Performance Indicators (KPIs) are utilized for post-hoc analysis and reporting and for setting goals for the Bank (Cisco, 2024). The two recommended KPI metrics that fall within network performance monitoring are the retransmission rate and network response time. Retransmissions occur when packets are lost, and the network needs to retransmit them to complete a data request. By analyzing the retransmission rate, the Bank can determine how often packets are being dropped, indicating congestion on the network. Additionally, by analyzing retransmission delay, or the time it takes for a dropped packet to be retransmitted, the Bank can understand how long it takes for the network to recover from packet loss (Hein, 2019). Network response time is the system's time to respond to a user request. Fast response times contribute to a positive digital experience, especially in web applications and interactive systems (Digital Samba, 2023). Monitoring and tracking these two KPIs quickly identify and deal with potential failures, performance issues, and bottlenecks before they result in an outage (Analytix, 2024).

Internet of Things

The Internet of Things (IoT) refers to a network of physical devices, vehicles, appliances, and other physical objects embedded with sensors, software, and network connectivity, allowing them to collect and share data (IBM, 2024). IoT helps departments save time and money by gathering and transferring data efficiently in the banking world. It helps automate core finance processes through efficient collection and processing of information. The application of IoT in finance also extends to improvements in enterprises' customer experience (Fisher, 2023).

IoT Management and Monitoring

IoT Monitoring (IoTM) is discovering, evaluating, monitoring, and managing the devices connected to the Internet. It allows for the real-time overseeing and data collection of the interconnected devices' functionalities, performances, and troubleshooting (Dilmegani, 2024). For monitoring IOT devices, it is recommended to go with a cloud SaaS solution. By utilizing the cloud, the Bank can analyze and present captured IoT sensor data to business users via dashboards. SaaS IoT applications can use machine learning algorithms to analyze massive amounts of connected sensor data in the cloud. Using real-time IoT dashboards and alerts, you gain visibility into key performance indicators, statistics for the mean time between failures, and other information. Machine learning-based algorithms can identify equipment anomalies, send users alerts, and even trigger automated fixes or proactive countermeasures (Oracle, 2024).

Another benefit of using a SaaS application for IoT monitoring is that the Bank does not have to maintain an infrastructure to house the collected data from IoT devices and sensors. IoT devices produce enormous amounts of data, which is readily multiplied by the number of devices involved (Bigelow, 2023). That data is a valuable business asset that must be stored and secured in accordance with proper compliance and retention requirements (Bigelow, 2023).

Internet of Things Security

Security for the IOT means protecting internet devices and the networks they connect to from online threats and breaches. This is achieved by identifying, monitoring, and addressing potential security vulnerabilities across devices. At its simplest, IoT security is the practice that keeps IoT systems safe (Kaspersky, 2024). The risks associated with IOT devices are lack of testing and developing IOT, default passwords, and insecure interfaces (Kaspersky, 2024).

To mitigate these risks of lack of testing and development, it is recommended that the Bank only use IOT devices that have been certified by industry regulators (Nederveen, 2022). IoT device certification ensures that devices meet the rigorous operating standards defined by industry, local regulations, and network operators in the region of operation (Nederveen, 2022). The certification processes often include stringent security testing to safeguard against vulnerabilities such as hacking, data breaches, and unauthorized access. This is vital for the device's protection, the security of the networks it connects to, and the data it handles (Heredia, 2024). IoT devices that have been certified by industry regulators will lower the risk of a compromised device and network.

To mitigate the risk of default passwords, it is recommended that IoT devices change the default password (Stapel, 2023). Many IoT devices come with passwords like default or admin that attackers can exploit to gain access (Stapel, 2023). The recommendation would be for IoT devices to be set up with a service account in AD (AWS, 2024). The permission of the service account will be controlled by group policy, so the device will only have permissions to the resource or services for the intended monitoring or automated function. Establishing a service account with group policy IoT devices will lower the risk of an attack with known default credentials, and IoT will only be used for approved functions.

To mitigate the insecure interfaces with IoT, the recommendation is that device communication uses an asymmetric encryption key for communication (Rupareliya, 2023). Asymmetric encryption keys use a public key for encryption and a private key for decryption, which are linked mathematically and logically to each other. Any sender can encrypt the data using the public key. However, the decryption is only possible by the intended recipient using the private key. Thus, asymmetric encryption involves authentication with strengthened security (Rupareliya, 2023). Asymmetric encryption is a reliable way to protect sensitive information when sent over untrusted networks like the Internet when connecting to IoT SaaS application. Two different keys to encrypt the data make it more secure (Vashishtha, 2023).

While IoT is great for the Bank regarding monitoring and automation, IoT devices can be network resource intensive. To address this concern, along with additional security measures, it is recommended to have a separate VLAN for all IoT devices (FBI Portland, 2019). One of the added benefits of having all IoT devices on a separate VLAN is the connection can be throttled to an optimal speed so the quality of service for other applications and services is not affected by IoT devices (HPE, 2024). As shown in Figure 5, the proposed network design architecture will have three separate VLANs with VLAN ID 3 for IoT devices.

Conclusion

The proposed network integration plan for acquiring the community bank is a comprehensive strategy that addresses current and future networking needs. By combining traditional and cloud-based technologies, the hybrid network model offers the scalability, resilience, and security essential for supporting the Bank's operations.

The proposed network architecture features a geo-distributed on-premise data center approach, with data centers in Ohio, Kansa City, and Boston creating a fault-tolerant multi-region active-active configuration. To enhance reliability and uptime, the proposal includes redundancy measures in layer two and layer three of the OSI model, such as Multiple Spanning Tree Protocol (MSTP) and Virtual Router Redundancy Protocol (VRRP), respectively. The network will consist of a WAN that connects each branch to a data center with the lowest latency and resources available for optimal task performance. Application and service components such as the banking database, application server, AD, email services, and network storage will be mirrored between data centers. Cloud applications like the Intranet, unified communications, and log analysis are integrated for seamless and consistent access. The proposed solution also incorporates proactive monitoring tools for the Bank to track the WAN, device, and security so the Bank will better understand its operations and potential security risks. Each branch location will have a segregated guest environment with its own web content filtering solution. The entire infrastructure supports a separate VLAN for all IoT devices. A secure VPN access policy supports remote working and is further supported by end-user training.

The redundancy, comprehensive testing plan, proactive monitoring, and security aim to provide a solution with a 99.999 percent uptime. The effectiveness of this approach will be measured through strategic KPIs, allowing the Bank to track progress over time and ensure that users and customers have a positive and seamless experience when utilizing the network's proposed design.

References

Aaryana. (2024, Feburary 14). *System Design | Online Banking System*. Retrieved from geeksforgeeks: https://www.geeksforgeeks.org/system-design-online-banking-system/

Analytix. (2024, March 16). *Managed IT Support: The Key to Proactive Monitoring and Issue Resolution*. Retrieved from Analytix IT Solutions: https://www.analytixit.com/the-key-to-proactive-monitoring-and-issue-resolution/#:~:text=Proactive%20monitoring%20involves%20continuously%20monitoring,bottlenecks%20before%20they%20become%20serious.

Arista. (2024, March 12). *10GigE_Whitepaper*. Retrieved from Arista: https://www.arista.com/assets/data/pdf/Whitepapers/10GigE_Whitepaper.pdf

AWS. (2024, March 15). *Identity and access management for AWS IoT*. Retrieved from AWS: https://docs.aws.amazon.com/iot/latest/developerguide/security-iam.html

AWS. (2024, Feburary 24). *What is load balancing?* Retrieved from AWS: https://aws.amazon.com/what-is/load-balancing/

Barracuda. (2024, March 9). *What is a VPN Client? Why VPN Clients are Important Learn More About VPN Clients What is a VPN Client?* Retrieved from Barracuda: https://www.barracuda.com/support/glossary/vpn-client

Berry, R. (2022, August 19). *What is Proactive Monitoring?* Retrieved from Eg Innovations: https://www.eginnovations.com/blog/what-is-proactive-monitoring/

Big Data. (2021, December 13). *Reasons to Start Planning Your IT Infrastructure Upgrade*. Retrieved from We Buy Used IT Equipment: https://webuyuseditequipment.net/reasons-to-start-planning-your-it-infrastructure-upgrade/

Bigelow, S. J. (2023, July 11). *Ultimate IoT implementation guide for businesses*. Retrieved from TechTarget: https://www.techtarget.com/iotagenda/Ultimate-IoT-implementation-guide-for-businesses

Brennen, A. (2024, January 3). *What's the difference between an event vs alert vs incident in IT operations?* Retrieved from Big Panda: https://www.bigpanda.io/blog/decode-events-alerts-incidents/#:~:text=Monitoring%20forms%20the%20foundation%20for,role%20in%20IT%20ecosystem%20management.

Buenning, M. (2024, March 7). *What Is Group Policy in Active Directory?* Retrieved from NinjaOne: https://www.ninjaone.com/blog/what-is-group-policy-in-active-directory/#:~:text=Active%20Directory%20Group%20Policies%20provide,consistent%2C%20and%20productive%20IT%20infrastructure.

Burns, S. (2020, February 14). *Practical advice to integrate IT systems after a merger*. Retrieved from Tech Target: https://www.techtarget.com/searchitoperations/tip/Practical-advice-to-integrate-IT-systems-after-a-merger

CenturyLink. (2024, March 12). *How to determine bandwidth needs for your small business*. Retrieved from CenturyLink: https://discover.centurylink.com/ldetermine-bandwidth-needs-for-small-business.html

Check Point. (2024, February 24). *Data Center vs Cloud*. Retrieved from Check Point: https://www.checkpoint.com/cyber-hub/cyber-security/what-is-data-center/data-center-vs-cloud/

Cisco. (2024, March 9). *Configuring Internet Key Exchange for IPsec VPNs*. Retrieved from Cisco: https://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_ikevpn/configuration/15-2mt/sec-key-exch-ipsec.html

Cisco. (2024, March 3). *Key Performance Indicators (KPIs)*. Retrieved from Cisco: https://developer.cisco.com/docs/network-automation-delivery-model/#!key-performance-indicators-kpis/key-performance-indicators-kpis

Cockroach Labs. (2024, February 27). *Multi-Active Availability*. Retrieved from Cockroach Labs: https://www.cockroachlabs.com/docs/stable/multi-active-availability#what-is-multi-active-availability

Daly, J. (2024, March 9). *12 Essential Security Awareness Training Topics for 2024*. Retrieved from usecure: https://blog.usecure.io/12-security-awareness-topics-you-need-to-know-in-2020

Davis, S. (2023, March 22). *HOW MUCH BANDWIDTH DOES YOUR BUSINESS REALLY NEED?* Retrieved from Velocity: https://www.velocityokc.com/blog/member-news/how-much-bandwidth-does-your-business-really-need/

Digital Samba. (2023, December 19). *Video API Embedded A Deep Dive into the Network Performance Monitoring Metrics*. Retrieved from Digital Samba: https://www.digitalsamba.com/blog/a-deep-dive-into-the-network-performance-metrics

Dilmegani, C. (2024, January 10). *A Guide to IoT Monitoring in 2024: Pros, Cons & Importance*. Retrieved from AIMultiple: https://research.aimultiple.com/iot-monitoring/

DTS Labs. (2021, April 26). *How to Handle Project Assumptions & Constraints?* Retrieved from Medium: https://medium.com/dlt-labs-publication/how-to-handle-project-assumptions-constraints-10483a675519

Dunham, D. (2021, January 27). *The 5 Benefits of UCaaS That Every Business Leader Should Know*. Retrieved from Telnet Worldwide: https://www.telnetww.com/blog/unified-communications/benefits-of-ucaas/

Endo, P. T., & et al. (2017). Minimizing and Managing Cloud Failures. *Computer*, pp. 86-90.

Falak, U. (2024, Feburary 24). *On-Prem Active Directory vs. Azure AD: A Comprehensive Comparison*. Retrieved from Xavor: https://www.xavor.com/blog/on-prem-active-directory-vs-azure-ad/#:~:text=and%20security%20policies.-,Key%20Features%20and%20Advantages%20of%20On%2DPrem%20AD,to%20the%20organization's%20specific%20needs.

FBI Portland. (2019, December 3). *Tech Tuesday: Internet of Things (IoT)*. Retrieved from FBI: https://www.fbi.gov/contact-us/field-offices/portland/news/press-releases/tech-tuesday-internet-of-things-iot

Fibertrain. (2023, August 6). *Cyber Security Monitoring Tools*. Retrieved from Fibertrain Cybersecurity Training & Certifications.: https://fibertrain.net/top-10-cyber-security-monitoring-tools/

Fisher, R. (2023, April 17). *IoT in Finance: Benefits and Use Cases*. Retrieved from highradius: https://www.highradius.com/resources/Blog/iot-in-finance/

Fortinet. (2024, March 7). *What Is Content Filtering?* Retrieved from Fortinet: https://www.fortinet.com/resources/cyberglossary/content-filtering

Freeman, C. (2023, December 1). *8 Essential Security Awareness Training Topics*. Retrieved from Code42: https://www.code42.com/blog/cyber-security-awareness-training-topics-for-employees/

Gill, J. K. (2023, December 15). *Log Analytics with Generative AI Dr. Jagreet Kaur Gill | 15 December 2023*. Retrieved from Xenonstack: https://www.xenonstack.com/blog/log-analytics-generative-ai

Han, B., & et al. (2017). On the resiliency of virtual network functions. *IEEE Communications Magazine*, 55(7), 152.

Hasen, A. (2024, March 11). *Storage Types (DAS, NAS & SAN)*. Retrieved from Network Walks: https://networkwalks.com/storage-types-das-nas-san/

Hein, D. (2019, June 27). *Network Performance Metrics: 7 Essential Network Metrics to Monitor*. Retrieved from Solution Review: https://solutionsreview.com/network-monitoring/network-performance-metrics-7-essential-network-metrics-to-monitor/

Heredia, R. (2024, March 5). *What Is IoT Device Certification & Why It Matters*. Retrieved from zipitwireless: https://www.zipitwireless.com/blog/what-is-iot-device-certification-why-it-matters

HPE. (2024, March 15). *VLAN-based rate-limiting*. Retrieved from Techhub HPE: https://techhub.hpe.com/eginfolib/networking/docs/switches/RA/15-18/5998-8161_ra_2620_mcg/content/ch05s02.html#:~:text=VLAN%2Dbased%20rate%2Dlimiting%20provides,that%20exceeds%20the%20configured%20rate.

HPE. (2024, February 24). *What is On-Premises Data Centers vs. Cloud Computing?* Retrieved from Hewlett Packard Enterprise: https://www.hpe.com/us/en/what-is/on-premises-vs-cloud.html#:~:text=On%2Dpremises%20data%20centers%2C%20commonly,to%20scale%20up%20and%20down.

IBM. (2022, July 25). *Enabling geo-redundancy*. Retrieved from IBM: https://www.ibm.com/docs/en/tncm-p/1.4.1?topic=settings-enabling-geo-redundancy

IBM. (2024, March 15). *What is the Internet of Things (IoT)?* Retrieved from IBM: https://www.ibm.com/topics/internet-of-things

inSpace. (2013, September 11). *How Much Data Center Bandwidth Do You Really Need?* Retrieved from inSpace: https://blog.ipspace.net/2013/09/how-much-data-center-bandwidth-do-you.html

Jive. (2024, March 9). *Cloud Intranet*. Retrieved from Jive Software: https://www.jivesoftware.com/blog/intranet/solutions/cloud-intranet#gsc.tab=0

Kapanadze, G. (2019, March 11). *Troubles with Email Migration Under M&A Project? Synchronize and Move Exchange Accounts Seamlessly with CB Exchange Server Sync*. Retrieved from Connecting Software: https://www.connecting-software.com/blog/troubles-with-email-merged-companies-sync-calendars-different-exchange-servers/

Karimyar, M. (2023, October 10). *Hyper-V vs VMware: What's the difference and which should you choose?* Retrieved from Server Mania: https://www.servermania.com/kb/articles/hyperv-vs-vmware

Kaspersky. (2024, March 15). *Internet of Things security challenges and best practices*. Retrieved from Kaspersky: https://usa.kaspersky.com/resource-center/preemptive-safety/best-practices-for-iot-security

Kavirajan, A. (2021, April 26). *How to Handle Project Assumptions & Constraints?* Retrieved from Medium: https://medium.com/dlt-labs-publication/how-to-handle-project-assumptions-constraints-10483a675519#id_token=eyJhbGciOiJSUzI1NiIsImtpZCI6IjU1YzE4OGE4MzU0NmZj

MTg4ZTUxNTc2YmE3MjgzNmUwNjAwZThiNzMiLCJ0eXAiOiJKV1QifQ.eyJpc3MiOiJodHRwczovL2FjY291bnRzLmdvb2dsZS5j

Kirvan, P. (2022, June). *acceptable use policy (AUP)*. Retrieved from TechTarget: https://www.techtarget.com/whatis/definition/acceptable-use-policy-AUP

KissFlow. (2024, March 9). *What is Remote Work?* Retrieved from Kissflow: https://kissflow.com/digital-workplace/remote-work/remote-working-101-ultimate-guide/

Lama, J. (2020, January 23). *Effective Dashboarding: Why Less Is More*. Retrieved from Merkle: https://www.cardinalpath.com/blog/effective-dashboarding-why-less-is-more

Levison, M. (2021, February 2). *Red-Yellow-Green Status Reports and Other Models – How They Should and Shouldn't Be Used*. Retrieved from Agile: https://agilepainrelief.com/blog/red-yellow-green-or-rygrag-reports-how-they-hide-the-truth.html

LogicMonitor. (2024, March 16). *How to Analyze Logs Using Artificial Intelligence*. Retrieved from LogicMonitor: https://www.logicmonitor.com/blog/how-to-analyze-logs-using-artificial-intelligence

Maggio, A. (2017, November 16). *WAN Connections and Technologies Explained*. Retrieved from ICT Shore: https://www.ictshore.com/free-ccna-course/wan-connections/

Magnusson, A. (2022, November 22). *Directory Services*. Retrieved from StrongDM: https://www.strongdm.com/what-is/directory-services

Malyshev, A. (2022, June 22). *Banking Software: Weighing The Pros And Cons of SaaS And On-Premise Solutions*. Retrieved from SDK.finance: https://sdk.finance/banking-software-saas-vs-on-premise/

Meyer, L. (2021, August 20). *How to Choose the Right Email Infrastructure for Your Business*. Retrieved from SocketLabs: https://www.socketlabs.com/blog/how-to-choose-the-right-email-infrastructure-for-your-business/

Meyer, L. (2023, January 23). *Email Infrastructure Landscape: Your Guide to Email Delivery in 2023*. Retrieved from SocketLabs: https://www.socketlabs.com/blog/email-infrastructure/

Nederveen, P. (2022, January 14). *What is IoT device certification?* Retrieved from eseye: https://www.eseye.com/resources/iot-explained/what-is-iot-device-certification/

Network Critical. (2019, March 19). *Why "Scaling Up" Your Network Infrastructure Always Leads to More Complexity and Cost*. Retrieved from Network Critical: https://www.networkcritical.com/single-post/2019/03/11/why-scaling-up-your-network-infrastructure-always-leads-to-more-complexity-and-cost

Newman, D. (2016, March 31). *Merging Technology – Infrastructure, Data Centers, and Networks During and After M&A (Merger and Acquisition)*. Retrieved from Converge Technolgy + Business: https://convergetechmedia.com/merging-technology-infrastructure-data-centers-networks-ma-merger-acquisition/

NSA. (2021, September 1). *Selecting and Hardening Remote Access VPN Solutions*. Retrieved from Defense.gov: https://media.defense.gov/2021/Sep/28/2002863184/-1/-1/0/CSI_SELECTING-HARDENING-REMOTE-ACCESS-VPNS-20210928.PDF

Oracle. (2024, March 15). *What is IoT?* Retrieved from Oracle: https://www.oracle.com/internet-of-things/what-is-iot/

Osowski, K. (2018, September 11). *NetFlow vs. sFlow: What’s the Difference?* Retrieved from Kentik: https://www.kentik.com/blog/netflow-vs-sflow/

Pearson Higher Ed. (2024, February 24). *Introducing Network Design Concepts*. Retrieved from Pearson Higher Ed: https://www.pearsonhighered.com/assets/samplechapter/1/5/8/7/1587132125.pdf

Peek, S. (2024, January 3). *Remote Work Best Practices (Plus Sample Policy)*. Retrieved from Business: https://www.business.com/articles/remote-work-best-practices/

Pehlivanov, M. (2021, March 1). *BankSystem*. Retrieved from Github: https://github.com/banksystembg/BankSystem

Piskorz, P. (2024, March 11). *What is RAID and How Does it Work?* Retrieved from Storware: https://storware.eu/blog/what-is-raid-and-how-does-it-work/

Poole, J. (2020, September 7). *Geo-Redundancy: a Top Business Priority in the Digital Era*. Retrieved from LinkedIn: https://www.linkedin.com/pulse/geo-redundancy-top-business-priority-digital-era-jim-poole

Preimesberger, C. (2020). Data Types Enterprises Should Use for High Network Visibility. *eWeek*, N.PAG.

Project Vision. (2024, March 10). *WiFi Law 101: Legal Compliance and Your Guest Wireless Network*. Retrieved from Project Vision: https://project-vision.co.uk/networks/wifi-law-101-legal-compliance-and-your-guest-wireless-network/

Radiant Logic. (2016). RadiantOne Consolidates Active Directory Domains/Forests Into Azure AD. *Business Wire*.

RiskXchange. (2024, March 3). *What You Need to Know About Signature-based Malware Detection*. Retrieved from RiskXchange: https://riskxchange.co/1006984/what-is-signature-based-malware-detection/#:~:text=Signature%2Dbased%20detection%20uses%20a,to%20signatures%20of%20known%20malware.

Rouse, M. (2015, June 2). *What Does OpenDNS Mean?* Retrieved from Techopedia: https://www.techopedia.com/definition/31257/opendns

Rupareliya, K. (2023, April 16). *Securing The IoT Data Landscape: IoT Encryption Algorithms*. Retrieved from Intuz: https://www.intuz.com/blog/securing-the-iot-data-landscape-iot-encryption-algorithms

Samuels, M. (2015). Standard Bank takes global approach to IT challenges following acquisition. *Computer Weekly*, 12-15.

Seagate. (2024, March 11). *What is NAS (Network Attached Storage) and Why is NAS Important for Small Businesses?* Retrieved from Seagate: https://www.seagate.com/blog/what-is-nas-master-ti/

SecurityMentor. (2024, March 9). *Remote Work Training Program*. Retrieved from SecurityMentor: https://www.securitymentor.com/products-services/security-awareness-training/remote-working

Simplify. (2024, February 24). *Different Types of WAN Technologies – Data Networking Services*. Retrieved from Simplify: https://www.bsimplify.com/types-wan-technologies-data-networking/

Sivakrishnan, A. (2022, February 9). *What is Unified Communications? Definition, System, Cloud Service, Best Practices and Examples*. Retrieved from https://www.spiceworks.com/collaboration/unified-communications/articles/what-is-unified-communications/: Spiceworks

Solarwinds. (2024, March 16). *Proactive Monitoring: Definition and Best Practices*. Retrieved from Solarwinds: https://www.loggly.com/use-cases/proactive-monitoring-definition-and-best-practices/#:~:text=What%20Is%20Proactive%20Monitoring%3F,or%20performance%20degradation%20sets%20in.

Sollitto, N. (2024, March 04). *What is Network Segmentation? Virtual & Physical Segmentation*. Retrieved from UpGuard: https://www.upguard.com/blog/what-is-network-segmentation

Stapel, G. (2023, October 26). *The Haunted House of IoT: When Everyday Devices Turn Against You*. Retrieved from Imperva: https://www.imperva.com/blog/understanding-internet-of-things-security-risks/#:~:text=How%20to%20Mitigate%20IoT%20Security,something%20both%20unique%20and%20strong.

Symantec. (2024, March 6). *Top Five Requirements for Guest Wi-Fi Access*. Retrieved from Broadcom: https://docs.broadcom.com/doc/top5-guest-wi-fi-access-en

Tigera. (2024, March 13). *Zero Trust Policy*. Retrieved from Tigera: https://www.tigera.io/learn/guides/zero-trust/zero-trust-policy/#:~:text=Key%20Elements%20of%20a%20Zero%20Trust%20Policy,-A%20zero%20trust&text=Access%20is%20denied%20by%20default,have%20access%20to%20any%20systems.

Vashishtha, G. (2023, March 21). *Exploring the Benefits and Challenges of Asymmetric Key Cryptography*. Retrieved from Zeeve: https://www.zeeve.io/blog/exploring-the-benefits-and-challenges-of-asymmetric-key-cryptography/

Verizon Business. (2024, February 22). *Dedicated Internet*. Retrieved from Verizon: https://www.verizon.com/business/products/internet/internet-dedicated/#faqs

What is a Data Center? (2024, February 24). Retrieved from Paloalto Networks: https://www.paloaltonetworks.com/cyberpedia/what-is-a-data-center

Williamson, B. (2024, March 9). *35+ Benefits of an Intranet & Why It Matters for Your Team*. Retrieved from lumapps: https://www.lumapps.com/modern-intranet/intranet-benefits-advantages/

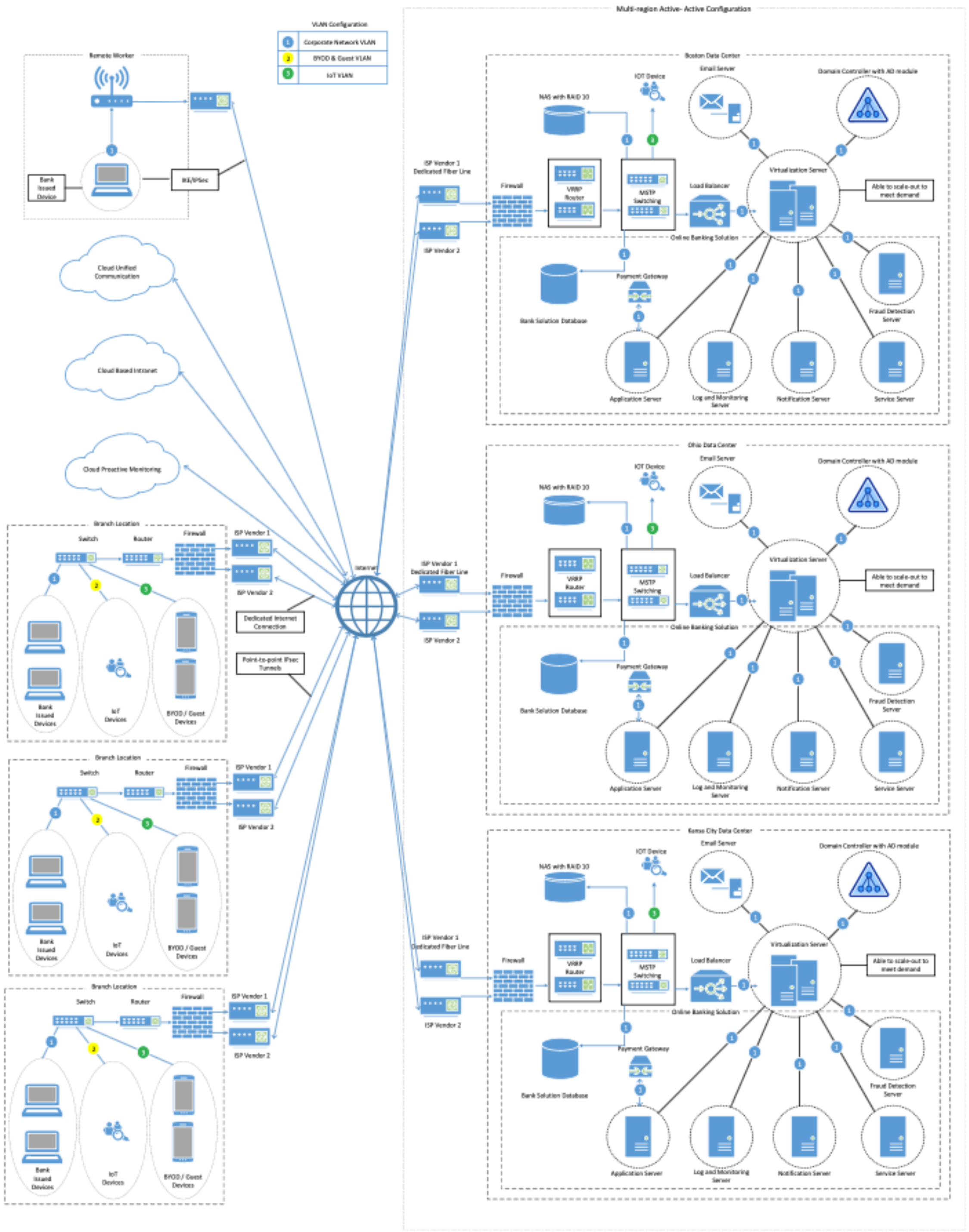
Wright, G., & Scarpati, J. (2024, March 12). *megabits per second (Mbps)*. Retrieved from TechTarget: https://www.techtarget.com/searchnetworking/definition/Mbps

YMD Tech. (2015, August 11). *Scalability Overview*. Retrieved from YMD Tech: http://diranieh.com/DistributedDesign_1/Scalability.htm#Designing%20for%20Scalability

Zenarmor. (2023, October 23). *What is Network Segmentation? Introduction to Network Segmentation*. Retrieved from Zenarmor: https://www.zenarmor.com/docs/network-basics/network-segmentation

Figure 1

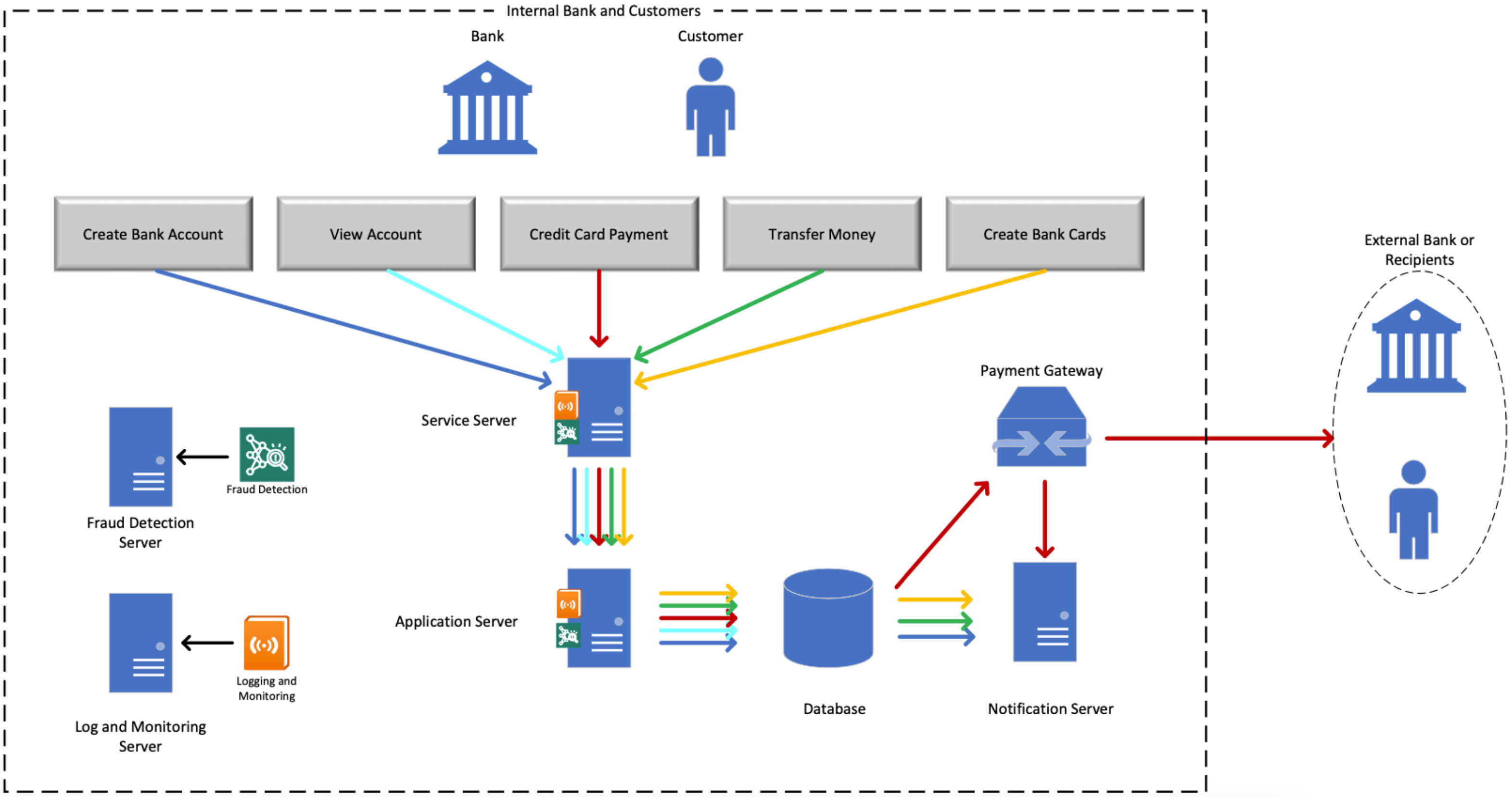
Network Design Architecture Diagram



Note. This depiction presents a network architecture diagram for the acquisition of a community bank.

Figure 2

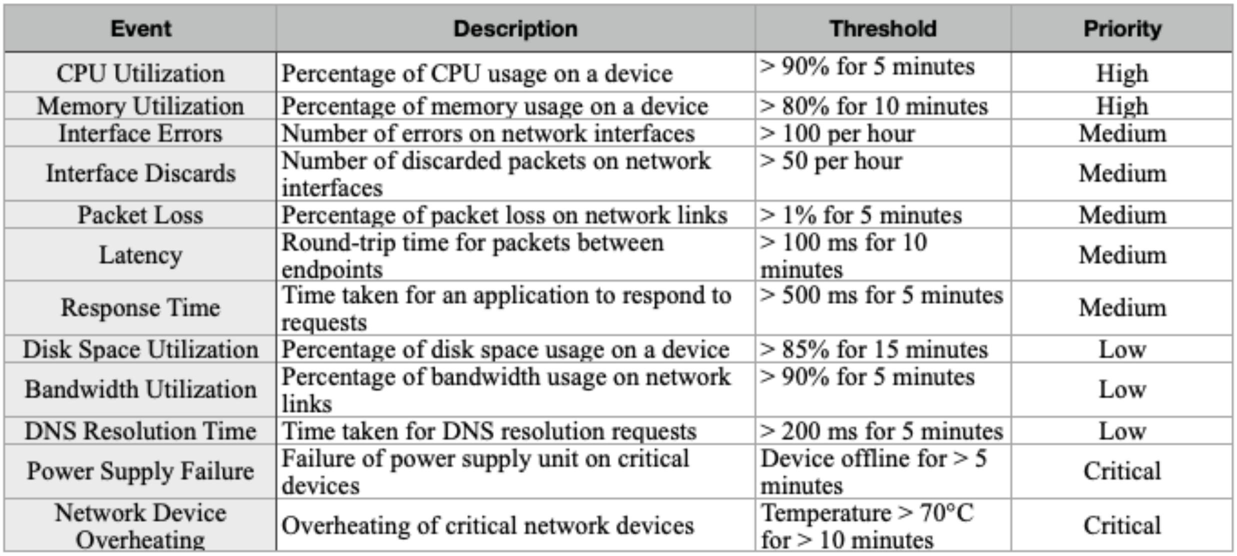
Online Banking Workflow



This workflow diagram illustrates how an internal bank user or customer can utilize the online banking solution with the associated processes for each function.

Figure 3

Event Threshold Table

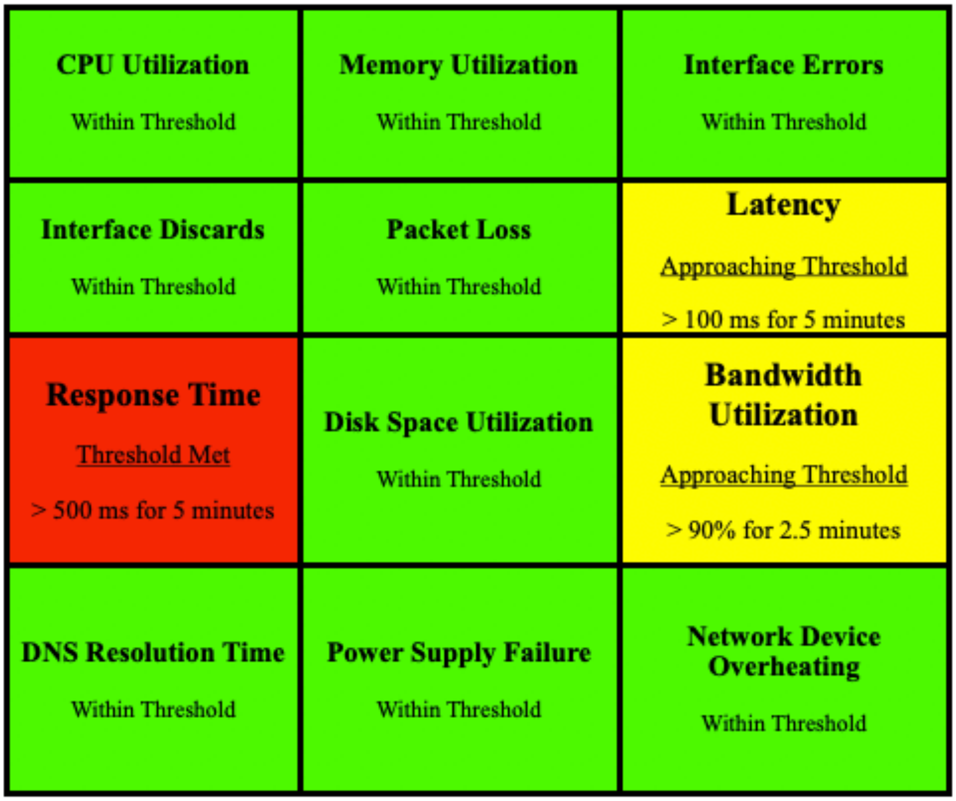


Event	Description	Threshold	Priority
CPU Utilization	Percentage of CPU usage on a device	> 90% for 5 minutes	High
Memory Utilization	Percentage of memory usage on a device	> 80% for 10 minutes	High
Interface Errors	Number of errors on network interfaces	> 100 per hour	Medium
Interface Discards	Number of discarded packets on network interfaces	> 50 per hour	Medium
Packet Loss	Percentage of packet loss on network links	> 1% for 5 minutes	Medium
Latency	Round-trip time for packets between endpoints	> 100 ms for 10 minutes	Medium
Response Time	Time taken for an application to respond to requests	> 500 ms for 5 minutes	Medium
Disk Space Utilization	Percentage of disk space usage on a device	> 85% for 15 minutes	Low
Bandwidth Utilization	Percentage of bandwidth usage on network links	> 90% for 5 minutes	Low
DNS Resolution Time	Time taken for DNS resolution requests	> 200 ms for 5 minutes	Low
Power Supply Failure	Failure of power supply unit on critical devices	Device offline for > 5 minutes	Critical
Network Device Overheating	Overheating of critical network devices	Temperature > 70°C for > 10 minutes	Critical

Note. This table represents the type of event with description, threshold, and associated priority for notification.

Figure 4

Status Dashboard

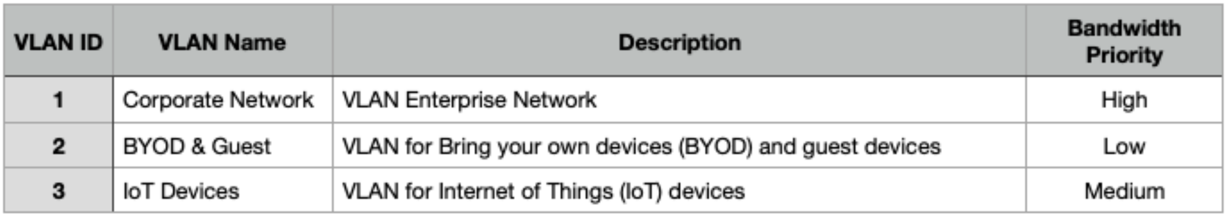


CPU Utilization Within Threshold	**Memory Utilization** Within Threshold	**Interface Errors** Within Threshold
Interface Discards Within Threshold	**Packet Loss** Within Threshold	**Latency** Approaching Threshold > 100 ms for 5 minutes
Response Time Threshold Met > 500 ms for 5 minutes	**Disk Space Utilization** Within Threshold	**Bandwidth Utilization** Approaching Threshold > 90% for 2.5 minutes
DNS Resolution Time Within Threshold	**Power Supply Failure** Within Threshold	**Network Device Overheating** Within Threshold

Note. *This dashboard highlights events and services not within or approaching a threshold.*

Figure 5

Proposed VLAN Configuration



VLAN ID	VLAN Name	Description	Bandwidth Priority
1	Corporate Network	VLAN Enterprise Network	High
2	BYOD & Guest	VLAN for Bring your own devices (BYOD) and guest devices	Low
3	IoT Devices	VLAN for Internet of Things (IoT) devices	Medium

Note. This table demonstrates the VLAN configuration proposal for the corporate network, BYOD and guest devices, and IoT devices.