TECHNICAL ARCHITECTURE

Monstrosity Inc.

Version 1.0 ● April 5, 2020

Project Delivery Methodology (PDM)

**TECHNICAL ARCHITECTURE**

**Group 17**

**Monstrosity Inc. Network**

|  |  |
| --- | --- |
| VERSION: 1.0 | REVISION DATE:4/5/2020 |

Approval of the Technical Architecture indicates an understanding of the purpose and content described in this deliverable. By signing this deliverable, each individual agrees with the content contained in this deliverable.

|  |  |  |  |
| --- | --- | --- | --- |
| **Approver Name** | **Title** | **Signature** | **Date** |
| Ryan Shepherd | Project Manager | Ryan Shepherd | 4/5/2020 |
| Liam Floyd | Architect | Liam Floyd | 4/5/2020 |
| Andrew Taylor | Architect | Andrew Taylor | 4/5/2020 |
|  |  |  |  |
|  |  |  |  |

**Contents**

[**Section 1 DOCUMENT SCOPE 3**](#_heading=h.30j0zll)

[**Section 2 OVERALL TECHNICAL ARCHITECTURE**](#_heading=h.1fob9te) **4**

[2.1 System Architecture Context Diagram](#_heading=h.3znysh7) 4

[2.2 System Architecture Model](#_heading=h.2et92p0) 5

[2.2.1 Overall Architectural Considerations](#_heading=h.tyjcwt) 5

[2.3 System Architecture Component Definitions](#_heading=h.3dy6vkm) 6

[2.3.1 System Architecture Component - Network](#_heading=h.1t3h5sf) 6

[*2.3.2* System Architecture Component - Cloud](#_heading=h.4d34og8) 6

[*2.3.2* System Architecture Component](#_heading=h.4d34og8) - Security 7

[**Section 3 SYSTEM ARCHITECTURE DESIGN**](#_heading=h.2s8eyo1) 7

[3.1 System Architecture Component - Network](#_heading=h.17dp8vu) 7

[3.1.1 Component Functions](#_heading=h.3rdcrjn) 7

[3.1.2 Technical Considerations](#_heading=h.26in1rg) 7

[3.1.3 Selected Product(s)](#_heading=h.lnxbz9) 7

[3.1.4 Selection Rationale](#_heading=h.35nkun2) 8

[3.1.5 Architecture Risks](#_heading=h.1ksv4uv) 8

[3.2 System Architecture Component - Cloud](#_heading=h.44sinio) 8

[3.2.1 Component Functions](#_heading=h.3rdcrjn) 8

[3.2.2 Technical Considerations](#_heading=h.26in1rg) 8

[3.2.3 Selected Product(s)](#_heading=h.lnxbz9) 8

[3.2.4 Selection Rationale](#_heading=h.35nkun2) 8

[3.2.5 Architecture Risks](#_heading=h.1ksv4uv) 9

[3.3 System Architecture Component - Cloud](#_heading=h.44sinio) 9

[3.3.1 Component Functions](#_heading=h.3rdcrjn) 9

[3.3.2 Technical Considerations](#_heading=h.26in1rg) 9

[3.3.3 Selected Product(s)](#_heading=h.lnxbz9) 9

[3.3.4 Selection Rationale](#_heading=h.35nkun2) 9

[3.3.5 Architecture Risks](#_heading=h.1ksv4uv) 9

# Section 1 DOCUMENT SCOPE

This document describes the Technical Architecture of the Monstrosity Inc Network infrastructure that satisfies business requirements as documented in the Business Requirements Document, 3/1/2020, and implements the functionality and satisfies technical, operational and transitional requirements described in the Functional Specification, 2/17/2020.

The goal of this Technical Architecture is to define the technologies, products, and techniques necessary to develop and support the system, and to ensure that the system components are compatible and comply with the enterprise-wide standards and direction defined by the Agency.

This document will also:

Identify and explain the risks inherent in this Technical Architecture;

Define baseline sizing, archiving and performance requirements;

Identify the hardware and software specifications for the Development, Testing, QA and Production environments;

Define procedures for both data and code migration among the environments.

## 1.1 Summary of Design Process

Our architecture design consulting team was contacted by a Monstrosity Inc, a real estate company, to design a technology architecture that will provide their employees and customers internet and wifi access as well as access to email and database functionality to employees. We are taking on the role of design consultants rather than the implementation team building out the infrastructure. We are putting together a written proposal of recommendations that would go to Monstrosity Inc. for approval before an actual build-out plan would be created and implemented. This document defines this design and the hardware that would be needed in its implementation.

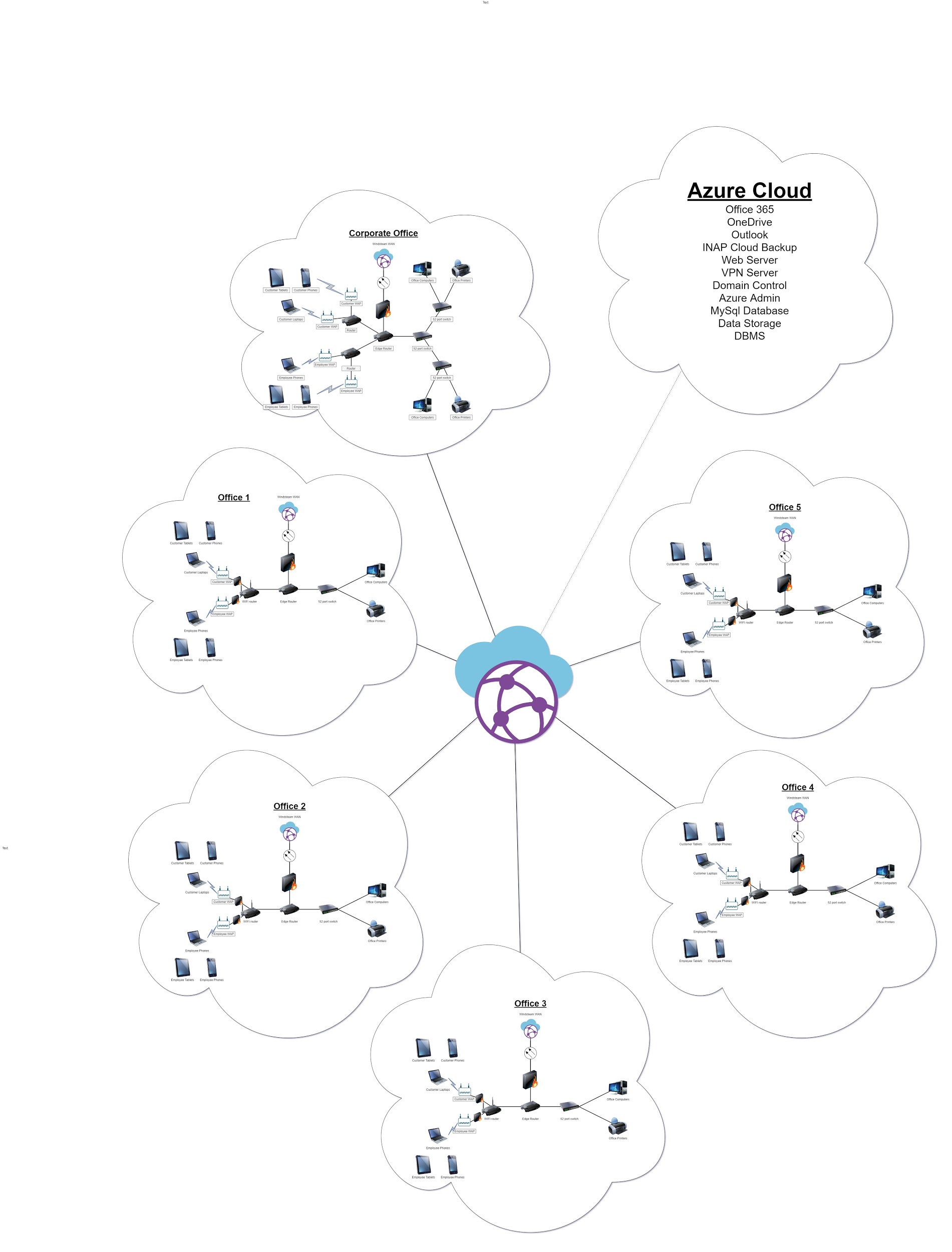
Monstrocity Inc is a real estate company that runs 5 satellite offices and 1 corporate office. Each satellite office will have limited infrastructure needs as most the resources will be hosted on-premise at the corporate office. The project specifies that employees at all sites (and presumably when working out in the field via a VPN connection) will need full access to company resources while customers would be limited to filtered internet access. We had to make some assumptions about the company as well as some imagined constraints that would impact our design. We assume that this client is spread across the same state managing and selling many properties. We are figuring there are approximately 200 employees. As such, we would classify this company as being a small-medium sized business. Based on this information, we are assuming that Monstrosity Inc has a limited budget for their IT infrastructure. Based on the size of the company and their budget, we also believe their needs would require a small scale infrastructure. We also are assuming that due to the size of Monstrosity that their ability to provide ongoing tech support and management of IT operations would be limited.

Given all these details, we have assigned roles to the team who will serve as architects for different components of the project. These components include database design, clustered server implementation, network infrastructure, cloud services implementation, and security services. The design team’s process included researching and designing the individual components of the architecture that would meet the requirements specifications as well as coordination efforts to implement the components within the overall system.

Our initial design called for an on-premise server cluster that would be hosted at the corporate office where satellite offices would connect to these services via WAN protocols. Server clusters offer efficiencies in reliability, performance, redundancy, and efficient distribution of workload. This server cluster would host several VM services that would provide domain control, web and application services, VPN access, and NAS storage. However, due to budgetary constraints, limited staff to support ongoing maintenance/operations, and limits on scaling to accommodate company growth, it would be more efficient to host all needed services via a cloud service provider. In the current design, we are recommending that Monstrosity Inc. host the majority of their services via the cloud service provider. This implementation will allow for ongoing IT management, including data redundancy, expandable data storage, easier remote access implementation, and allow for easier and more efficient scaling.

**Section 2 OVERALL TECHNICAL ARCHITECTURE**

**2.1 System Architecture Context Diagram**



## System Architecture Model

This section represents the various architecture components that comprise the system. The Monstrosity Inc architecture will have the following components:

* Network:
  + Internet connection
  + Wifi access
  + Separated networks for employee and customer access
  + WAN configuration
  + Network components - firewalls, routers, switches, wireless gateways
  + IT service provider to set up and configure the network and provide ongoing network support
  + End-user internet connected devices - laptops, desktops, printers, tablets, phones, etc
* Cloud services:
  + VM’s that provide web/application services, VPN, domain control, and email service
  + Database system and storage
  + Redundancy and data backup
  + Engineers to manage the infrastructure
  + Data center safety measures (power backup, cooling units, protection from fire)
  + Pipe to connect cloud services to Monstrosity Inc infrastructure
  + File storage
  + Security and protection of data
* Required security:
  + Physical protections such as keycard entry to premise
  + Access controls to services requiring login with valid user ID and password
  + Web filtering
  + Antivirus software including spamware, spyware, and ransomware protection
  + Secure and encrypted end-user (employee) devices
  + Use of security protocols (https, TLS, SSL, etc)
  + Physical intrusion detection hardware
  + Separation of employee network/services access and customers access to the internet
  + Secure access to the cloud

### 2.2.1 Overall Architectural Considerations

*This section defines how additional technical requirements have been addressed by the architecture.*

* *Security Strategy*
  + A multi-layered security approach will be taken that includes physical secured access controls (for example, hardware secured behind locked doors), encrypted employee end-user devices, access controls requiring logon with correct user ID and strong password requirements using WPA2-Enterprise, use of industry approved security protocols (HTTPS, SSL, TLS, etc), correctly configured firewalls/routers/switches, different network access points for employees and customers to ensure separation of network access, use of strong antivirus software that includes malware protection, use of physical hardware to protect against unauthorized entry into the system, utilizing security services provided by the Cloud provider, Web filtering, keeping end-user devices updated and patched to reduce vulnerabilities, use of VPN
* *Performance requirements*
  + Fast and reliable internet, reliable access to cloud services, redundancy and data backup systems, correctly configured WAN and pipe to cloud provider, low latency, quick response times from IT management team when issues arise, easy to access services
* *Accessibility*
  + Wifi and ethernet connections with secure login procedures, use of VPN when connecting remotely, access services from a variety of mobile and desktop devices, access via HTTPs web/application portals
* *Database sizing*
  + Database storage size must be flexible and scalable
* *Concurrent user* 
  + Infrastructure and services must be able to accomodate employees and customer traffic between the 5 satellite offices, the corporate office, and any employee working in the field. With 200 employees and customers accessing system resources, it is estimated that the system should be able to handle 250 CCU’s without any degradation in service quality.
* *Data import and export*
  + Employees should be able to safely and securely add, modify, delete, import and export data from system services from a variety of devices and in a variety of locations.
* *Data encryption and decryption*
  + End-user devices should be encrypted, any connections to services and data should utilize encrypted connections, confidential information should be encrypted. Decryption of data should take place at the endpoint and destination of intended use.
* *Disaster recovery*
  + Cloud service provider shall provide disaster recovery with automated data backup, systems redundancy, and fail safes for power failure, fire, and overheating protection.

## 2.3 System Architecture Component Definitions

### System Architecture Component - Network

The network component will provide wifi and ethernet internet access to the 5 satellite offices and 1 corporate office. All 6 offices will be connected to the corporate office via WAN which will serve as the network hub. The network will be able to accommodate a variety of device types (mobile and desktop) being connected securely. The network will offer access to customers and employees while maintaining separation so that customers can not access company resources.

|  |  |
| --- | --- |
| **Architecture Component** | **Component Elements** |
| WAN | Windstream, Edge router |
| WIFI | WAP |
| LAN | 52 port switches, ethernet cables |

### *2.3.2* System Architecture Component - Cloud

Monstrosity Inc. will need access to services such as email, calendars, database, file storage, and front-end access to services via a web browser.

|  |  |
| --- | --- |
| **Architecture Component** | **Component Elements** |
| File and Web Server Backup | INAP Cloud Backup |
| Authentication and Identity | Microsoft Azure  Office 365 |
| Email | Office 365 |
| Administration and Security | Azure Admin |
| Database | DBMS, MySql VM server |
| Database storage | Data storage instance (VM) |
| Front-end access to cloud services via HTTP | Web server instance (VM), Azure access services |
| Remote access | Azure VPN instance |

### *2.3.3* System Architecture Component - Security

The system will need to secure confidential information and maintain security of hardware and prevent tampering or unauthorized access.

|  |  |
| --- | --- |
| **Architecture Component** | **Component Elements** |
| Firewall | Cisco ASA 5525-X |
| Intrusion Detection System | SolarWind Security Event Manager |
| Physical Security | Keypad entry |
| Authorized access | Azure Domain Controller |
| Web filtering | router and firewall configuration |

# Section 3 SYSTEM ARCHITECTURE DESIGN

## 3.1 System Architecture Component - Network

### 3.1.1 Component Functions

The function of the WAN is to connect all of the offices together into one network. It will allow all of the employees to access all of the data they need to despite which office they are located in. All employees will be able to connect to the servers that are located in the corporate office. A WAN will be used because it is a good way to connect several different locations together and it is relatively cheap.

The WIFI will allow customers and employees to securely connect their wireless devices to the network. Customers and employees will have different restrictions and permissions. The WIFI will be utilizing the bandwidth provided by the WAN, however will have to use our own hardware to set it up.

The LAN will allow the desktops and printers to be set up on the same local network. It will all connect back to the WAN however we have to utilize our own hardware to connect the systems that are needed to connect.

### 3.1.2 Technical Considerations

When it came to the WIFI we needed a way to ensure that the employees and customers were not utilizing the same network and that the router could handle all of the traffic. This was achieved through the use of wireless access points, which will separate the two groups and allow for more devices to access the network. When deciding on a network service provider we decided on Windstream due to their lower price and higher speeds.

### 3.1.3 Selected Product(s)

For the wireless access points we decided to go with the Ubiquiti Networks UAP-AC-PRO UniFi Access Point Enterprise Wi-Fi System for $137. This product was chosen due to its low cost, high speed capabilities, decent range and sleek design. I will not look out of place and it serves its purpose well. For the wireless routers we chose the NETGEAR Nighthawk X6 Smart WiFi Router which is $143. We chose this product due to its low cost, long range, and high speed capabilities. For the switches we decided to go with the Cisco Small Business SG350-52 for $580. We chose this product due to the number of ports and cheaper cost. We need a higher number of ports because it makes it cheaper to buy one of these than to buy two 24 port switches. It will also be easier to tell which one went out and will be replaced faster.

### 3.1.4 Selection Rationale

There are many other routers, switches, and wireless access points on the market. There were many others that were considered however these seemed to fit the price and performance that we were looking for.

### 3.1.5 Architecture Risks

Should we purchase a product that does not fulfill the role it is meant for, it could cause a lot of problems for our customers and employees. If the wireless access points do not have a long enough range then not everyone will be able to connect to the network. Should the switches not be able to connect all of the devices it needs to people will be left without desktops or printers. Should the WAN provider not be able to provide a strong reliable connection then many people will be unable to connect to the system at all. The network is the backbone of the company, and the hardware needs to be up to the task.

## 3.2 System Architecture Component - Cloud

### 3.2.1 Component Functions

Azure syncs with the local active directory, sharing security rules and distribution groups to a cloud account for each user. Office 365 integrates into Azure handling email hosting, spam filtering, and applications that are assigned to the users. It also offers extensive admin tools for IT staff to configure settings and manage users, as well as built in security components. Users are assigned Microsoft Office Suite software, which they can in turn easily download and self install. All groups are kept intact from email to the local file server.

The use of INAP’s Cloud Backup provides a granular backup of connected local servers. Allowing Monstrosity to keep automated backups of the file server, web server, and database.

### 3.2.2 Technical Considerations

Azure can operate as its own cloud directory service, and will need to be properly configured to exist in a hybrid with the on-prem user directory and servers. Likewise for the local directory, it will need to be configured for a hybridized environment with email residing on cloud servers rather than a local exchange server. INAP will also have to be setup with the local file server rather than utilizing their own cloud hosting.

### 3.2.3 Selected Product(s)

Microsoft Azure

Microsoft Office 365

INAP Cloud Backup

### 3.2.4 Selection Rationale

The decision to use primarily cloud services was made to alleviate strain on a limited IT staff and transfer downtime risk to the cloud provider. To maintain locally hosted AD with a cloud backup as well as good integration with Windows and the Microsoft Suite of apps, we opted for using Azure to implement a hybrid environment with our local system, and Office 365 to manage user email and applications. We selected INAP cloud backup services to create backups of our local servers for convenience and good integration with local hosted servers. They also provide a granular backup which is helpful for recovering individual files deleted by unsuspecting users.

### 3.2.5 Architecture Risks

The primary risks for cloud hosting come down to internet outage, availability, and pricing. A local power or internet outage would still result in downtime with a severance of cloud connection. Also the availability of services is dependent on Microsoft and INAP respectively. Also pricing is subject to change and could become out of budget on the next contract renewal.

## 3.3 System Architecture Component - Security

### 3.3.1 Component Functions

We selected a Cisco ASA 5525-X as the primary physical firewall in the setup. It will be used to face the brunt of network activity. A second logical firewall is to be setup on the internal network. SolarWind’s Security Event Manager will be hosted and used for intrusion detection as well as a secondary source of network logging to the firewall. The server room will be locked, using a keypad with only IT staff and executives having access.

### 3.3.2 Technical Considerations

The firewall will need to be configured to manage proper inbound and outbound traffic, web traffic, logging, and proper filtering. The event manager will need to be setup on either a physical server or virtual machine server and also configured to give proper alerts and notifications.

### 3.3.3 Selected Product(s)

Cisco ASA 5525-X Firewall

SolarWind Security Event Manager

### 3.3.4 Selection Rationale

Cisco offers high quality machines that are highly configurable and very well documented, with support if needed for Monstrosity IT staff. With a limited IT staff, Cisco offers services in configuration if needed. SolarWind has a very well rounded event manager that gives good insight to the network’s security and activity. Physical security is rather straightforward, restricting access only to team members who can or should have access.

### 3.3.5 Architecture Risks

Time training staff on utilizing administrative functions. There is the risk of downtime or out of date standards that could lead to security breaches. While not strictly under security, the cloud backup of data does offer another point of failure for security concerns. Misconfigured security devices can also lead to breaches and further vulnerabilities.