Acme, Corporation
The Master Plan

Joel Gomez
jgome043@ucr.edu

David Phan
dphan015@ucr.edu

Nick Willhite
nwill016@ucr.edu

June 3, 2017

Contents

1 Overview

1.1 Purpose

This document contains pertinent information for the architecture and implementation of Acme Corporation's network upgrade, including details over topology, services, and high-level configuration descriptions where applicable.

1.2 Services

All existing services must be upgraded to accommodate the network upgrade. The scope of each service upgrade will vary based on the need, but each service will be reimplemented to better fit within the post-upgrade network architecture.

1.2.1 Existing Services

The following existing services will be upgraded (in no particular order):

Service Description	Preferred Package/Application
Network File System (NFS)	nfs-kernel-server, nfs-client
Webserver	apache2
Database	mariadb
Email	???
Active Directory (AD)	openldap
Domain Name Server (DNS)	-$30,000
Dynamic Host Configuration Protocol (DHCP)	dhcpd

1.2.2 New Services

The following new services will be implemented on the network (in no particular order):

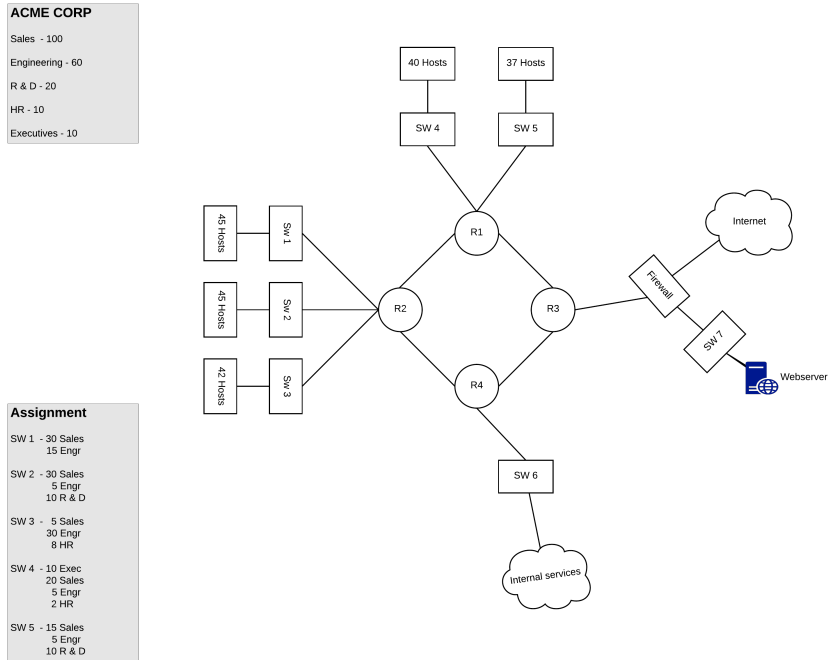| Service Description	Preferred Package/Application
Virtual Local Area Network (VLAN)	vlan
Configuration Management	puppet
Monitoring	nagios
Virtual Private Network (VPN)	openvpn

Figure 1: Subplots from housetrain.data

1.3 Architecture

1.3.1 Architecture Overview

1.3.2 Network Topology

2 Network Access

3 NFS

4 Webserver

5 Email

6 Firewall & Security

Router 1							
From Zone	To Zone	SRC ADDR	DST ADDR	SRC Port	DST Port	App	Deny / Allow
Trusted	Trusted	10.1.110.0/24	Any	Any	Any	Any	Allow
Trusted	Trusted	10.1.150.0/24	Any	Any	Any	Any	Deny
Trusted	Trusted	10.1.130.0/24	10.1.140.0/24	Any	Any	Any	Allow
Trusted	Trusted	10.1.140.0/24	10.1.130.0/24	Any	Any	Any	Allow
Trusted	Trusted	10.1.120.0/24	Any	Any	Any	Any	Allow
Trusted	Trusted	10.1.120.0/24	10.1.110.0/24	Any	Any	Any	Deny

Router 2							
From Zone	To Zone	SRC ADDR	DST ADDR	SRC Port	DST Port	App	Deny / Allow
Trusted	Trusted	10.1.110.0/24	Any	Any	Any	Any	Allow
Trusted	Trusted	10.1.150.0/24	Any	Any	Any	Any	Deny
Trusted	Trusted	10.1.130.0/24	10.1.140.0/24	Any	Any	Any	Allow
Trusted	Trusted	10.1.140.0/24	10.1.130.0/24	Any	Any	Any	Allow
Trusted	Trusted	10.1.120.0/24	Any	Any	Any	Any	Allow
Trusted	Trusted	10.1.120.0/24	10.1.110.0/24	Any	Any	Any	Deny
Trusted	Server	Any	10.1.160.0/24	Any	53, 389, 994	Any	Allow
Server	Trusted	10.1.160.0/24	Any	Any	53, 389, 994	Any	Allow
Trusted	Server	10.1.120.0/24	10.1.160.0/24	Any	3306	Any	Allow
Server	Trusted	10.1.160.0/24	10.1.120.0/24	Any	3306	Any	Allow
Trusted	DMZ	Any	10.1.170.0/24	Any	25, 993, 80, 443	Any	Allow
DMZ	Trusted	10.1.170.0/24	Any	Any	25, 993, 80, 443	Any	Allow
Any	Any	Any	Any	Any	Any	Any	Deny

Router 3							
From Zone	To Zone	SRC ADDR	DST ADDR	SRC Port	DST Port	App	Deny / Allow
Trusted	DMZ	10.1.0.0/24	10.1.170.0/24	Any	25 ,993 , 80, 443	Any	Allow
DMZ	Trusted	10.1.170.0/24	10.1.0.0/24	Any	25, 993, 80, 443	Any	Allow
Server	DMZ	10.1.160.0/24	10.1.170.0/24	Any	3306	Any	Allow
DMZ	Server	10.1.170.0/24	10.1.160.0/24	Any	3306	Any	Allow
Any	Any	Any	Any	Any	Any	Any	Deny

Router 4							
From Zone	To Zone	SRC ADDR	DST ADDR	SRC Port	DST Port	App	Deny / Allow
Server	Server	Any	Any	Any	Any	Any	Allow
Trusted	Server	10.1.0.0/24	Any	Any	53, 389, 994	Any	Allow
Server	Trusted	10.1.160.0/24	10.1.0.0/24	Any	53, 389, 994	Any	Allow
DMZ	Trusted	10.1.170.0/24	10.1.0.0/24	Any	25, 993, 80, 443	Any	Allow
Trusted	Server	10.1.120.0/24	10.1.160.0/24	Any	3306	Any	Allow
Server	Trusted	10.1.160.0/24	10.1.120.0/24	Any	3306	Any	Allow
Server	DMZ	10.1.160.0/24	10.1.170.0/24	Any	3306	Any	Allow
DMZ	Server	10.1.170.0/24	Any	Any	3306	Any	Allow
Any	Any	Any	Any	Any	Any	Any	Deny

Firewall							
From Zone	To Zone	SRC ADDR	DST ADDR	SRC Port	DST Port	App	Deny / Allow
Trusted	DMZ	10.1.0.0/24	10.1.170.0/24	Any	80, 443	Meme.com	Deny
DMZ	Trusted	10.1.170.0/24	10.1.0.0/24	Any	25, 993, 80, 443	Any	Allow
Server	DMZ	10.1.160.0/24	10.1.170.0/24	Any	3306	Any	Allow
DMZ	Server	10.1.170.0/24	10.1.160.0/24	Any	3306	Any	Allow
Any	Any	Any	Any	Any	Any	Any	Deny

7 Active Directory

8 DNS / DHCP

9 Configuration Management