ACME Corporation

The Master Plan

Joel Gomez David Phan Nick Willhite

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 Database

We are going with a MariaDB database for ACME as it widely used, easily maintainable, and secure. In order to set up the MariaDB database we would need to install it both the client and server packages.

- sudo apt-get install mariadb-server

After running the installation of MariaDB we then would need to set up our admin user so we are then able to populate the database with data that ACME CORP needs to be stored.
By running:

- sudo mysql_secure_installation

We are able to do all of the following:

- set root password

- disable remote root login
- remove test database
- remove anonymous users and
- reload privileges

After adding the data that needs to be stored we would then set up the user accounts and privileges for the HR department as they are the only department needing access to the database.

- MariaDB > CREATE USER frankHR@'localhost' IDENTIFIED BY 'password'
- MariaDB > GRANT ALL PRIVILEGES on employees.* to frankHR@'%';
- MariaDB > FLUSH PRIVILEGES;

By the above commands we created a user account from Frank from HR and then have given Frank privileges to access the database 'employees'. Following this same style we would be able to add new tables and users and also give and take away privileges based on needs.

1.2.3 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

1.3 Architecture

1.3.1 Architecture Overview

1.3.2 Network Topology

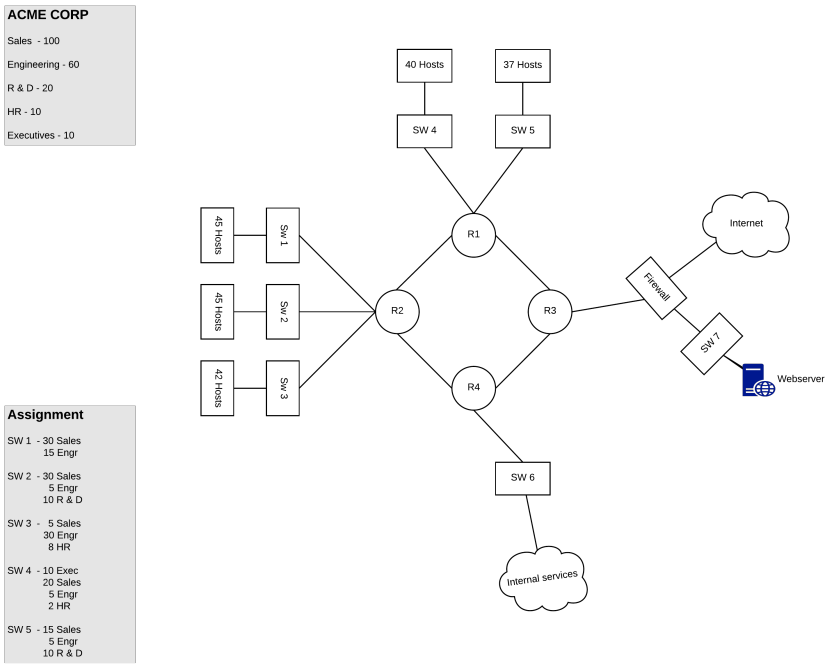

Figure 1: Topology for ACME CORP. Network

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
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

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