F-Secure DNS Integration: Project Plan and System Design Document

Vince Rosas

Southern New Hampshire University

Contents

Project Plan

Work breakdown Structure

1. Gathering Requirements
    1.1. Software requirements
        1.1.1. Operating System choice
        1.1.2. Database software
        1.1.3. Project design software
        1.1.4. Backup and recovery software
    1.2. Hardware requirements
        1.2.1. Design hardware
        1.2.2. Production hardware
        1.2.3. Backup hardware
        1.2.4. Failover hardware
    1.3. Networking requirements
        1.3.1. Secure Connection to OpenDNS
2. Design
    2.1. Design database for storing malicious IP addresses and web addresses
    2.2. Design secure connection to OpenDNS platform
    2.3. Create backup and recovery plan
    2.4. Create failover plan
    2.5. Create database update schedule
3. Implementation
    3.1. Create database of malicious IP addresses and web addresses
    3.2. Create secure connection to OpenDNS platform
    3.3. Implement backup plan
4. Verification
    4.1. Test connection to OpenDNS
    4.2. Test blocking of multiple websites
    4.3. Validate database update plan
    4.4. Validate backup and recovery plan
    4.5. Validate failover
5. Maintenance
    5.1. Scheduled backups
        5.1.1. Local backup
        5.1.2. Off-site backups
    5.2. System updates
    5.3. Database updates
    5.4. Bug Fixes
    5.5. Security Fixes

Timeline with Sample dates and dependencies

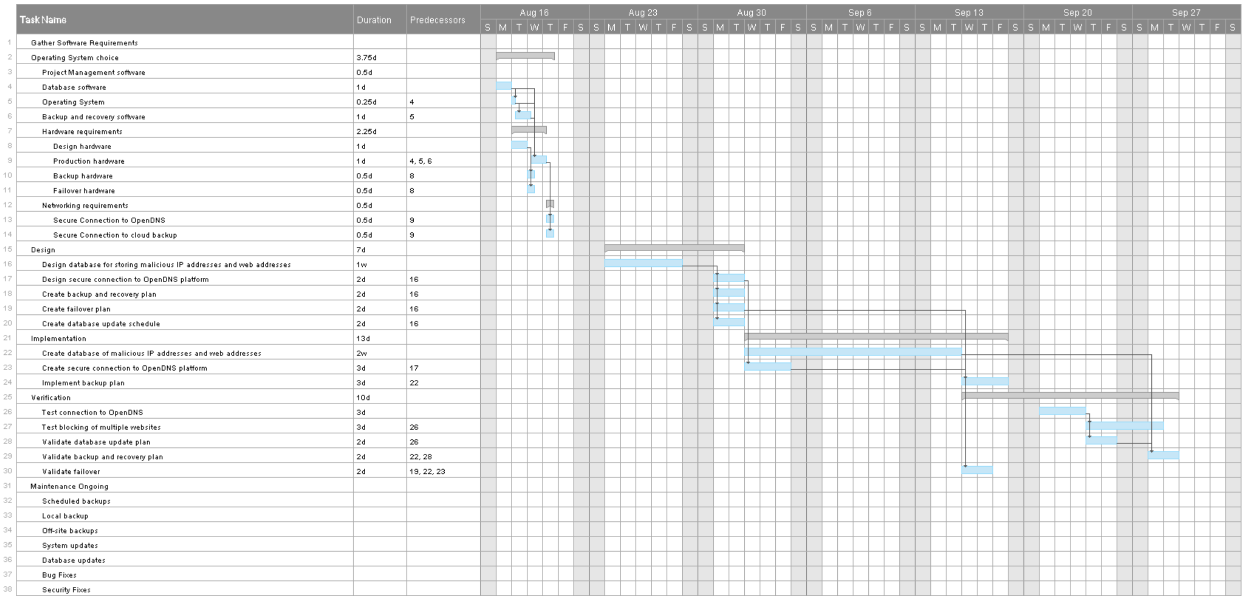
Task	Task Name	Duration	Start	Finish	Dependencies
1	Gather Software Requirements				
2	Operating System choice	3.75d	08/17/20	08/20/20	
3	Project Management software	0.5d			
4	Database software	1d	08/17/20	08/17/20	
5	Operating System	0.25d	08/18/20	08/18/20	4
6	Backup and recovery software	1d	08/18/20	08/19/20	5
7	Hardware requirements	2.25d	08/18/20	08/20/20	
8	Design hardware	1d	08/18/20	08/18/20	
9	Production hardware	1d	08/19/20	08/20/20	4, 5, 6
10	Backup hardware	0.5d	08/19/20	08/19/20	8
11	Failover hardware	0.5d	08/19/20	08/19/20	8
12	Networking requirements	0.5d	08/20/20	08/20/20	
13	Secure Connection to OpenDNS	0.5d	08/20/20	08/20/20	9
14	Secure Connection to cloud backup	0.5d	08/20/20	08/20/20	9
15	Design	7d	08/24/20	09/01/20	
16	Design database for storing malicious IP addresses and web addresses	1w	08/24/20	08/28/20	
17	Design secure connection to OpenDNS platform	2d	08/31/20	09/01/20	16
18	Create backup and recovery plan	2d	08/31/20	09/01/20	16
19	Create failover plan	2d	08/31/20	09/01/20	16
20	Create database update schedule	2d	08/31/20	09/01/20	16
21	Implementation	13d	09/02/20	09/18/20	
22	Create database of malicious IP addresses and web addresses	2w	09/02/20	09/15/20	
23	Create secure connection to OpenDNS platform	3d	09/02/20	09/04/20	17
24	Implement backup plan	3d	09/16/20	09/18/20	22
25	Verification	10d	09/16/20	09/29/20	
26	Test connection to OpenDNS	3d	09/21/20	09/23/20	
27	Test blocking of multiple websites	3d	09/24/20	09/28/20	26
28	Validate database update plan	2d	09/24/20	09/25/20	26
29	Validate backup and recovery plan	2d	09/28/20	09/29/20	22, 28
30	Validate failover	2d	09/16/20	09/17/20	19, 22, 23
31	Maintenance - Ongoing				
32	Scheduled backups				
33	Local backup				
34	Off-site backups				

35 System updates

36 Database updates

37 Bug Fixes

38 Security Fixes



	Task Name	Duration	Predecessors
1	Gather Software Requirements		
2	Operating System choice	3.75d	
3	Project Management software	0.5d	
4	Database software	1d	
5	Operating System	0.25d	4
6	Backup and recovery software	1d	5
7	Hardware requirements	2.25d	
8	Design hardware	1d	
9	Production hardware	1d	4, 5, 6
10	Backup hardware	0.5d	8
11	Failover hardware	0.5d	8
12	Networking requirements	0.5d	
13	Secure Connection to OpenDNS	0.5d	9
14	Secure Connection to cloud backup	0.5d	9
15	Design	7d	
16	Design database for storing malicious IP addresses and web addresses	1w	
17	Design secure connection to OpenDNS platform	2d	16
18	Create backup and recovery plan	2d	16
19	Create failover plan	2d	16
20	Create database update schedule	2d	16
21	Implementation	13d	
22	Create database of malicious IP addresses and web addresses	2w	
23	Create secure connection to OpenDNS platform	3d	17
24	Implement backup plan	3d	22
25	Verification	10d	
26	Test connection to OpenDNS	3d	
27	Test blocking of multiple websites	3d	26
28	Validate database update plan	2d	26
29	Validate backup and recovery plan	2d	22, 28
30	Validate failover	2d	19, 22, 23
31	Maintenance Ongoing		
32	Scheduled backups		
33	Local backup		
34	Off-site backups		
35	System updates		
36	Database updates		
37	Bug Fixes		
38	Security Fixes		

DNS Integration.pdf

Dependencies

Some of the above tasks are required to be completed before the beginning the next task.

- Operating System selection – Before choosing an operating system to run the new system runs on, the database software needs to be chosen first. Choosing the operating system first would limit the choices for the database software
- Backup and recovery software – Not all backup and recovery software can run on every operating system. Once the operating system is chosen then the backup and recovery software can be chosen. Because the operating system is chosen after the database, the database selection is not a requirement of the backup software, it will already have been chosen.
- Production hardware – before choosing the hardware, the software needs to be chosen. Each program, including the operating system, has its own hardware requirements that must be considered before choosing the hardware.
- Backup hardware – Once the production hardware has been decided, the appropriate backup hardware can be decided. This can include full hardware replacements or just replacements of critical parts.
- Failover hardware – Failover can be to cover hardware failure, software crashes, or network connectivity dreams. Because failover is so all-encompassing, this also requires the production hardware to be decided first. This includes production hardware and software as well as networking equipment.
- Secure connection to OpenDNS/Cloud backups – Production hardware must be chosen before the networking requirements. The OS, database software, updates, and backups will each have their own bandwidth requirements that have to be accounted for. Network

throughput will need to be fast enough to possibly handle traffic to or from all the sources simultaneously.

- Design Connection to OpenDNS/backup and recovery plan/failover plan/Database update plan – Each of these plans cannot be created until the database has been designed. Once the database is designed, the disaster recovery, update, and connectivity plans can all be created.

Introduction

The purpose of this project is to add additional functionality to F-Secure's software platform by integrating their database of IP addresses and websites linked to malicious activities with OpenDNS's DNS filtering platform for consumers and businesses. The scope of the project is being limited to integrating F-Secure's database with OpenDNS's platform. Reliability and performance of OpenDNS's platform is not being considered for evaluation.

Requirements

REQ001	The system shall be updated twice a day
REQ002	The system shall be backed up daily
REQ003	The system shall have a disaster recovery plan to ensure system up time
REQ004	The system shall use a secure, encrypted connection to connect to OpenDNS
REQ005	The system shall maintain a 99% up time or better

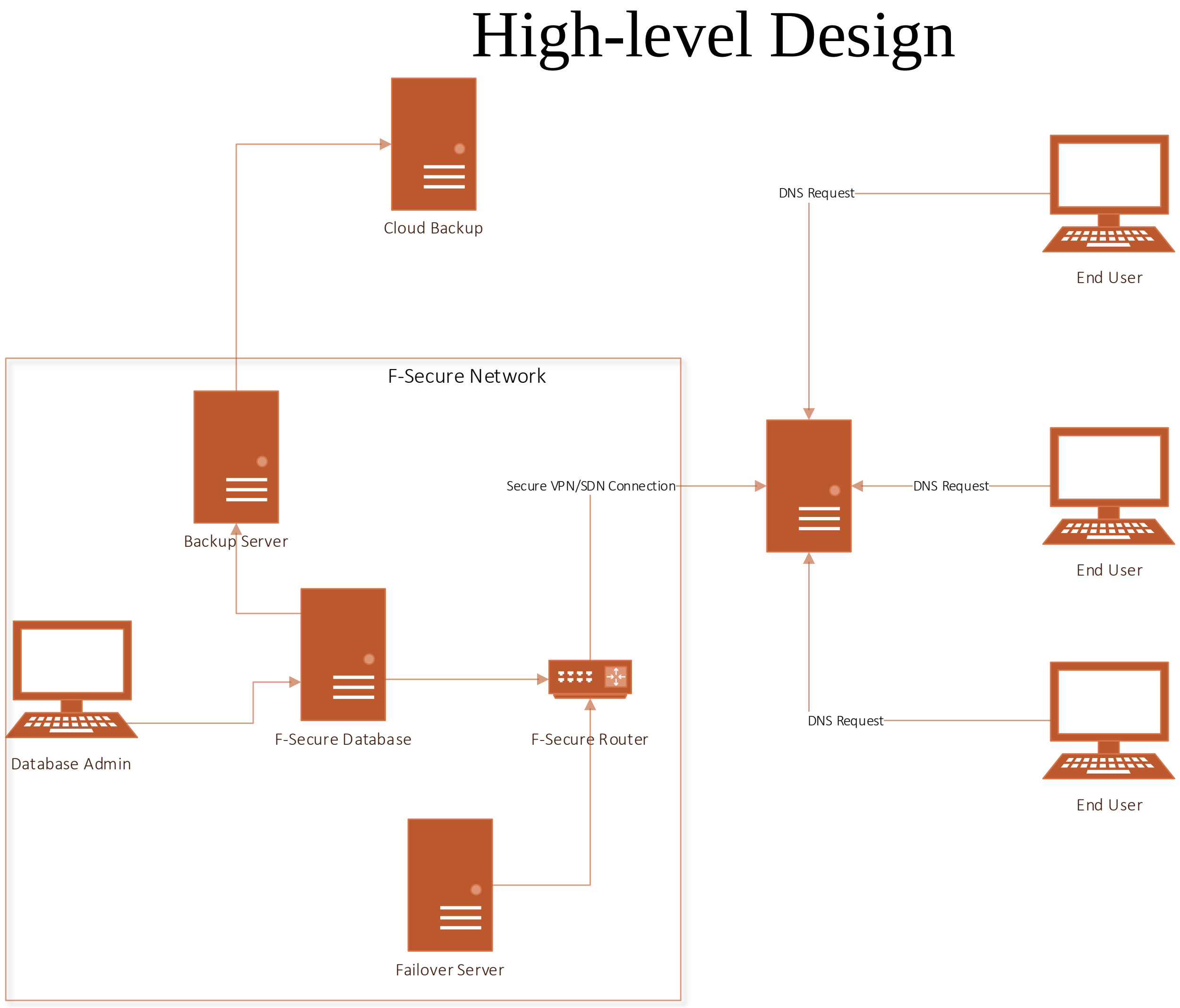
Constraints

The estimated time frame for the initial project rollout is approximately 7 weeks. Because this is a new service being offered by F-Secure, current operations will not be impacted during the development and implementation. Once the project is put into production status, it will need to be maintained with system updates, security fixes, database updates, etc. This will require an ongoing investment from F-Secure to maintain the system. The new feature will require relying on OpenDNS's platform for blocking malicious sites from users. Users will only need to make an account with OpenDNS if they want to take advantage of advanced features such as blocking specific websites. Because the new system will rely on OpenDNS they will be responsible for maintaining the availability of their systems. F-Secure will be responsible for maintaining the availability of the database and updating it.

Resources

Workstations	For developers to program the various software components.
Servers	To run the database
Networking equipment	Required hardware to connect database to network, cloud, and partner resources
Database software	To maintain IP and web addresses of known malicious sites.
Program Management Software	To manage and track the project deliverables.
Operating System software	To run the workstations and servers.

System Overview



Documented Detail Design

I unfortunately ran out of time to complete this section of the document. I'm sure it will be needed in IT-420 but, with the hours I typically put in at work I just did not have the time to work on it. I do have an idea in my head on how this would be implemented, just not on paper yet. I was planning on using newer technology like software defined networking, or SDN, to create secure connections between F-Secure and OpenDNS as well as the cloud backups. I have experience in SDN because we use it at work a lot. It allows us to use private IP addresses for communication between devices on different networks such as F-Secure, OpenDNS, and whatever cloud solution is utilized for off-site backups. This way, there is no need to complicated VPN setups or firewall ports to be opened and expose devices to the internet unnecessarily. I use it at work to allow for clients to access surveillance systems from anywhere without needing to setup port-forwarding on their firewalls either because it is a sensitive network, such as a city government network, or they are behind multiple firewalls, a firewall they don’t have access to, or are unwilling to open any ports. I have been studying an open-source implementation called “Tailscale” and have been using it with my personal devices as well and it has some great features but there are also plenty of commercial implementations to choose from.