Sample Co Software Development Lifecycle

Standard Operating Procedure
Security and Confidential Information

SOP-000001
Revision X
12/8/2016

Sample Co
Confidential and Proprietary, All rights reserved

IMPORTANT NOTE: This document contains confidential information that belongs solely to Sample Co. This document shall not be copied, delivered, transferred, made available, or otherwise disclosed by you to any third party without the advance written consent of Sample Co.

Documentation History

Date	Rev	Author	Comments
8/30/2015	A	Robin Coles	Initial Release
12/8/16	B	Robin Coles	updates

Approvals

Authors:	Approved by:
Name(s):	Name: Date:
	Name: Date:
	Name: Date:
	Name: Date:
	Name: Date:
	Name: Date:
	Name: Date:
	Name: Date:

Table of Contents

Glossary

Term	Description
AV	Anti-virus software
CA	Certificate Authority
DNS	Domain Name Servers
DMZ	Demilitarized zone
Firewall	A network security system that monitors and controls the incoming and outgoing network traffic based on predetermined security rules
FTP	File transfer protocol
FTPS	File transfer protocol over secured server
IP	Internet Protocol, uniquely identifies every computer on the web via an IP address
Lan	Local area network
PHI	Protected Health Information
SSH	The server creates its own public key.
SSL	Secure Socket Layer. This requires a certificate which vouches for the identity of the server.
TCP	Transmission Control Protocol, enables two hosts to establish a connection and exchange streams of data

1. PROCESS SUMMARY

This document provides key information on the security and protection of confidential information as it relates to both Sample Co and it's partners best practices. They are:

1.1 System Evaulation

The primary goal of System Evaluation is as follows:

- Evaluate the quality of a system throughout the software development process
- Verify systems function according to requirement and design specifications
- Verify system meets business and user needs

1.2 Best Practices

The following are recommended best practices:

- Involve team early in a project to review requirements and scope
- Check encryption for:
  - Emails
  - Storage
  - Communication
- Check servers are protected via a firewall
- Get all employees involved in system's with PHI HIPAA certified

1.3 Parent Process

Sample Co SDLC

2. INPUT

2.1 Mail Servers

The email server should be set up to perform only the job of accepting and transmitting mail. This means that the email server should be strict according to the information provided in the System Security section. The email server should be placed in the DMZ, if you have one, and have the latest versions of email and bind software required to fulfill its role.

"Spam" is often sent out using other mail servers without the knowledge of the owners. Sample's mail system should be configured to prevent mail relaying.

Anti-virus software may be incorporated into the mail server to catch and quarantine infected mail before it is allowed inside the network.

The following diagram illustrates placement of the mail server.

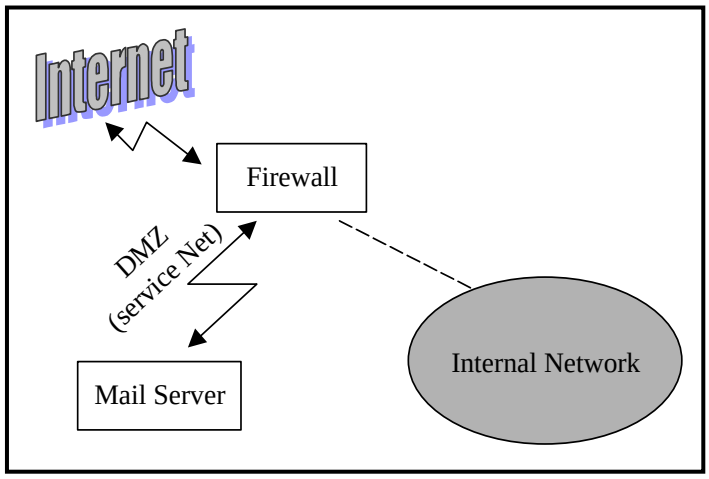

Exhibit 1. Mail Server Placement

The email server should not run other software or be placed into service to perform other functions (such as serving as a Domain Name System (DNS) server). This opens the mail server up to other kinds of attacks.

Sample's employees are not authorized to peruse users email accounts. This is considered a very serious breach of ethics, a violation of privacy rights and is unacceptable behavior. Only under controlled circumstances will such an action be undertaken.

2.2 Physical Security

Physical security of the system relies on adequately controlled access to the systems.

Servers will be set up in an area that has been designated for this purpose. They should be in an environment that will protect them from environmental damage and casual access by personnel. Examples of environmental damage include:

- Fire damage
- Water damage
- Temperature extremes
- Humidity
- Dust, dirt, and smoke.

The location of the emergency shut-off valves for only the computer room should be noted by all personnel.

2.3 Anti-virus

An active anti-virus (AV) defense for Sample's site should set up.

You should install AV software on all systems and maintain the updates on a regularly scheduled basis.

A recommended approach is to install a two-tier architecture for AV support. The first tier (or level) should be network-based and provide protection at the mail server. This allows the AV software installed on the mail server to catch viruses before they can get to a user's workstation. This also provides the System Administrator with control during the times when a new virus is spreading, because it allows "bulk" cleaning of the mail system. The second, workstation-based tier provides protection at the individual workstation level, so AV software should be installed on all the workstations. This provides a redundant AV mechanism and protects the individual system from contamination by files that a user may introduce via diskette or Internet downloads.

2.4 System Configuration

All systems introduced on Sample's network should be made secure before placing them online.

All systems should have the latest patches for their operating system (OS) installed. This is the single, most important action an administrator can take to secure a site. Additionally, hotfixes or updates for operating systems and applications will be installed.

A review of the services offered by each networked computer should be made to determine which protocols and services are active on the system.

While hardening the individual systems, their logbook entries should be updated to indicate the activities performed. Some of the recommended procedures include:

- Install patches and warning banners.
- Disable unnecessary services.
- Modify registry access permissions to allow only System Admins (SA) to access certain entries.
- Set up administrator accounts for individual administrators.
- Update anti-virus software.
- Enable auditing.
- Verify the need for modems; remove them if they are unnecessary.
- Locate systems according to the security required (i.e., behind a firewall or in the DMZ).

2.5 Network Architecture

The system administrator has the responsibility to establish the network in a secure manner. This is done through the use of network architectures suited to protecting information systems and setting up an appropriate infrastructure to guard the network.

The network should be protected by a suitable firewall. It is important to know that a firewall does little to protect certain systems, like the Web server. Make sure the web server is also secured.

If public access is permitted, consider setting up a service network or demilitarized zones (DMZ) where these special servers can be placed.

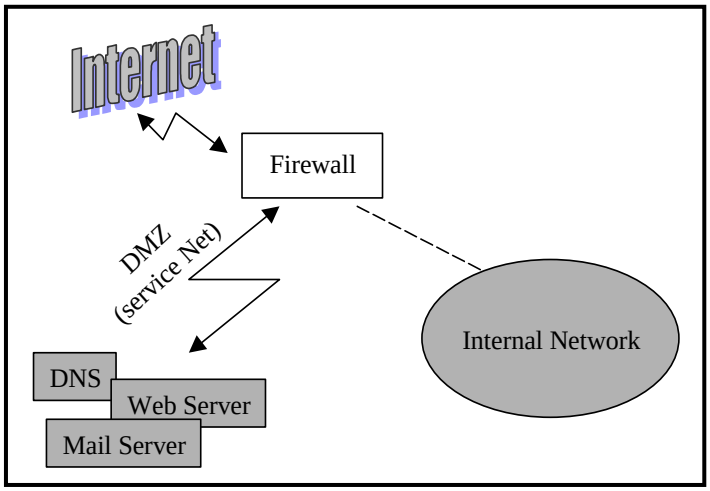

Exhibit 2. Firewall and Web Server Placement

There are many different configurations, and each has its own advantages and disadvantages. There are many different ways to build a DMZ. The use of routers can help form a screen or buffer between the internal and external network. You may consider the setup illustrated on the next page when you do not have a firewall available.

2.6 Port Number and Firewalls

Secure Shell (SSH) uses a single Transaction Control Protocol (TCP) port number - usually port 22 - for all types of connections. By contrast, Secured Sockets Layer (SSL) uses different port numbers for different applications. For instance, port 443 is typically used for Hypertext Transfer Protocol (HTTP) over SSL, and port 990 is used for one version of FTP over SSL. Furthermore, File Transfer Protocol (FTP) requires multiple port numbers during file transfers, as each individual file transfer creates a new connection on a new port.

2.7 Encryption and Certificates

Both SSH and SSL use public key cryptography to exchange a session key, which is then used to encrypt the commands and data transmitted over the network. The security of the algorithms used by SSH is similar to those used by SSL, but SSH does NOT support the concept of a Certificate Authority (CA).

SSL requires a certificate, which is usually purchased from a Certificating Authority like www.thawte.com. A certificate vouches for the identity of the server. SSH uses a different approach, in which each server creates its own public key. There is no trusted authority to vouch for the identity of an SSH server. To make up for this, by convention, each SSH client remembers the public key of each server it has ever connected to. If, on a subsequent connection attempt, the server presents a different

public key, the SSH client will warn the user that the SSH server may be a hostile server masquerading as the original server.

As a result of these differences, FTP over SSL (FTPS) servers can be more cumbersome to administer than SSH/FTP (SFTP) servers. But by virtue of the more sophisticated certificate scheme, FTPS servers are slightly more secure.

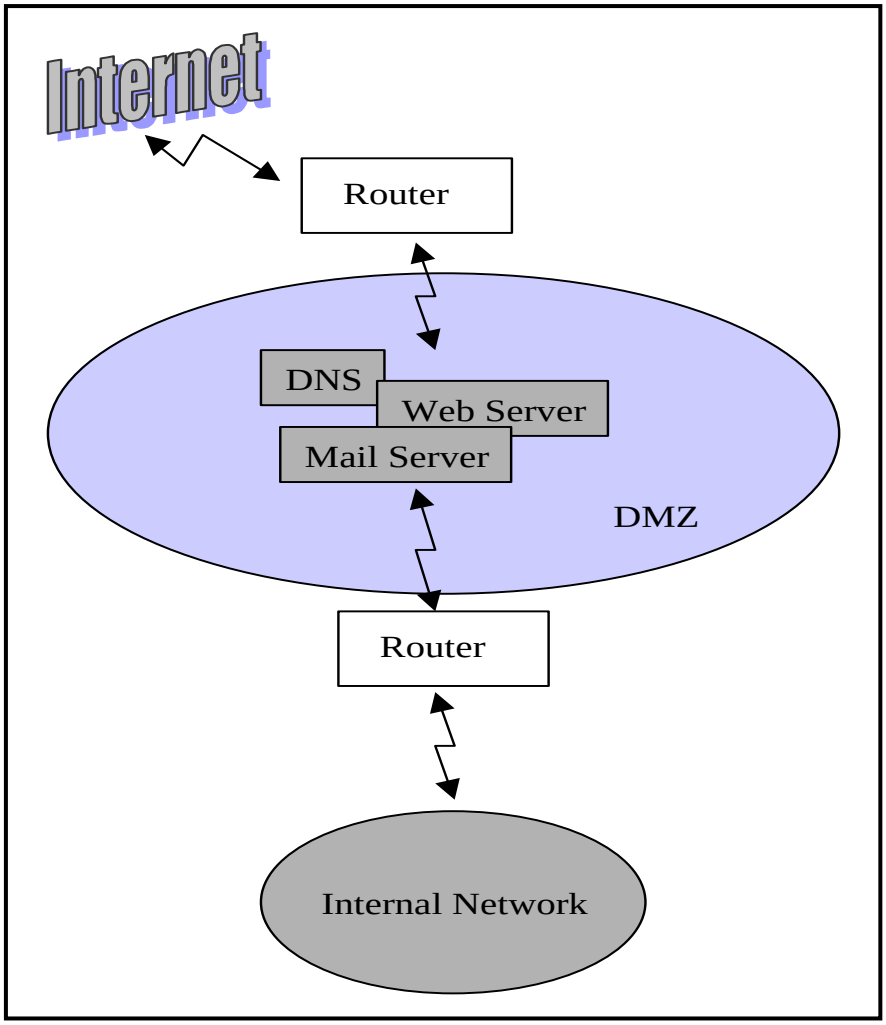

Exhibit 3. Web and Mail Servers Without a Firewall

3. OUTPUTS

4. REFERENCES