

Implementation Plan

NSF, Inc.

Background

NSF, Inc.'s IT department evaluated the current network structure and discovered that due to growth in the organization there is now a lack of proper security and functionality. A new plan has been proposed to implement new technologies to allow for better communication, security, and functionality on the network.

Architectural Implementation

STEP 1 – Physical Topology

Improvements to the physical network will better the security of the domain. All telecommunications closets containing routers, switches, and other connectivity devices will be secured with locks. The servers currently in use and those added in the future will be moved to a centralized location and also secured behind a locked door in an environment suitable for servers and other high-end systems. The server room will provide the proper temperature and positive pressurization to help ensure longer life of the systems.

STEP 2 – Domain

Microsoft's Active Directory will be utilized to create a domain. Active Directory will allow for better user authentication, file security, group policies, and other role based security. The NSF, Inc. domain will have two domain controllers for redundancy purposes.

The domain controllers will be installed on top of the Microsoft Server 2003, Enterprise Edition operating system.

Domain controllers will be secured utilizing the Hardening Domain Controller Checklist.

STEP 3 – DMZ

Due to the growth in the organization, a need to provide easily accessible information to customers and the public via the Internet has arisen. The creation of a DMZ will help to provide secure gateway in which data can be safely transferred between our network and the Internet.

STEP 4 – ISA Server

STEP 5 – Web Server

A web server will host the website that customers, employees, and others can use to access information about the organization, events, and data deemed appropriate or necessary by NSF, Inc.

The web server will be IIS 6.0 installed on top of the Microsoft Server 2003, Enterprise Edition operating system.

The web server will be secured utilizing Hardening Web Servers Implementation Guide and Hardening Web Servers Checklist.

STEP 6 – Exchange

STEP 7 – Site Security Plan

STEP 8 – Certification and Assessment

