SOP: Network Enhancement with pfSense and OpenVPN

Purpose:
This Standard Operating Procedure (SOP) outlines the process for enhancing the network's usability and security using pfSense and OpenVPN.

Scope:
This procedure applies to all employees and authorized personnel involved in the enhancement of network usability, security, and the implementation of pfSense and OpenVPN.
Responsibilities:

- Implementation: IT Administrators and Network Security Team
- Following: All employees and authorized personnel involved in network enhancement
- Reviewing: IT Security Team
- Maintaining and Updating: IT Administrators

Prerequisites:

- Access to the pfSense administration interface.
- Knowledge of OpenVPN configuration settings.
- Valid user credentials for authentication.

Definitions:

- Policy: Broad, overarching guidance explaining "why" certain practices are implemented.
- SOP (Standard Operating Procedure): Specifies "what, when, why" actions; may consist of multiple SOPs supporting a specific policy.
- Work Instructions: Detailed "how-to" guides providing step-by-step directions for a particular task.

Procedure:

1. Network Enhancement with pfSense:

- Overview: Improve network security and usability using pfSense.
- Steps:
    - Log in to the pfSense web interface:
        - Access the pfSense web interface using secure credentials.
    - Review and enhance firewall rules:
        - Identify and configure firewall rules to allow necessary traffic while blocking unauthorized access.
    - Implement VPN policies using OpenVPN:
        - Set up OpenVPN on pfSense to establish a secure Virtual Private Network (VPN).
        - Configure user authentication and encryption settings.
        - Define access policies to control remote user access.
        - Periodically review and update VPN configurations to align with security best practices.

2. Securing Windows 10 Endpoint Workstations:

- Overview: Ensure Windows 10 workstations are secure from data loss and malware threats.
- Steps:
    Implement endpoint protection solutions:
        - Install and configure endpoint protection software on Windows 10 workstations.
        - Enable real-time scanning, firewall protection, and regular updates.
    Enforce security policies for Windows 10 workstations:
        - Define and implement security policies through Group Policy.
        - Restrict user permissions to prevent data loss and malware threats.
        - Regularly update and patch Windows 10 systems to address vulnerabilities.

Expected Results:

- Network Enhancement: The network will have strengthened security through well-defined firewall rules, and remote access will be secured using OpenVPN.
- Endpoint Security: Windows 10 workstations will be protected against data loss and malware threats through endpoint protection solutions and security policy enforcement.

Revision History:

- Version 1.0 (2023.11.13): Initial document creation. Dominique Bruso

References:

- Source 1: So, You Want to Write an SOP?
- Source 2: 37 Best Standard Operating Procedure (SOP) Templates

---