SOP: Network Security Management

Purpose:
This Standard Operating Procedure (SOP) outlines the secure deployment and configuration of Wireless Access Points (WAPs) within a Windows-based environment. Additionally, it includes the use of a server-based firewall to control network traffic and designates Windows Defender as the company-wide antivirus protection tool.

Scope:
This procedure is applicable to IT technicians responsible for deploying and configuring WAPs within the organization.

Responsibilities:

- Implementation: IT Technicians
- Following: All IT technicians involved in WAP deployment
- Reviewing: IT Security Management
- Maintaining and Updating: IT Technicians

Prerequisites:

- Windows Server configured with Active Directory.
- PFsense firewall configured.
- VPN tunnel established between office locations.

Procedure:

1. Physical Deployment:
    a. Physically install WAPs in strategic locations for optimal coverage.
    b. Ensure proper power and network connectivity.
2. Configuration in Windows Server:
    a. Integrate WAPs into Active Directory for centralized management.
    b. Assign appropriate security groups and policies.
    c. Utilize the server-based firewall to control and limit network traffic.
3. Network Segmentation (VLANs):
    a. Implement VLANs to segregate WAP traffic based on departments.
    b. Configure PFsense firewall rules to control inter-VLAN communication.
4. VPN Integration:
    a. Ensure VPN connectivity extends to WAPs for secure remote access.
    b. Configure firewall rules, including the server-based firewall, to permit VPN traffic to WAPs.

Security Measures:

- Enable WPA3 encryption on WAPs.
- Implement strong passphrase policies.
- Regularly update WAP firmware for security patches.
- Designate Windows Defender as the company-wide antivirus protection tool.

Monitoring and Logging:

- Set up logging for WAP activities.
- Monitor for any unusual or unauthorized access.
- Expected Results: Secure deployment and configuration of WAPs in alignment with organizational security policies, with traffic controlled by the server-based firewall and protection provided by Windows Defender.

References:

- Code Fellows Github: https://github.com/codefellows/seattle-ops-301d14/blob/main/class-15/SOP-example-template.md
- Windows AD User Guide: https://learn.microsoft.com/en-us/troubleshoot/windows-server/identity/active-directory-overview
- Windows Defender User Guide: https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/mde-sec-ops-guide?view=o365-worldwide

Definitions:

- Policy: Provides broad, overarching guidance on the "why" of this procedure.
- SOP: Specifies "what, when, why," and there could be multiple SOPs to support a specific policy.
- Work Instructions: Offer in-depth, step-by-step directions for a particular task.

Revision History:

- Version 1.0 (12-18-2023): Initial document creation by Dominique Bruso