Ethan Pham

Standard Operating Procedure (SOP) to monitor network traffic between Windows workstation and Windows server

Objective:
This SOP provides information for monitoring the traffic that travels on the Corporate Home Network for administrators using pfSense.

Scope:
This SOP applies to IT administrators, Network administrators, and Help Desk Staff.

Procedure

Accessing pfSense on the default browser

- On the default browser, go to the pfSense website by entering the router's LAN IPv4 address
- You will initially be met with a warning that the website is insecure
- Disregard this warning and click on advanced settings and proceeding

pfSense dashboard

- The pfSense dashboard there are multiple tabs including system, interfaces, firewall, services, VPN, status, diagnostics, and help
- From the dashboard, focus on diagnostics and status

Monitor traffic through pfSense

- Click on the diagnostics tab, and then select the option "Packet Capture"
- In packet capture options, configure the settings in order to capture the desired packets.
- Click start at the bottom of the page after configuring the capture options
- If new traffic has occurred after a packet capture, click start again in order to capture the new packets

Document the packets

- Provide detailed documentation of the packets for any important or unusual information.

Monitor system logs

- Click on the status tab, and then select the option "System Logs"
- Use this tab to view system configurations such as firewall, DHCP, and Authentication, and view pathways like gateway and routing

Document the logs

- Document any system logs that may be important or unusual.