IDS-IPS

NIST Standards and other best practices.

NIST 800-53r5 – SI-4 – System Monitoring

NIST 800-82r3 – 5.2.3.3. – Network Monitoring

NIST SP 800-94 – Guide to Intrusion Detection and Prevention Systems (IDPS)

The background of this scenario covers the reason for and the differences between IDS and IPS systems. The lab allows the students to configure an IDS/IPS system and discover the differences between the two.