

Lab Report

---

## Your Performance

Your Score: 4 of 4 (100%)

Elapsed Time: 2 minutes 12 seconds

Pass Status: Pass

Required Score: 100%

## Task Summary

### Required Actions

- ✓ Enable IPSHide Details

- ✚ Enable IPS for the LAN
- ✚ Enable IPS for the DMZ

- ✓ Update signature manually with SBIPS000018.bin
- ✓ Set to update signature automaticallyHide Details

- ✚ Automatically Update Signatures selected
- ✚ User Name: mary.r.brown
- ✚ Password: Upd@teN0w

- ✓ Set IPS Policies to Detect and PreventHide Details

- ✚ Set Backdoor to Detect and Prevent
- ✚ Set DOS to Detect and Prevent
- ✚ Set Exploit to Detect and Prevent
- ✚ Set FTP to Detect and Prevent
- ✚ Set LDAP to Detect and Prevent
- ✚ Set Shellcode to Detect and Prevent
- ✚ Set SQL-DB to Detect and Prevent
- ✚ Set TrojanVirus to Detect and Prevent
- ✚ Set WebServer to Detect and Prevent

## Explanation

In this lab, your task is to:

- Enable the IPS on the LAN and DMZ interface.
- Manually update the IPS signature using **C:\signatures\srips000018.bin**
- Use the following credentials to configure the NSA to automatically update the signature in the future:
  - Username: **mary.r.brown**
  - Password: **Upd@teN0w** (0 is a zero)
- Set the IPS policies to detect and prevent all known threats.

Complete this lab as follows:

1. Enable IPS as follows:
  - a. In the Security Appliance Configuration utility, select **IPS**.
  - b. Under IPS Enable, select **Enable IPS Protection for LAN**.
  - c. Select **Enable IPS Protection for DMZ**.
  - d. Select **Apply**.
2. Update the IPS signature as follows:
  - a. Under Manual Signature Updates, select **Browse**.

- b. Browse to and select **C:\Signatures\SBIPS000018.bin**.
  - c. Select **Open**.
  - d. Select **Upload**.
  - e. Refresh the page to update the IPS Signatures status.
  - f. Select **Automatically Update Signatures**.
  - g. In the Cisco.com User Name field, enter **mary.r.brown**.
  - h. In the Password field, enter **Upd@teN0w** (0 is a zero).
  - i. Select **Apply**.
3. Configure IPS policies as follows:
- a. In the left menu, select **IPS Policy**.
  - b. For each IPS Category, select **Detect and Prevent**.
  - c. Select **Apply**.