IPS Initial Setup Using SDM

1. What is the function of SDM's IPS Migration Wizard?

A. Initially set up IPS on the router.
B. Convert signatures in a version 3 or version 4 format to a version 5 format.
C. Convert signatures in a version 4 or version 5 format to a version 6 format.
D. Convert signatures in a version 4 format to a version 5 format.

2. Which of the following is not asked for when running the IPS Rule Wizard?

A. PKG file location
B. Private key of the signature file
C. IPS configuration location in flash
D. Interfaces and direction IPS is enabled

3. What is the name of the public key used to sign the Cisco signature file?

A. real-cisco.pub
B. real-cisco.key
C. cisco-key.pub
D. cisco-pub.key

Answers

1.
   - ☑ **D.** To migrate your IPS version 4 configuration to version 5 in SDM, go to Configure | Intrusion Prevention | IPS Migration and use the Migration Wizard.
   - ☒ **A** refers to the IPS Rule Wizard. **B** is incorrect because version 3 is not supported. **C** is incorrect because the wizard converts from version 4 to 5, not 6.
2.
   - ☑ **B.** The public, not the private key, is required.
   - ☒ **A**, **C**, and **D** are required and therefore incorrect answers.
3.
   - ☑ **A.** The name of the public key used to sign the Cisco signature file is "real-cisco.pub."
   - ☒ **B**, **C**, and **D** are nonexistent names.

General IPS Settings Using SDM

4. If the IPS Engine Fail Closed option is enabled, what does this indicate?

A. IPS is disabled.
B. IPS is enabled.
C. IPS will drop associated traffic if the SME fails to start.
D. IPS will allow associated traffic if the SME fails to start.

5. What is Cisco's recommendation before you enable Auto Update for IPS?

A. Enable NTP.
B. Back up the IPS signature configuration.
C. Disable ZBF.
D. Enable SEAP.

Answers

4.

- ☑ **C.** If the IPS Engine Fail Closed option is enabled, IPS will drop associated traffic if the SME fails to start.
- ☒ **A** and **B** are controlled by the `ip ips` command on an interface. **D** is true if the Engine Fail Closed option is not enabled.

5.

- ☑ **A.** Before enabling Auto Update for IPS, you should synchronize the router's clock using NTP, since auto update periodically polls the AUS server.
- ☒ **B**, **C**, and **D** having nothing to do with the Auto Update function.

Signature Event Action Processing

6. What SEAP component defines the importance of an asset? ?

A. AVR
B. TVR
C. EAF
D. EAO

7. What feature subtracts actions that should be taken, based on the risk rating, when a signature fires? ?

A. EAO
B. EAF
C. TVR
D. IPS Rule Wizard

Answers

6.

- ☑ **B.** The TVR defines the importance of an asset that is attacked.
- ☒ **A** is a nonexistent term. **C** defines actions to subtract based on the risk rating. **D** defines actions to add based on the risk rating.

7.

- ☑ **B.** An event action filter (EAF) subtracts actions that should be taken, based on the risk rating, when a signature fires.
- ☒ **A** adds actions. **C** defines the importance of an asset. **D** initially sets up IPS.

Signature Tuning

8. Which of the following is not an event action supported by IPS on the routers? ?

A. Deny packet inline
B. Reset TCP connection
C. Deny victim inline
D. Produce alert

9. What feature is supported by SDM that will navigate you to Cisco's site to list a description and benign trigger(s) of a signature? ?

A. NDSB
B. CCO
C. REALM
D. NSDB

Answers

8.

- ☑ **C.** Deny attacker, not victim, inline is the correct event action.
- ☒ Answers **A**, **B**, and **D** are supported event actions by IPS.

9.

- ☑ **D.** The Network Security Database (NSDB) is a feature supported by SDM that will navigate you to Cisco's site to list a description and benign trigger(s) of a signature.
- ☒ **A** and **C** are nonexistent terms. **B** is required to access the NSDB on Cisco's site.

IPS Verification

10. Enter the IOS IPS command that only displays the IPS configuration on the router: _________.

Answers

10.

- ☑ **`show ip ips configuration`** command displays only the IPS configuration on the router.