

# McAfee MA0-101

**McAfee Certified Product Specialist – NSP** 

Version: 4.0



#### **QUESTION NO: 1**

Which port needs to be opened for Alert Channel communication between Sensor and Manager through a firewall?

- **A.** 8501
- **B.** 8502
- **C.** 8503
- **D.** 8555

Answer: B Explanation:

#### **QUESTION NO: 2**

Setting a threshold to allow an IPS to react when traffic volume exceeds the set limit is an example of what type of detection method?

- A. Signature based
- B. Pattern matching
- C. Denial of Service
- **D.** Remediation

Answer: C Explanation:

#### **QUESTION NO: 3**

Performance debugging mode can be enabled on a sensor for a specified time duration by issuing which of the following CLI commands?

- A. sensor perf-debug 100
- B. sensor perf-debug on 100
- C. sensor perf-debug Interface all 100
- D. sensor perf-debug assert 100

Answer: A Explanation:



#### **QUESTION NO: 4**

What ty	pe of	encryption	is used	for file	transfers	between t	he Sensor	and the	Manager?
---------	-------	------------	---------	----------	-----------	-----------	-----------	---------	----------

- A. SSL with RC4
- B. SSL with MD5
- C. SSL with RC4 and MD5
- D. DES

Answer: D Explanation:

### **QUESTION NO: 5**

When placed in Layer3 mode, a Sensor detects a Layer2 device based on which of the following?

- A. MAC address
- B. IP address
- C. DNS
- **D.** Subnet

Answer: B Explanation:

## **QUESTION NO: 6**

What is the CLI command that enables the output of the MAC/IP address mapping table to the sensor debug files?

- A. arp spoof status
- B. arp spoof enable
- C. arp dump
- **D.** arp flush

Answer: C Explanation:

**QUESTION NO: 7** 



DoS detection is implemented in which of the following modes? (Choose two)

<ul> <li>A. Learning mode</li> <li>B. Configuration mode</li> <li>C. Threshold mode</li> <li>D. Bidirectional mode</li> <li>E. Inbound mode</li> </ul>
Answer: A,C Explanation:
QUESTION NO: 8
Which port needs to be opened for Packet Log Channel communication between Sensor and Manager through a firewall?
<b>A.</b> 8501 <b>B.</b> 8502 <b>C.</b> 8503 <b>D.</b> 8555
Answer: C
Explanation:
QUESTION NO: 9
Which port is correctly defined for the Alert Channel on the Network Security Manager?
<b>A.</b> 8500 <b>B.</b> 8501 <b>C.</b> 8502 <b>D.</b> 8504
Answer: C Explanation:

https://certkill.com

**QUESTION NO: 10** 



In double VLAN tagging, a second VLAN tag that is inserted into the frame is referred to as which of the following?

- A. Customer Identification tag (CD)
- **B.** VLAN Identification tag (VID)
- **C.** Outer Identification tag (OID)
- **D.** Inner Identification tag (HD)

Answer: A Explanation:

#### **QUESTION NO: 11**

Which of the following information is unique to Host Intrusion Prevention alerts? (Choose three)

- A. Destination IP
- B. User
- C. Source IP
- D. Agent IP
- E. Agent name

Answer: B,D,E Explanation:

#### **QUESTION NO: 12**

Which mode is used when certain hosts are located on the same network as a sensor and other hosts enter through a router or VPN?

- A. Mixed
- **B.** Hybrid
- C. Enforcement
- **D.** Prevention

Answer: A Explanation:

**QUESTION NO: 13** 



Which mode needs to be set to redirect an unmanaged system to the guest portal?

A. Audit

B. Simulation

C. Enforcement  D. Prevention
Answer: C Explanation:
QUESTION NO: 14
Which attack cannot be blocked when the sensor has been set for in-line mode?
<ul> <li>A. TCP Control Anomaly</li> <li>B. ICMP Echo Anomaly</li> <li>C. Too Many Inbound Syn</li> <li>D. SCADA Attacks</li> </ul>
Answer: A Explanation:
QUESTION NO: 15
Which database is supported for Network Security Manager?
A. MSSQL B. Oracle C. MySQL D. Sybase
Answer: C Explanation:
QUESTION NO: 16
Which of the following is the correct extension for a Sensor image imported into the Manager?