

Andree Salvo
Southern New Hampshire University
CYB 310 - 6-2 Project Two Submission: IDS Analysis Paper
Instructor: Raschid Muller

IDS and Security Objectives—Critical Thinking Questions

An IDS component that's best suited to help prevent the loss of confidentiality is signature-based detection. According to Fortinet, "*Signature-based detection uses uniquely identifiable signatures that are in exploit code. When exploits are discovered, their signatures go into an increasingly expanding database.*" (Fortinet, n.d.) Meaning that using a signature-based detection component can monitor known attack patterns, like brute force logins, credential harvesting, and unauthorized data exfiltration signatures. When the IDS detects suspicious outbound traffic or unusual encryption tunnels, it can quickly identify attempts to steal sensitive information, such as customer records or intellectual property. Keeping data confidential means ensuring that sensitive information isn't visible or accessible to anyone who shouldn't have access to it.

Indicators of malware that an IDS could detect. First, **file system changes:** Unexpected changes in files or directories could be a sign of malware. Second, **unusual system behavior:** if a computer system is running abnormally slow, crashes, or a pop-up message appears on your screen, it could be a sign of malware or ransomware. Third, **unexpected system configuration changes:** Unexpected modifications to system settings or configurations can be indicative of malware activity. These alterations might affect system services, firewall configurations, or user account settings. An IDS can detect these suspicious activities through log analysis, signature

matching, and anomaly detection. When malware alters or corrupts files, settings, or processes, it directly threatens the system's integrity by making the data unreliable or untrustworthy to use.

An Intrusion Detection System (IDS) can detect threats to availability by monitoring network traffic patterns of denial-of-service (DoS) or distributed denial-of-service (DDoS) attacks, such as unusually high volumes of traffic targeting a server or repeated unsuccessful connection attempts. Additionally, IDS components can issue alerts when network resources become overloaded, potentially causing downtime. By promptly recognizing these attacks, the Intrusion Detection System (IDS) helps maintain availability by ensuring that legitimate users continue to have access to essential resources.

Configuring an IDS—Scenario Based Questions

Secure Cloud is a **cloud service provider** that offers safe data storage, backup, and collaboration platforms for enterprise clients worldwide. The company has **1,000 employees** operating out of **two office buildings**. The first building houses administrative, finance, and compliance teams who manage sensitive corporate and client records. The second building is dedicated to IT, development, and cybersecurity teams who oversee the company's cloud infrastructure, servers, and customer applications.

The data assets that Secure Cloud Protects are:

- Customer Cloud Storage files and backups
- Virtual machines and application hosting environments
- Client billing, compliance, and support records
- Identity and access management (IAM) credentials and keys
- System and security logs

To provide the best IDS protection for Secure Cloud, I would implement a Network-Based Intrusion Detection System (NIDS) and a Host-Based Intrusion Detection System (HIDS). According to Redscan, ***“A Network Intrusion Detection System (NIDS) continuously monitors on-premise and cloud networks to detect malicious activity such as policy violations, lateral movement, or data exfiltration.”*** (RedScan, n.d) According to Sysdig, ***“A Host-Based Intrusion Detection System (HIDS) monitors IT systems for suspicious activity, detecting unusual behaviors or patterns that may signal a security breach or attack.”*** (Sysdig, n.d)

The NIDS would be installed at pivotal points within the network, such as the perimeter where external traffic enters and the corridor between the two office buildings where sensitive data is exchanged between departments. With both incoming and outgoing traffic, the NIDS can identify threats such as port scans, data exfiltration attempts, distributed denial-of-service (DDoS) attacks, and suspicious connections to command-and-control servers. This configuration ensures that customer cloud storage files, backups, and virtual machines are shielded from external threats that could compromise confidentiality and availability.

The deployment of HIDS would occur on essential servers, particularly those responsible for collecting/storing data, managing client billing systems, and overseeing the company's identity and access management framework. Its role would involve monitoring log files, verifying file integrity, and evaluating system configurations to identify unauthorized modifications, malware, or insider threats. This proactive approach will help ensure that development repositories, IAM credentials, and compliance records remain intact and protected from any malicious activities.

Resources

Fortinet. (n.d.). *Signature-based detection* (FortiGate / FortiOS 7.4.2 NGFW ATP Concept Guide). <https://docs.fortinet.com/document/fortigate/7.4.2/ngfw-atp-concept-guide/756476/signature-based-detection>

Sysdig. (n.d.). *What is HIDS (Host-Based Intrusion Detection System)?*
<https://www.sysdig.com/learn-cloud-native/what-is-hids>

Redscan. (n.d.). *NIDS | Network Intrusion Detection System*.
<https://www.redscan.com/services/nids/>