IDPS TECHNOLOGIES: AN OVERVIEW

Introduction

1. *Intrusion detection* is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents, which are violations or imminent threats of violation of computer security policies, acceptable use policies, or standard security practices. *Intrusion prevention* is the process of performing intrusion detection and attempting to stop detected possible incidents. An intrusion detection system (IDS) is software that automates the intrusion detection process. An intrusion prevention system (IPS) is software that has all the capabilities of an intrusion detection system and can also attempt to stop possible incidents. Intrusion detection and prevention systems (IDPS) are primarily focused on identifying possible incidents, logging information about them, attempting to stop them, and reporting them to security administrators. In addition, organizations use IDPSs for other purposes, such as identifying problems with security policies, documenting existing threats, and deterring individuals from violating security policies. IDPSs have become a necessary addition to the security infrastructure of nearly every organization.

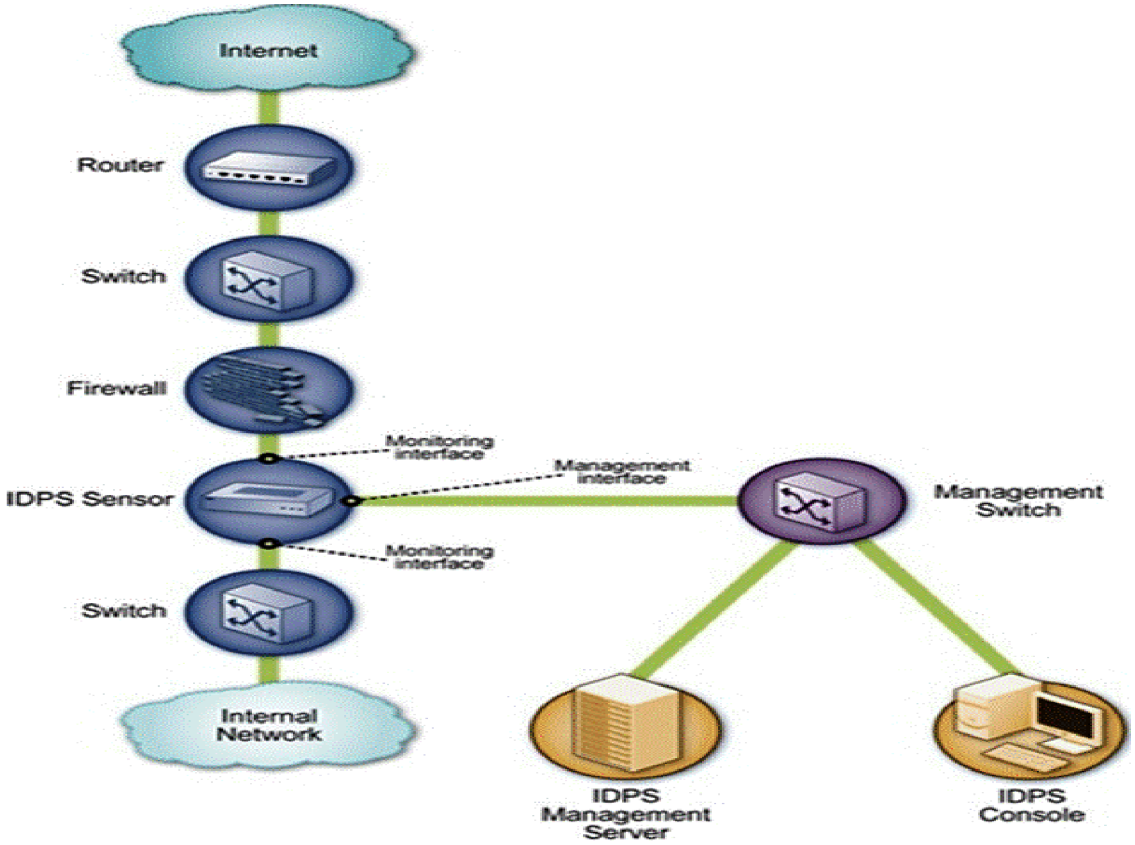
2. **The four types of IDPS technologies are**:

- Network-Based, which monitors network traffic for particular network segments or devices and analyzes the network and application protocol activity to identify suspicious activity.
- Wireless, which monitors wireless network traffic and analyzes it to identify suspicious activity involving the wireless networking protocols themselves.
- Network Behavior Analysis (NBA), which examines network traffic to identify threats that generate unusual traffic flows, such as distributed denial of service (DDoS) attacks, certain forms of malware, and policy violations (e.g., a client system providing network services to other systems).
- Host-Based, which monitors the characteristics of a single host and the events occurring within that host for suspicious activity.

Network Architectures and Sensor Locations

3. Organizations should consider using management networks for their network-based IDPS deployments whenever feasible. In addition to choosing the appropriate network for the components, administrators also need to decide where the IDPS sensors should be located. Sensors can be deployed in one of two modes:

- **Inline**: An inline sensor is deployed so that the network traffic it is monitoring must pass through it, much like the traffic flow associated with a firewall. The primary motivation for deploying IDPS sensors inline is to enable them to stop attacks by blocking network traffic. Inline sensors are typically placed where network firewalls and other network security devices would be placed. Sensors can also be placed on the less secure side of a network division to provide protection for and reduce the load on the dividing device, such as a firewall.



Inline Network-Based IDPS Sensor Architecture

- **Passive**: A passive sensor is deployed so that it monitors a copy of the actual network traffic; no traffic actually passes through the sensor. Passive sensors are typically deployed so that they can monitor key network locations, such as the divisions between networks, and key network segments. Since passive techniques monitor a copy of the traffic, they typically provide no reliable way for a sensor to stop the traffic from reaching its destination. In some cases, a passive sensor can place packets onto a network to attempt to disrupt a connection, but such methods are generally less effective than inline methods.

Key Functions of IDPS Technologies

4. In addition to monitoring and analyzing events to identify undesirable activity, all types of IDPS technologies typically perform the following functions:

- **Recording information related to observed events**: Information is usually recorded locally, and might also be sent to separate systems such as centralized logging servers, security information and event management (SIEM) solutions, and enterprise management systems.

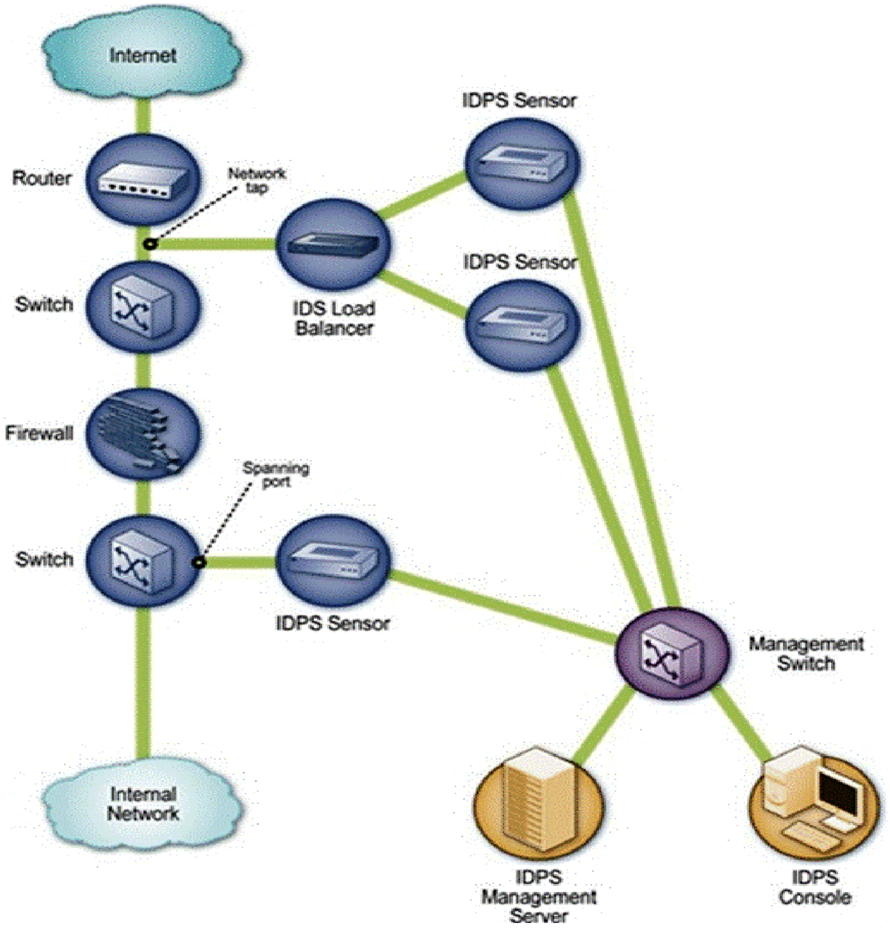
- **Notifying security administrators of important observed events**: This notification, known as an alert, occurs through any of several methods, including the following: e-mails, pages, messages on the IDPS user interface, Simple Network Management Protocol (SNMP) traps, system log messages, and user-defined programs and scripts.

- **Producing reports**: Reports summarize the monitored events or provide details on particular events of interest.

Components and Architecture

5. Major components of the IDPS system are:-

- **<u>Sensor or Agent</u>**: Sensors and agents monitor and analyze activity. The term sensor is typically used for IDPSs that monitor networks, including network-based, wireless, and network behavior analysis technologies. The term agent is typically used for host-based IDPS technologies.



Passive Network-Based IDPS Sensor Architecture

- **<u>Management Server</u>**: A management server is a centralized device that receives information from the sensors or agents and manages them. Some management servers perform analysis on the event information that the sensors or agents provide and can identify events that the individual sensors or agents cannot. Matching event information from multiple sensors or agents, such as finding events triggered by the same IP address, is known as correlation. Management servers are available as both appliance and software-only products. Some small IDPS deployments do not use any management servers, but most IDPS deployments do.

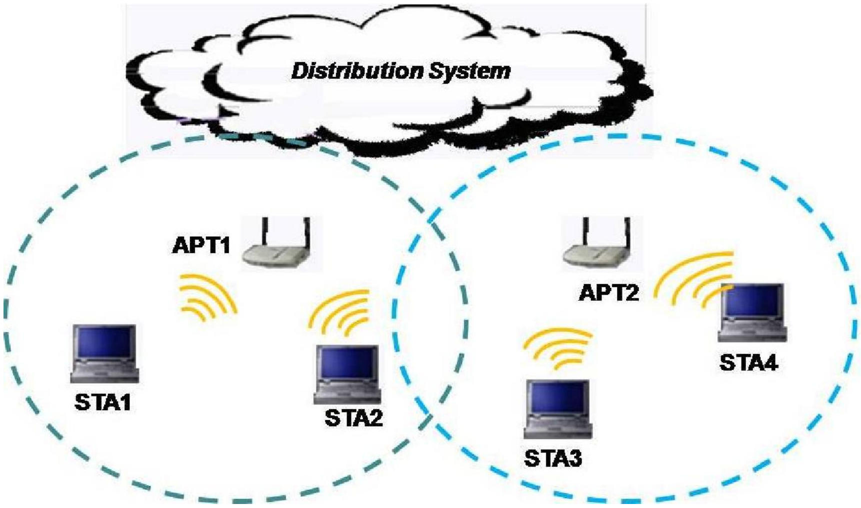
- **<u>Database Server</u>**: A database server is a repository for event information recorded by sensors, agents, and/or management servers. Many IDPSs provide support for database servers.

- **<u>Console</u>**: A console is a program that provides an interface for the IDPS's users and administrators. Console software is typically installed onto standard desktop or laptop computers. Some consoles are used for IDPS administration only, such as configuring sensors or agents and applying software updates, while other consoles are used strictly for monitoring and analysis. Some IDPS consoles provide both administration and monitoring capabilities.

WLAN Components

6. WLANs have two fundamental architectural components:

- **Station (STA)**: A STA is a wireless endpoint device. Typical examples of STAs are laptop computers, personal digital assistants (PDA), mobile phones, and other wireless consumer electronic devices.
- **Access Point (AP)**: An AP logically connects STAs with a distribution system (DS), which is typically an organization's wired infrastructure. The DS is the means by which STAs can communicate with the organization's wired LANs and external networks such as the Internet.

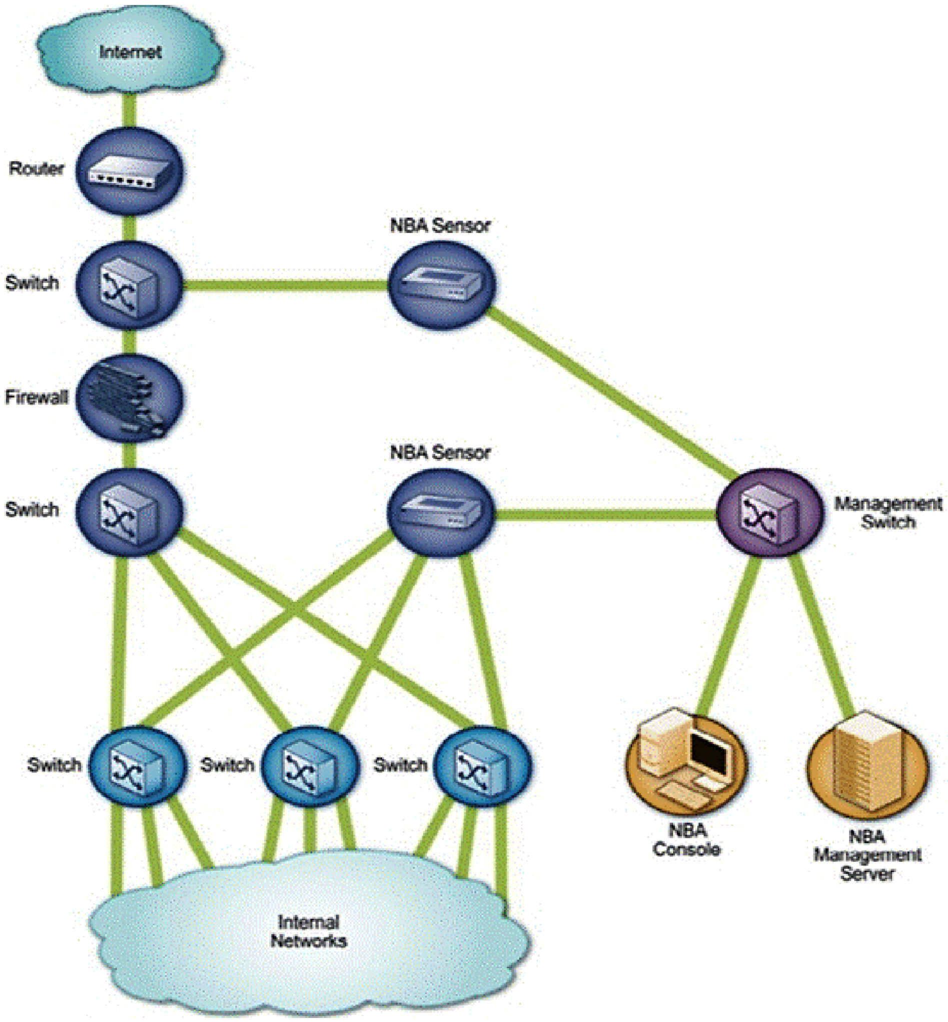


Wireless LAN Architecture

Some WLANs also use wireless switches. A wireless switch is a device that acts as an intermediary between APs and the DS. The purpose of the switch is to assist administrators in managing the WLAN infrastructure. In WLANs without wireless switches, the APs connect directly to the DS. Each AP in a WLAN has a name assigned to it called a service set identifier (SSID). The SSID allows STAs to distinguish one WLAN from another. SSIDs are broadcast in plaintext by APs, so any listening wireless device can easily learn the SSID for each WLAN in its range.

7. A network behavior analysis (NBA) system examines network traffic or statistics on network traffic to identify unusual traffic flows, such as distributed denial of service (DDoS) attacks, certain forms of malware (e.g., worms, backdoors), and policy violations (e.g., a client system providing network services to other systems). NBA solutions usually have sensors and consoles. NBA sensors are usually available only as appliances. Some sensors are similar to network-based IDPS sensors in that they sniff packets to monitor network activity on one or a few network segments. Other NBA sensors do not monitor the networks directly, but instead rely on network flow information provided by routers and other networking devices. Flow refers to a particular communication session occurring between hosts and includes the following:

- Source and destination IP addresses.
- Source and destination TCP or UDP ports or ICMP types and codes.
- Number of packets and number of bytes transmitted in the session.



NBA Sensor Architecture

- Timestamps for the start and end of the session.
- Types of Events Detected.

8. The types of events most commonly detected by NBA sensors include the following:

- **<u>Denial of service (DoS) attacks</u>**: These attacks typically involve significantly increased bandwidth usage or a much larger number of packets or connections to or from a particular host than usual. By monitoring these characteristics, anomaly detection methods can determine if the observed activity is significantly different than the expected activity. Some NBA sensors are aware of the characteristics of common DoS tools and methods, which can help them to recognize the threats more quickly and prioritize them more accurately.

- **<u>Scanning</u>**: Scanning can be detected by a typical flow patterns at the application layer, transport layer and network layer.

- **Worms**: Worms spreading among hosts can be detected in more than one way. Some worms propagate quickly and use large amounts of bandwidth. Worms can also be detected because they can cause hosts to communicate with each other that typically do not, and they can also cause hosts to use ports that they normally do not use.

- **Unexpected application services**: These are usually detected through protocol analysis methods, which can determine if the activity within a connection is consistent with the expected application protocol.

- **Policy violations**: Most NBA sensors allow administrators to specify detailed policies, such as which hosts or groups of hosts a particular system may or may not contact, and what types of activity are permissible only during certain hours or days of the week. Most sensors also detect many possible policy violations automatically, such as detecting new hosts or new services running on hosts, which could be unauthorized.

Integrating Different IDPS Technologies

9. In many environments, a robust IDPS solution cannot be achieved without using multiple types of IDPS technologies. For example, network-based IDPSs cannot monitor wireless protocols, and wireless IDPSs cannot monitor application protocol activity. Many organizations use multiple IDPS products, usually from different vendors. These products function completely independently of each other. However, if the products are not integrated in any way, the effectiveness of the entire IDPS implementation may be somewhat limited. IDPS products can be directly integrated, such as one product feeding alert data to another product, or they can be indirectly integrated, such as all the IDPS products feeding alert data into a security information and event management system.

Network Forensic Analysis Tool (NFAT) Software

10. In addition to dedicated IDPS technologies, organizations also use other types of technologies that offer some IDPS capabilities and complement the primary IDPSs. Network forensic analysis tools (NFAT) focus primarily on collecting and analyzing wired network traffic. Unlike a network-based IDPS, which performs in-depth analysis and stores only the necessary network traffic, an NFAT typically stores most or all of the traffic that it sees, and then performs analysis on that stored traffic. In addition to its forensic capabilities, NFAT software also offers features that facilitate network traffic analysis, such as the following:

- Reconstructing events by replaying network traffic within the tool.
- Visualizing the traffic flows and the relationships among hosts.
- Building profiles of typical activity and identifying significant deviations.
- Searching application content for keywords (e.g., “confidential”, “proprietary”).

Common Detection Methodologies

11. IDPS technologies primarily use signature-based, anomaly-based, and stateful protocol analysis methodologies to detect incidents. Most IDPS technologies use multiple detection methodologies, either separately or integrated, to provide more broad and accurate detection.

- **Signature-Based Detection**: A signature is a pattern that corresponds to a known threat. Signature-based detection is the process of comparing signatures against observed events to identify possible incidents. For examples, a telnet attempt with a username of “root”, which is a violation of an organization’s security policy or an e-mail with a subject of “Free pictures!” and an attachment filename of “freepics.exe”, which are characteristics of a known form of malware. Signature-based detection is the simplest detection method because it just compares the current unit of activity, such as a packet or a log entry, to a list of signatures using string comparison operations.

- **Anomaly-Based Detection** : Anomaly-based detection is the process of comparing definitions of what activity is considered normal against observed events to identify significant deviations. An IDPS using anomaly-based detection has profiles that represent the normal behavior of such things as users, hosts, network connections, or applications. The profiles are developed by monitoring the characteristics of typical activity over a period of time. For example, a profile for a network might show that Web activity comprises an average of 13% of network bandwidth at the Internet border during typical workday hours. The IDPS then uses statistical methods to compare the characteristics of current activity to thresholds related to the profile, such as detecting when Web activity comprises significantly more bandwidth than expected and alerting an administrator of the anomaly. The major benefit of anomaly-based detection methods is that they can be very effective at detecting previously unknown threats.

Implementation

12. Once a network-based IDPS product has been selected, the administrators need to design architecture, perform IDPS component testing, secure the IDPS components, and then deploy them.

- **Architecture Design**: A consideration specific to network-based IDPSs is where the sensors should be placed on the network, which includes deciding how many sensors are needed, which sensors should be inline and which should be passive and how passive sensors should be connected to the network (e.g., IDS load balancer, network tap, switch spanning port).

- **Component Testing and Deployment**: Implementing a network-based IDPS can necessitate brief network outages, particularly when deploying inline sensors. However, passive sensor deployment can also cause outages for several reasons, including installation of network taps and IDS load balancers, and reconfiguration of switches to activate spanning port functions.

- **Securing the IDPS Components**: Administrators should ensure that for both passive and inline sensors, IP addresses are not assigned to the network interfaces used to monitor network traffic, except for network interfaces also used for IDPS management. Operating a sensor without IP addresses assigned to its monitoring interfaces is known as operating in stealth mode. Stealth mode improves the security of the IDPS sensors because it prevents other hosts from initiating connections to them. This conceals the sensors from attackers and thus limits their exposure to attacks. However, attackers may be able to identify the existence of an IDPS sensor and determine which product is in use by analyzing the characteristics of its prevention actions. Such analysis might include monitoring protected networks, and determining which scan patterns trigger particular responses and what values are set in certain packet header fields.

Technology Limitations

13. Although network-based IDPSs offer extensive detection capabilities, they do have some significant limitations. Three of the most important are analyzing encrypted network traffic, handling high traffic loads, and withstanding attacks against the IDPSs themselves. To ensure that sufficient analysis is performed on payloads within encrypted network traffic, organizations should use IDPSs that can analyze the payloads before they are encrypted or after they are decrypted. Examples include placing network-based IDPS sensors to monitor unencrypted traffic and using host-based IDPS software to monitor activity within the source or destination host. Network-based

IDPSs may be unable to perform full analysis under high loads. Passive IDPS sensors might drop some packets, which could cause some incidents to go undetected, especially if stateful protocol analysis methods are in use. For inline IDPS sensors, dropping packets under high loads causes disruptions in network availability; also, delays in processing packets could cause unacceptably high latency. To avoid this, organizations using inline IDPS sensors should select ones that can recognize high load conditions and either passes certain types of network traffic through the sensor without performing full analysis or drop low-priority traffic to reduce load. Many vendors attempt to optimize their sensors to provide better performance under high loads by taking measures such as using specialized hardware (e.g., high-bandwidth network cards) and recompiling components of their software to incorporate settings and other customizations made by administrators. Although vendors typically rate their sensors by maximum bandwidth capability, the actual capacity of any product depends on several factors, including the following:

- The network, transport, and application layer protocols in use, and the depth of analysis performed for each protocol.
- The longevity of connections e.g. a sensor might have less overhead for one long-term connection than several consecutive short-term connections.
- The number of simultaneous connections. Sensors usually are limited as to how many connections for which they can track state.

14. IDPS sensors are susceptible to various types of attacks. Attackers can generate unusually large volumes of traffic, such as distributed denial of service (DDoS) attacks, and anomalous activity to attempt to exhaust a sensor's resources or cause it to crash. Another attack technique, known as blinding, generates network traffic that is likely to trigger many IDPS alerts in a short period of time. The attacker's goal is that the blinding traffic will either cause the IDPS to fail in some way or generate so many alerts that the alerts for the real attack will go unnoticed. Many IDPS sensors can recognize the use of common DDoS and blinding tools and techniques; the sensors can alert administrators to the attack and then ignore the rest of the activity, reducing the load on the sensors. Organizations should select products that offer features that make them resistant to failure due to attack.

Conclusion

15. Before evaluating IDPS products, organizations should first define the general requirements that the Products should meet. The features provided by IDPS products and the methodologies that they use vary considerably, so a product that best meets one organization's requirements might not be suitable for meeting another organization's requirements. Evaluators first need to understand the characteristics of the organization's system and network environments and plans for near-term changes, so that an IDPS can be selected that will be compatible with them and able to monitor the events of interest on the systems and/or networks. This knowledge is also needed to design the IDPS solution. After gaining an understanding of the existing system and network environments, evaluators should articulate the goals and objectives they wish to attain by using an IDPS. Evaluators should also review their existing security and other IT policies before selecting products. The policies serve as a specification for many of the features that the IDPS products need to provide. In addition, evaluators should understand whether or not the organization is subject to oversight or review by another organization. If so, they should determine if that oversight authority requires IDPSs or other specific system security resources. Resource constraints should also be taken into consideration by evaluators.