Homeland Security
Science and Technology

TechNote

U.S. Department of Homeland Security
SAVER
System Assessment and Validation for Emergency Responders

The U.S. Department of Homeland Security (DHS) established the System Assessment and Validation for Emergency Responders (SAVER) Program to assist emergency responders making procurement decisions. Located within the Science and Technology Directorate (S&T) of DHS, the SAVER Program conducts objective assessments and validations on commercially available equipment and systems, and develops knowledge products that provide relevant equipment information to the emergency responder community.

SAVER Program knowledge products provide information on equipment that falls under the categories listed in the DHS Authorized Equipment List (AEL), focusing primarily on two main questions for the emergency responder community: "What equipment is available?" and "How does it perform?" These knowledge products are shared nationally with the responder community, providing a life- and cost-saving asset to DHS, as well as to Federal, state, and local responders.

The SAVER Program is supported by a network of Technical Agents who perform assessment and validation activities. This TechNote was prepared for the SAVER Program by the Space and Naval Warfare Systems Center Atlantic.

SPAWAR Systems Center ATLANTIC

For more information on this and other technologies, contact the SAVER Program by e-mail or visit the SAVER website.

E-mail: saver@hq.dhs.gov
Website: www.firstresponder.gov/SAVER

Network Monitoring Tools

Network monitoring tools are software applications designed to monitor and protect networks from intrusions and malicious traffic as well as monitor the overall network health and performance. Law enforcement agencies use these tools to protect systems and databases, including records management systems, computer-aided dispatch systems, and gang and fugitive intelligence databases, which contain information that must be kept secure and confidential per Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Security Policy and various other legal mandates. Network monitoring tools are also used by fire departments to protect their databases, which often include medical information that must be secured based on the federal Health Insurance Portability and Accountability Act (HIPAA) privacy rules.

Detecting and Preventing Threats

Thousands of data exchanges can occur daily on a typical network rendering it vulnerable to unauthorized intrusion. The first layer of protection is typically provided by a firewall, which blocks malicious Internet Protocol (IP) traffic by analyzing network activity and enforcing policy based on a number of selected criteria (e.g., protocol types, IP addresses, ports). Data that does not match policy is immediately rejected; however, some malicious IP traffic activity is less obvious for the firewall to detect because it is hidden within approved network activities. The longer this type of IP traffic goes undetected, the greater the risk of security breaches, including those that involve financial data, criminal records, or other sensitive information. Therefore, for improved protection against malicious IP traffic on their network, agencies often utilize intrusion detection and prevention systems (IDPS) to protect against threats that may be missed by firewalls (Figure 1).

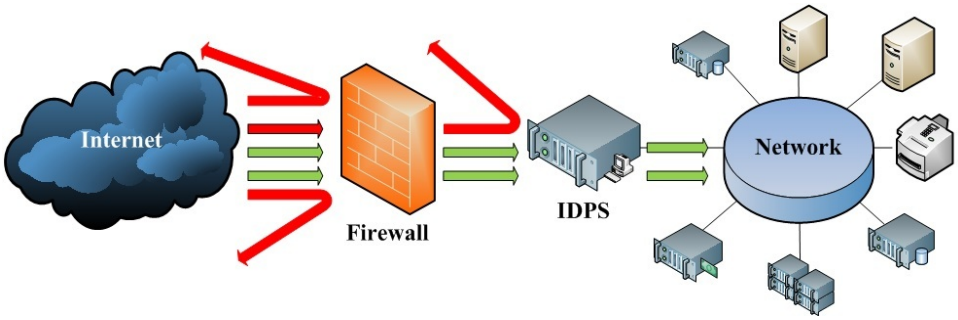

Figure 1. An IDPS protects against malicious IP traffic (red arrows) that may be missed by firewalls.

IDPS encompass both intrusion detection systems (IDS), which use software to automate the detection process, and intrusion prevention systems (IPS), which use software to detect and attempt to deter potential breaches. IDS monitor the IP traffic and passively analyze it for malicious patterns and violations of computer security policies, acceptable use policies, and/or standard security practices. Once a malicious pattern or violation is detected, the IDS alerts the proper system administrators so that appropriate action may be taken. IPS analyze IP traffic actively and block malicious traffic, thus preventing an attack and protecting the network. When intrusions are discovered, IDPS are designed to log all activity related to the breach. Logs are instrumental in the investigative phase of a breach and may include the following information: the username of the host being analyzed, the operating system and service pack information, and a list of installed products to determine if an application can provide a countermeasure to a threat under review.

According to the National Institute of Standards and Technology (NIST), there are four classifications of IDPS technologies:

1) Network-based, which monitors network traffic for particular network segments or devices and analyzes the network and application protocol activity to identify suspicious activity.
2) Wireless, which monitors traffic on wireless networks and analyzes it to identify suspicious activity involving wireless networking protocols.
3) 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).
4) Host-based, which monitors the characteristics of a single host (e.g., client PC, server) and the events occurring within that host for suspicious activity.

The majority of IDPS offer a variety of security capabilities, including information gathering, logging, detection, and prevention. Agencies should consider using more than one type of IDPS, or an integrated product, to address the different classifications of IDPS technologies. For example, an agency's network may have both wired and wireless network components. In this case, the agency may consider employing a wireless IDPS in combination with one of the other classifications depending on the type of protection required and characteristics of the wired network.

Performance and Health Monitoring

IDPS use network resources and, if not properly managed, can cause performance issues. While protection of data is paramount, the network must also be properly monitored and managed. Performance and health monitoring solutions monitor the performance of critical components within a network to identify hindrances that may be affecting network performance. A typical solution can provide health reports related to applications, databases, processor utilization, storage capacities, memory availability, power demands, temperature, and a variety of other important metrics. These metrics are often presented in a real-time dashboard and/or snapshot reports that can be generated on demand by system administrators. Performance and health monitoring systems can alert system administrators of network issues before they reach critical status.

Summary

Network monitoring tools encompass IDS, IPS, and/or IDPS deployed at the host or network level to detect and protect against unauthorized or irregular behavior on the network through software solutions. Network monitoring tools also encompass software solutions to monitor the health and performance of a system. Because no single IDPS technology can prevent all attacks, it is most effective to use a combination of firewalls along with a combination of IDPS classifications to protect against unwanted security attacks.

Additional Information

National Institute of Standards and Technology. *Guide to Intrusion Detection and Prevention Systems (IDPS)* (2007). http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf. Accessed February 2015.

System Assessment and Validation for Emergency Responders (SAVER) Program. *Intrusion Detection and Prevention Systems Application Note* (2011). https://communities.firstresponder.gov/web/saver-community/home/-/document_library/view/486695/31943. Accessed February 2015.