GB

NATIONAL STANDARD OF THE

PEOPLE'S REPUBLIC OF CHINA

ICS 35.040

L 80

GB/T 28454-2020

Replacing GB/T 28454-2012

Information technology - Security techniques - Selection, deployment and operation of intrusion detection and prevention system (IDPS)

信息技术 安全技术 入侵检测和防御系统（IDPS）的选择、部署和操作

(ISO/IEC 27039:2015, MOD)

Issued on: April 28, 2020 **Implemented on: November 01, 2020**

Issued by: State Administration for Market Regulation;

National Standardization Administration.

Table of Contents

Information technology - Security techniques - Selection, deployment and operation of intrusion detection and prevention system (IDPS)

1 Scope

This standard gives guidance for organizations to deploy intrusion detection and prevention systems (IDPS). This standard details the selection, deployment, and operation of IDPS. This standard also provides the background information on which these guidelines are developed.

This standard is applicable to organizations preparing to deploy intrusion detection and prevention systems (IDPS).

2 Normative references

The following documents are essential to the application of this document. For the dated documents, only the versions with the dates indicated are applicable to this document; for the undated documents, only the latest version (including all the amendments) is applicable to this standard.

GB/T 18336 (all parts) Information technology - Security techniques - Evaluation criteria for IT security [ISO/IEC 15408 (all parts)]

GB/T 20275 Information security technology - Technical requirements and testing and evaluation approaches for network-based intrusion detection system

GB/T 20985.1-2017 Information technology - Security techniques - Information security incident management - Part 1: Principles of incident management (ISO/IEC 27035-1:2006, IDT)

GB/T 25068.2 Information technology - Security techniques - Network security - Part 2: Guidelines for the design and implementation of network security (ISO/IEC 18028-2:2006, IDT)

GB/T 28451 Information security technology - Technical requirements and testing and evaluation approaches for network-based intrusion prevention system products

GB/T 29246-2017 Information technology - Security techniques - Information security management systems - Overview and vocabulary (ISO/IEC 27000:2016,

7 Selection

7.1 Introduction

There are many types of IDPS products to choose from, including free products (can be deployed on low-cost hosts) and more expensive commercial paid products (requiring the latest hardware support). Since there are many IDPS products to choose from, it is necessary to comprehensively consider the needs of the organization to select the product that best meets the requirements. In addition, different IDPS products will have compatibility issues. When the same organization uses different IDPS products (due to organizational mergers and wide geographical distribution, it has to use different IDPS products), it also needs to pay attention to the integration issues of different IDPS.

The IDPS manual provided by the supplier gives the types of attacks that IDPS can detect, but it cannot describe how well IDPS can detect intrusions in large-traffic networks, nor can it describe the difficulty of deploying, operating and maintaining IDPS, because in high-traffic networks, it cannot describe the difficulty of deploying, operating, maintaining IDPS. Without understanding the organization's network traffic, it is impossible to accurately describe how IDPS can effectively avoid false negatives and false positives. At the same time, it is also necessary to independently evaluate the active response and passive response capabilities of IDPS according to the organization's own requirements (at this time, the need for deep packet inspection and reassembly is mainly considered, without considering network performance and cost). Therefore, it is not enough to only rely on the IDPS manual provided by the supplier to understand the capabilities of IDPS. IDPS products need to be selected according to the organization's own needs.

GB/T 18336 can be used for third-party evaluation of IDPS. At this time, unlike the IDPS manual, the "security goal" document can describe the performance of the IDPS more accurately and reliably, which will be an important consideration in selecting an IDPS.

During the IDPS selection process, it needs to focus on the relevant factors 7.2 ~ 7.7.

7.2 Information security risk assessment

Before selecting an IDPS, it first needs to conduct an information security risk assessment based on relevant factors (such as the nature of the information used by the information system, how this information needs to be protected, the type of communication systems used, other operational and environmental factors), to identify the attacks and intrusions (threats) to the information systems of organization (which may have vulnerabilities). Then, based on the organization's information security objectives, low-cost controls that can effectively reduce risks are identified for these

potential threats. These controls can serve as the basis for selecting an IDPS.

Note: Information security risk assessment and management is the subject of GB/T 22080.

After the IDPS is installed and operational, the risk management process needs to be continuously implemented based on changes in system operations and changes in the threat environment, to periodically review the effectiveness of controls.

7.3 Host or network IDPS

7.3.1 Overview

The deployment of IDPS needs to be based on the organization's information security risk assessment and asset protection priorities. At the same time, when selecting IDPS, it needs to study the most effective method for IDPS to monitor the situation, that is, choose NIDPS and HIDPS to deploy together: first deploy NIDPS in stages (because NIDPS installation and maintenance are usually easiest), then deploy HIDPS on the key servers.

Each option has its advantages and disadvantages. For example, when IDPS is deployed outside the external firewall, since the external firewall can effectively block a large number of alarm events that need to be scanned, IDPS does not need to conduct in-depth analysis of most alarm events.

Where there are security level requirements for IDPS products, follow GB/T 20275 and GB/T 28451.

7.3.2 Network-based IDPS (NIDPS)

When deploying NIDPS, place sensors mainly in the following locations:

- Inside the external firewall;

- Outside the external firewall;

- On major backbone networks;

- Critical subnets.

7.3.3 Host-based IDPS (HIDPS)

When selecting HIDPS, the target host needs to be identified. At the same time, because its deployment cost is high, HIDPS needs to be deployed on key hosts, based on the target host risk analysis results and cost-effectiveness (prioritizing the hosts). When the number of hosts deployed in HIDPS is large, it needs to consider deploying IDPS with centralized management and reporting functions.

terms of confidentiality, integrity, availability, non-repudiation (the above four are standard security goals), privacy, liability protection, ease of management, etc.

When IDPS detects a security policy violation, the response strategy of IDPS needs to be determined. When responding to information security policy violations, IDPS needs to be configured and operators are required to understand the response strategy in order to correctly handle IDPS alarms. For example, law enforcement agencies can be requested to conduct an investigation to help resolve a security incident; relevant information (including IDPS logs) can be turned over to law enforcement agencies for evidence.

Additional information related to security incident management can be found in GB/T 20985.1-2017.

7.4.4 Performance

When choosing an IDPS, it also needs to consider performance factors, which at least include:

- The size of bandwidth that IDPS needs to handle;

- The maximum range of false alarm rates for a given bandwidth;

- Can it provides valid reasons for choosing a high-speed IDPS, or can a medium-speed or low-speed IDPS meet the needs;

- The consequences of missing potential intrusions due to IDPS performance limitations;

- Impact on IDPS performance when deep packet inspection and reassembly occur.

Organizations need to avoid the following two types of IDPS: In most environments, IDPS will miss a part of the traffic packets that may be attacks. At some point, as bandwidth and/or network traffic increase, IDPS can no longer effectively and continuously detect the intrusions (sustainability is primarily the ability to continuously detect attacks within a given available bandwidth).

Combining load balancing and tuning optimization can improve IDPS efficiency and performance. For example:

- Relevant knowledge of the organization's network and its vulnerabilities is required: Through the information security risk assessment process, it is clear which network assets need to be protected (every network is different) and which attack signatures are related to the adjustment and optimization of these assets.

- IDPS performs better when it is used to handle a limited number of network traffic and services. For example, an enterprise engaged in e-commerce needs to monitor

all HTTP traffic and need to tune and optimize the IDPS, to look for attack signatures related only to web traffic.

- Proper load balancing configuration can make signature-based IDPS run faster and more thoroughly, because signature-based IDPS does not need to traverse all attack signature databases, but only needs to traverse an optimized smaller attack signature database.

In the deployment of IDPS, load balancing can be used to divide the available bandwidth, but this measure will cause problems such as additional costs, management overhead, traffic synchronization failure, repeated alarms, false negatives. Under the current technical conditions, the cost-benefit rate of IDPS and load balancing may be the lowest.

7.4.5 Verification of capabilities

Relying solely on vendor-provided information about IDPS capabilities is often not sufficient. Therefore, when choosing an IDPS, it can ask the supplier to provide additional instructions or provide a demonstration of the applicability of the IDPS, that is suitable for the organization's specific environment and security objectives. Specifically, IDPS suppliers can be required [most IDPS suppliers have experience in adapting their IDPS products (for target network expansion), some suppliers can support new protocol standards in the threat environment, and have accumulated experience in platform types and changes, etc.] to provide the following information to verify IDPS capabilities:

- What assumptions shall be made about the applicability of IDPS in a specific environment;

- Details of tests performed to verify IDPS capabilities;

- What assumptions shall be made about IDPS operators;

- Provided IDPS interface (for example, physical interface, communication protocol, report format for interaction with the correlation engine, etc.);

- Alarm output mechanisms or formats, and whether they are well documented [e.g., format, management information base (MIB) for syslog messages or Simple Network Management Protocol (SNMP) messages];

- Whether the IDPS interface can be configured with shortcut keys, customizable alarm functions, customized attack signatures;

- When dynamically configuring IDPS, whether the features that can be provided are well documented;

- Whether the product can adapt to the development and changes of information

- If it needs to customize attack signatures, whether there are enough available technologies;

- In order to immediately respond to high-risk vulnerabilities or persistent attacks, whether custom attack signatures can be written or received.

7.4.7.3 Validity of internal distribution and implementation of updates

After the attack signature is updated, specific updates need to be quickly distributed and implemented to all relevant systems. At this time, the updated information of attack signatures needs to be modified in time, to include the IP address, port, etc. of the specific site. Therefore, when choosing IDPS, it needs to pay attention to the following aspects at the network trust boundary:

- When manually distributed, can administrators or users implement attack signature updates within an acceptable time frame;

- Can the effectiveness of automated distribution and installation processes be measured;

- Whether there is a mechanism to effectively track attack signature updates.

7.4.7.4 System impact

In order to minimize the impact of attack signature updates on system performance, it needs to pay attention to the following aspects when selecting an IDPS:

- Whether the update of attack signatures affects the performance of important services or applications;

- Can it selectively pay attention to the update of attack signatures, to avoid conflicts that affect the performance of services or applications.

7.4.8 Alarm strategy

The configuration and operation of IDPS are mainly based on set monitoring policies. When choosing an IDPS, in terms of alarm strategy, it needs to consider alarm methods that are compatible with existing information infrastructure, such as email, web pages, short message systems (SMS), SNMP events, automatic blocking of attack sources.

When IDPS data is used for evidence collection (including internal evidence), IDPS data needs to be processed, managed, applied or submitted in accordance with the requirements of laws and regulations.

7.4.9 Identity management

7.4.9.1 General

When choosing IDPS, it also needs to consider IDPS identity management (used to protect the security and controllability of IDPS data and identity exchange). The key is that IDPS remote certification and provisioning require the use of a trusted third party as an authority (similar to authority in public key infrastructure). In addition, IDPS identity management is also important for seamless, secure, controllable IDPS data and IDPS identity exchange at the trust boundary of the enterprise network.

7.4.9.2 Remote attestation

IDPS contains millions of lines of code, which may be inserted by attackers into malware to control the output of IDPS. To address this problem, the access control of IDPS software and hardware can be strictly authenticated based on the identity of the visitor, who initiates the access request through remote attestation (without anyone issuing instructions).

In IDPS hardware, remote attestation mainly verifies the identity of the hardware device or the identity of the software running on the device, by generating encryption certificates or hash values. Among them, the hash value (the simplest form of identity) can distinguish different software and devices and detect software changes. The encryption certificate can be provided to the remote party requested by the IDPS user; it can also be used to verify the remote party (that is, the IDPS is using the expected and unmodified software). When the IDPS software is modified, the IDPS encoding in the generated encryption certificate will also change.

The purpose of remote attestation is to detect unauthorized changes to IDPS software (for example, if an attacker has replaced or modified an IDPS application or part of the operating system, remote services or other software will not be able to recognize them). Therefore, when the remote party (such as the Network Operation Center NOC) detects the IDPS software that is damaged by a virus or Trojan horse, it must take corresponding measures and remotely notify other IDPS associated with this IDPS (this IDPS has been compromised), meanwhile prevent it from sending relevant information before this IDPS resumes functionality.

Therefore, IDPS needs to use remote certification to achieve the following functions:

- Prove or report its status, configuration or other important information to the remote party;

- Evaluate the robustness of IDPS and its ability to perform a large number of IDPS configuration and update operations;

- Remotely test IDPS integrity;

- Summarize IDPS attestation reports to provide a situational assessment of network defense status, as an important component of the overall network situational assessment.

Honeypot is the technical term for a decoy system used to deceive, distract, divert, lure attackers to spend time on information that appears to be valuable, but is actually fabricated and of no value to legitimate users. The main purpose of a honeypot is to collect information that is threatening to an organization and lure intruders away from critical systems.

A honeypot is not an operating system, but an information system that can lure an attacker to stay online for enough time to assess the attacker's intentions, skill level, operating methods.

Analyzing the activities of intruders in honeypots can allow organizations to better understand the threats to the system and its vulnerabilities, thereby improving the operation of the IDPS and helping advancing the organization's development on IDPS strategy, attack signature database, overall approach (this method is the best practices for IDPS to avoid known attack threats).

Before using a honeypot, seek the guidance of legal counsel. Given that honeypots are a decoy technique, the legitimacy of the honeypot and its data needs to be determined.

When choosing a honeypot, it needs to consider its advantages and disadvantages.

Advantage:

- Move attackers to target systems where they cannot compromise;
- The honeypot does not manage authorized activity, so all activity captured by the honeypot is suspicious;
- Administrators have more time to decide how to deal with attackers;
- It is easier and more extensive to monitor attacker activities; the monitoring results can be used to optimize threat models and improve the ability to protect the system;
- Can effectively catch insiders snooping on the network.

Disadvantages:

- The legality of using this device is uncertain;
- Once entering the decoy system, the attacker may launch more destructive attacks;
- In order to use these systems, administrators and security managers need to have more professional knowledge.

7.5.5 Network management tools

Network management tools use detection technology to monitor the availability and performance of network devices; configure and manage network infrastructure by

collecting network component and topology information.

Network management tools are primarily associated with IDPS alarms, helping IDPS operators to handle alarms appropriately and evaluate their impact on the monitored system.

7.5.6 Security information event management (SIEM) tools

SIEM tools are mainly used to integrate information from IDPS, firewalls, sniffers, etc. (collect relevant information and reduce overload information), meanwhile send the integrated information to the management platform and alarm control platform, so that analysts can manage and utilize these tons of information. At the same time, the data collected by SIEM through correlation analysis (correlating countless small individual packets and multiple data sources under radar control for long periods of time) can greatly reduce the number of false negatives.

SIEM tools can also be used to process data obtained from IDPS. Its main functions include:

- Collect and maintain incident data from different security-related data sources, which may include data from one or more IDPS, log files from network devices and hosts, event data from anti-virus tools;

- Further process the collected data, in particular to provide further event correlation, event filtering, event aggregation;

- Event correlation: Detect non-pattern-related security vulnerabilities by establishing scenarios of security and non-security-related events;

- Event filtering: Reduce alarm levels through correlation-based correlation (e.g., IDPS alarms and security patch levels);

- Event aggregation: Reduce IDPS alarm overflow by collecting and normalizing events based on source, destination, timestamp, event description, etc.;

- Provides a simple and easy-to-use interface for reporting related alarms; provides assistance for in-depth analysis of alarms based on collected data.

The primary goal of SIEM is to automatically differentiate between high-threat alerts and false positives that are irrelevant or pose no threat. When planning to introduce a SIEM tool, it needs to be an important task to configure the SIEM correctly. When SIEM is used in conjunction with IDPS, it can provide more valuable information, thereby triggering further processes and activities such as incident management; however, SIEM configuration requires a high level of expertise and a lot of work.

7.5.7 Virus (content) protection tools

- Host-based vulnerability assessment tools are typically more expensive to set up, manage, maintain than network-based tools;

- Network-based vulnerability assessment tools are platform-independent and therefore less targeted than host-based tools;

- Vulnerability assessments consume resources (may be impractical, may come at the expense of system or network performance, or may run under specified date and time constraints);

- In many cases, vulnerability assessment is a cyclical (weekly, monthly or random) activity and security incidents may not be detected in a timely manner;

- Like IDPS, vulnerability assessment tools are susceptible to false positives or negatives and require careful analysis;

- Repeated vulnerability assessments can cause anomaly-based IDPS to ignore real attacks;

- Need to update attack signatures;

- Host-based vulnerability assessment tools are unable to detect unauthorized systems in the network.

Network vulnerability assessment needs to be limited to the target system. Since the collected data is sensitive information (easily used by intruders to invade the information system), attention needs to be paid to protecting the privacy of sensitive information and data.

7.6 Scalability

When choosing an IDPS, it also needs to consider its scalability. After the bandwidth of many IDPS is increased, the performance will decrease (IDPS performs better when the data transmission rate is lower), resulting in data packet loss and significant increase of false positives (alarms are generated when there is no attack) and false negatives (no alarm is generated when an attack occurs); therefore, this type of IDPS is not suitable for large-scale or wide-area distributed enterprise network environments.

Scalability is mainly suitable for NIDPS deployments and HIDPS that require high-performance host equipment.

7.7 Technical support

IDPS is not "plug and play", so IDPS requires suppliers to provide technical support and maintenance. Some suppliers will provide technical support during the IDPS

This is an excerpt of the PDF (Some pages are marked off intentionally)

------ The End ------