GM

CRYPTOGRAPHY INDUSTRY STANDARD

OF THE PEOPLE'S REPUBLIC OF CHINA

ICS 35.040
L 80
File No.: 58557-2017

GM/T 0052-2016

Cryptographic equipment management – Monitoring management specification of VPN device

密码设备管理 - VPN 设备监察管理规范

Issued on: December 23, 2016 **Implemented on: December 23, 2016**

Issued by: State Cryptography Administration

Table of Contents

Foreword

This Standard was drafted in accordance with the rules given in GB/T 1.1-2009.

GM/T 0052 Cryptographic equipment management - VPN device monitoring management specification is one of the cryptography device management standards. This type of standard consists of a basic specification and a series of management application specifications and currently includes:

- Basic specifications: GM/T 0050 Cryptography device management - Equipment management technical specifications;
- Management application specification: GM/T 0051 Cryptography device management - Specifications of symmetric key management technology;
- Management application specification: GM/T 0052 Cryptographic equipment management - VPN device monitoring management specification;
- Management application specification: GM/T 0053 Cryptographic device management - Remote monitoring and compliance verification interface data specification.

Any contents of this standard related to the contents of cryptographic algorithms are implemented in accordance with relevant national laws and regulations.

This Standard was proposed by and shall be under the jurisdiction of Cryptography Industry Standardization Technical Committee.

Main drafting organizations of this Standard: Shanghai Information Security Engineering Technology Research Center, Shanghai Jiao Tong University School of Information Security, Shanghai Pengyue Jinghong Information Technology Development Co., Ltd., Shanghai Huatang Network Co., Ltd., Weishitong Information Industry Co., Ltd., Shanghai Tianrongxin Network Security Technology Co., Ltd., Shanghai Xinhao Information Technology Co., Ltd.

Main drafters of this Standard: Wang Hao, Tian Li, Zhou Zhihong, Huang Zhirong, Liao Wei, Zou Ru, Yuan Feng, Pan Shuyuan, Wang Hegang, Li Junshan, Zhang Yuanchen, Lv Mingzhong, Pan Limin, Li Gaojian.

Cryptographic equipment management - Monitoring management specification of VPN device

1 Scope

This standard specifies the monitoring management of VPN device in important information systems and networks, to detect and locate illegal VPN device in the network and to detect illegal operations of the legal equipment in use.

This standard applies to the development and application of VPN device monitoring management systems and monitoring equipment. It can also be used to guide the detection of such monitoring equipment.

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) are applicable to this standard.

GM/T 0022-2014 IPSec VPN technical specifications

GM/T 0024-2014 SSL VPN technical specifications

GM/T 0050-2016 Cryptography device management -Equipment management technical specifications

GM/T 0053-2016 Cryptographic device management - Remote monitoring and compliance verification interface data specification.

3 Terms and definitions

The following terms and definitions apply to this document.

3.1

VPN device

Devices that use VPN technology to implement secure communications services in the network. The VPN device in this standard refers to the IPsec VPN and SSL VPN devices, including the network cryptographic machines

forensic analysis;

d) Maintain (add, change, and delete) a list of violation algorithms;

e) Maintain a list of filtered IP and establish a white list mechanism;

f) Count the number of communication of VPN devices in the entire network;

g) Provide query and statistical analysis of historical data.

5.3 Management application layer

The management application involved in this standard is the monitoring management of VPN device.

For the monitoring management of VPN device, it shall capture and detect the data packets in the VPN key negotiation phase to analyze the VPN device application conditions in the network, to alert the illegal VPN device, to ensure the legal compliance of the VPN device.

5.4 Management platform layer

Requirements for the management platform layer follow clause 5.5 of GM/T 0050-2016.

5.5 Monitoring equipment layer of VPN device

The monitoring equipment of the VPN device is managed by the management agent, it follows clause 5.6 of GM/T 0050-2016 and clauses 5.3 and 5.4 of GM/T 0053-2016.

The monitoring equipment of VPN device is deployed in the entry-exit of the monitored network. It performs monitoring management for all VPN device in the network by means of bypass packet capture, is responsible for receiving the policies and instructions issued by the management application layer through the equipment management platform and security tunnel, parses the instruction, and returns the result of the execution.

The logical structure of the VPN device monitoring equipment is shown in Figure 2.

parsing and operating in accordance with the instruction content.

The monitoring equipment of the VPN device is managed by the management agent. All messages between the VPN device and the equipment management platform are sent through the security tunnel. The message PDU and usage instructions of the security tunnel follow clause 6 of GM/T 0050-2016.

The interaction information between the management application layer and the monitoring equipment of the VPN device includes two aspects:

a) The monitoring equipment of the VPN device reports information to the management application layer, including illegal VPN alert information;

b) The information issued by the management application layer to the monitoring equipment of the VPN device, including the configuration information and filtering rule information of the monitoring equipment of the VPN device.

5.7 Monitoring management process of VPN device

The monitoring management system workflow is as follows:

a) Deploy the monitoring device of the VPN device to the network backbone node, initialize it, and configure the uplink IP address;

b) After the VPN device's monitoring device is powered on, it automatically initiates a connection with the management application layer to perform identity authentication, including two-way IP binding and device ID authentication with the uplink device;

c) After the management application layer authenticates the identity of the monitoring equipment of the VPN device, it performs initialized configuration for this monitoring equipment;

d) The VPN monitoring device filters the captured data packets and collects various types of VPN packets in accordance with the configuration rules.

e) Check the captured VPN packets and determine if the VPN device is in the white list in accordance with the IP address information, skip the follow-up inspection steps and do not need further inspection;

f) If the VPN device is not on the white list, then extract the value of the cryptographic algorithm attribute (referring to the key algorithm attribute value of the first phase of the key exchange protocol), if the extraction fails, it skips to step i);

g) Compare the extracted algorithm attribute values with the definitions of

6 Monitoring data collection rules for VPN devices

6.1 Filtering rules

VPN device encrypted by private protocol shall be registered at the state cryptographic administration, the registered VPN device will be deemed as compliant if it passes the equipment compliance test. The equipment compliant test follows clause 6.2 of GM/T 0053-2016. For other VPN devices, the compliance of their applications is monitored in accordance with the data collection rules in this clause.

The management application layer sends a data packet filtering rule to the monitoring equipment of the VPN device. After the monitoring equipment receives the packet filtering rule message, it performs packet filtering and packet content analysis in accordance with the filtering rule database at the entry-exit node of the VPN network communication. The acquisition information is submitted to the management application layer in real time.

The default message filtering rules delivered by the management application layer are port 443 of the TCP protocol and ports 500 and 4500 of the UDP protocol, wherein:

Port 443 of the TCP protocol corresponds to the SSL VPN protocol.

Port 500 of the UDP protocol corresponds to the ISAKMP protocol of IPSec VPN.

Port 4500 of the UDP protocol corresponds to the presence of NAT traversal with IPSec VPN and UDP sealing.

The default rule can be written as:

tcp port 443 or udp port 500 or udp port 4500

For the case that the manufacturer may modify the standard network port, the port range of the packet filtering rule can be relaxed to all ports of TCP and UDP.

The message filtering rule language complies with the BPF syntax. The detailed BPF filter rule language is described in the reference [1].

6.2 Detection rules based on the IPSec VPN protocol

The monitoring management of IPSec VPN includes the monitoring of equipment and the monitoring of algorithms used by the equipment. The specific monitoring steps are:

the agent. The management application layer assigns an ID to the monitoring equipment, as one of the authorized identifiers for monitoring equipment access network, the management application layer receives the monitoring equipment information of the VPN device, it is necessary to identify the message format, and determine the legitimacy of the equipment in accordance with the conditions such as the monitoring equipment ID. If the format is incorrect, the processing is rejected and the monitoring equipment is instructed to resend.

The operation types of the VPN device monitoring management include the agent-config (VPN device monitoring management message), the agent-rule (monitoring equipment rule message of the VPN device), and the agent-alert (monitoring equipment alert of the VPN device), and so on.

7.2 Monitoring equipment configuration messages of VPN devices

The configuration information agent-config of the VPN device monitoring equipment is used to manage the configuration delivered from the application layer to the monitoring equipment. It is directly a subclass of the agent. It mainly involves the management, configuration maintenance, and policy rule issuing of the monitoring management application layer for multiple monitoring equipment, it defines the uplink device (servers class), heartbeat interval, information report time window, timestamp and other subclasses, servers class shall contain multiple server subclasses, through the server's element value, it is determined to be used for the master server or other applications, the message format is defined as follows:

Agent-config = {update time (YYYY-MM-DD-HH:MM:SS format) || uplink device configuration (name, ID, IP, port) || VPN device monitoring equipment configuration (VPN device monitoring equipment name, ID, IP, port) || Heartbeat interval || Sampling time}.

<? xml version = “1.0” encoding = “UTF-8”?>

<agent xmltype = “agent-config” name = “monitoring equipment name of the VPN device” id = “monitoring equipment id of the VPN device” ip = “monitoring equipment IP of the VPN device”>

<agent-config>

<update-time) YYYY-MM-DD HH:MM:SS</update-time>

<servers>

<server name = “uplink device name” ip = “uplink device IP” status= “1” default

Agent-report = {VPN device monitoring equipment detection start time (YYYY-MM-DD HH:MM:SS format> || Detection end time (YYYY-MM-DD HH:MM:SS format) || IPSec/SSL flag bit || symmetric algorithm attribute value || hash algorithm attribute value || authentication algorithm attribute value || group algorithm attribute value || VPN device monitoring equipment IP || uplink equipment IP || VPN device monitoring equipment port || up-link equipment port || Is it legal || Is it a cryptographic device

<? xml version = “1.0” encoding = “UTF-8”?>

<agent ip = “VPN device monitoring equipment IP” id = “VPN device monitoring equipment id” name = “VPN device monitoring equipment name” description = “agent.xml” xmltype = “alert-report”>

<agent-reports>

<agent-report type = “alert-report” description = “report commu-alert”>

<vpn>

<detecting-time> YYYY-MM-DD HH:MM:SS </detecting-time>

<end-time> YYYY-MM-DD HH:MM:SS </end-time>

<protocol> IPSEC (/protocol>

<arithmetic-enc> encryption algorithm attribute value (/arithmetic-enc>

<arithmetic-hash> hash algorithm attribute value </arithmetic-hash>

<arithmetic-auth> public key algorithm attribute value </arithmetic-auth>

<arithmetic-group> group algorithm attribute value </arithmetic-group>

<sourceAddress> VPN device monitoring device IP </sourceAddress>

<destAddress) uplink device IP (/destAddress>

<sourcePort> VPN device monitoring device IP </sourcePort>

(destPort) uplink device port </destPort>

<islegal> unknown </islegal>

<isdevice> unknown </isdevice>

</vpn>

</agent-report>

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

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