ATLANTIS PRESS
Advances in Social Science, Education and Humanities Research (ASSEHR), volume 130
2nd International Forum on Management, Education and Information Technology Application (IFMEITA 2017)

Design and implementation of industrial firewall configuration management system

Xinwei Zhang 1[a] Wen Zhang 2[b] Xiaowang Guo 3[a]

[1] The 6th Research Institute of China Electronics Corporation Beijing 100083, China

[2]IThinking Inc, Beijing 100083, China

[3] The 6th Research Institute of China Electronics Corporation Beijing 100083, China
[a]15001108521@163.com [b]839334049@qq.com [c]guoxiaowang@ncse.com.cn

Keywords: Firewall; Industrial control; Protocol Protection; Strategy

Abstract. Ministry of industry association [2011] no. 451 notice made clear that there are still many problems in the information security management of China's industrial control system. It is mainly because the concern on the information security of industrial control system is not enough. The management system is not perfect, and lack of standard specification, technical protection measures are not in place. The ability of safety protection and emergency disposal is not high. These problems threatened the safety of industrial production and the functioning of society. The configuration software for industrial communication protocol based on the built-in firewall protection mode of industry provide configuration function. It mainly achieves port protection configuration, the depth of packet inspection configuration, built-in protocol configuration, and provides a graphical statistics analysis and reporting features. It provides professional industrial safety protection for industrial communication solutions. The system has the function of modifying the configuration online, and can modify the firewall strategy in real time, without affecting industrial real time communication, avoiding power failure, restart, etc.

Introduction

With the development of industrial control technology, information technology, Windows, Ethernet and TCP/IP, fieldbus, OPC and other technologies are widely used in process control systems (DCS/PLC/PCS) and SCADA systems. These technologies make the interface of industrial equipment easier, The control system and the SCADA system are weakened and isolated from the outside world. More and more security incidents in control system network showed that network security issues from the business network, the Internet and other factors are gradually spreading in the control system and SCADA system, directly affected the safety of industrial production. Especially in 2010, tThe outbreak of the Stuxnet virus has ravaged Iran and caused huge losses to Iran. It shows the seriousness of the problem and the necessity of solving the problem. Ministry of industry association [2011] no. 451 notice made clear that there are still many problems in the information security management of China's industrial control system. It is mainly because the concern on the information security of industrial control system is not enough. The management system is not perfect, and lack of standard specification, technical protection measures are not in place. The ability of safety protection and emergency disposal is not high. These problems threatened the safety of industrial production and the functioning of society.

Industrial firewall is based on the built-in industrial communication protocol protection mode, implements port protection, packet depth check, protocol identification and analysis. It provides professional industrial safety protection solutions for industrial communication. The system has the function of modifying the configuration online, it can make changes to the configured firewall policies in real time. It does not affect industrial real time communication, avoid power failure, restart, etc. Comply with ANSI/ISA - 99 industrial control system safety standard design, it belongs to industrial security firewall. It mainly implemented: ACL (black and white list control), network access control D-DoS protection (control) threshold distributed denial of service, protect the vulnerable system vulnerabilities and agreement, Zero Day attack prevention, detection,

authentication and user behavior audit, protocol control, protocol translation, seven layer security, industrial engine firewall, flow control, VPN, etc.

Configure software functions

This software is aimed at the management and configuration of the industrial security firewall, includes the following functions：

a) Reliability HA;
b) Strategic compliance Check;
c) Statistical analysis: Establish a baseline based on different protocol types, statistics flow, attack events, types and frequency, normal behavior statistics;
d) Bypass function;
e) Log and Reports: Chart shows, daily weekly and monthly report, attack log (by protocol, by event), operation log, system log, log export import (format: PDF, WORD, EXCEL, HTML), log restore and backup;
f) Alarm: alarm type (color, sound, mail, SMS), external alarm interface;
g) Diagnostic tool;
h) The device management: the CLI command line/character control terminal interface;
i) License management;
j) Protocol Identification (CAN, FF, PROFIBUS, Modbus TCP)
k) System management platform (B/S) : equipment IP address, protocol object, parameter Settings, account password, system configuration backup reduction, reduction, user access control, License, system diagnostic tool.

The goal to achieve：

Secure area: the industrial control firewall can filter the communication between two regional networks and control the network attack in the original area.

Communication control: communication rules can be preconfigured and tested online.

Real-time alarm: any illegal access will generate real-time alarm information and notify the manager via email or text message via a centralized log analysis system.

Configuration is simple: Different from the virus library upgrade and other tedious work in the traditional firewall, this firewall can do the protection work and do not change the operation mode of the original application In the meantime. It greatly reduces the work of network maintenance in control system.

System Design

Functional Design. The main functional structure of the configuration management system is shown in Figure 1.

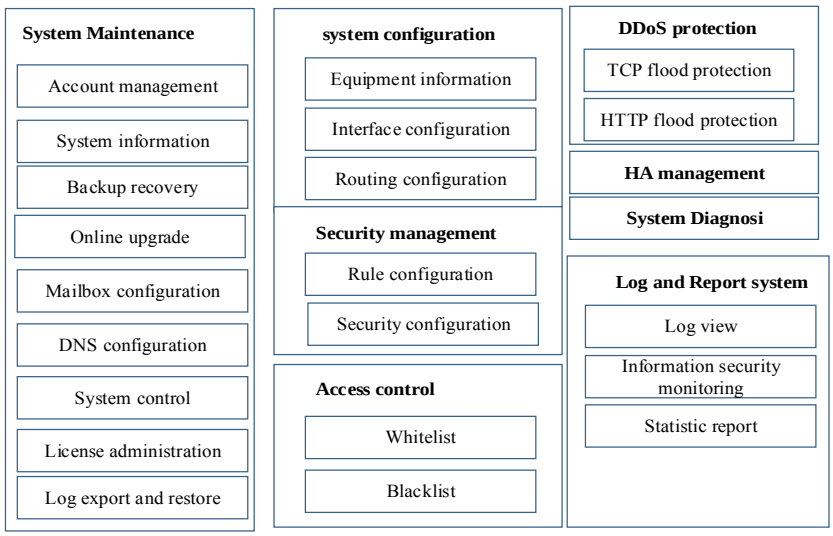

Fig.1 configuration management system capabilities

System Maintenance. Account management: Management of the Account information of the system, including the addition, deletion and modification of three types of users;

System information: system information includes basic system information and time management. Basic information of the system provides basic information about the system, such as firmware version, system version, hardware ID, and system time setting. Time management provides time to manually set in the system and also time server synchronization with system time.

Backup recovery: backup is primarily for backup of configuration files. The backup data can also be imported into the export system, which increases the reliability of the system.

Online upgrade: system upgrade is completed by uploading and upgrading files. It also includes the recovery of the factory model. Once the factory mode is restored, all configuration of the system will be lost and unable to recover. If not, please backup the system to restore it.

Mailbox configuration: configuration is mainly used to report the alarm, when the system is attacked, it is possible to check the attack log through the log system, You can also email notification by setting your mailbox, you can send the test mail after the configuration is completed and saved to determine the configuration is correct.

DNS configuration: use this feature to configure your firewall's domain name server. Once the configuration is successful, the firewall will use the domain name server configured to resolve the domain name.

System control: when making certain configurations or installing hardware, we need to restart the firewall to take effect. Execute the shutdown command to close the firewall system, which can be used to restart and close the firewall. Warning: unsaved data will be lost.

License administration: License is a restriction and regulation on the behavior of product users by copyright owners, which generally defines the conditions for users to use the product. License binds the serial number and model information of the firewall. If the serial number of the License is not matched with the serial number of the current firewall, the License is illegal and cannot be used. License is produced by the manufacturer. The License issued by different manufacturers cannot be replaced by each other. Only when the firewall is uploaded to the License, the user can configure the firewall. Only an administrator can make a Licenses configuration.

Log export and restore: export and restore the logs stored in the database.

System Configuration. Equipment information: manage and display the information of the equipment, provide editing and viewing operations. The device information comes from the background configuration, which cannot be added and deleted in this system, but can modify the specific name of the equipment display.

Interface configuration: manages and displays information about the interface on the device,

providing editing and viewing operations. The device information comes from the background configuration, and the interface information cannot be added and deleted in this system. But you can modify the work mode of the interface.

Routing configuration: routing leads message transmissions, after some intermediate nodes, to their final destination. Routing is usually guided by routing tables, and routing tables are the best route to be stored to each destination. The entry of each route is the destination network address, the next hop gateway.

Security Management. Rule configuration: provides two kinds of rules, one is the predefined rule library, and the other is the user custom rule library. Predefined rule libraries that contain default rules libraries for various protocols and attacks.

Security configuration: the administrator can make targeted user rules according to different requirements, thus avoids the traditional rule checking of the gateway in the traditional sense.

Access control. Whitelist: Access control is mainly configured to filter the protocol, and directly reject or release (do not do security checks) in the form of black and white lists. The white list is a list of agreements that meet the rules of the agreement. In the configuration management system, you can add protocols and rules to see the rule list, protocol list, etc.

Blacklist: Blacklist is a list of agreements that do not comply with protocol rules. In the configuration management system, you can add protocols and rules to see the rule list, protocol list, etc.

DDoS protection. TCP flood protection: TCP flood protection includes Syn flood and Ack flood protection Settings, and users can set thresholds. The above threshold of syn and ack access will be discarded. This feature can block illegal syn requests and ack requests when there is a large number of syn flood and ack flood attacks.

HTTP flood protection: users can configure global parameters in the management system to keep attacks on time, trust time, verification code automatic update cycle, and maximum trust number. Configure the site, IP, and port to be protected.

HA Management. The HA configuration and ByPass function, which requires hardware support, is enabled by default on the supported hardware without any configuration required.

Log and Report system. Log view: this function is used to display the time of the threat, sources, using methods as well as your reactions in the firewall, the system support paging view, and according to the time order from new to old automatic sorting. The main types of logging include security protection logs, access logs, running logs, audit logs, and so on.

Information security monitoring: mainly used to display various attack to intercept, mainly includes: 1 hour in recent attacks (1 days attack): statistics all attacks within an hour, including name of the attack and attack information; Interface traffic: statistic system runs the flow information of each interface; Engine connection number: statistics current engine connection number current value and new increment.

Statistic report: the analysis of alarm time is divided into monthly statistics, weekly statistics and daily statistics; Alarm classification statistics according to the types of protection incidents.

Each statistical mode has a variety of display modes, graphs, histograms and pie charts.

System Diagnosis. Provide CLI capabilities: users can conduct CLI management directly through CLI; Other auxiliary tools such as Ping, Trace route, ARP, and grab bag are provided.

System Architecture.

The configuration management system adopts three layers of structure, including: performance layer, control layer and business layer. Presentation layer: mainly responsible for user interaction and results display, using the tpl.php file that can be embedded in PHP. Control layer: mainly responsible for system access control, data loading and management, is the core control unit of the system. The control layer organizes the work through the system description. Corresponds to the controller file. Business layer: the main business logic of the system is realized, which is the main operation unit of

the system. The persistence management of static data and database data is realized, and data service is provided to the control layer, which is the unified interface of data operation of the system. Corresponding to the models file.

References

[1] MUTHUPRASANNA M，WEI K，KOTHARI S. Eliminating SQL Injection Attacks-A Transparent Defense Mechanism[C]. IEEE. Symposium on Web Site Evolution (WSE'06). Philadelphia：[s.n.], 2006：22-32.

[2] ZHANG Y，SREEDHAR V. Adaptive Rule Loading and Session Control for Securing Web-Delivered Services[C]//IEEE. Proceedings of the 2009 Congress on Services-I. Los Angeles, CA：IEEE，2009：645-652.

[3] Altendorf E, Hohman M, Zabicki R. Using J2EE on a large Web-based Project Software[J]. IEEE. 2002, 19(2):81-89.

[4] Ben Smith, Laurie Williams, Andrew Austin. Idea Using System Level Testing for Revealing SQL Injection-Related Error Message Information Leaks[J]. North Carolina State University, Computer Science Department 890 Oval Drive, Raleigh, NC, USA. 2010

[5] Andrew Crmack. Web Site Security[J], Third Institutional Web Management Workshop, March,1999