Automation of Abnormal IP Blocking in Security Systems Using OCR-Driven Web Interaction and Real-Time Alert Integration

Yin Yuzhen*, Fang Xiaoliang and Zhang Wei

Shandong Earthquake Agency, Jinan 250100, China
E-mail: Yinyuzhen6@163.com; fang@163.com; zhang@163.com
**Corresponding Author*

Received 23 June 2025; Accepted 21 August 2025

Abstract

The Shandong Earthquake Agency has established a comprehensive protection system that meets the national third-level safety requirements. However, challenges remain, such as delayed detection of malicious attacks and overly complex procedures for blocking abnormal IP addresses. To address these issues, this paper proposes a solution that leverages Selenium crawler technology, a Qt-based graphical user interface, and the integration of Baidu OCR and WeChat public account interfaces. The system enables simulated logins to network security equipment, real-time abnormal IP monitoring, automated alarm notifications, and automated interactions such as interface clicks and text input. With these functions, it achieves one-click blocking of abnormal IP addresses on security devices while storing related information for future reference. Since its deployment, the software has effectively enhanced the

Journal of Cyber Security and Mobility, Vol. 14_4, 981–1006.
doi: 10.13052/jcsm2245-1439.1449
© 2025 River Publishers

push of high-risk alarm information in the full-flow network security analysis system and streamlined the blocking of abnormal IPs in security devices such as firewalls, significantly improving the timeliness and efficiency of security protection.

Keywords: Abnormal IP, selenium crawler technology, WeChat push, one-click blocking, security protection.

0 Introduction

In recent years, malicious network attacks have become increasingly stealthy, diverse, and persistent. Threats such as ransomware, cryptojacking, and WebLogic vulnerability exploits can cause severe network congestion and even paralysis at the Shandong Earthquake Agency (SEA). Rapid identification and timely blocking of such attacks before they degrade network performance are critical cybersecurity concerns for the agency. With the continuous improvement of public service capabilities, SEA's network structures have grown more complex, public-facing applications have proliferated, and the associated risks have intensified [1, 2]. Guided by the province's '13th Five-Year Plan' for enhancing earthquake disaster prevention and mitigation information services, SEA has deployed a range of systems and devices, including the Colasoft full-traffic security analysis system, internet behavior management system, antivirus gateway, internet boundary firewall, and private cloud platform firewall. These systems are designed to identify malicious attack behaviors and block abnormal IP addresses, thereby strengthening threat analysis and prevention capabilities. At present, intrusion detection systems (IDS) and firewalls remain the primary security technologies in use. Firewalls act as network access control devices by managing inbound and outbound traffic, but because their security policies are preset, they function as static and passive defenses, incapable of dynamically adjusting to evolving attack patterns. Moreover, firewalls cannot mitigate threats originating from within the network. By contrast, intrusion detection is a proactive measure that can identify potential intrusion attempts and issue alerts, but it lacks the ability to automatically block malicious activity. Consequently, IDS alone is insufficient to ensure comprehensive network protection.

Further complicating SEA's defense efforts is the heterogeneous composition of its cybersecurity infrastructure. Since the devices were procured from different vendors – including Topsec, Leadsec, Renzixing, and Colasoft – they rely on distinct interface protocols and operate independently

without sharing protection data. This lack of interoperability leads to delays in detecting and blocking abnormal IP addresses. In addition, the procedures for blocking IPs differ across brands, are often cumbersome, and place a heavy burden on duty personnel who must operate multiple devices. Currently, staff must manually log into the Colasoft full-traffic security analysis system to identify abnormal IP activity, then separately access the appropriate firewall to block the IP based on the attack type. This manual process is inefficient, error-prone, and increases the likelihood of overlooked incidents, undermining the timeliness and effectiveness of security protection. Integrating intrusion detection with firewalls through intelligent linkage offers a promising solution, enabling real-time detection and immediate response, and providing the foundation for a unified security system. Linkage technology represents a key trend in cybersecurity development, allowing complementary use of diverse technologies to overcome the functional limitations of individual devices. However, most security products from different vendors still operate in isolation, lacking centralized management and linkage mechanisms. This prevents them from working synergistically and complicates operations and maintenance. Personnel must repeatedly log into separate devices for configuration, increasing workload and introducing inconsistency, as different individuals may apply divergent policies, thereby creating risks of misconfiguration or data blockage.

To address these challenges, this paper presents an abnormal IP monitoring and blocking software solution based on Selenium web crawling technology. The software periodically retrieves high-risk alerts from the Colasoft full-traffic security analysis system and delivers them to duty personnel via a WeChat public account. Depending on the attack type and operational context, personnel can enter the abnormal IP into the software and execute a one-click blocking operation. The system then automatically carries out the firewall blocking process while storing the relevant information. This solution provides reliable technical support for enhancing SEA's network security by improving alert responsiveness, simplifying IP blocking, and reducing the risk of oversight.

1 Research Status

Traditional network security management typically adopts a reactive, technology-centric strategy, relying on a static, localized, ad-hoc, and post-event corrective approach. To address the growing security threats, it is necessary to continuously install, configure, and update security products and

systems from various vendors. This process ultimately leads to inefficient network security management and potential security risks, such as mutual constraints among the functions of security devices. In response to these challenges, a policy-based network security linkage framework was proposed. This framework integrates, consolidates, and correlates data from security devices across different vendors, filters out false positives from events, generates confirmed security alerts, and dynamically configures devices based on predefined linkage policies to trigger coordinated responses. Currently, many organizations, both domestically and internationally, have begun researching and developing policy-based network management solutions, and some have already launched policy-based security products. For instance, Topsec's Network Security Management System (TSM) provides centralized policy management for the entire network. TSM enables the centralized and uniform management of network devices, monitors network status, collects, filters, and analyzes event information from various security products, and adjusts network security policies based on security risks to facilitate rapid responses. Additionally, Venus Tech's Taihe Information Security Operation Center (SOC) offers security policy configuration management, providing unified security policies for network security operation managers across the network and guiding the implementation of various security tasks. This effectively addresses security risks arising from the lack of policies related to passwords, authentication, access control, and other aspects. Although significant progress has been made in the development of security device linkage systems and policy-based security device management, several challenges and shortcomings remain.

Based on the current status of network information security and the need to support public service operations, the SEA has enhanced the protection capabilities of its network security devices and established a comprehensive security system that meets the national Level 3 information security protection standards. This system provides capabilities for intrusion detection, hazard control, and post-event traceability, offering robust security support for the integration of the SEA's internet and industry network services. The full-traffic security analysis system serves as the core of intrusion detection, featuring large-scale, distributed capabilities for collecting, analyzing, storing, and managing full-traffic security data. It can quickly search, identify, and extract various malicious behaviors from hundreds of types of metadata, enabling operation and maintenance personnel to rapidly and timely detect unknown and malicious threats. The response time to potential threats has been reduced from several days to just a few minutes. The antivirus

gateway and next-generation firewall system can defend against malicious software such as viruses, Trojans, worms, and spyware, detecting and blocking increasingly prevalent worm attacks in real time. This effectively prevents the network from being paralyzed by abnormal IP attacks. Although the Colasoft full-traffic security analysis system at the SEA can quickly identify malicious behaviors from hundreds of types of metadata, it cannot promptly notify network operation and maintenance administrators about the location results of abnormal IPs. Furthermore, there is a lack of unified standards, with various research institutions and security device manufacturers adopting their own description languages, implementation models, protocols, and API functions. This leads to a lack of compatibility and interoperability between different policy management systems and security products. The network security devices at the Shandong Earthquake Administration, which consist of multiple brands such as Topsec, Venus Tech, Sangfor, and others, make it difficult to achieve centralized control and management through a single product. Currently, network duty personnel are required to log in to each device daily for manual checks, making it challenging to detect malicious internet attacks in a timely manner. Additionally, the process for blocking abnormal IPs on the antivirus gateway and next-generation firewall is complex, resulting in poor timeliness in security protection.

Currently, the security protection work at the SEA requires duty officers to manually log into the intrusion detection system to check for abnormal attack behaviors and then log into the firewall to manually block IPs based on the type of attack. This operational process is inefficient and ineffective, and some network attack issues may be overlooked by duty officers, potentially leading to network security incidents. To enhance the effectiveness of abnormal IP monitoring and blocking, and to address the repetitive and cumbersome manual operations in web systems, Selenium technology can be utilized to simulate various user interactions with web pages, including system logins, page clicks, text input, and form submissions, thereby enabling web automation. Drawing from the concept of automated testing, Wang Ming proposed an automated inspection method based on Selenium, which significantly improved work efficiency and reduced costs [3]. Huang Qian implemented automated user permission configuration in the electric power marketing system using Selenium technology, enabling the automated execution of large-volume tasks [4]. However, Selenium technology has not yet been applied in the earthquake system to simulate manual operations for automatic inter-device coordination. Based on Selenium, this paper integrates the Baidu OCR API and the WeChat Official Account interface to simulate

logins to security device systems such as the full-traffic security analysis system and firewalls. It also monitors abnormal IPs, pushes alert notifications, and performs system interface clicks and text entries, thereby achieving automated monitoring and blocking of abnormal IPs.

2 Technical Approach

The method for abnormal IP monitoring and blocking, based on Selenium crawler technology, can automatically identify malicious attack behaviors by relying on network security devices and block abnormal IPs on the firewall. The system is set to inspect the Colasoft full-traffic security analysis system every 10 minutes to obtain internet link alert information. If the alert is of medium to high risk, the alert information will be immediately pushed to the duty officer via the WeChat Official Account. The duty officer will then confirm the situation with the business system manager to determine if the alert pertains to a business requirement. If the 'attack behavior' is determined to be a malicious attack unrelated to business needs, the duty officer can input the abnormal IP into the software and click a button to automatically block the abnormal IP on the firewall with one click. Additionally, the software will store the relevant information in a database table for record-keeping. The software's business process is shown in Figure 1.

When external network data flows containing attacks enter the network, as indicated by the solid arrow labeled 'DATA' in Figure 2, they are filtered by the firewall. Data flows (DATA1) that comply with the access control rules pass through the firewall and enter the internal network. The intrusion detection system then inspects the data (DATA1) that has entered the internal network. When an attack is detected, an alert is immediately generated. The operation and maintenance management system acquires the alarm information (ALARM), generates a security policy, and distributes the policy (POLICY) to the firewall. Upon receiving the response policy (POLICY), the firewall dynamically adjusts the relevant access control rules to block the attack's network connection. If the same attack attempts to pass through the firewall again, it is blocked by the firewall. By combining 'active monitoring' with 'passive defense, ' a cyclic protection loop of 'protection – detection – response – re-protection' is formed, providing robust security assurance for the protected network.

Based on the network structure and business requirements of the SEA, the security protection device that blocks abnormal IPs varies depending on the location of the affected local IP. The specific principles are as follows:

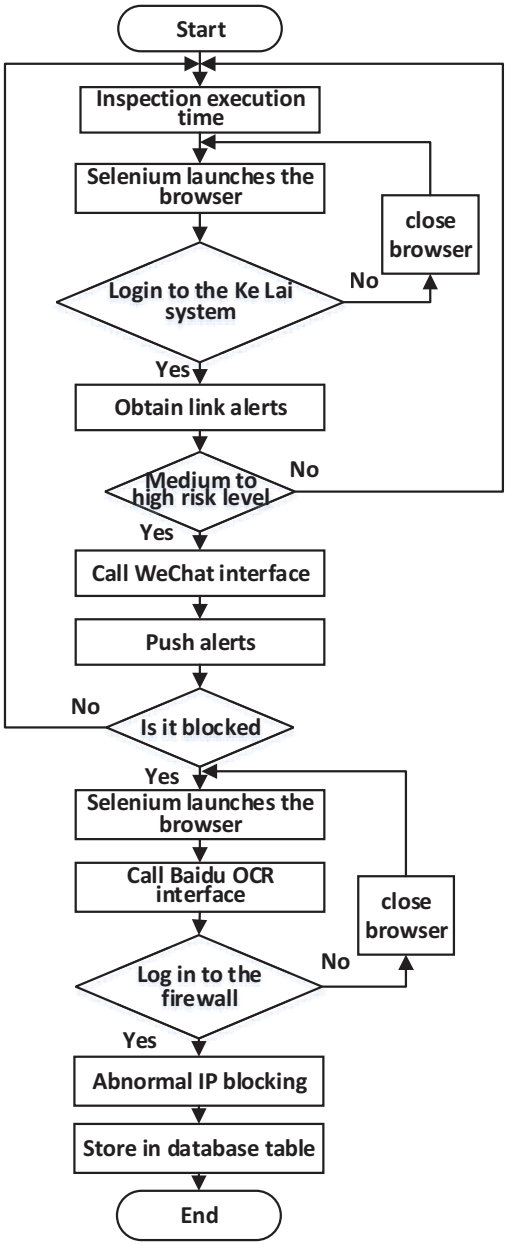

Figure 1 Software business flow chart.

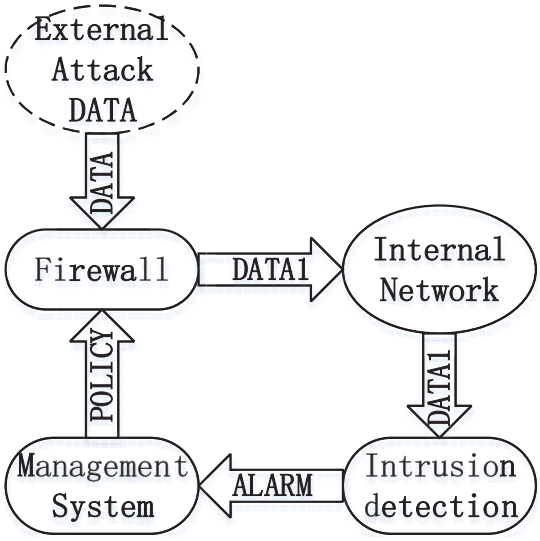

Figure 2 Interactive response model.

1. If the affected local IP is located in the office area, the blocking of abnormal IPs must be performed at the antivirus gateway system.
2. If the affected local IP is located in the earthquake private cloud platform area, the blocking of abnormal IPs must be completed at the internet exit firewall of the earthquake private cloud platform.
3. If the affected local IP is neither located in the office area nor in the earthquake private cloud platform area, the blocking of abnormal IPs must be carried out at the global internet exit firewall.

3 Key Technologies

This article develops a set of abnormal IP monitoring and blocking software based on Selenium crawler technology, with the functional design shown in Figure 3. The software simulates various operations performed by duty officers on web pages, automating web operations to replace tedious and repetitive tasks, thereby improving work efficiency. The software includes the following features:

1. **Timeliness in abnormal IP identification**: By utilizing web crawler technology, the software obtains real-time defense information from the Colasoft full-traffic security analysis system and promptly pushes

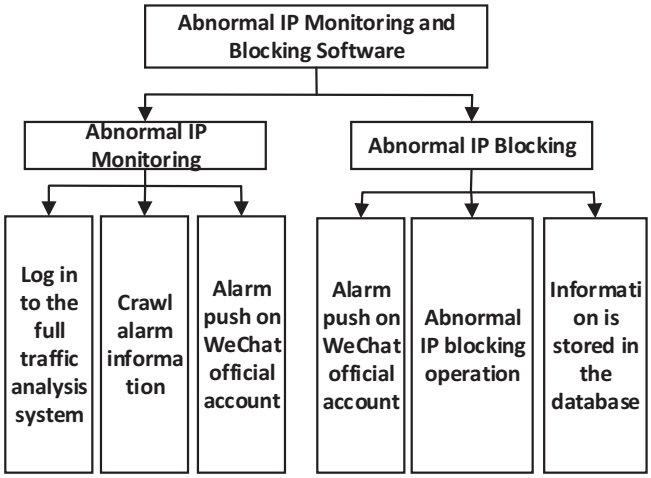

Figure 3 Software function design diagram.

it to network operation and maintenance administrators via the WeChat Official Account. This replaces the previous method of regular inspections by duty personnel, significantly improving network operation and maintenance efficiency.

2. **Automated abnormal IP blocking**: Using Selenium-based simulated login technology, the software automatically logs into the antivirus gateway and next-generation firewall. Duty personnel only need to input the IP to be blocked and click a button to automatically execute the complex process of abnormal IP blocking. This frees operation and maintenance personnel from cumbersome tasks, enhancing operational reliability.
3. **Traceability of abnormal IP blocking**: To facilitate timely troubleshooting of fault causes by business systems, the software stores information such as local IP, abnormal IP, attack type, operator, operating device, and operation time in a MySQL database each time an IP blocking is completed. This ensures one record per blocking for easy future queries and traceability, safeguarding the normal operation of earthquake business systems.

3.1 User Interface Design

To enhance the interaction between network duty officers and security protection devices, and to facilitate visual and simplified operations for duty

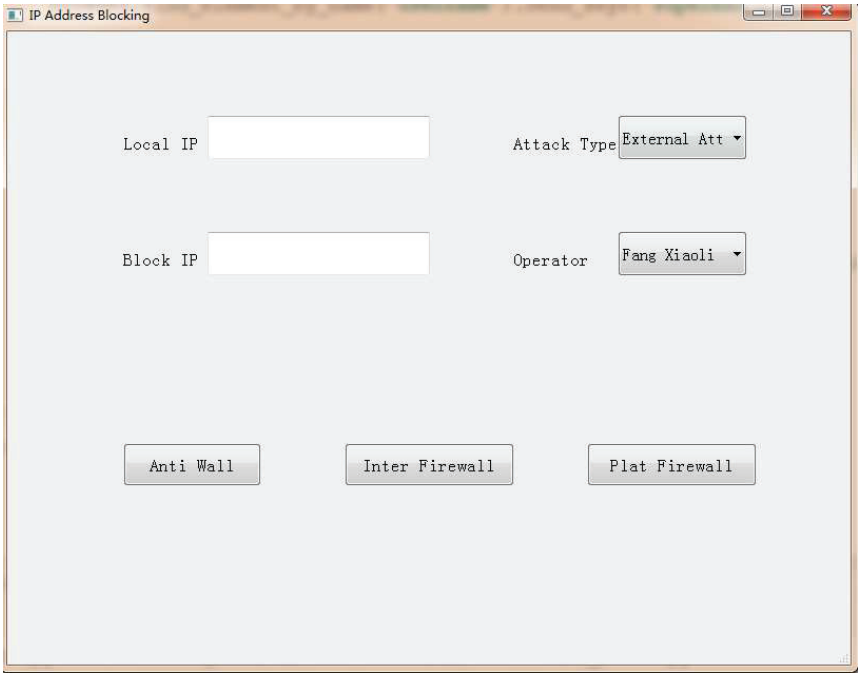

Figure 4 Software user interface diagram.

officers, abnormal IP monitoring and blocking software based on Selenium crawler technology has been developed using the Python programming language, with the graphical user interface created using Qt Designer. By combining Python with Qt through PyQt, the advantages of both are integrated. The user interface of the software is shown in Figure 4. It allows for the input of 'Local IP' and 'Blocked IP,' the selection of 'Attack Type' and 'Operator,' and one-click execution on network security protection devices.

To facilitate data transmission between the functional components of the software's user interface, this article creates a new .py file that inherits the main window class from the interface file, thereby separating the interface from the business logic. The .py file is then converted into an .exe executable file.

3.2 Selenium Crawler Technology

The network security protection devices of the SEA are deployed based on a C/S architecture, with relevant operations carried out through a web

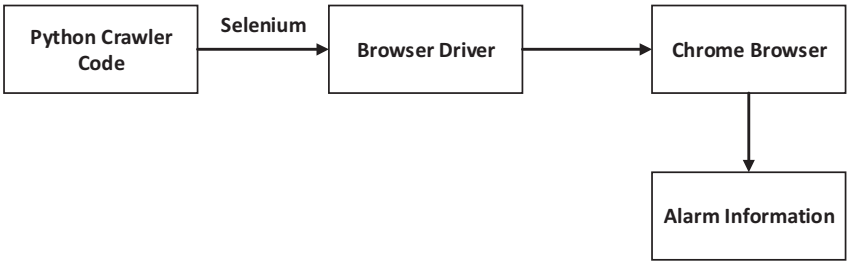

Figure 5 Selenium work flow chart.

interface. The abnormal IP monitoring and blocking software, based on Selenium crawler technology, simulates manual operations on network security devices. First, it automatically drives the browser to execute actions such as clicking and text entry. Second, it requires accurate positioning of the web elements involved in the operations. The web management interface of security devices typically uses modern front-end frameworks, heavily relying on AJAX/XHR for asynchronous data loading and dynamic rendering of DOM elements. Traditional automated scripts based on static DOM operations are prone to failure due to incomplete element loading and state updates. To enhance the stability and robustness of Selenium in simulating login and subsequent operations, we establish a basic guarantee layer through explicit waiting and intelligent state detection. This is further supplemented by robust locator strategies and advanced interaction techniques, significantly improving Selenium's success rate and stability in automating complex and dynamic web interfaces of security devices.

(1) Browser Automation

Selenium is a web application tool that supports multiple operating systems and mainstream browsers, including Mozilla Firefox and Google Chrome. It also supports the execution of script files in various programming languages, such as Python and Java. Selenium can automatically handle browser interactions, simulating various web operations typically performed by users [5, 6]. The workflow of Selenium is shown in Figure 5.

WebDriver is a powerful set of interfaces and communication protocols compatible with multiple browsers. It allows browsers to perform any operation, enabling interaction with browsers even without external devices such as mice and keyboards. This article uses ChromeDriver, which is based on the Chrome browser, to facilitate communication between Selenium and the Chrome browser, thus enabling the browser to be controlled and web page

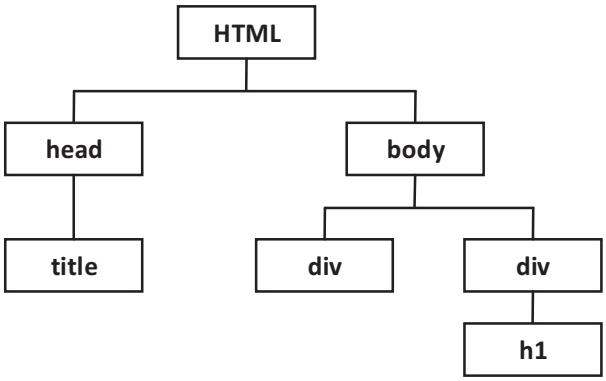

Figure 6 Structure of DOM tree.

information to be retrieved. The version compatibility between the Chrome browser and its driver is quite strict; the corresponding driver for the specific browser version must be installed for the program to run. Additionally, to address the 'Your connection is not private' prompt that appears when the browser starts, the ignore-certificate-errors parameter can be added to configure the browser to bypass SSL certificate verification errors. The code is as follows:

```
options = webdriver.ChromeOptions() # Start Chrome browser
options.add_argument('ignore-certificate-errors') # Set to ignore SSL certificate verification errors
```

(2) Element Localization

An important step in automating browser operations using Selenium crawler technology is locating web elements. The web interface of the security device system can be viewed as an HTML document composed of many tags, each with a different tag name and various attributes, such as the id attribute and class attribute of a DIV tag. The hierarchical relationship of tags in an HTML document can be represented as a DOM tree, the structure of which is shown in Figure 6. This path expression method can be used to locate a unique element.

XPath (XML Path Language) is used to manipulate elements and attributes in an XML document. This article employs XPath expressions to locate web elements, using absolute paths as the location information for the elements. When constructing an XPath, it is necessary to obtain attribute values such as tagName, id, and class of the element. WebDriver provides

multiple methods for this purpose. This article uses the find_elements method to locate elements on a web page through various means, such as the id attribute, name attribute, XPath path, and CSS Selector. This allows for precise operations, including clicking buttons, filling in text, and navigating between pages.

The code for logging into the firewall using the id attribute is as follows:

```
browser.get('https://192.168.200.10/') # Open the system interface
browser.find_element_by_id('name').send_keys('superman') # Enter the username
browser.find_element_by_id('input_text_psw').send_keys('Sddzj66')
# Enter the password
```

(3) Page Switching

In the process of obtaining warning information and operating security devices in this paper, there is a need to switch between pages, such as navigating to the next page, jumping between pages, and crawling information from sub-pages. Selenium provides the switch_to command to facilitate page switching and navigation. The code is as follows:

```
browser.switch_to.parent_frame() #Switch back to the parent page
browser.switch_to.frame('rightFrame') #Switch to the page with the frame labeled as 'rightFrame'
```

(4) Alert Extraction

To locate the page for fetching alarm information in the Colasoft Network Total Traffic Security Analysis System, BeautifulSoup is used to parse the page. The find_all and find methods are employed to extract medium and high-risk alarm information. For the crawled information that contains formatting errors or unwanted symbols, further cleaning is performed using regular expressions[7]. Information such as trigger time, destination IP, source IP, alarm category, and alarm level is extracted. Finally, the processed and integrated alarm information is pushed to the network duty officer by calling the WeChat public account interface.

3.3 WeChat Alert Push

To enable network duty officers to promptly receive alerts identified by the Colasoft Total Network Traffic Security Analysis System, the abnormal IP monitoring and blocking software, based on Selenium web crawling technology, uses the WeChat Official Account method to push alert information to

Table 1 Test account interface permissions

Category	Function	Interface	Maximum Number of Calls Per Day/Times
Dialogue service	Basic support	Get access_token	2000
		Get the IP address of WeChat server	No upper limit
	Receive a message	Verify the authenticity of the message	No upper limit
		Receive ordinary messages	No upper limit
		Receive event push	No upper limit
		Receive speech recognition results	No upper limit
	Send a message	Automatic reply	No upper limit
		Customer service interface	500,000
		Group sending interface	Details
		Template Message (Business Notification)	100,000
	User management	User grouping management	Details
		Set the user comment name	10000
		Get basic user information	500,000
		Get a list of users	500
		Get the user's geographic location	No upper limit

the duty officers. Since the WeChat Official Account test account provides access to almost all official account interfaces and has a daily call limit of 2,000, which meets the demand [8, 9], this paper utilizes a test account to implement the alert information push function. The interface permissions of the test account are shown in Table 1.

In the development process of the WeChat Official Account platform, the basic interfaces primarily include obtaining the access_token and the server IP address. The access_token is a unique secret key that allows developers to call various interface services of the WeChat Official Account platform, and it is refreshed every two hours by default. To obtain the access_token, the AppID and AppSecret of the official account must be retrieved from the

Table 2 Interface call request description

Request mode	GET
Request address	https://api.weixin.qq.com/cgi-bin/token?grant_type=client_credential &appid=appID&secret=appsecret
Parameter description	appID and appsecret are WeChat authentication credentials for developers

developer center page. The program then calls the interface shown in Table 2 to obtain the access_token [10, 11].

According to the WeChat Developer Documentation, response messages are categorized into two types: passive responses and customer service messages. This paper utilizes the customer service message interface to send messages to network duty officers by POSTing a JSON data packet, thereby implementing the push function for alert information. The message template is as follows:

Alert category: {{sort.DATA}}
Trigger time: {{time.DATA}}
Source IP address: {{source.DATA}}
Destination IP address: {{target.DATA}}
Attack type: {{attack.DATA}}
Blocking device: {{equipment.DATA}}
Alert level: {{level.DATA}}

3.4 Verification Code Identification

The abnormal IP monitoring and blocking software based on Selenium web crawling technology requires CAPTCHA recognition when simulating login to the Leadsec Anti-Virus Gateway System and the Topsec Next-Generation Firewall, as the CAPTCHA changes each time the system is accessed. Currently, OCR (Optical Character Recognition) technology is rapidly developing and maturing, with stable and efficient options such as Baidu OCR, Tencent OCR, Wentong OCR, and Alibaba Cloud OCR available in China [12, 13]. This paper implements character extraction from CAPTCHA images using the Baidu OCR API. To use the Baidu OCR API, one must apply for an AppID, API Key, and Secret Key from Baidu Intelligent Cloud.

(1) Get the verification code picture

There are usually two ways to obtain CAPTCHA images. One method is to extract the CAPTCHA image link, but sometimes the content of the current

CAPTCHA and the CAPTCHA accessed via the URL link do not match. The other method is to use Selenium to take a screenshot of the visible area and then crop the image using the Image tool based on the position and size of the CAPTCHA element, saving the CAPTCHA image locally. Since the CAPTCHA changes when accessed via the URL link in the Leadsec Anti-Virus Gateway System and the Topsec Next-Generation Firewall System, which can lead to failed system logins, this paper adopts the second method for obtaining CAPTCHA images. The code for capturing the CAPTCHA image is as follows:

```
# Get the coordinates of the verification code relative to the entire HTML page
captchaX = int(captchaElem.location['x'])
captchaY = int(captchaElem.location['y'])
# Get CAPTCHA picture width and height
captchaWidth = captchaElem.size['width']
captchaHeight = captchaElem.size['height']
captchaRight = captchaX + captchaWidth
captchaBottom = captchaY + captchaHeight
# Capture the picture
imgObject = Image.open(_file_url)
imgCaptcha = imgObject.crop((captchaX, captchaY, captchaRight, captchaBottom)) # Crop
```

(2)Picture character recognition

Since the CAPTCHA image is a color image, it is first converted to grayscale, where the R (Red), G (Green), and B (Blue) components are made equal to filter out some interfering information. The originally three-dimensional pixel descriptions are mapped to one-dimensional descriptions. Common algorithms for image grayscaling include the maximum method, average method, and weighted average method. The grayscaled image is then binarized, converting the grayscale image signal into a binary image signal consisting only of black (1) and white (0), further separating the text from the background. Binarization methods can be divided into local threshold binarization and global threshold binarization. Character segmentation is used to cut each character in the binarized image into individual character images. Typically, each individual character forms a connected image region. In the character recognition process, by obtaining the starting and ending positions of each connected region's rows and columns, the minimum bounding rectangle of the character can be obtained, achieving the purpose

of character segmentation. Finally, the CAPTCHA characters are extracted through feature extraction and recognition modules.

This paper chooses Baidu OCR for CAPTCHA character recognition and calls the general text recognition API provided by Baidu OCR service to recognize the character information in the image.

3.5 Database Interaction

To prevent the business system from being unable to communicate with the outside world due to IP blocking and to promptly locate and identify issues, this paper uses a MySQL database to store information on abnormal IP operations. Accessing a MySQL database from Python is simple and flexible, with Pymysql serving as the data interface API for interaction between the two. The Connect(parameters) function establishes a connection between the client and the database, and the Cursor object provides the ability to browse data in one or more rows, allowing users to process data at specified locations. Among these, the execute() method is the most important method of the Cursor object, enabling the addition, modification, and deletion of data in database tables [14–16].

The code for inserting data is as follows:

```
# Connect to the database
db=pymysql.connect(host='localhost',user='test123987456', passwd=
'test123!@#', db='pytest')
#Inserts the record
cursor=db.cursor()
cursor.execute('INSERT INTO table_safe(S_IP, B_IP, Type, Name,
Equipment, Time) VALUES ('%s','%s','%s','%s','%s','%s') %(txt_source,
txt_ip, txt_type, txt_name, txt,txt_time));
db.commit() # Commit to database for execution
```

The design of the abnormal IP database table primarily records the local IP, blocking IP, attack type, operator, blocking equipment, and operation time. The blocking abnormal IP information is shown in Table 3.

4 Application Results

The abnormal IP monitoring and blocking software, based on Selenium web crawling technology, uses PyCharm as the integrated development environment, Python as the programming language, and MySQL as the

Table 3 Block illegal IP information table

Table Name: Table_ip				
Logical Name	Field Name	Data Type	Whether it is a Primary Key	Default Value
Serial number	ID	INT	YES	NONE
Local IP	S_IP	VARCHAR	NO	NONE
Blocking IP	B_IP	VARCHAR	NO	NONE
Attack type	Type	VARCHAR	NO	NONE
Operator	Name	VARCHAR	NO	NONE
Blocking device	Equipment	VARCHAR	NO	NONE
Operation time	Time	DATETIME	NO	NONE

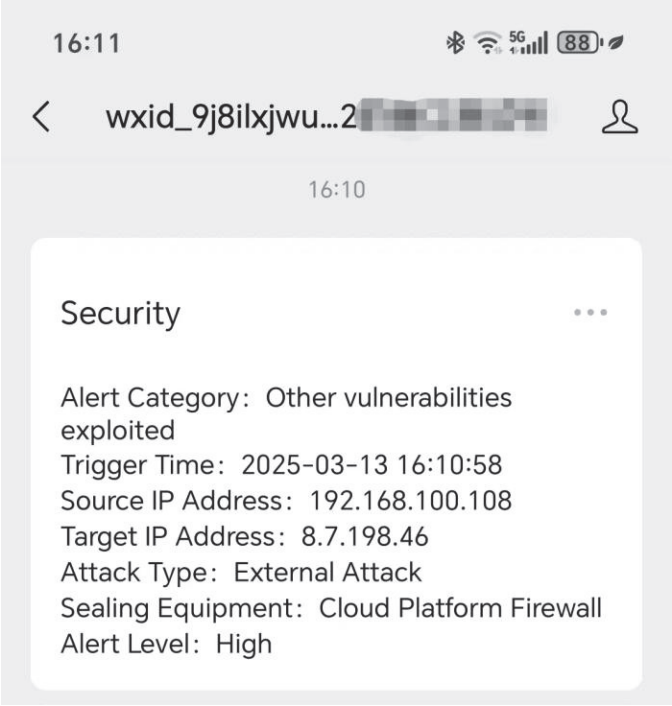

Figure 7 Alarm information push map.

database. It is deployed on the Windows 10 operating system. Since its deployment, the software has effectively pushed high-risk alert information from the network full-traffic security analysis system. This includes alert category, alert trigger time, source IP address of the attack, target IP address,

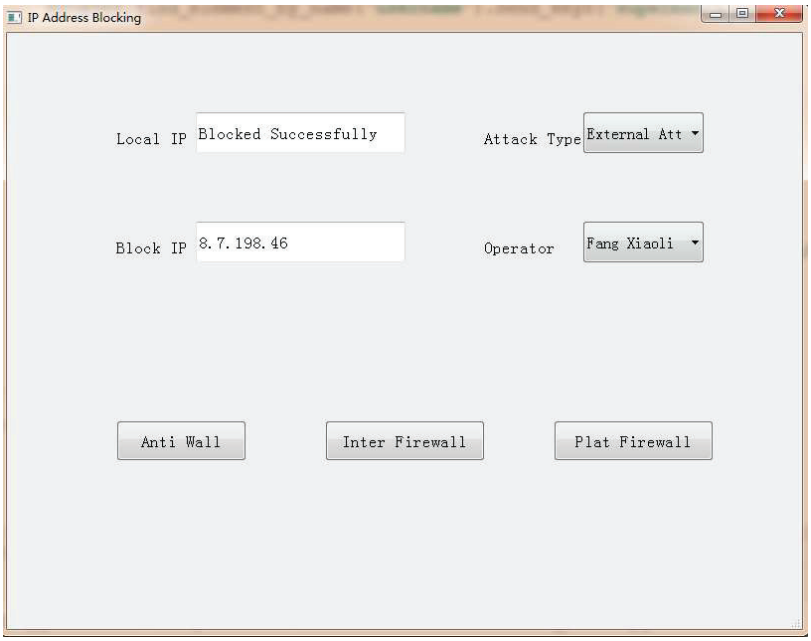

Figure 8 Blocking success information diagram.

attack type, recommended blocking device, and alert level, as shown in Figure 7.

The network duty officer receives alert information pushed by the WeChat public account and confirms with the business system manager whether the communication between the 'abnormal IP' and the local IP is for normal business needs. If the behavior is determined to be a malicious attack, the duty officer can input the relevant information into the software and click a button. The software will then automatically open the Chrome browser to simulate logging into the security device system and complete the blocking operation of the abnormal IP in the firewall. The software automatically carries out the blocking operation, and the local IP input box will display a message indicating either 'Blocking Successful' or 'Blocking Failed,' as shown in Figure 8, to help the duty officer understand the result of the operation. Additionally, the duty officer can view information related to abnormal IP blocking in the database table using Navicat Premium software, with some of the information shown in Table 4.

Table 4 Database information table

S_IP	B_IP	Type	Name	Equipment	Time
192.168.100.106	120.39.55.42	Under attack	Fang Xiaoliang	Internet firewall	2025/02/00 13:30:11
192.168.100.123	125.117.145.25	Under attack	Fang Xiaoliang	Internet firewall	2025/02/22 21:30:51
192.168.100.106	175.43.172.249	Under attack	Fang Xiaoliang	Internet firewall	2025/02/24 03:30:33
192.168.100.113	180.122.145.216	Under attack	Fang Xiaoliang	Internet firewall	2025/02/24 16:30:17
192.168.100.106	183.165.129.132	Under attack	Fang Xiaoliang	Internet firewall	2025/02/25 21:40:15
192.168.100.228	183.165.129.132	Under attack	Fang Xiaoliang	Internet firewall	2025/02/26 17:40:36
192.168.100.106	42.4.118.213	Under attack	Fang Xiaoliang	Internet firewall	2025/02/27 06:40:18
192.168.0.8	223.5.5.5	Under attack	Fang Xiaoliang	Anti-virus wall	2025/02/27 11:20:29
192.168.0.5	223.6.6.6	Under attack	Fang Xiaoliang	Anti-virus wall	2025/02/27 19:30:59
192.168.56.176	123.130.122.240	Under attack	Yin Yuzhen	Anti-virus wall	2025/02/28 12:20:47
192.168.100.106	39.71.241.90	Under attack	Yin Yuzhen	Internet firewall	2025/02/28 16:20:56
192.168.100.106	117.24.80.127	Under attack	Fang Xiaoliang	Internet firewall	2025/02/28 22:30:29
192.168.100.225	101.74.2.199	Under attack	Yin Yuzhen	Internet firewall	2025/03/01 10:30:09
192.168.100.106	122.241.216.51	Under attack	Yin Yuzhen	Internet firewall	2025/03/01 13:30:40
192.168.100.168	125.117.140.27	Under attack	Yin Yuzhen	Internet firewall	2025/03/01 21:40:02
192.168.100.106	183.165.128.76	Under attack	Yin Yuzhen	Internet firewall	2025/03/02 09:40:35
192.168.100.133	222.79.55.86	Under attack	Yin Yuzhen	Internet firewall	2025/03/02 13:40:04
192.168.2.17	52.80.52.30	Under attack	Cao Qi	Anti-virus wall	2025/03/03 15:50:42
192.168.100.106	8.142.97.33	Under attack	Yin Yuzhen	Internet firewall	2025/03/04 8:20:49
192.168.0.180	124.132.134.162	Under attack	Yin Yuzhen	Anti-virus wall	2025/03/04 15:40:34
192.168.100.106	118.123.247.233	Under attack	Yin Yuzhen	Internet firewall	2025/03/05 9:00:50
192.168.0.2	124.128.85.194	External attack	Yin Yuzhen	Anti-virus wall	2025/03/05 10:30:36
192.168.100.106	8.142.110.216	Under attack	Yin Yuzhen	Internet firewall	2025/03/06 7:50:15
192.168.100.136	211.149.208.173	Under attack	Fang Xiaoliang	Internet firewall	2025/03/06 20:40:23
192.168.100.106	123.114.100.125	Under attack	Fang Xiaoliang	Internet firewall	2025/03/07 11:40:58
192.168.100.228	118.195.149.112	Under attack	Fang Xiaoliang	Internet firewall	2025/03/07 19:40:18
192.168.0.21	98.197.25.34	Under attack	Fang Xiaoliang	Anti-virus wall	2025/03/08 09:20:29
192.168.0.8	36.156.170.134	Under attack	Fang Xiaoliang	Anti-virus wall	2025/03/08 13:30:59
192.168.56.176	112.119.183.68	Under attack	Yin Yuzhen	Anti-virus wall	2025/03/08 23:20:47
192.168.100.133	139.196.168.100	Under attack	Yin Yuzhen	Internet firewall	2025/03/09 02:00:56
192.168.100.106	117.72.10.184	Under attack	Fang Xiaoliang	Internet firewall	2025/03/09 07:30:29
192.168.100.106	124.133.255.174	Under attack	Yin Yuzhen	Internet firewall	2025/03/10 19:50:09
192.168.100.228	60.13.6.201	Under attack	Yin Yuzhen	Internet firewall	2025/03/11 15:00:40
192.168.100.106	92.255.57.58	Under attack	Fang Xiaoliang	Internet firewall	2025/03/11 21:40:23
192.168.100.106	223.113.128.228	Under attack	Fang Xiaoliang	Internet firewall	2025/03/12 10:40:58
192.168.59.115	51.254.71.191	Under attack	Yin Yuzhen	Anti-virus wall	2025/03/12 13:30:56
192.168.100.108	8.7.198.46	External attack	Yin Yuzhen	Cloud platform firewall	2025/03/13 16:10:28

5 Conclusion

Addressing issues such as the inability to share and synchronize information among network security devices, the delay in detecting malicious network attacks, and the complex process of blocking abnormal IPs at the Shandong Earthquake Administration, this paper presents abnormal IP monitoring and blocking software based on Selenium crawler technology. The software uses web crawling technology to obtain real-time defense information from

the Colasoft Network Total Traffic Security Analysis System and promptly pushes it to network operation and maintenance administrators via a WeChat public account. On-duty personnel only need to input information such as the IP to be blocked, and with a single click, the complex steps for blocking abnormal IPs are automatically executed. Additionally, the operation information is stored in a MySQL database, ensuring one record per blocking for easy future querying and traceability, thereby safeguarding the normal operation of the earthquake business system. Since the software's launch, it has pushed 55 high-level alerts via WeChat. After verification with the business department, 37 abnormal IPs were required to be blocked, with 3 login failures due to incorrect system CAPTCHA recognition. A total of 37 abnormal IPs were blocked on the firewall. The software boasts a 100% success rate in pushing alert information via WeChat, a 90.32% success rate in simulating login to the firewall system, and a 100% success rate in blocking abnormal IPs on the firewall. In the early experimental stage, the software encountered errors in the CAPTCHA recognition process during the simulation of logging into the firewall system, resulting in some login operations failing. However, the actual test data shows that the login success rate is currently 90.32%, with room for improvement. The next step will focus on introducing advanced algorithms, such as machine learning, to further optimize the recognition engine, significantly improving recognition accuracy. This will ensure smoother and more reliable system login processes, further enhancing overall usability.

The software, leveraging Selenium-based web crawling technology, implements real-time monitoring of network attack behaviors in intrusion detection systems and intelligently blocks malicious attacks on firewalls and other network security devices. It achieves coordinated responses among security devices, addressing issues such as the lack of device information sharing and the complexity of manual operation processes. The software stores information related to the blocking of malicious attacks and pushes notifications via WeChat Official Accounts, resolving problems related to untraceable blocking records and the difficulty of issue traceability, thereby preventing disruptions to the normal operation of earthquake-related business systems. In traditional manual operations, on-duty personnel typically take an average of 3 hours to block abnormal IP addresses, resulting in significant response delays and leaving ample opportunity for potential threats to exploit vulnerabilities. The application of this software significantly reduces the average duration of this critical security action to 10 minutes, increasing efficiency by up to 17 times, and greatly enhancing the real-time

containment capability of network threats. A comprehensive analysis reveals that the software provides timely identification of abnormal IPs, automated blocking of abnormal IPs, and traceability of abnormal IP blocking events. It effectively pushes high-risk alert information from network-wide traffic security analysis systems and blocks abnormal IPs on network security devices, ensuring both the integrity and independence of interconnected device functions. Furthermore, it establishes a cyclic protection model of 'prevention-detection-response-re-prevention,' enhancing the timeliness and effectiveness of detecting and blocking network malicious attacks, while enabling rapid responses to overall network security incidents. However, the success rate of simulated login systems and the level of full automation in business processes require improvement to further enhance the timeliness of security protection. These improvements will contribute more significantly to the development of informatization in earthquake prevention and disaster reduction.

Acknowledgment

Supported by the Monitoring and Early Warning Task of the China Earthquake Agency (CEA-JCYJ-202501037), the Key Task for Young Professionals in Earthquake Information of the China Earthquake Agency (CEA-ITNS-2025), and the Shandong Earthquake Agency.

References

[1] Yang Y, Chen Y D, Zhao R, et al., 2025. A review of active defense research in network security. Science Technology and Engineering, 25(07), 2654–2663.

[2] Bai B X, Tan Y M, Wang Sh, et al., 2020. Research on Mass Prediction and Disaster Prevention Information Reporting System based on B/S Architecture[J]. Journal of Disaster Prevention and Mitigation Engineering, 40(3):447–452.

[3] Wang M, Ma S Sh, Zhao Y L, et al., 2015. Selenium-based application inspection automation service[J]. Application of Electronic Technique, (S1):64–66.

[4] Huang Q, 2018. User-authority Automated Configuration of The Power Marketing System Based on Selenium[J]. Computer Applications and Software, 35(4):187–190.

[5] Zeng J R, Zhang Y S, Zheng J, et al., 2019. Implementation Technology and Application of Web Crawler for Multi-data Sources[J]. Computer Science, 46(5):304–309.
[6] Zhu J Y, 2023. Design and Implementation of Selenium based Automated Testing Framework[D]. Zhenjiang: Jiangsu University of Science and Technology.
[7] Li Ch H, 2021. Implementation and Performance Comparison of Crawler Web Page Automatic Processing Based on BeautifulSoup + requests and selenium[J]. Modern Information Technology, 16(5):10–13.
[8] Zheng Y, Yang T Q, Wang Q P, et al, 2021. MQTT-based Design and Implementation of Automatic Earthquake Thematic Map Generation and Push System[J]. Earthquake Research in China, 37(4):837–842.
[9] Yu Y Ch, Wang Y J, Wan X Ch, 2020. Realization of Accurate Intelligent Early-Warning Push Technology Based on WeChat[J]. Meteorological Science and Technology, 48(2):195–199.
[10] Cheng W Zh, 2013. Design and Implementation of School Library Service System Based on WeChat[D]. Chengdu: School of Information and Communication Engineering.
[11] Ding X G, Zhai H G, He Y, 2021. Design and Implementation of Operation Monitoring for Unmanned Stations Based on WeChat Applet[J]. Technology for Earthquake Disaster Prevention, 16(4):754–762.
[12] Wang D Q, Wushouer S, Xu M M, 2020. Review of Research on Scene Text Recognition Technology[J]. Computer Engineering and Applications, 56(18):1–15.
[13] Zhang T T, Ma M D, Wang D Y, 2020. Research on OCR Technology[J]. Computer Technology and Development, 30(4):85–88.
[14] Li Zh H, Jin X, Li H, et al., 2021. Design and implementation of the publishing system for WAMP-based earthquake science information database[J]. China Earthquake Engineering Journal, 43(5):1214–1219.
[15] Zhang Y, Lu Q, Lu X, et al., 2023. Design and Implementation of Research Paper Management System Based on MySQL. Microcomputer Applications, 39(01), 4–6+10.
[16] Cai Y, Zhang M, Zhao R, et al., 2019. Research on the Earthquake Early Warning Information Rapid Release System[J]. Technology for Earthquake Disaster Prevention, 14(1):247–258.

Biographies

Yin Yuzhen, graduated from Hohai University with a master's degree in Communication and Information Systems. I am currently mainly responsible for information technology construction such as network security. In the past five years, I have participated in 4 national and provincial level projects, been responsible for 2 provincial and bureau level projects, published 2 academic papers, and obtained 2 software copyrights.

Fang Xiaoliang, female, graduated from Southwest University with a master's degree. She is mainly responsible for network security construction, leading or participating in 3 provincial and ministerial level projects, 2 departmental and bureau level projects, and publishing 3 scientific research papers.

Zhang Wei, female, graduated from Heilongjiang University with a master's degree. She is mainly responsible for network security construction, leading or participating in one department level project, and publishing one scientific research paper.