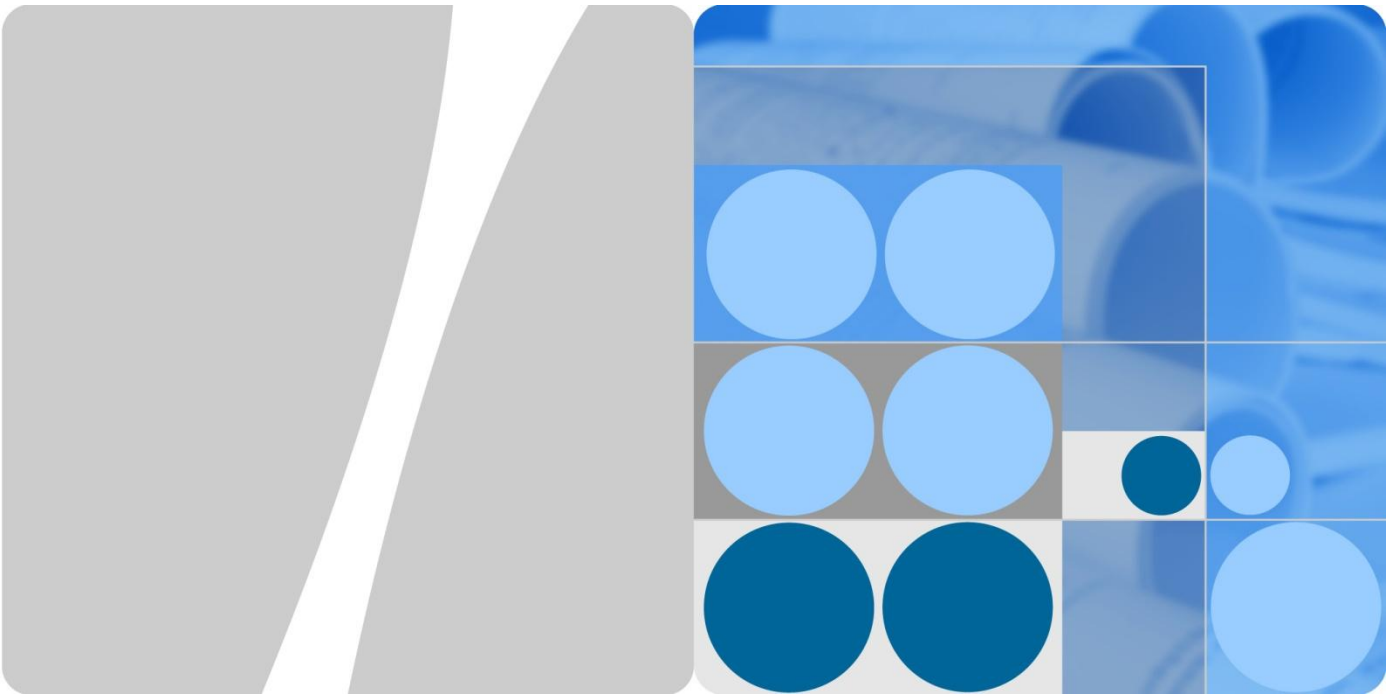


HUAWEI USG6000 Series Next-Generation Firewall Intelligent Management Technical White Paper

Issue 1.1

Date 2014-03-13

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: http://www.huawei.com

Email: support@huawei.com

About This Document

Keywords

NGFW, intelligent management, traffic learning, policy optimization

Abstract

This technical white paper describes the implementation principles and solutions of the NGFW intelligent management feature. The intelligent learning, policy suggestions, and analysis technologies of this feature simplify the Next-Generation Firewall (NGFW) management and reduce the total cost of ownership (TCO) by 30%.

Acronym and Abbreviation	Full Spelling
NGFW	Next Generation Firewall
DLP	Data Leakage Prevention
IPS	Intrusion Prevention System
AV	Antivirus

Contents

1 Technical Background

Increasingly complex network environments: Hackers have been industrialized to hack for illegal gains, and new attacks, such as Advanced Persistent Threat (APT), emerge one after another. Therefore, enterprises must implement strictest security policies. Enterprises must apply the minimum authorization principle to allow only necessary applications and perform in-depth defense based on application risks. For example, enterprises can allow employees only to receive and send emails and perform content filtering on outgoing emails and virus scanning on email attachments.

Challenges facing firewall administrators: Traditional firewalls provide port-based protection, and the number of managed ports is less than 100. NGFWs provide application-based protection. Thousands of applications to be managed increase management complexity, making it difficult to meet the minimum authorization principle during policy configuration. The complex firewall management proposes higher requirements for administrators. First, administrators must be familiar with massive applications to configure specific control and security policies. Second, manual configuration is inefficient and error-prone and may generate redundant or inefficient policies that are difficult to discover. Third, manual configuration cannot adapt to changing requirements. A well-functioned policy may not work well after a few months. The administrators must be aware of new issues timely and adjust the policies.

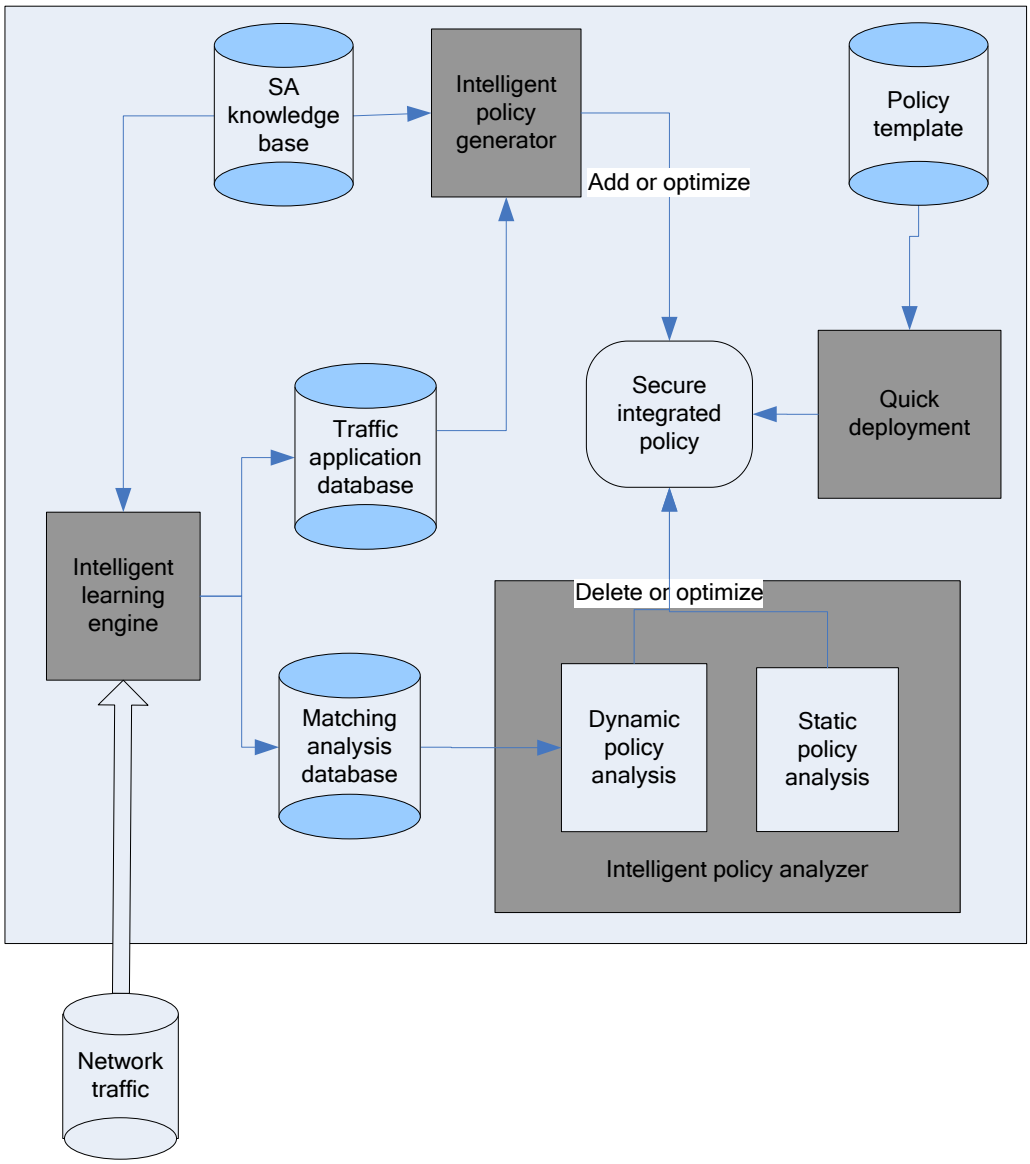
Demand for intelligent management: A simple, efficient, and adaptive policy management technology is required to solve current management issues and challenges of NGFWs. Huawei's innovative intelligent management technology, which is described in the following part, simplifies the NGFW management and reduces the TCO by 30%.

2 Concept and Principle

2.1 Intelligent Management Concept

Intelligent management is a systematic solution for policy management and is simple, efficient, and adaptive. As shown in Figure 2-1, this solution consists of four components: intelligent learning engine, intelligent policy generator, intelligent policy analyzer, and quick policy deployment. The intelligent learning engine component learns network traffic, analyzes the traffic intelligently, and obtains application types and policy matching information. The intelligent policy generator component provides suggested security policies based on learned network applications and risks. The intelligent policy analyzer component uses static and dynamic analysis methods to identify existing redundant and inefficient policies to help administrators streamline firewall policies. Administrators can use the quick deployment module to use predefined policy templates and configure security policies quickly. The intelligent management organizes these components to solve the issues that the NGFW policy management faces.

Figure 2-1 Intelligent management operating principle

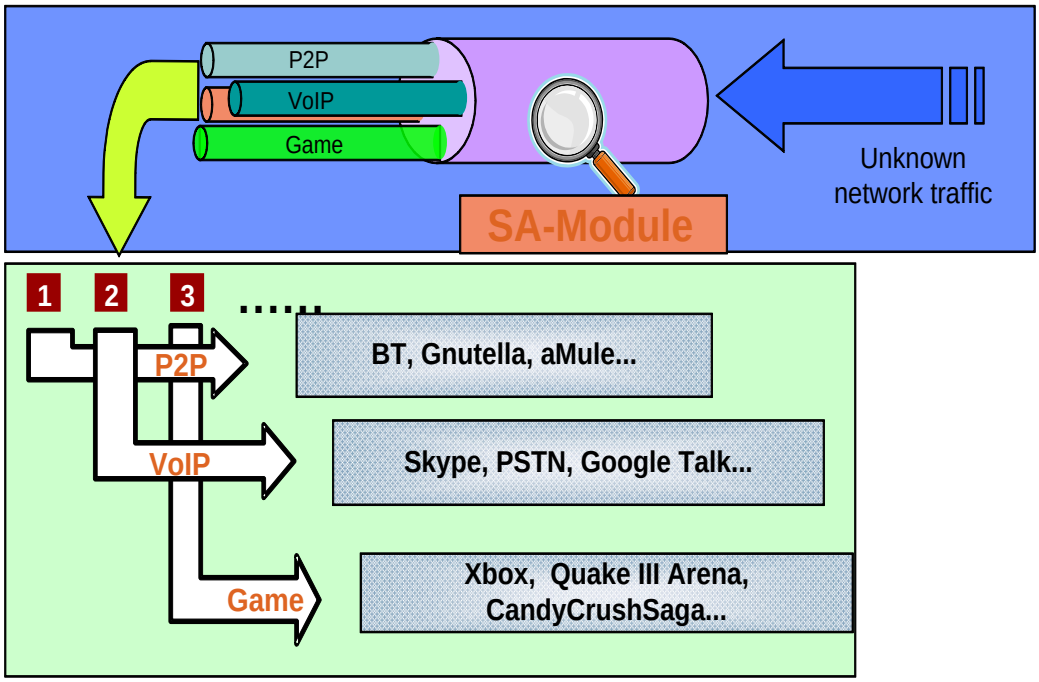


2.2 Mechanism of the Intelligent Learning Engine

The intelligent learning engine collects the sample of network traffic in real time, uses the leading Huawei application service awareness (SA) technology to identify applications carried in the network traffic and policy matching statistics, and saves the result in to the database.

2.3 Application SA technology

Figure 2-2 Deep packet identification technology



As shown in Figure 2-2, The SA module identifies unknown network traffic. The SA module identifies packet types, extracts the signature, payload length, content or length change pattern, IP address, and port. Then, the SA module accurately classifies traffic based on the extracted information and the packet correlation.

Huawei cloud security competence center, by virtue of its experience and expertise, provides an SA knowledge database of more than 6000 applications. The USG6000 series can use the SA identification engine and online update of the signature database to identify the latest applications.

2.4 Mechanism of the Intelligent Policy Generator

The intelligent policy generator generates optimized security policies automatically. The generator analyzes the types of allowed applications in a policy, identifies the applications that are unused in a long period as unnecessary, analyzes risk level (such as malware infected, data leak risk, exploitable) of allowed applications based on the predefined application risk database and provides suggested policies to help administrators optimize firewall policies. The intelligent policy generator is based on the following technologies:

- Integrated policy technology

  Huawei USG6000 series uses the integrated policy technology to analyze traffic in six dimensions, including application, content, time, user, attack, and location and implements comprehensive network protection to identify hidden threats and perform refined control and defense.
- Application risk evaluation technology

Huawei USG6000 series uses Huawei application risk evaluation technology to evaluate application risk levels, such as malware infected, data leak risk, exploitable, rates risks, and delivers the SA knowledge base to each NGFW using Huawei cloud security center.

- Deep defense technology

  The intelligent management uses the leading deep defense technologies provided by Huawei security competence center, including AV scanning, IPS, URL filtering, content filtering, application behavior control, and email filtering, to minimize the risks.

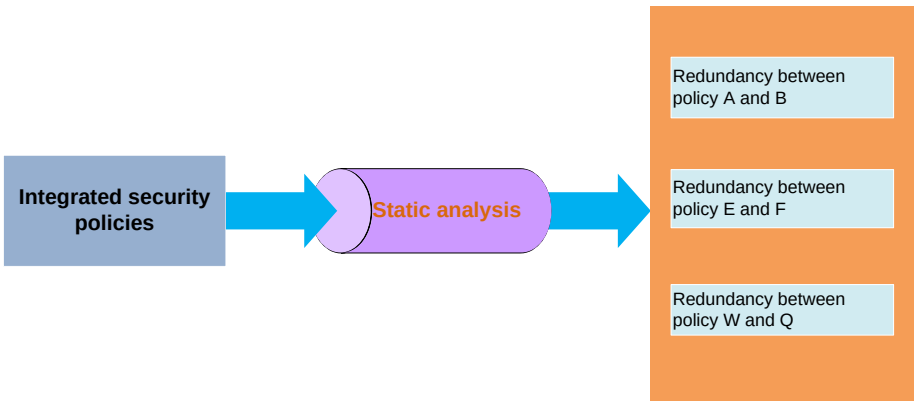
2.5 Mechanism of the Intelligent Policy Analyzer

Some policies may become invalid and redundant due to frequent manual configurations. If not eliminated promptly, the number of such policies will keep rising, increasing policy maintenance complexity. The intelligent policy analyzer analyzes existing policies, identifies redundant and inefficient policies, and helps administrators to streamline policies. The intelligent policy analyzer uses the static and dynamic analysis technologies to detect redundant and inefficient policies.

- Static analysis technology

  Huawei USG6000 series provides the static analysis technology to simplify the policy maintenance without using third-party software. The static analysis technology compares the configurations of existing firewall policies, identifies the redundant policies, and helps administrators to optimize the policies. As shown in Figure 2-3, the redundancy analyzing module abstracts the configurations of all policies and compares the configurations for redundant policies.

Figure 2-3 Operating principle of the static analysis technology



- Dynamic analysis technology

  Huawei USG6000 series uses the dynamic analysis technology to analyze the matching condition of network traffic, identifies invalid policies, and helps administrators to adjust existing policies.

2.6 Mechanism of the Quick Policy Deployment Component

Huawei provides predefined security policy templates based on typical network management and control behaviors of enterprises. Administrators can choose a most suitable template and modify it to create policies for their needs.

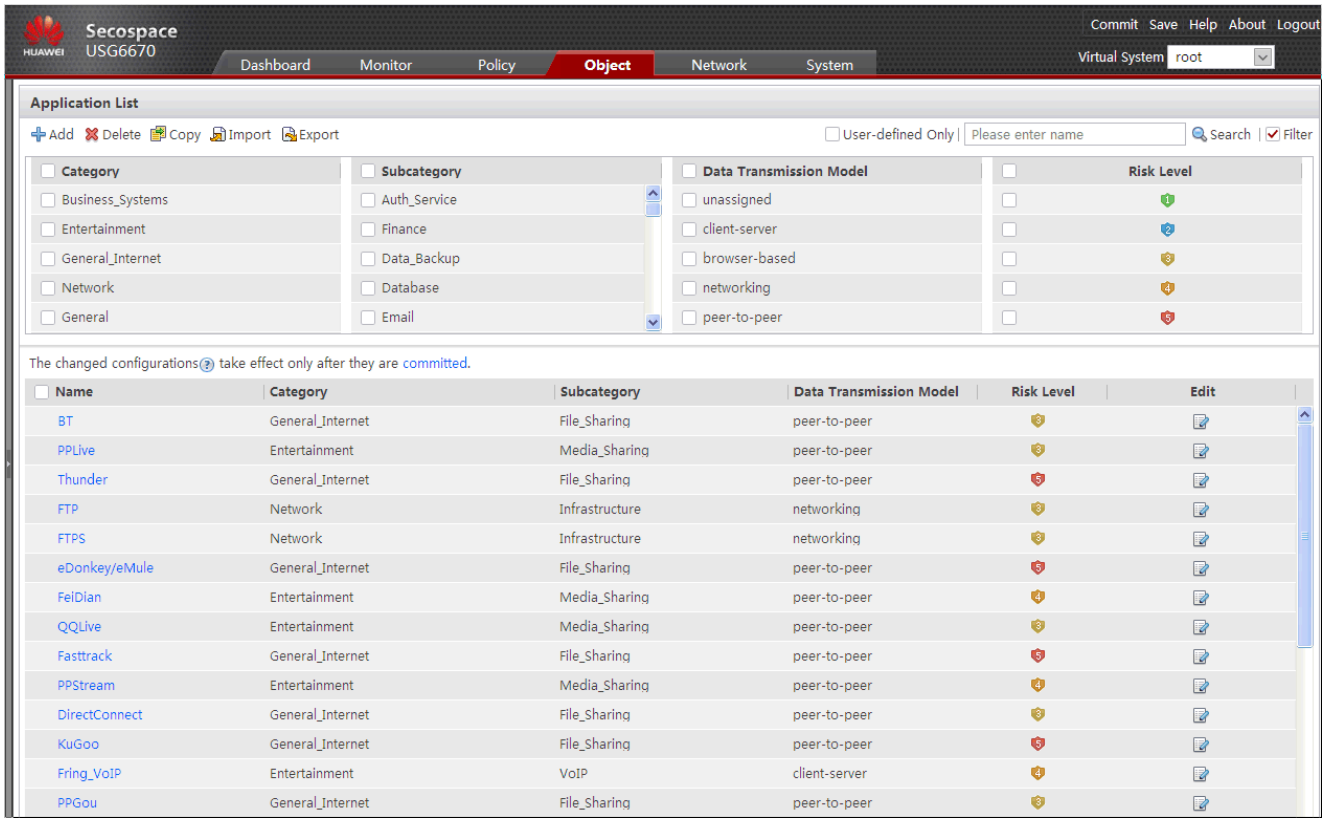
3 Service and Function

3.1 Quick Deployment

Small- and medium-sized enterprises (SMEs) do not have high requirements on refined application defense, and therefore, the IT administrators in these enterprises usually hold concurrent posts. Some enterprises may have no administrators at all.

The intelligent management provides a quick policy deployment component for theses enterprises. An administrator needs only to reference the predefined policy templates and generate a practical integrated policy, as shown in Figure 3-1.

Figure 3-1 Policy template function

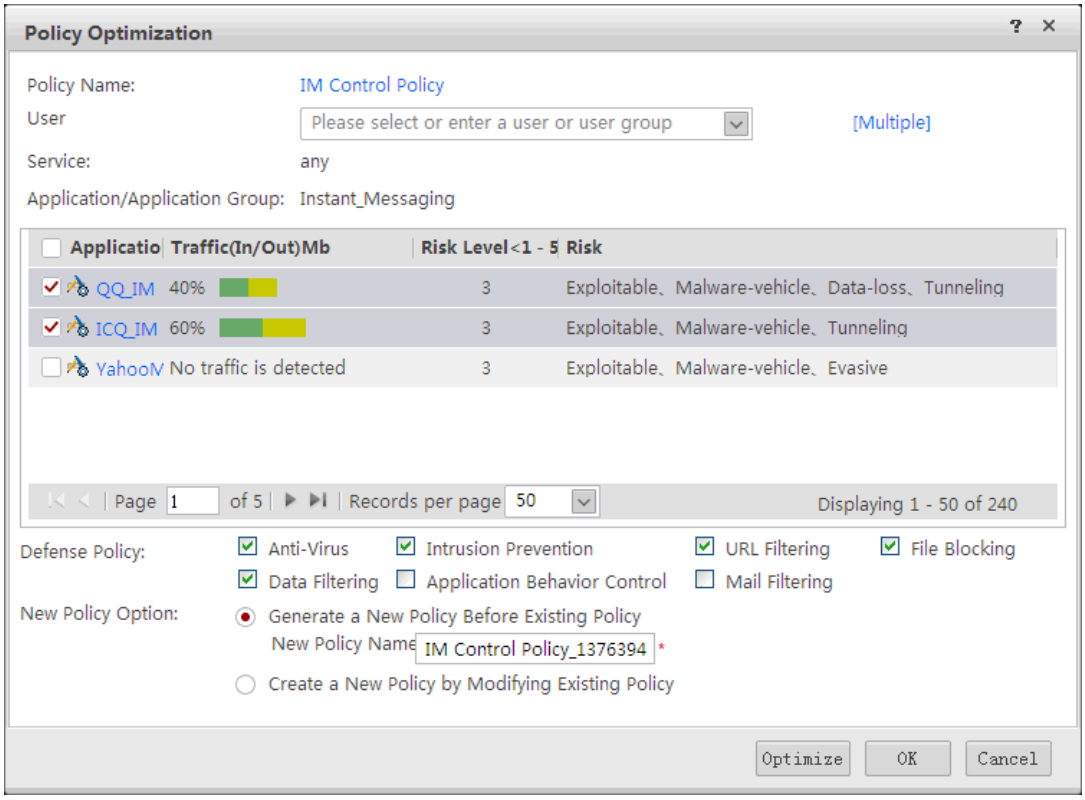


The quick policy deployment component greatly facilitates the policy deployment of SMEs and enables administrators to configure integrated policies easily.

3.2 Security Defense Based on Applications

The firewall management must comply with the minimum authorization principle for network security. Traditional firewall policies perform defense based on ports, which breaches the minimum authorization principle. For example, port 80 can carry HTTP application and email applications. To allow employees to access HTTP applications, port 80 must be enabled, and unwanted applications that use the same port are also allowed. Therefore, the USG6000 series allows administrators to fine-tune policies to allow only necessary application and block unwanted applications, even when they use the same port, as shown in Figure 3-2.

Figure 3-2 Policy tuning function



For the migration of port-based policies, the intelligent management learns the network traffic, identifies applications permitted by policies, displays the result for administrators, and helps the administrators configure security policies based on applications to replace the port-based policies. For the risks in identified applications, the policy tuning function provides tuning suggestions to administrators, and prompts administrators to use related deep defense technologies.

For the scenario of improper authorization of application-based policies, the intelligent management learns the network traffic, identifies applications types, displays the result to administrators, and helps the administrators narrow down the scope of permitted applications. For the risks in identified applications, the policy tuning function provides tuning suggestions to administrators.

The policy tuning function effectively simplifies the management based on applications, provides proper deep defense suggestions to prevent risks in applications, and secure the access of legitimate applications.

3.3 Policy Streamlining

Firewalls generate massive useless and redundant policies over time. Even advanced administrators find it difficult to discover these policies. Because there is no effective method to discover these policies, the increase of useless and redundant policies brings more difficulty for maintenance. Customers have to pay extra money for third-party redundant policy analysis software.

To solve this issue, the intelligent management solution provides the policy streamlining function. This function helps administrators identify redundant policies (shown in Figure 3-3) and invalid policies.

Figure 3-3 The redundancy analysis function