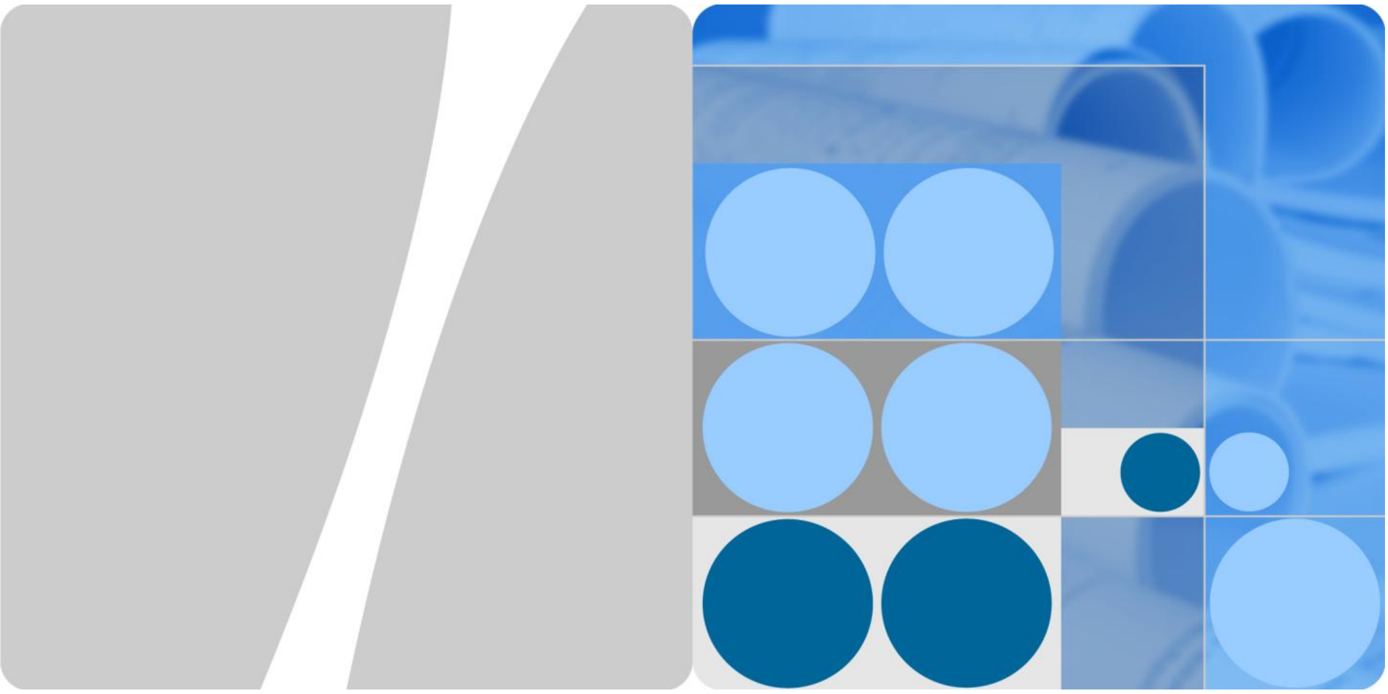


HUAWEI USG6000 Series Next-Generation Firewall

ACTUAL Awareness Technical White Paper

Issue	**V1.1**
Date	**2014-03-14**

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

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

Contents

HUAWEI Secospace USG6000 Series

ACTUAL Awareness Technical White Paper

Keywords: NGFW, ACTUAL awareness

Abstract: This document describes the implementation mechanisms and solutions of the ACTUAL awareness technology.

Acronym and Abbreviation	Full Spelling
NGFW	Next-Generation Firewall
ACL	Access Control List
DDoS	Distributed Denial of Service

1 Technical Background

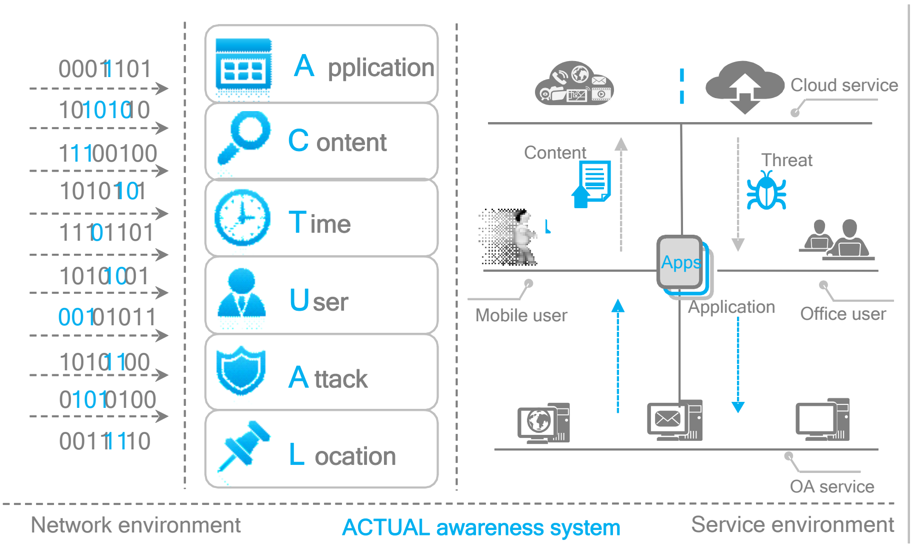
The development of computer network technologies and e-commerce brings about great convenience in human life and serious network security issues. Firewalls become the core devices that protect various networks. Networks are evolving into next-generation networks that feature explosive information growth, borderless network, mobile Internet, and Web2.0. Cybercriminals can easily penetrate a traditional firewall that uses quintuple ACLs by spoofing or using Trojan horses, malware, or botnets.

Under this background, Huawei USG6000 series provides an "ACTUAL" (Application, Content, Time, User, Attack, and Location) awareness technology to accurately control network traffic in a refined manner, defend against security threats, and ensure intranet security.

2 Definition and Mechanism

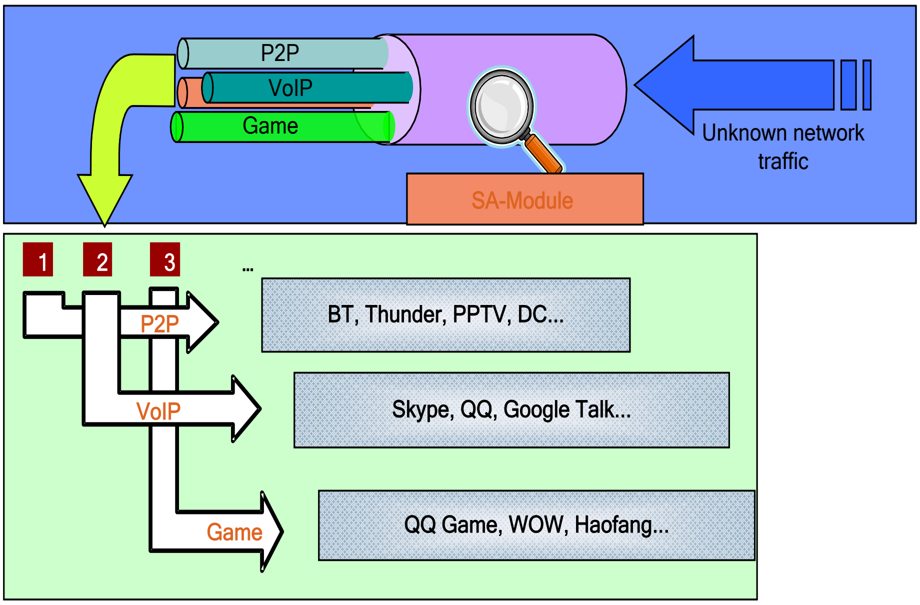
2.1 Definition

ACTUAL awareness is the capability of identifying network traffic by application, content, time, user, attack, and location. Based on the ACTUAL awareness results, you can configure security policies such as the filtering, route selection, traffic control, and NAT policies.



As shown in the previous figure, network traffic is complex. The administrator of a traditional firewall cannot accurately analyze or obtain real service traffic types, and cannot apply security policies to control network traffic. ACTUAL awareness of the USG6000 series analyzes the traffic of complex network environments, provides the administrator visibility into statistics on traffic by application, content, time, user, attack, and location, and helps the administrator configure security policies in a refined manner.

2.2 Application Awareness

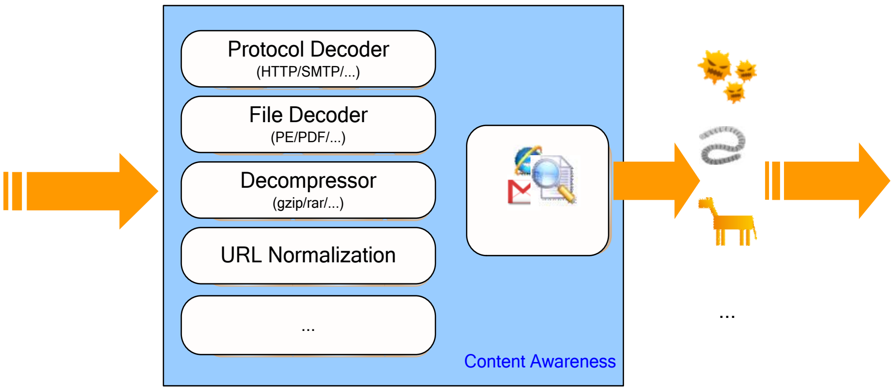


As shown in the previous figure, the application awareness module identifies unknown traffic and packet formats, extracts the signature, payload length, content or length change rule, IP address, and port of a packet, and incorporates statistics on and relationship of packets to accurately categorize applications of the traffic.

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

2.3 Content Awareness

The USG6000 series analyzes application protocols to obtain the content transmitted by the application protocols and applies security policies by content.



The content awareness module consists of a protocol decoding module and a content matching module. The protocol decoding module categorizes incoming packets by protocol, obtains information based on the category, decompresses and unpacks the obtained files, identifies real file types, sorts the obtained URLs, and sends them to the content matching module. The content matching module matches traffic information with virus signatures, intrusion rule signatures, sensitive information, and email contents and determines whether the traffic triggers security policies based on the matching results. The signatures can be updated on the cloud, or traffic information can be sent to the cloud for detection, which ensures the up-to-date and effectiveness of signatures.

2.4 Time Awareness

The USG6000 series implements time awareness based on the following technologies:

- Automatic clock synchronization

The USG6000 series uses Network Time Protocol (NTP) to obtain standard network time and adjust the local clock.

- Automatic conversion of DST

Some countries and regions use the DST system. The USG6000 series sets the DST clock based on the VRP, and the device clock is automatically switched with the DST clock.

- Time-specific security policy

The USG6000 series has integrated the time or time segment into the security, traffic control, and authentication policies as a matching condition and updates the policies by time or time segment to implement time-specific control. You can configure the USG6000 series to apply traffic control policies on network traffic by time segment.

2.5 User Awareness

Enterprise networks become borderless with increasing mobile office employees whose IP addresses are dynamically changed. The security policies of traditional firewalls are based on IP configurations, which cannot meet requirements on security management and control. How to accurately identify users and effectively manage and control user behaviors has become a top issue of network security.

User awareness of the USG6000 series identifies users of network traffic and implements security management and control by user.

2.5.1 User Authentication and Identification

User identification is the prerequisite of applying differentiated policies on users. The user management and control module provides multiple authentication modes to meet the requirements of different user types and scenarios.

- Authentication exemption

Upper executives require high efficiency and authentication exemption. However, their activities must be highly secure. You can bind their accounts to IP or MAC addresses and configure authentication exemption for them. The USG6000 series then exempts upper executives from authentication and allows the login only from the bound IP or MAC address.

Some enterprises have guests who may need to access the enterprise networks. The guests do not have dedicated accounts and cannot be authenticated. Therefore, their network access permissions must be controlled. To accommodate this situation, the user management and control module automatically creates temporary accounts for the guests with their IP addresses as user names.

- Password authentication

For common employees, password authentication is applied.

Users can access the URL of an authentication page before starting service access. The USG6000 series supports HTTP and HTTPS authentication. You are advised to choose HTTPS authentication to meet high security requirements.

The USG6000 series supports authentication based on user names and passwords. It can also interwork with the LDAP, RADIUS, and AD authentication servers and send user information to the authentication servers.

In addition, the USG6000 series supports redirected web authentication. When an unauthenticated employee accesses HTTP services, the USG6000 series redirects the user to an authentication page and prompts the user to get authenticated.

- Single Sign-On (SSO)

If an AD server with an identity authentication system has been deployed on a network, the USG6000 series can interwork with the AD server to implement SSO. After identifying that a user is authenticated by the AD server, the USG6000 series permits the user without requesting the user name and password.

If a user has used a VPN (such as an L2TP or SSL VPN) for access and the USG6000 series has authenticated the user, the USG6000 series normalizes the access user and the user whose online behaviors are managed to implement SSO and avoid re-authentication.

2.5.2 User-Specific Management and Control Policy

- Online user management and control

To restrict all online behaviors of some users within a time segment, you can lock out the online users.

You can also force some untrustworthy online users to log out.

- Policy management and control

The USG6000 series supports user-specific online behavior management that includes application-layer management and control functions, such as user-specific and quintuple-based behavior control, user-specific application-layer protocol control, user-specific URL access control, mail filtering, and file filtering by keyword or type. For example, you can forbid instant messaging tools such as Skype during working hours and forbid the access to certain game or forum URLs to ensure working efficiency.

The USG6000 series provides user-specific traffic management and control and limits the number of concurrent connections by user to effectively allocate and manage bandwidth resources. The USG6000 series can audit and analyze the traffic statistics of users and user groups for follow-up optimization.

The USG6000 series provides reports, such as user-specific traffic rankings by category and time

Users can inherit management and control policies from user groups, and the user groups can inherit the policies from parent user groups.

2.6 Attack Awareness

Attack awareness of the USG6000 series identifies network security events and content security events and incorporates the awareness results of attack events, attack behaviors, and abnormal traffic into the reports of unified security policies and security postures. Attack awareness enables the USG6000 series to defend against attack behaviors and provides administrators and CIOs visibility into security postures for accurate understanding.

Huawei security R&D team has sustained accumulation of attack awareness technologies as follows:

- DoS/DDoS Detection and Defense

The USG6000 series provides powerful DDoS detection capabilities based on the behavior analysis, legitimate traffic identification, feature identification and filtering, abnormal traffic baseline learning, dynamic fingerprint identification, reverse source detection technologies to detect malformed packet attacks (such as Winnuke and Teardrop), scanning and sniffing attacks (such as the IP sweep, port scanning, and IP source routing option attacks), and flood or traffic attacks. The USG6000 series also incorporates the Netstream and route-based traffic injection and diversion technologies and interworks with the upstream and downstream devices to implement DDoS detection, layer-specific attack traffic cleaning, and attack defense on the entire network.

- IPS

Botnets, Trojan horses, worms, SQL injection attacks, and XSS attacks are predominant on the Internet. The USG6000 series has integrated IPS that provides the in-line deployment mode to proactively detect and block intrusion behaviors.

IPS of the USG6000 series uses Huawei-proprietary integrated detection engine and multi-core hardware platform with acceleration feature to obtain high-performance detection capabilities. The predefined and user-defined detection rules, online update of the engine and signature database, and intrusion tracking results of Huawei security attack defense lab enable the USG6000 series to accurately detect intrusions and zero-day attacks.

- AV

AV of the USG6000 series detects and blocks the files infected with viruses based on the flow reassembly, file reassembly, unpacking, decompression, PE virus detection, and flow-based heuristic detection technologies. The engine and virus database of AV also supports real-time online updates.

- Spam Detection

Anti-spam of the USG6000 series detects spam and enables the data filtering and management and control of incoming and outgoing emails based on the Real-time Blackhole List (RBL) technology using dynamic blacklists and real-time filtering of emails over SMTP, POP3, and Webmail.

- Malicious URL Detection

Malicious URL detection of the USG6000 series blocks access to malicious websites such as the Trojan horse and phishing websites. Huawei security team maintains malicious URL categories to be up to date. The malicious URL categories of the USG6000 series support real-time online query and update.

In addition, attack awareness of the USG6000 series has powerful cloud security capabilities. The USG6000 series collects and sends all attack awareness results to cloud servers for analysis and processing, obtains Internet security postures, and synchronizes real-time detection capabilities from other devices.

2.7 Location Awareness

Location awareness of the USG6000 series analyzes the location (such as the city, region, or country) that traffic is initiated from or destined for based on the source and destination IP addresses.

The USG6000 series incorporates the network address and geographical location information and integrates user-defined locations and location sets into unified policies to provide location-specific security policies, traffic limiting policies, routing policies, audit policies, and statistics and reports of traffic and threats.

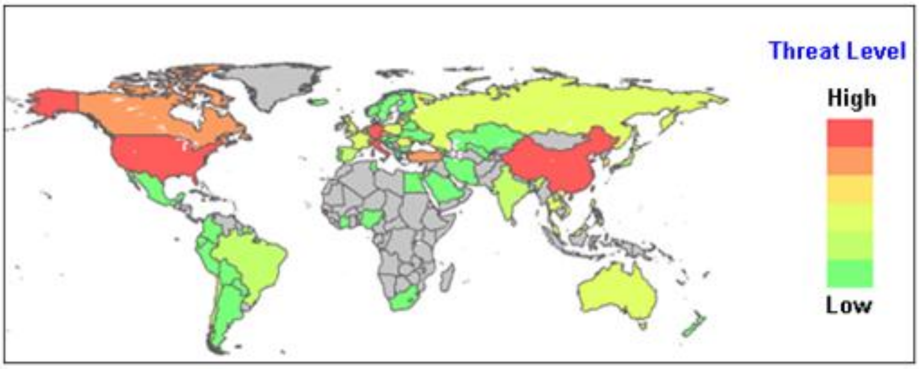
The USG6000 series implements location awareness as follows:

- Location-specific policy configuration

Location-specific policy configuration helps you manage users and traffic by location. The USG6000 series can provide the security filtering, bandwidth control, authentication, and audit policies based on location awareness. For example, you can configure location-specific security policies to allow Internet users in Hong Kong and London to access intranet resources and prevent Internet users of the USA from accessing the resources.

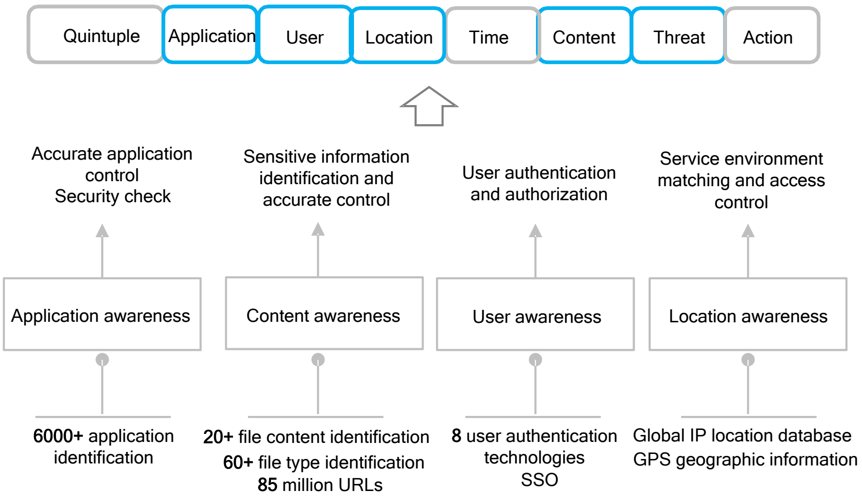
- Location-specific traffic statistics collection, threat statistics collection, and analysis

The USG6000 series automatically collects location information of the local device and packets, analyzes traffic, threats, and security threats by location, and provides location-specific traffic and threat trend reports. The reports provide you visibility into traffic rankings by source location and destination location. You can click a location to view all statistics and trends of the location.


Threat Level
High
Low

3 ACTUAL Awareness Services and Functions

In the open network environment, the USG6000 series must have comprehensive service awareness capabilities to achieve effective management and security protection. Based on ACTUAL awareness dimensions, the USG6000 series extracts important elements that clearly define a service. The service model of the ACTUAL awareness system makes the cloud and mobile borders clear, facilitates access control, and clearly defines a service, covering Who, When, Where, What, and How. ACTUAL awareness helps the USG6000 series provide service-oriented accurate control and visualized management.


Quintuple
Application
User
Location
Time
Content
Threat
Action
Accurate application control
Security check
Sensitive information identification and accurate control
User authentication and authorization
Service environment matching and access control
Application awareness
Content awareness
User awareness
Location awareness
6000+ application identification
20+ file content identification
60+ file type identification
85 million URLs
8 user authentication technologies
SSO
Global IP location database
GPS geographic information

3.1 Integrated Acceleration Matching Technology

After the dimensions such as user, application, content, location, and time segment are added for matching, the matching efficiency of the quintuple-based ACL matching technology cannot meet the requirements of network security devices.

Based on the RFC and Tries algorithms, Huawei has developed a set of integrated acceleration matching algorithms to establish the search structure of all matching elements in advance and compile the elements into an integrated matching state machine. In addition, the matching duration does not increase with the rule quantity because the matching of all elements is implemented at a time, and the processing flow prevents performance insufficiency.

The USG6000 series is based on the hardware platform that has HFA pattern matching capabilities. In addition, the USG6000 series can use the pattern matching capabilities of hardware co-processors to further accelerate the matching.

3.2 Cloud Detection Technology

Serving as the "brain" of Huawei security products, the Power Fortress Cloud detection system is an automatic platform for analyzing the security postures of the live network. The seamless collaboration between the platform and malicious sample collection system enables the automatic, highly efficient, and accurate sample analysis and threat identification, such as content awareness–based traffic detection, virus detection, zero-day attack defense, phishing website identification, Botnet analysis, and malicious website analysis. After analyzing the samples, the Power Fortress extracts valuable information from them, marks the reputation of the IP addresses, domain names, files, geographical locations, spam, user IDs, historical traces of the samples, and upgrades the reputation marks to the global reputation detection and query system for the query about threat reputation from security devices.

In addition to the previous layered cloud security detection service, Huawei cloud security capabilities apply to security devices through the security knowledge base. The security devices undertake fundamental and principal detection tasks in the attack defense chain (client-cloud attack detection-cloud center). The knowledge database consists of multiple closely related components including the Power WebFilter database, Power WebRepute database, Power SA database, Power IPS database, Power AM (worm and Botnet databases), Power AV database, vulnerability database, and phishing website database. The USG6000 series has integrated the remote detection capabilities of Huawei cloud security competence center. The Power Fortress Cloud-U Upgrade Center pushes updates around the clock to ensure that devices can obtain the latest defense capabilities and protect the network users around the globe.