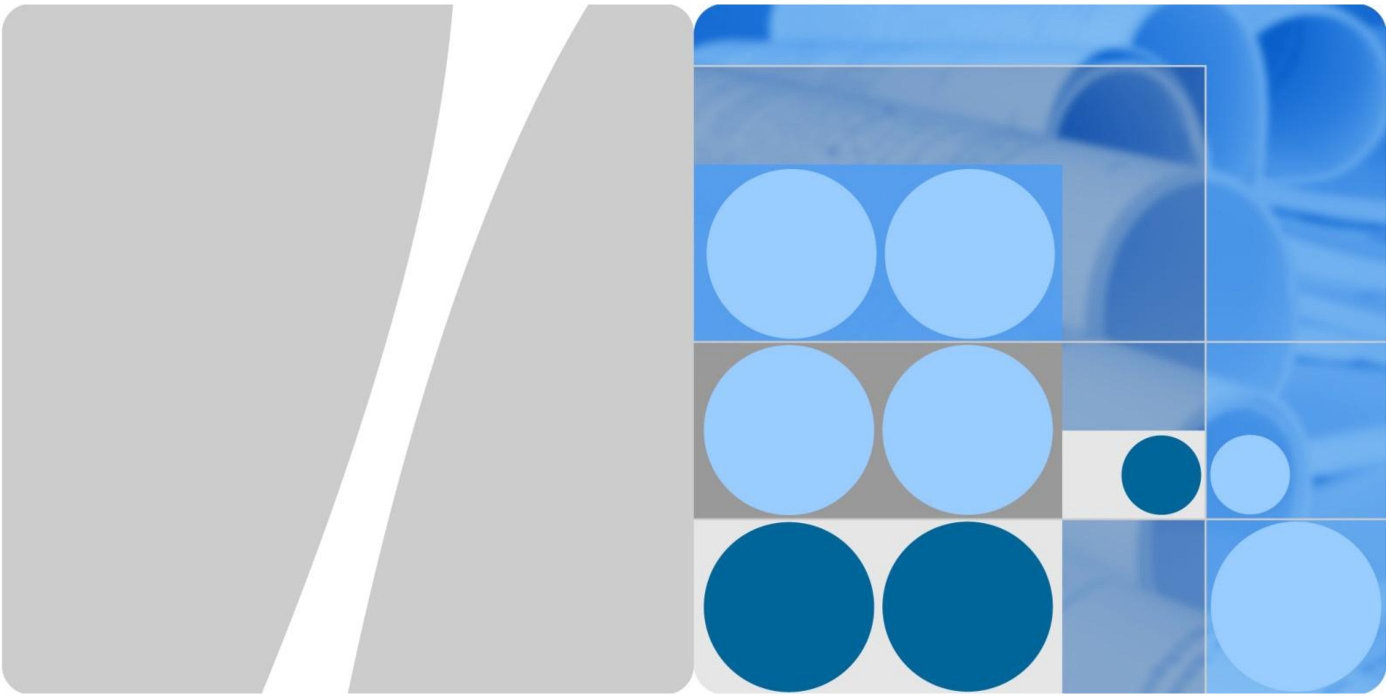


HUAWEI USG6000 Series Next-Generation Firewall Security Technology White Paper

Issue **1.1**

Date 2016-07-29

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

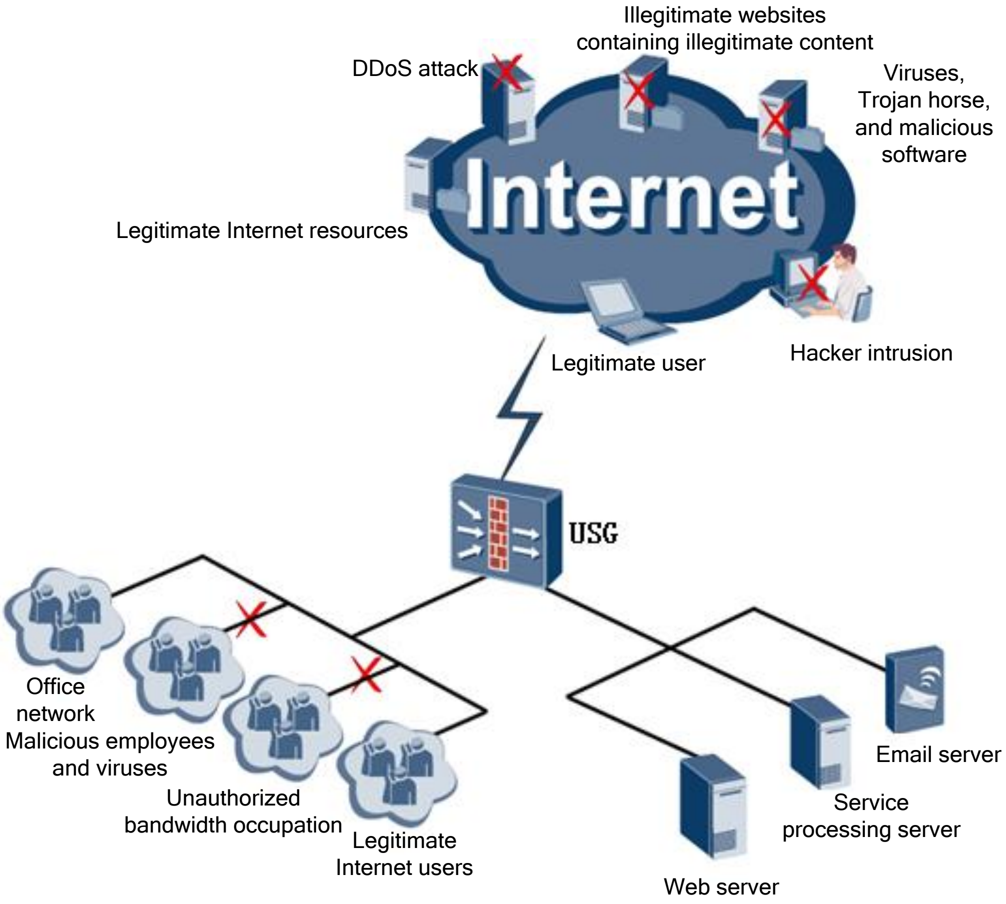
Contents

1 Executive Summary

1.1 Overview of the USG6000

The USG6000 is a series of new-generation carrier-class security gateways developed by Huawei for telecommunication carriers and large-, medium-, and small-scale enterprises or branches. It is widely applied on the borders of carrier, enterprise, government, financial, energy, and campus networks to meet market demands for 100 Mbit/s, 1000 Mbit/s, and 10 GE security gateways. The USG6000 comprises multiple models such as the USG6300 series, USG6500 series, and USG6600 series, provides powerful interface extension capabilities, and supports diversified interface cards such as 10 GE interface cards. The USG6000 provides powerful unified threat management (UTM) for content security protection and online behavior management in addition to basic firewall functions, offering all-round security protection for users. As shown in Figure 1-1, the USG6000 can be deployed at the egress of a network to protect the network against Internet hacker attacks and distributed denial of service (DDoS) attacks, prevent internal network users from accessing unauthorized websites, and restrict bandwidths available to users, offering a secure and reliable network environment for internal users.

Figure 1-1 Typical application scenario of the USG6000


Illegitimate websites containing illegitimate content
DDoS attack
Viruses, Trojan horse, and malicious software
Internet
Legitimate Internet resources
Legitimate user
Hacker intrusion
USG
Office network
Malicious employees and viruses
Unauthorized bandwidth occupation
Legitimate Internet users
Email server
Service processing server
Web server

1.2 Security Threats to the USG6000

Security Threats in the Management Layer

The following security threats may exist in the management layer:

- Security management regulations are not defined or not strictly applied.
- Personnel do not have security consciousness.
- System or application security patches are not installed in time, causing potential security vulnerabilities in the system.
- Multiple users share the same account, causing it difficult to trace back and delimit liabilities.
- Security documents are incomplete and cannot provide guidelines for secure production.

Security Threats in the Application Layer

The following security threats may exist in the application layer:

- Input authentication: buffer overflow, cross-site scripting, and SQL injection.
- Identity authentication: network interception, brute force attacks, dictionary attacks, cookie replay, and credential theft.
- Authorization: elevation of privilege, disclosure of confidential data, unauthorized data modification, and luring attacks.
- Configuration management: unauthorized access to management interfaces or configuration memory, retrieval of plain text configuration data, lack of personal accountability, and processes or service accounts beyond authority.
- Sensitive data: access to sensitive data in storage devices, network interception, and unauthorized data modification.
- Session management: session hijacking, session replay, and man-in-the-middle attacks.
- Encryption: insecure key generation or management, and fragile or user-defined encryption technologies.
- Parameter operations: character string query, window field operations, cookie operations, and HTTP header operations.
- Exception handling: information disclosure and denial of service (DoS) attacks.
- Security audit: users refuse to perform certain operations, attackers utilize application programs without tracing records, or attackers conceal their tracing records.

Security Threats in the System Layer

The following security threats may exist in the system layer:

- Common viruses, Trojan horses, and worm viruses: Viruses are programs designed with malicious behaviors to destroy the operating system or application software. Trojan horse programs are viruses which include malicious codes in seemingly harmless data files or executable programs. Worm viruses are similar to Trojan horse viruses, and can duplicate themselves from one server to another server. Worm viruses can hardly be detected, because they do not regularly create visible files. In general, worm viruses are noticeable only when they start consuming system resources, because the system will run slowly or other executable programs will stop running at that time.
- Tracks: Port scanning, ping scanning, and NetBIOS enumeration are examples of tracks, which may be utilized by attackers to collect valuable system-level information to wage severer attacks. Tracks may reveal multiple types of information, such as account details, operating system version or other software versions, server names, and details about database architecture.
- Password cracking: If an attacker cannot establish an anonymous connection to the server, he or she will attempt to establish an authentication connection. For this purpose, the attacker must obtain a valid combination of a user name and a password. A user who uses a default account name will create a good beginning for the attacker. Next, the attacker needs only to crack the account password. Users with null or fragile passwords enable the attacker to be even more at ease.
- DoS: DoS attacks may appear in multiple means and aim at several infrastructure targets. The attacker on a host can brutally attack application software to destroy services, or utilizes the defects of services where application software resides or defects of the operating system on a server to wage DoS attacks.
- Arbitrary code attacks: Attackers may run malicious codes on a server to damage server resources or further attack the downstream system. If the server processes that run for the malicious codes are executed beyond authority, arbitrary codes will cause greater risks. Common defects include servers subject to recursive routing or buffer overflow attacks because patches are not installed. In this case, arbitrary code attacks may occur.

- Unauthorized access: Unauthorized users may be able to access information or perform operations beyond their rights if access control is improperly implemented.

Security Threats in the Network Layer

The following security threats may exist in the network layer:

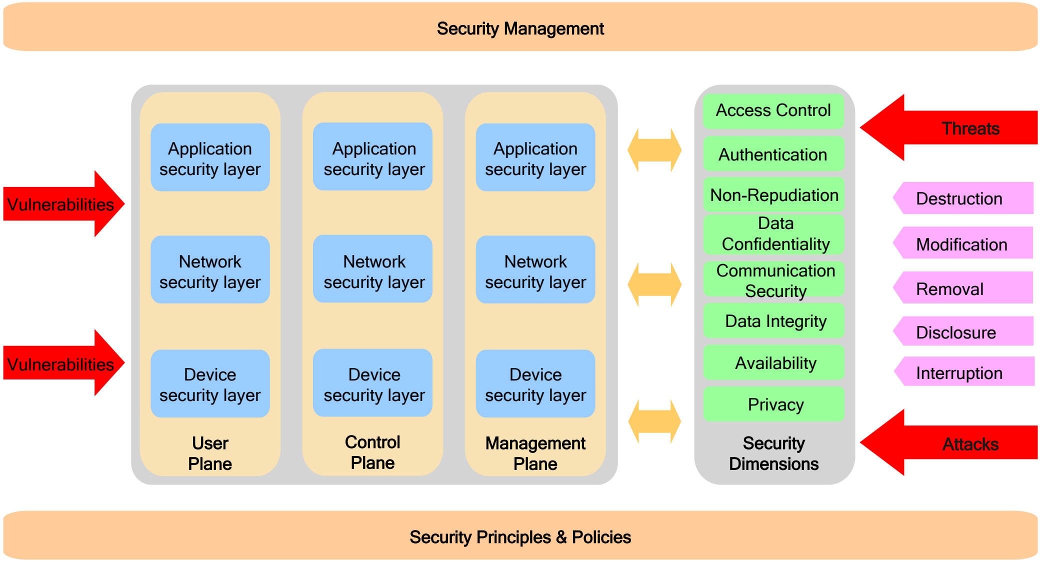
- Information collection: Attackers can discover and analyze network devices using methods for similar systems. In general, attackers scan ports first. After identifying open ports, they detect the device type using the title capturing and enumeration method and determine the versions of the operating system and application software. With such information, attackers may attack known defects for which the latest security patches are not installed.
- Sniffing: Sniffing is a way to monitor the transmission of data such as plain text password or configuration information on a network. Attackers can easily access all plain text information transmitted on a network using a simple data packet sniffer. They can also crack data packets that are encrypted with lightweight hash algorithms and decrypt payload information that is considered secure. A data packet sniffer must be installed on the communication channel between the server and the client to sniff data packets.
- Spoofing: Spoofing is a way to conceal one's real identity on a network. To create a false identity, the attacker must use a false source address which does not represent the real address of a data packet. The attacker can conceal the initial attack source or bypass an access control list (ACL) which is used to restrict host access based on source address rules.
- Session hijacking: Also known as man-in-the-middle attacks, session hijacking cheats a server or client into believing that the upstream host is a real legitimate host. In fact, the upstream host is the attacking host, which controls the network so that the attacking host seems to be the expected destination.
- DoS/DDoS: Legitimate users cannot access servers or services.

2 USG6000 Security Solution

2.1 Security Architecture

The reference security model defined in ITU-T Recommendation X.800 for communication systems consists of three security layers, three security planes, and eight security dimensions. It technically provides respective security solutions to possible threats in each layer and one each plane, as shown in Figure 2-1.

Figure 2-1 Security architecture



The three security layers, three security planes, and eight security dimensions are not parallel but are crossed. The security dimensions are described in the following sections.

2.2 Security Dimensions

According to ITU-T Recommendation X.800, a telecommunication system may be subject to the following security risks or attacks:

- Destruction: destruction of information or other resources

- Modification: unauthorized information modification
- Removal: stealing, deletion, or loss of information or other resources
- Disclosure: information disclosure
- Interruption: service interruption

The USG6000 provides security protection against these attacks and threats from the following eight security dimensions.

2.2.1 Access Control

In general, access control is applied to prevent unauthorized access to or invocation of network resources. For example, an access control policy can be applied to protect the accessed system from malicious behaviors in the case of access from an untrusted network to a trusted network. Access control is a common network control technology.

The USG6000 supports several access control mechanisms, such as MAC Address-based ACL, IP Address-based ACL, and user-based ACL.

2.2.2 Authentication

Security is a security mechanism applied to ensure that users own legitimate identities before they access a network or system. For example, carriers' login accounts will be authenticated before logging in to a system.

Authentication is required for access between users and between system components of the USG6000. To prevent unauthorized users from illegally logging in to the system by brute force attacks or other means which may cause damage to the system, the USG6000 has defined strict password security policies. The policies ensure that only authorized users can log in to the system and therefore maximally protect system security.

2.2.3 Non-Repudiation

Non-repudiation is a method for preventing individual users or entities from denying operations performed on data or a network, and provides useful evidences. These evidences include the data origin, ownership, and resource applications. The system must ensure that these evidences can be presented to a third party to prove the occurrence of certain events or operations. Non-repudiation is related to login, authentication, authorization, access, and other security events.

The USG6000 provides detailed log audit and monitoring. It provides numerous types of logs such as operation logs and security event logs to record details about user login, authentication, and operations.

2.2.4 Data Confidentiality

Data confidentiality is a method for preventing unauthorized disclosure of data or information to ensure that data content is unavailable for unauthorized entities or users. Data encryption and decryption is a common mechanism for data confidentiality protection.

The USG6000 uses encryption and decryption technology while storing user’s sensitive data (such as password, private keys) on the device.

2.2.5 Communication Security

Communication security is implemented by guaranteeing the security of mutual access between different systems or networks. Security protection must be provided for data flows involved during transmission to prevent unauthorized modification or falsification of data and other malicious behaviors.

USG6000 provides security transmit protocols such as SSL/TLS, SSH, SNMP v3.

2.2.6 Data Integrity

Data integrity is used to describe the integrity and accuracy of data and files to prevent malicious modification or substitution of data or files.

2.2.7 Availability

Availability reflects the degree to which the system or network can work properly or is available for services at any moment whenever necessary or when a task needs to be executed. Redundancy and backup policies related to availability are also important security means. The USG6000 features high reliability with redundancy backup of hardware and deployment. It supports automatic dumping and backup of user data.

2.2.8 Privacy

The privacy dimension is used to protect the information to be observed during network operations. For example, user information such as the geographical location and IP address of the user and the DNS name must be protected against disclosure when a user accesses a certain site. User information must also be stored in the form of encrypted data and presented anonymously.

2.3 Security Planes

The traditional mono-plane structure of security products leaves much room for security problems. Using logically isolated planes and ensuring the security of these planes are significant for security protection.

2.3.1 Management Plane

The USG6000 provides security guarantee for the fault management, performance management, and maintenance of data centers and supporting systems for network device transmission, such as operating systems, service systems, and customer systems. Security hardening is needed for both devices and the entire system to protect against threats to the management plane. The USG6000 implements hierarchical authority control and records detailed logs for configuration changes. It provides enhanced user management for local and remote login, secure data transmission, and access control.

2.3.2 Control Plane

Control information must be transmitted on a network to control network operations to implement effective information transmission and provide normal network services and applications. The control plane provides security protection for proper network control, including system construction, network element (NE) authentication, data integrity, and data confidentiality.

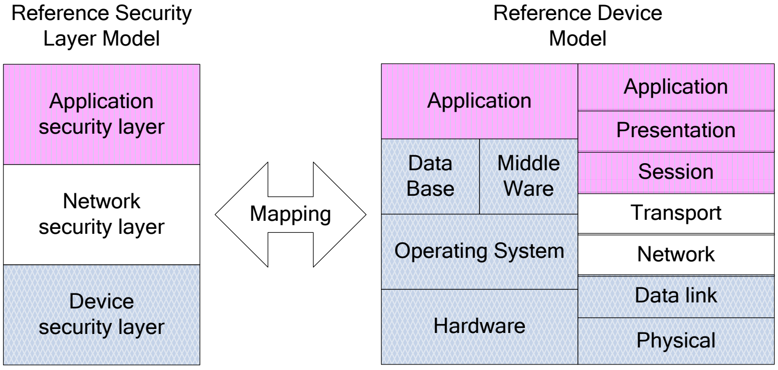
2.3.3 User Plane

The USG6000 provides security protection for both user access and network operations. It filters the traffic of unauthorized users to prevent attack traffic and enhance real-time security monitoring.

2.4 Security Layer

The reference security model also defines three security layers, which are the device security layer, the network security layer, and the application security layer, in addition to the preceding security dimensions and planes. The three security layers can map to the seven-layer TCP/IP open system interconnection (OSI) model, as shown in Figure 2-2. The security dimensions must be applied to the security layer of network devices and the facility group so that security measures can be defined for each layer according to the weaknesses of the layers.

Figure 2-2 Mapping between the three security layers and the TCP/IP OSI reference model



2.4.1 Device Security Layer

The device security layer consists of network transmission facilities and independent network units, which are a basis for the network and services. A security challenge to the device security layer is to guarantee secure communication between devices. The security of the device security layer is reflected in the reliability of communication lines, such as the backup of hardware, operating system, database, basic protocols, middleware, and devices, anti-disaster capability, and anti-interference capability. The device security layer can map to the link layer and physical layer in the TCP/IP OSI reference model.

2.4.2 Network Security Layer

The network security layer provides security for network services. It consists of network protocols and logical networks. The network security layer should focus on the security of network protocols and device interconnection. Security rules and policies, such as deep defense, collaborative defense, and security plane isolation, are applied to improve the security of device interconnection. The security of network protocols involves numerous network layer protocols and transport layer protocols, such as TCP, IP, OSPF, RIP, ICMP, and MPLS.

2.4.3 Application Security Layer

The application security layer covers all applications, services, and application protocols of the device layer and the network layer. Therefore, the security of the application security layer covers the security of services and applications and the security of related protocols. Services and applications include web applications, O&M services and applications, and the charging service system. Application layer protocols are protocols of the session layer, presentation layer, and application layer, such as HTTP, DNS, SSH, FTP, RPC, SNMP, and AAA.

2.5 Overview of the USG6000 Security Solution

As described previously, the USG6000 system is well designed in terms of platform security, network security, and application security.

- Platform security: The USG6000 system provides multiple protection means, such as system enhancement and security patching. It provides a secure and reliable platform for services and applications by improving the security of the operating system.
- Network security: Multiple security solutions, such as networking isolation, access control, and remote maintenance, are available to protect the security of the USG6000 through secure networking.
- Application security: Multiple security policies, such as transmission security, user management, log management, and user data management, are available. These security policies are applicable to specific services and applications.

For details about platform security, network security, and application security, see later chapters.

3 Platform Security

3.1 Operating System Security

Operating System

The USG6000 uses a style of secure system software specially designed by Huawei based on service security features as its real-time operating system. The operating system is highly real-time, reliable, and compatible, offering various applications and management services for users. Since the operating system is not universal, it is not so vulnerable to attacks as with universal operating systems and therefore guarantees device security to the maximum extent.

Only service-related software packages and components need to be installed. This reduces system vulnerabilities and alleviates the risk of attacks to the system.

The applied operating system is the latest or most stable.

Security hardening is performed for the operating system during system installation. Security settings are implemented for all services of the operating system.

System Logs

All events related to authentication are recorded as logs.

Minimum network services and ports are enabled.

Ports are enabled based on services. Useless ports are disabled by default.

A network service can only be bound to the network interface where the network service will be provided. For example, the security shell (SSH) service can only be bound to a management interface.

Audit Logs

All events related to authentication, including login errors and other authentication events, are recorded as logs to facilitate user login analysis.

Logs generated by scheduled tasks are recorded.

System audit logs can be viewed on the versatile security management (eSight) platform. In addition, logs and alarms can be sent to third-party log servers or network management systems (NMSs).

System Access, Authentication, and Authorization

Only the minimum rights required for task accomplishment are assigned to a user, and only application accounts are allowed to perform application operations.

The user login timeout period can be set. Users must be re-authenticated upon expiry of the login timeout period.

Accounts and Operating Environment

Account passwords must meet basic complexity requirements.

Accounts will be locked upon repeated retry to prevent brute force attacks.

3.2 Database Security

The USG6000 uses an embedded database, which provides only internal interfaces but no external interfaces to ensure that data in the database is inaccessible to external users. This eliminates the possibility of external intrusion to the database.

When entries in the database are stored, the password is encrypted during storage. Therefore, sensitive data will not be disclosed even if database files are maliciously exported.

The database is accessed in minimum authorization mode. It is for internal logic use only.

4 Network Security

4.1 Networking Isolation

The USG6000 provides fixed interfaces to allow for external service access. There is no protocol stack between the data plane and the interconnected device network, and IP addresses are not externally disclosed. Therefore, external users cannot attack IP addresses. In addition, the USG6000 provides independent out-of-band management interfaces to completely isolate management from services.

The USG6000 can be independently managed through its embedded web environment. The eSight is also available to manage and monitor multiple USG6000 firewalls in a centralized manner.

The Secure Hypertext Transfer Protocol (HTTPS) can be applied between the web console used for standalone management and the USG6000, whereas the SSH protocol can be applied for encrypting management and control data between the eSight and the USG6000. This effectively prevents communication data from being stolen by hackers and therefore avoids the disclosure of carriers' or public customers' data or information.

4.2 Access Control

The USG6000 provides strict access control and defines ACLs to control the IP addresses connecting to the USG6000. Only authorized addresses can log in to the USG6000, check information on the USG6000, and configure data on the USG6000. The ACLs are combined with identification and authentication mechanisms to prevent unauthorized users or devices from accessing the USG6000.

4.3 Remote Maintenance

The USG6000 supports remote maintenance and management using the SSH or HTTPS protocol. Secure file transfer protocols such as sFTP can be applied for file transfer.

The USG6000 can also be managed and monitored through third-party NMSs. The SNMPv3 protocol can be selected for this purpose.

5 Application Security

5.1 User Data Security

User Data Protection

Personal data identifies a natural person directly or along with other information. Personal data includes the name of the end user, account, calling number, called number, conversation record, conversation time, and location information.

Sensitive data depends on the specific application scenario of the product. It is analyzed and judged based on possible risks. Typical sensitive data includes passwords, bank accounts, bulky personal data, user conversation content, and keys.

Personal data, if improperly used, may often relate to personal privacy. Different countries raise different security requirements concerning personal data protection. The USG6000 provides related measures for personal data protection during practical use.

System Compliance

The USG6000 does not involve public customers' bank accounts, private passwords, user names, or user accounts such as mobile phone numbers, international mobile subscriber identities (IMSIs), international mobile equipment identities (IMEIs), and Internet access accounts.

The USG6000 records only events related to security threats to minimize personal data records. When detecting an attack event, the USG6000 records the attacker of the attack event and the IP address and port number of the victim. Its attack packet capturing function enables it to capture the data content of attack packets, whereas its application control function enables it to record the user IP address, online/offline time, and application protocol related to IM traffic. The security of personal data is guaranteed by secure networking, login authentication, security protocols, and authority control.

User Data Security Solution

1. Technical measures
   - Secure communication protocol: The USG6000 supports multiple secure communication protocols, such as SSH V2, SNMP V3, and HTTPS.
   - Login authentication: The USG6000 may involve access to personal data through web user interfaces (UIs) or logs. A user must enter a correct user name and password to log in to the web UIs, operating system, or database involving the presentation of personal data.

- Authority control: The web UIs support role control and authority control. Unauthorized users cannot access personal data and cannot perform functions involving personal data.

2. Audit measures
   - All non-query operations are logged.
3. Management measures
   - Logs and captured packet files cannot be transferred outside the enterprise's or carrier's network. Permission from the user is required and the virtual private network (VPN) function must be enabled to access such logs or files.

5.2 Authentication and Authorization Management

5.2.1 Role-based User Management

A role-based authorization system is applied. Minimum rights are granted to accounts and roles. In other words, only rights necessary for work are granted to each role and only roles necessary for work are granted to each account. The USG6000 supports role control at a data-level granularity, so that users with different roles can perform the same function but cannot view internal sensitive information related to the function. This ensures that management, maintenance, and operations are separated from each other.

The USG6000 supports different rights for different users. It also supports custom administrator roles, in addition to default system administrators, operators, and auditors. Administrator roles can be defined at a fine granularity based on the content of configuration management and the devices to be managed, and are granted to users with respective rights.

5.2.2 Security Management

To prevent unauthorized users from logging in to the system by brute force attacks or other means which may destroy the system, the USG6000 provides strict password security policies. These policies ensure that only authorized users log in to the system and therefore guarantee system security to the maximum extent.

User and Password Policies

Forced user logout

Administrators can forcibly log out users whose legality is suspected.

Password complexity

The following user password complexity rules are recommended for the USG6000:

1. The password contains at least eight characters.
2. The password must contain at least three types of the following:
   - lower-case letter
   - upper-case letter
   - digit
   - special character, such as `~!@#$%^&*()-_=+\|[{}];:'",<.>/? and blanks
3. The password cannot be the account in a reverse order.

Password locking upon errors

A user will be locked if he or she enters an incorrect password for a number of times, which is configurable in the system and five by default.

After a user is locked because of login failures with N consecutive retries, the system supports the setting of automatic unlocking time for the locked user.

A locked user will be automatically unlocked when the user lockout duration reaches the predefined time.

Encrypted password storage

Web passwords, FTP passwords, operating system accounts and passwords, database accounts and passwords, SNMP v2 community names, and SNMP v3 passwords cannot be stored in plain text mode in the system. These passwords are encrypted with the SHA algorithm if they do not need to be recovered later or encrypted with the AES algorithm if they need to be recovered later.

Password usage rules

Passwords entered on the USG6000 cannot be echoed in plain text mode and cannot be copied.

A user can modify only his or her own password, and must enter the old password for verification during password modification, except for password reset by administrators.

Idle Logout Policy

Web clients in the USG6000 system support an automatic locking policy. An inactivity period can be set so that the web UI is locked when a login user does not perform any operations within the specified time. To perform web operations later, the user must enter the account and password again for authentication.

5.3 Data Transmission Security

5.3.1 Secure Transfer Protocol

The USG6000 uses a series of secure protocols and applications to guarantee data transmission security.

1. HTTPS is applied for web applications.
2. SSH v2 is applied for connections and access between system components by default.
3. SNMP v3 can be applied for network management.
4. HTTPS is applied for web-based file transmission with external systems.
5. File integrity check is performed before live upgrade packets and other data are imported.

5.4 Log Management

The USG6000 records logs in compliance with Huawei log specifications. The logs indicate the event time, user ID, event type, the name of the accessed resource, and event handling results.

Logs can be periodically audited to check security problems and eliminate hidden security vulnerabilities.

5.4.1 Operation Log

User operations initiated from web clients of the USG6000 system and ultimate results are recorded as operation logs. Operation logs show operations performed within a specific time period and can be checked to help O&M personnel locate faults. Auditors can export and view operation logs through web UIs, and periodically audit operations performed by O&M personnel to discover improper or malicious operations in time. Operation logs can also serve as evidences for non-repudiation.

Operation logs record the following information:

- User login events, such as user login and logout
- User management events, such as user addition, deletion, or modification, password modification, and authority changes
- System management events, such as the addition, deletion or modification of parameter values

5.4.2 Running Log

Running logs record information about the running status of the system and servers. They are generated by service modules in the system. O&M personnel can check running logs to learn or analyze the running status of the system, and to discover and handle exceptions in time. O&M personnel can also export and send running logs to technical support engineers for fault location.

Running logs record the following information:

- Abnormal states and actions during system running, such as configuration failures
- Key events during system running, such as system startup and shutdown
- System management events, such as the addition, deletion or modification of parameter values

5.4.3 System Log

The system logs of the USG6000 record the following information:

- System startup events
- System resource information, such as CPU usage, memory usage, temperature, and storage medium usage
- Hardware information
- Network port traffic information