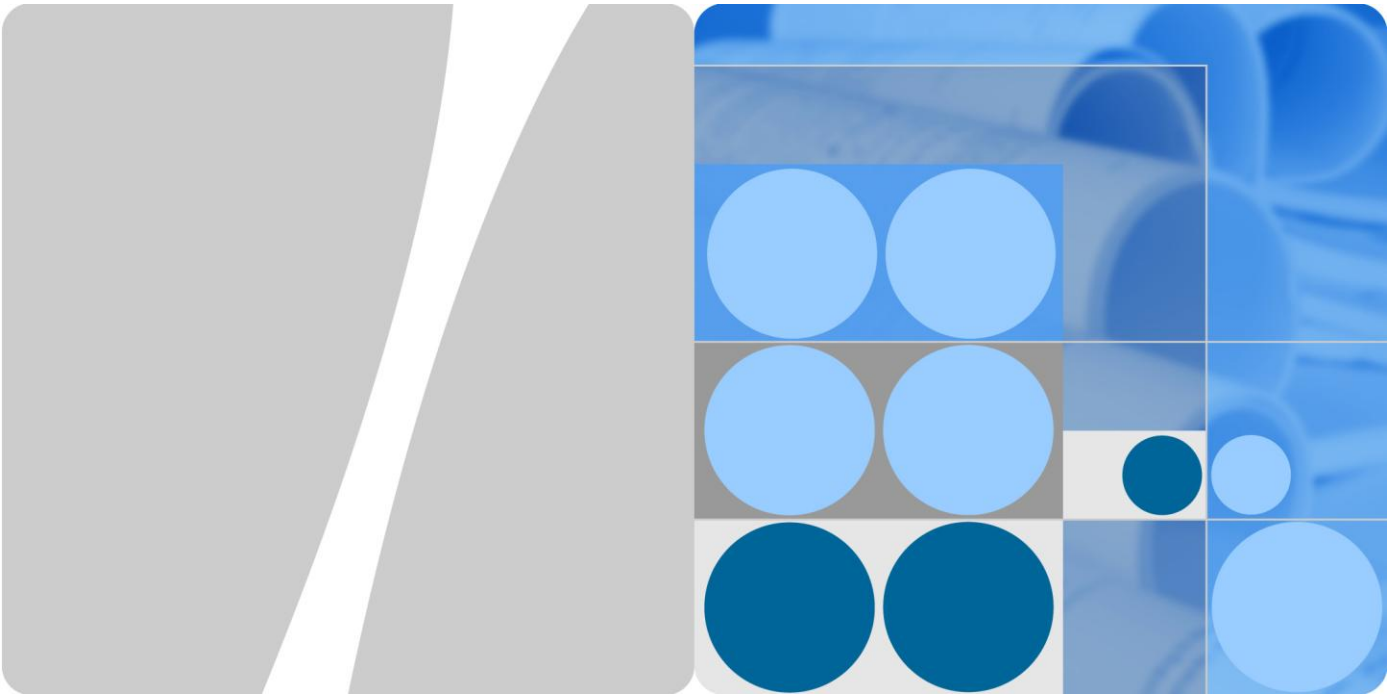
Doc. code



HUAWEI Secospace USG Series User Management and Control White Paper

Issue 1.0

Date 2014-03-27

HUAWEI TECHNOLOGIES CO., LTD.

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

User Management and Control White Paper

Abstract: As the Internet develops rapidly, the application of dynamic IP addresses becomes increasingly common. The IP address-specific traffic control policy used on traditional firewalls now turns out to be inadequate. Then, user-specific management and control measures accommodate dynamic IP address allocation. Meanwhile, the management granularity of user/user group refines the management of online behaviors and bandwidths. This white paper describes the background of user management and control technology of the USG and the application scenarios and methods.

Keywords: Single sign-on, LDAP, Active Directory, RADIUS

1 Background

Nowadays, networks play an integral role in improving the administration and working efficiency of enterprises and governments. However, the boundless and free network is plagued with viruses, hacker attacks, and illegitimate applications. Networks not only bring benefits but also pose great risks of legal liability and data leaks.

IT managers then turned attention to exploring a way to manage and control network user behaviors effectively and economically. The first problem they encountered is the dynamic mapping of IP addresses and users. Since most of networks use dynamic IP address allocation, the IP-specific access control policies of traditional firewalls fail to work effectively. How to accurately identify users and effectively manage and control user behaviors become the greatest focus in network security.

With the user-specific management measures, the administrator of an enterprise can monitor and manage internal users in the hierarchical manner which resembles to the common organization structure of enterprises. Behavior control, access rights, and bandwidth allocation are exerted in a user/user group dimension. Meanwhile, the customized authentication schemes for different users contribute to refined and flexible management.

2 User Management and Control

2.1 User Organization Management

To assign differentiated network access rights to users or departments, a well planned and maintained organization structure is required. The USG provides an organization structure tree that resembles to common administrative structures and therefore brings convenience to planning and management. Also, the USG allows a user to belong to multiple user groups as the following figure shows:

The administrator can quickly import user information to the USG and create user organization structures using the following methods:

- Create the user or user group through the Web GUI or CLI and assign the user to the specified group.
- User information can be exported to or imported from a .csv file to facilitate the creation of user and user group information.
- The user or user group information can also be imported from the LDAP or Active Directory (AD) domain server and the import policies can be customized. For example, you can set filtering conditions to determine where to import from in the user organization structure on

the source database.

- The personnel and organization structure are constantly changing. When new employees join in an organization, it is inconvenient to manually add every new user or user group to the LDAP or AD server and import the information to the USG. To make configuration easier, the user management function of the USG provides the automatic import of new users who are authenticated. During import, the organizational structure of the users is kept intact and unchanged. If the user group on the LDAP or AD server does not exist in the local database, the system automatically creates the group in the local database. The administrator also can add a user to a specified group other than the original group as required.
- When scaling up the network, you may need to add devices or upgrade existing devices. In this case, you can export the user organization structure stored on a device into a database file, and then import the database file to a specified device.

2.2 User Identification and Authentication Technologies

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

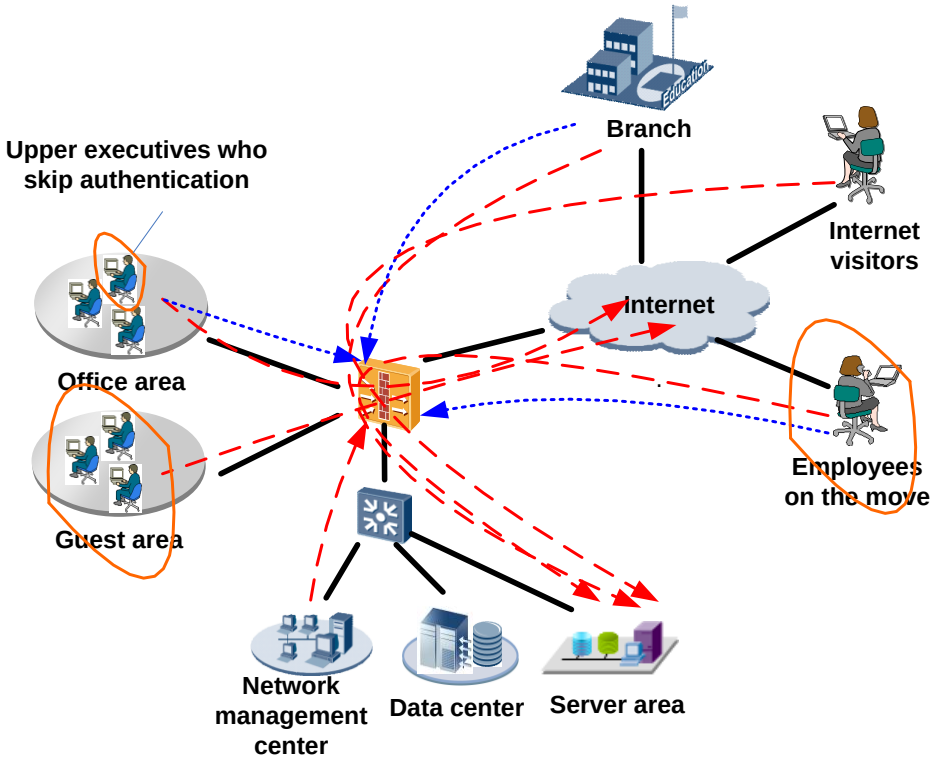
- **Authentication exemption:**
  - ✧ Upper executives demand high efficiency and require skipping authentication. However, their network activities also require high security. For such users, bidirectional bind their user accounts with their IP addresses, MAC addresses, or IP/MAC address pairs and configure authentication exemption for them. With this configuration, the USG exempts upper executives from authentication but allow the login from only the IP or MAC address bound to the user account.Companies often have guests who may need to user their company networks. These users do not have accounts and cannot be authenticated; however, their network access rights must be controlled. To accommodate this situation, the user management module can automatically create temporary accounts for guests with their IP addresses as their user names.
- **Password authentication:**
  - ✧ For common employees, the convenient password authentication is usually applied. Password authentication falls into the following three modes:
  - ✧ Redirected web authentication: When an unauthenticated employee accesses HTTP services, the USG redirects the user to a login page and prompts the user to get authenticated.
  - ✧ User-initiated web authentication: An employee can initiate authentication simply by entering the URL of the login page in a browser. Both HTTP and HTTPS authentication are supported. An HTTPS is recommended for users with high security requirement.
  - ✧ Both redirected and user-initiated web authentication can be implemented locally or on an LDAP, RADIUS, or AD server. If an authentication server is used, the server returns the authentication messages to the USG.

- **Single sign-on:**
  - ✧ If an AD server with an identity authentication system has been deployed at the current network, the USG can collaborate with the AD server to provide single sign-on. If the USG identifies that a user has been authenticated by the AD server, the USG permits the user without requesting the user name and password. In the authentication process, the USG is transparent to users.

2.3 User-specific Management and Control Policy

- **Online user management**
  - ✧ The administrator can view online user status covering login time, online duration, login IP address and so on.
  - ✧ The administrator can lock out a user to limit its online behavior in a specified time period.
  - ✧ The administrator can force off an online user who is regarded as untrustworthy.
- **Management by policies**
  - ✧ The USG supports user-specific forwarding. You can associate a user with a septet (source IP address, destination IP address, source port, destination port, protocol, time, and traffic direction) in the forwarding policy applied to the user. In so doing, you can flexibly adjust the forwarding policy on a user. For example, you can permit or deny the user to access a certain service during a time period and in a traffic direction.
  - ✧ The USG can limit the traffic and concurrent connections to effectively allocate and manage bandwidth resources. The USG can audit and analyze the traffic statistics of users and user groups for future adjustment.
  - ✧ The USG supports user-specific online behavior management that includes application layer management and monitoring 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 MSN during working hours and forbid the access to certain game or forum URLs to ensure employee working efficiency.
  - ✧ The USG supports user-specific intelligent routing that enables you to specify different outgoing links for the traffic of different users (user groups). This function facilitates flexible traffic and link control.

3 Typical Application Scenario



The preceding figure shows a typical enterprise intranet. There are several types of users: upper executives, guests, common employees, and employees on the move. You can configure different authentication modes for different user types.

For upper executives, you can configure authentication exemption (bidirectional binding of user account and IP/MAC address) or assign them with special network access rights and bandwidths. If there are numerous users to manage, you can group them and assign network access rights and bandwidth to the group.

For guests, you can enable automatic account creation and authentication exemption, and create a guest group for them. All guests have only the access rights and bandwidth assigned to the guest group.

For common employees, you can use local authentication or password authentication by a third party. In terms of organization structure, you can create user groups according to the administration structure, add users to corresponding groups, and then assign online behavior rights and bandwidths to user groups as required.

For employees on the move, you can use local database authentication or password authentication by a third party, but only through VPN connections to secure user information.

Appendix: Acronyms and Abbreviations

Abbreviation	Full Spelling
SSO	Single Sign-On
LDAP	Lightweight Directory Access Protocol
RADIUS	Remote Authentication Dial In User Service
AD	Active Directory

