

Firewall User Management

Lecture 7

HCIA-Security

Prepared by
Dr. Abdelrhman Ahmed

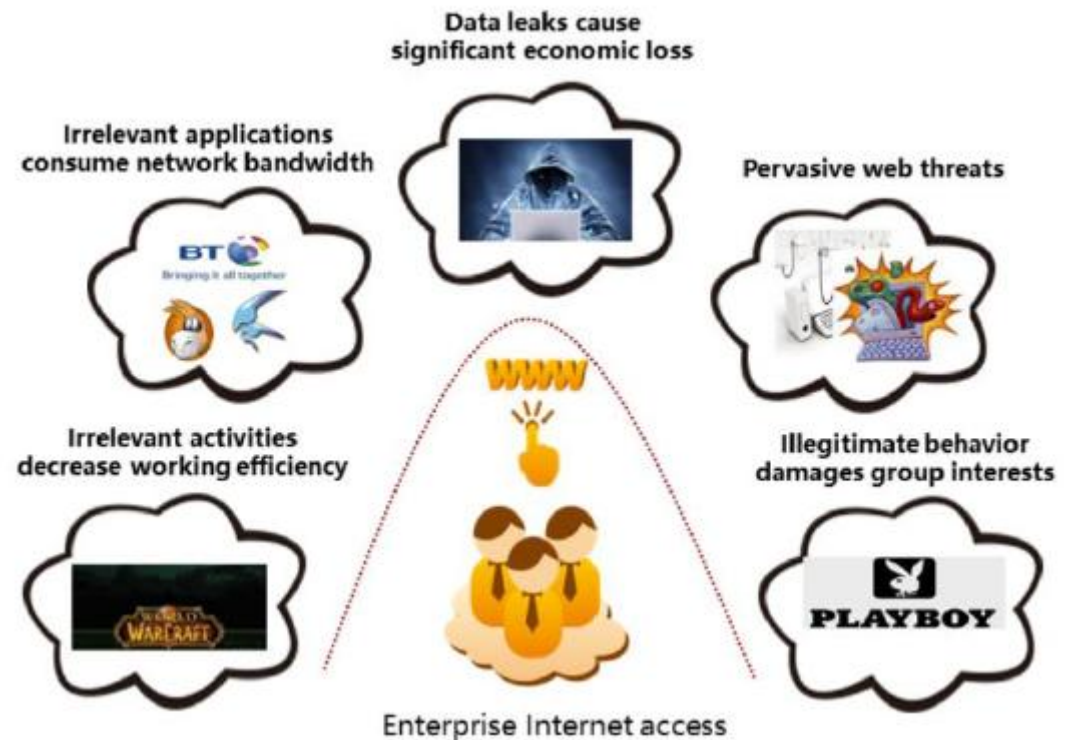
Objectives

- **Upon completion of this course, you will be able to understand:**
 - ❑ **AAA technologies**
 - ❑ **User authentication technologies**
 - ❑ **User authentication management configurations**

Chapter
07

User Authentication Background

- The growing number of application-layer attacks not only brings additional threats to network security but also places further strain on network access control. Enterprises want the capability to precisely identify users, ensure legitimate applications operate normally, and block applications that may bring security risks. However, IP addresses and ports are no longer sufficient to distinguish users and applications. Traditional access control policies based on quintuples cannot adapt to changes in the current network environment.



Chapter
07

What is AAA?

- Authentication
- Authorization
- Accounting



- Example:

- When accessing the Internet, a user needs to enter a username and a password for authentication.
- After authentication, the firewall starts to authorize the user and grant permissions for access to different resources, such as baidu.com or google.com.
- During user access, accounting is performed to record the user's operations and online duration.

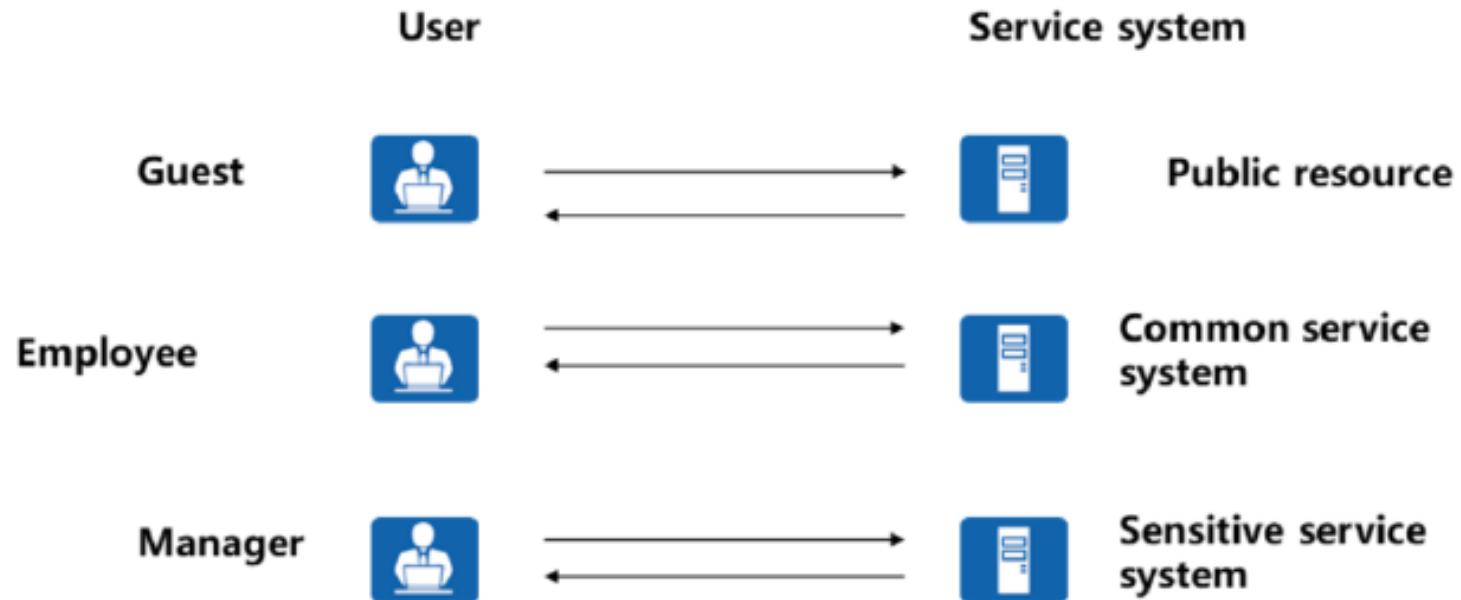
Authentication refers to the confirmation of user identities using various factors.

- **Authentication mode:**

- **What I know:** includes the information that a user knows (password and PIN)
- **What I have:** includes the information that a user has (token cards, smart cards, and various bank cards)
- **What I am:** includes unique biometric features that a user has (fingerprint, voice, iris, and DNA)



- Authorizes accessible resources.
- Authorizes available commands.
- Authorizes users to access certain services, including public services and sensitive services.
- Authorizes users to use certain commands for device management. For example, authorizes users to use only display commands but not delete or copy commands.



- The accounting function covers the following aspects:

- ☐ How long do users stay online?
- ☐ How much money do users spend?
- ☐ What operations do users perform?

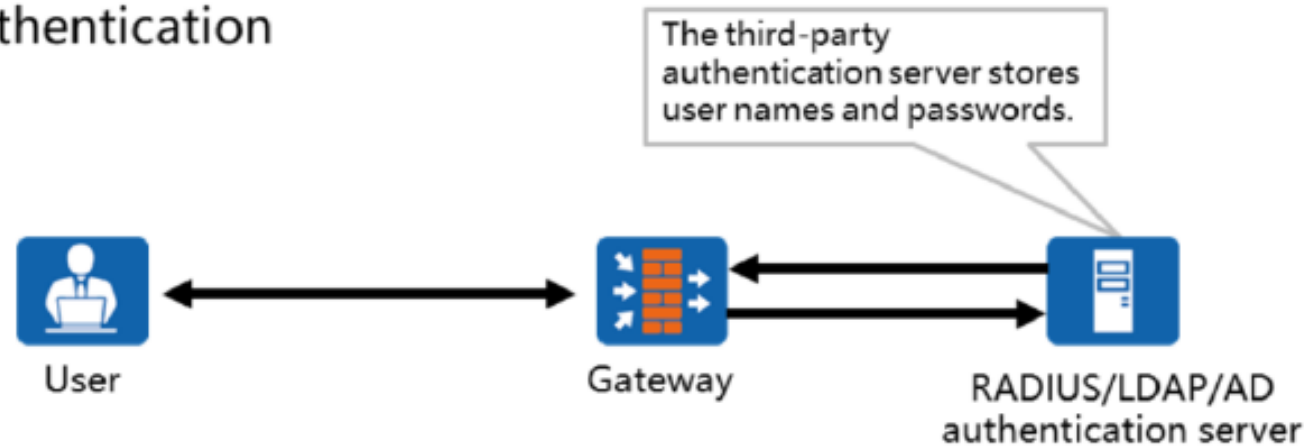


AAA Technologies

- Local authentication



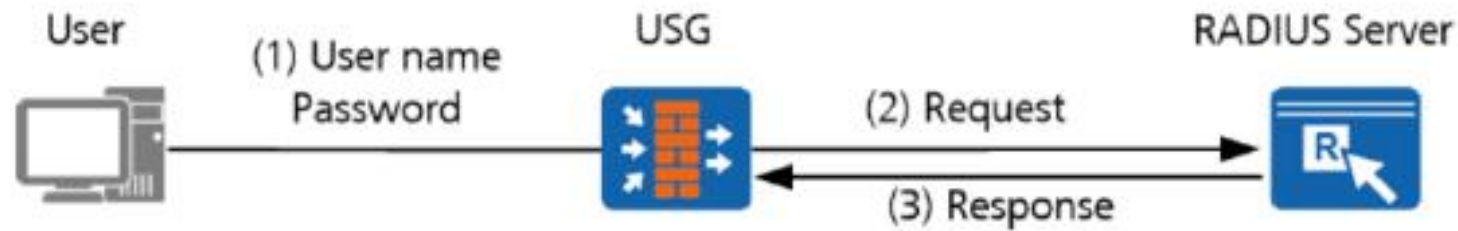
- Server authentication



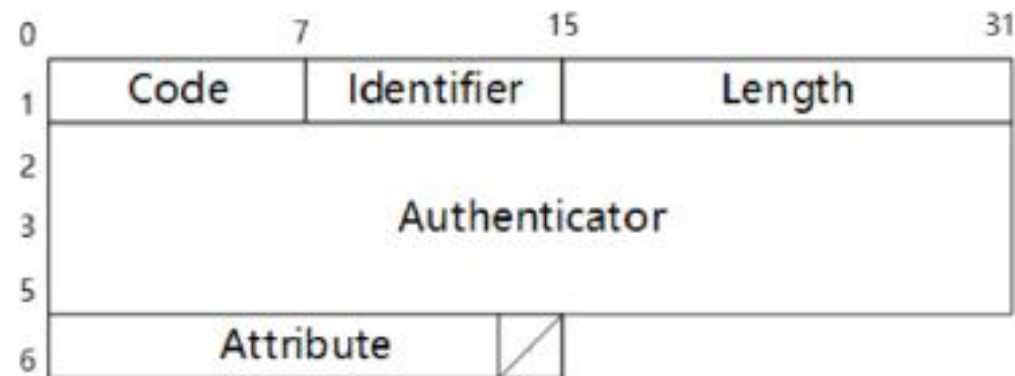
AAA Technologies

- **No authentication:**
 - No authentication is performed on trusted users. In most cases, this type of authentication mode is not recommended.
- **Local authentication:**
 - Configures user information, including the username, password, and attributes of local users, on a Network Access Server (NAS). Local authentication offers fast processing and low operation cost. However, the capacity to store user information is limited by the hardware.
- **Server authentication:**
 - Configures user information, including the username, password, and attributes, on a third-party authentication server. AAA can remotely authenticate users through the Remote Authentication Dial In User Service (RADIUS) protocol or the Huawei Terminal Access Controller Access Control System (HWTACACS) protocol.

- The RADIUS server sets up a unique database to store user names and passwords for authenticating users.

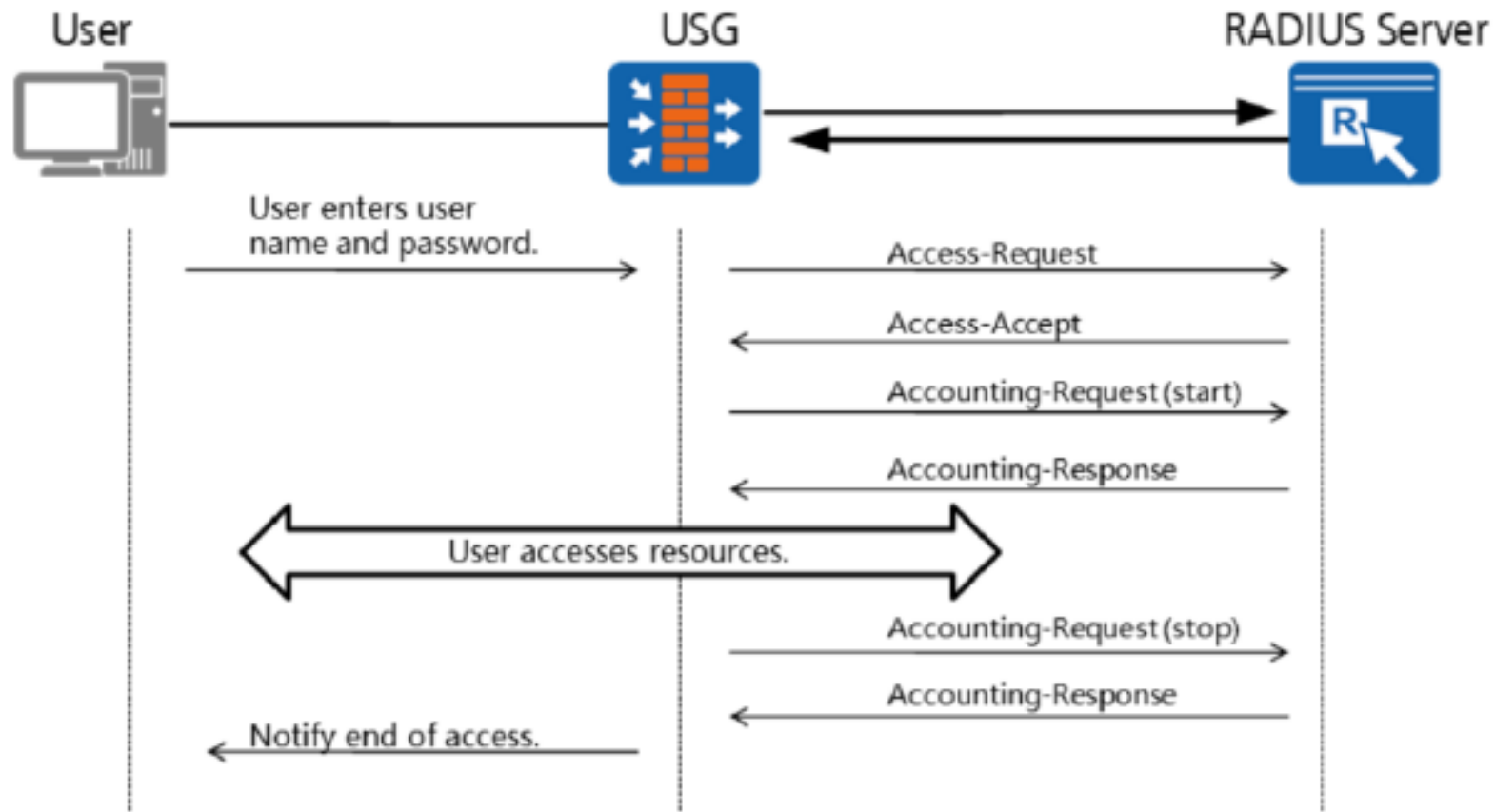


- RADIUS message structure



Chapter
07

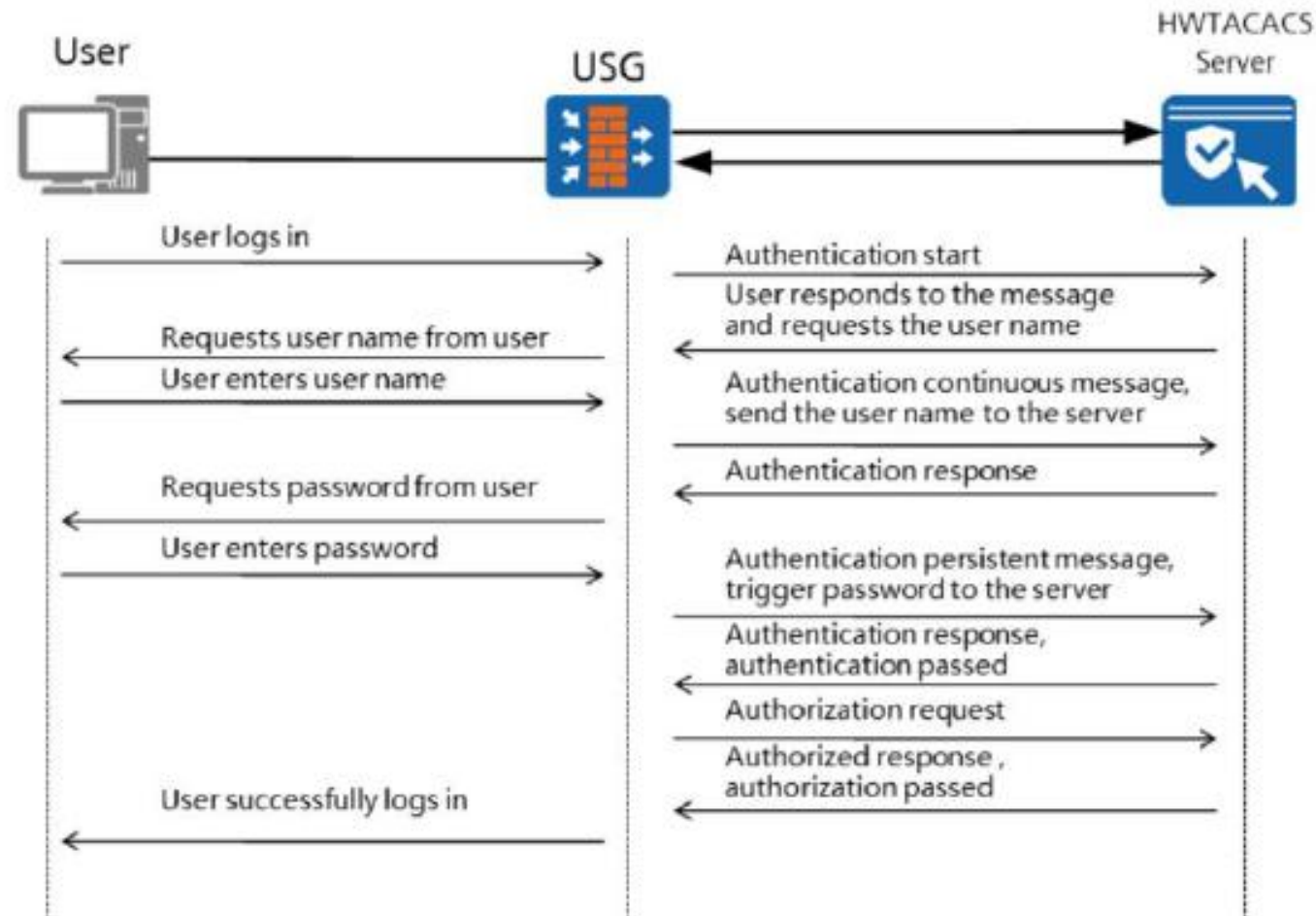
RADIUS Application Scenarios



HWTACACS Overview

- HWTACACS is an enhancement of TACACS. Similar to RADIUS, HWTACACS uses the client/server model to implement communication between NAS and TACACS+ servers.
- A typical application of HWTACACS is to perform authentication, authorization, and accounting for a user logging in to a device. The device functions as the HWTACACS client to send the username and password to the HWTACACS server for authentication. If a user is authenticated and authorized, the user can log in to the device to perform operations.
- HWTACACS: Huawei Terminal Access Controller Access Control System

HWTACACS Application Scenario



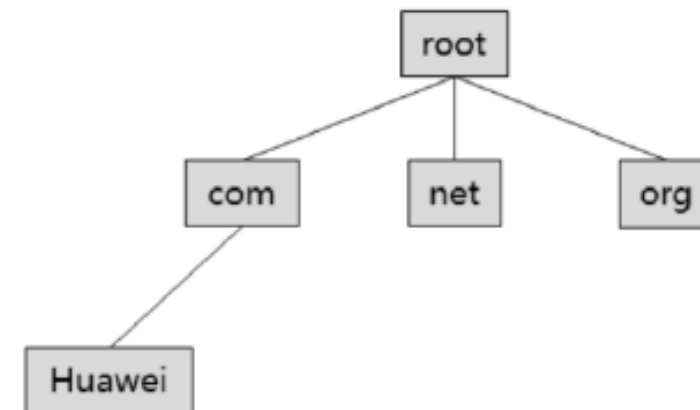
Comparison of HWTACACS and RADIUS

- Comparison of HWTACACS and RADIUS

	HWTACACS	RADIUS
Port	Uses TCP.	Uses UDP. The authentication and authorization port numbers are either 1812 and 1813, or 1645 and 1646, respectively.
Encryption	The device encrypts a packet except its HWTACACS header.	The device encrypts only the password field in a packet.
Authentication and Authorization	Authentication and authorization are separate.	Authentication and authorization are implemented together.
Application	Applies to security control.	Applies to accounting.
Configuration Command Authorization	Supports the authorization of configuration commands.	Does not support the authorization of configuration commands.

LDAP Overview

- **Lightweight Directory Access Protocol (LDAP)** is developed from the X.500 directory access protocol. X.500 organizes objects hierarchically into a tree structure. The X.500 directory service implements identity authentication and access control. LDAP simplifies the X.500 directory and meets Internet requirements.
- The directory service is a system consisting of directory databases and a set of access protocols. The following information can be stored in the directory:
 - ☐ Information about an enterprise employee, for example, a name, email address, and mobile number
 - ☐ Physical information of a device, for example, the IP address, location, vendor, and purchase time
 - ☐ Public certificate and security key
- The features are as follows:
 - ☐ Data is organized in directory mode.
 - ☐ A unified access point is provided for external systems.
 - ☐ Data is stored in distributed mode.
 - ☐ Data query is optimized for fast read operations.

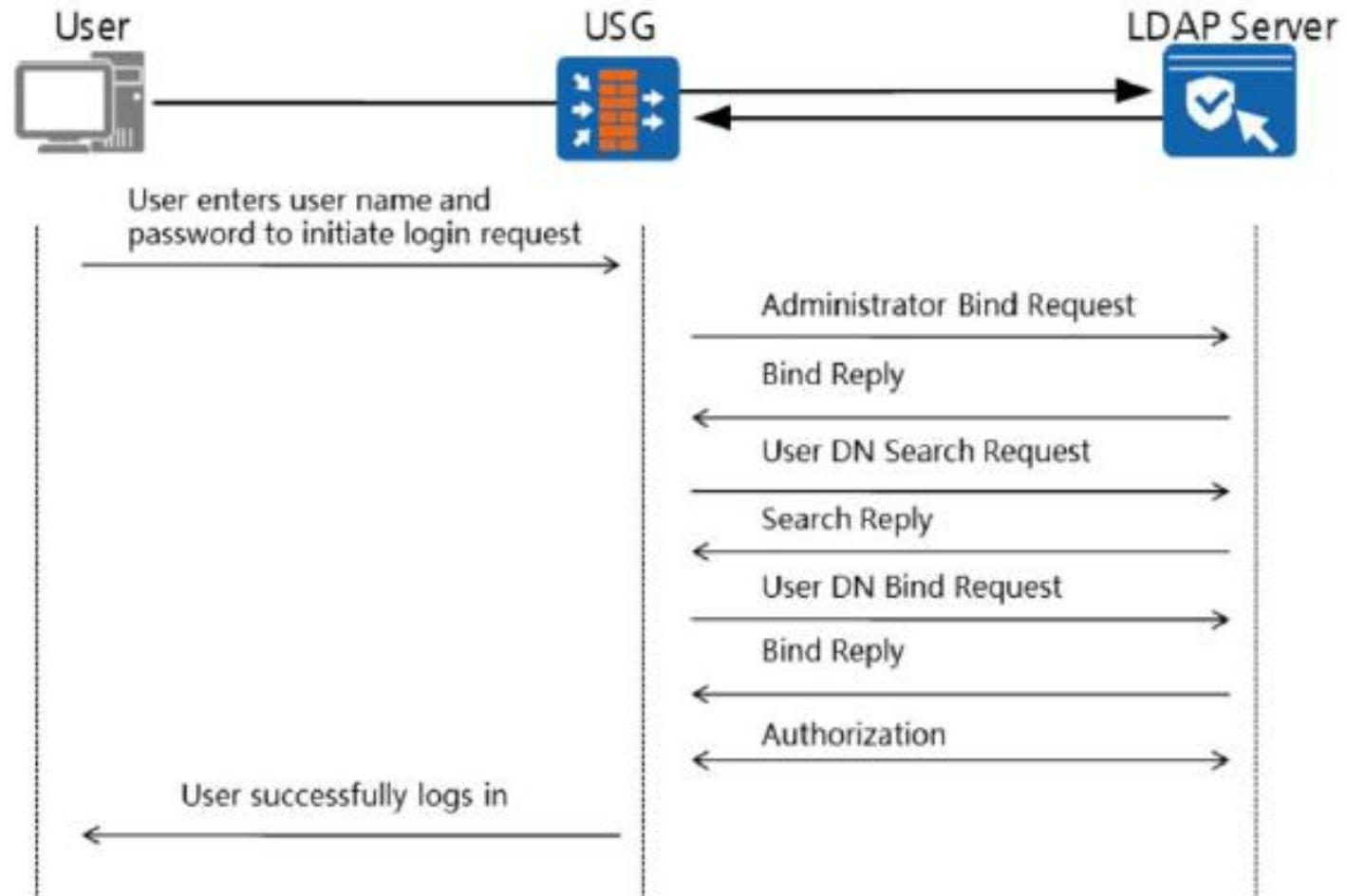


LDAP's Basic Concepts

- In LDAP, information is organized in a tree structure. The basic data unit is an entry, and each entry consists of multiple attributes. An attribute consists of a type and one or more values.
- Directory Information Tree (DIT)
 - A DIT is a collection of directory entries.
- Entry
 - An entry is a node in a DIT and consists of a series of attributes.
- Attribute
 - An attribute describes a feature of an object. It consists of an attribute type and one or more attribute values.
- Relative Distinguished Name (RDN)
 - An RDN uniquely identifies child entries of an entry.
- Distinguished Name (DN)
 - A DN uniquely identifies an entry in a DIT.

Chapter
07

LDAP Authentication Process



The AAA technology provides various user authentication methods.

- User authentication methods include:

- Local authentication

□ A user sends the username and password that identify the user to the firewall through the portal authentication page. The firewall stores the password and performs authentication. This method is called local authentication.

- Server authentication

□ A user sends the username and password that identify the user to the firewall through the portal authentication page. The firewall does not store the password. Instead, the firewall sends the username and password to a third-party authentication server for it to perform authentication. This method is called server authentication.

- Single Sign-on SSO

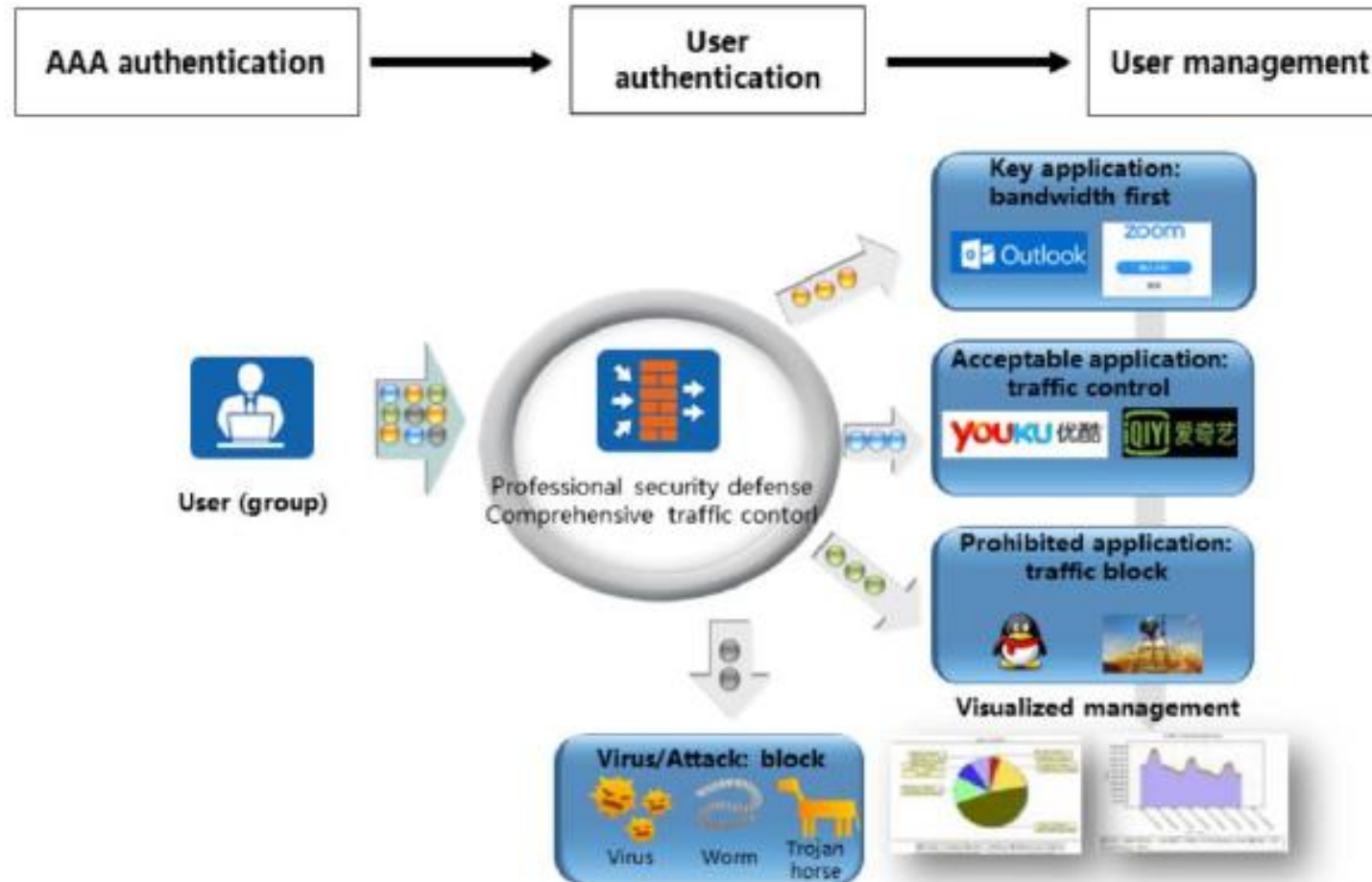
□ A user sends the username and password that identify the user to a third-party authentication server. After the user passes the authentication, the third-party authentication server sends the user's identity information to the firewall. The firewall only records the user's identity information but does not perform authentication. This process is called SSO.

- SMS authentication

□ A user accesses the portal authentication page and requests an SMS verification code. Authentication succeeds after the user enters the correct verification code on the portal authentication page. This process is called SMS authentication.

Chapter
07

User Management Background



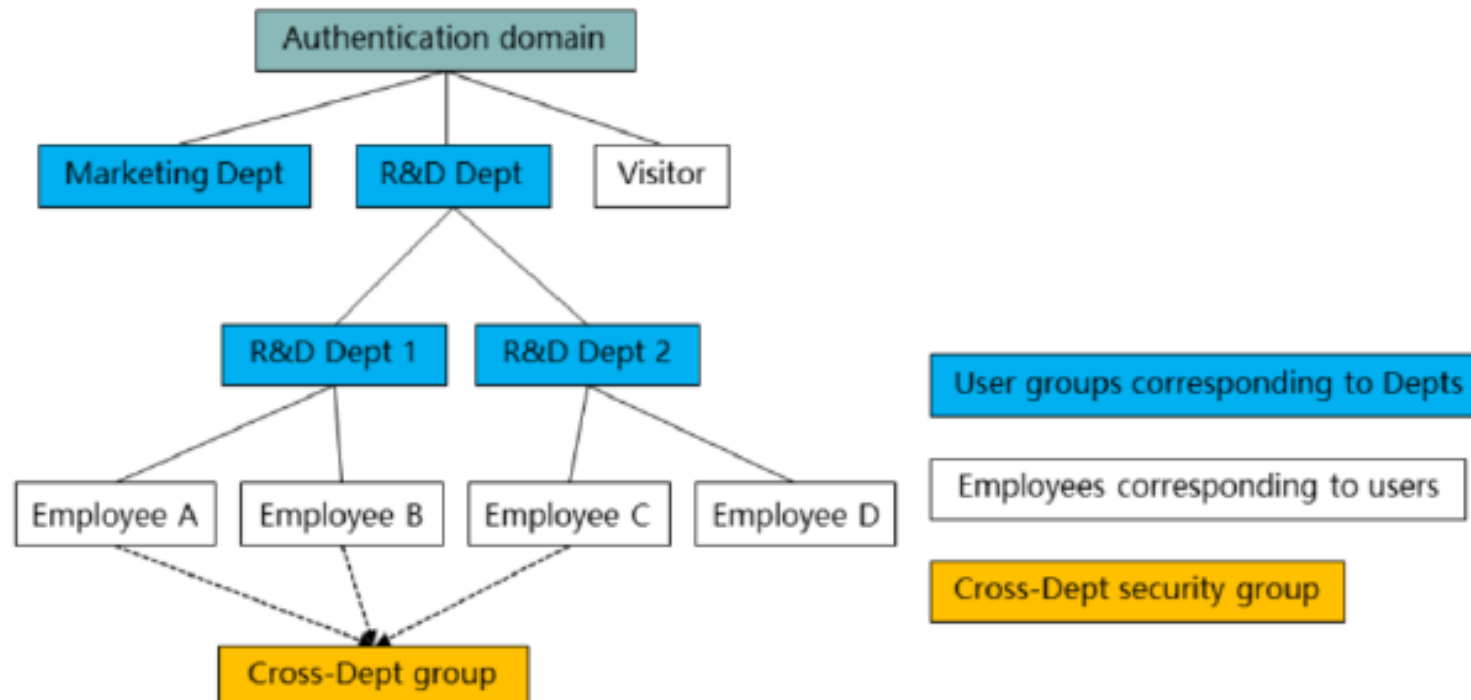
Organizational Structure of Users

- A firewall provides user-level behavior and access control on a network.
- The user organizational structure involves three concepts:
 - **Authentication domain:** The authentication domain is a container of the user organizational structure, similar to the domain in Microsoft's Active Directory (AD) service. The firewall provides a default authentication domain and supports additional user-created authentication domains.
 - **User/User group:** Users and the departments to which they belong are the basic units of an enterprise. An administrator can divide users into user groups based on their departments to form a tree-shaped organizational structure for the intranet. This commonly used structure facilitates lookup and location of users and user groups.
 - **Security group:** A security group is a cross-department group in the horizontal organizational structure. Security groups enable you to manage users in a dimension other than by department. For example, you can create a group between multiple departments.
 - Similar horizontal groups can be used for enterprises that use third-party authentication servers to store organizational structures. For policies based on cross-department security groups, the security groups created on the firewall must be consistent with the organizational structures on the authentication servers.

Chapter
07

Organizational Structure Management

- The system has a default authentication domain. Each user group can contain multiple users and user groups.
- Each user group belongs to only one parent user group, and each user belongs to at least one user groups.



User Classification

- **Administrator**

- An administrator is a user who accesses the device through Telnet, SSH, web, FTP, or the console port and configures or operates the device.

- **Internet access user**

- An Internet access user is an intranet entity that accesses Internet resources-for example, an internal employee at the headquarters of an enterprise. Such a user can directly access network resources through the firewall, which authenticates the user and performs access control according to the policy applied to the user.

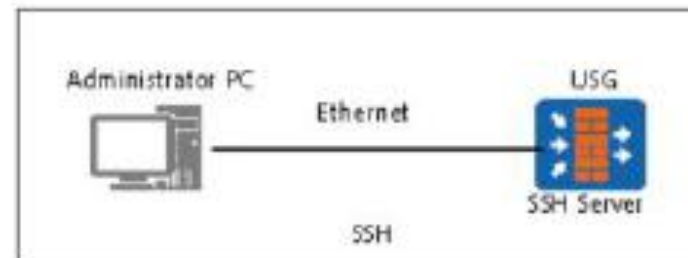
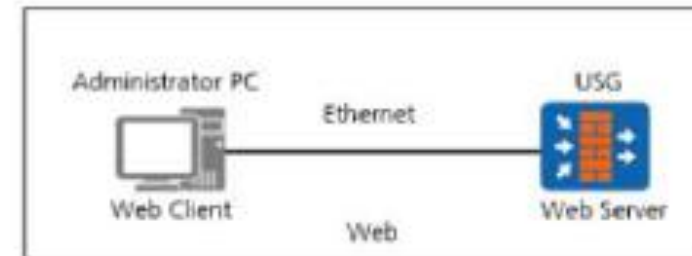
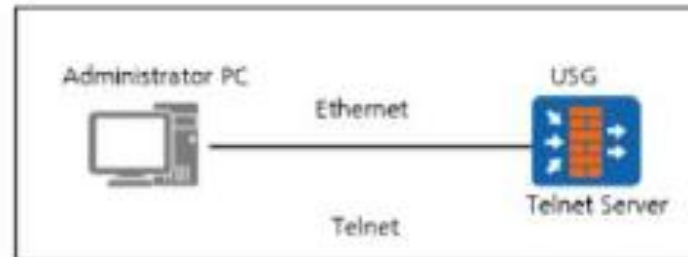
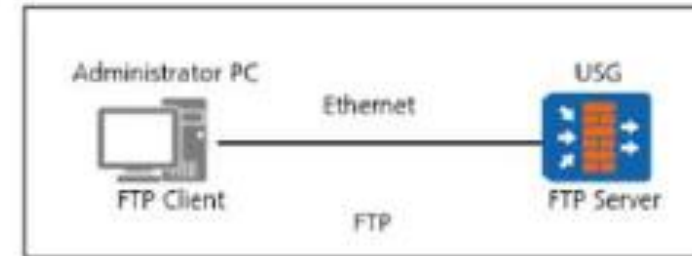
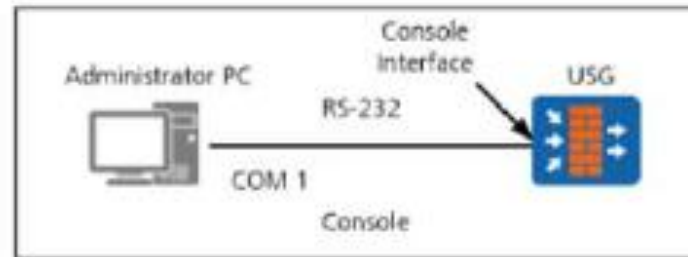
- **Remote access user**

- A remote access user is an extranet entity that accesses intranet resources-for example, an employee at a branch of an enterprise or an employee on a business trip. Such a user must first access the firewall through SSL VPN, L2TP VPN, IPsec VPN, or PPPoE before accessing network resources at the headquarters.

Chapter
07

Administrator Login Modes

- Console
- Telnet
- SSH
- FTP
- Web



Chapter
07

Device Management Using Console, Telnet & FTP

- Choose System > Administrator > Administrator and click Add to create administrator Client 01. Set the device management type to Console, Telnet, and FTP.

The screenshot shows the 'Add Administrator' dialog box with the following fields and settings:

- Name:** Client01
- Authentication Type:** Local authentication (selected)
- Password:** (masked with asterisks, note: 8-64 characters)
- Confirm Password:** (masked with asterisks)
- Role:** system-admin
- Trusted Host 1:** (empty field)
- Advanced Settings:**
 - Service Type:** Web (unchecked), Telnet (checked), SSH (unchecked), Console (checked), FTP (checked), API (unchecked)

Annotations and instructions:

- Set IP addresses of trusted hosts to allow access of only these hosts.** (Points to the Trusted Host 1 field)
- You can configure different roles, including the system administrator, configuration administrator, and audit administrator, for Client01.** (Points to the Role dropdown)
- Select device management types.** (Points to the Service Type checkboxes)

Chapter
07

Device Management Using SSH

- Create administrator Client01 and set the device management type to SSH.

Add Administrator

Name: schuler

Authentication Type: ☒ Local authentication
☐ Server authentication
☐ Server authentication/Local authentication

Password: [REDACTED]

The password must contain at least 8 characters, including uppercase letters, lowercase letters, digits, and special characters. The password cannot contain two or more consecutive identical characters. The password cannot be the same as the administrator name or its reverse form.

Confirm Password: [REDACTED]

Role: system-admin

Trusted Host 1: [REDACTED]

Advanced Settings

Service Type: ☐ Web ☐ Telnet ☒ SSH
☐ Console ☐ FTP ☐ API

SSH Authentication: PASSWORD

SSH Service Settings

STelnet Service (IPv4 and IPv6): ☒ Enable

SFTP Service (IPv4 and IPv6): ☒ Enable

SSH Port (IPv4 and IPv6): 22 (1025-65535=Default Port: 22)

Authentication Attempts: 3 (1-5)

Authentication Timeout: 60 (1-120 seconds)

Key Generation Interval: 0 (0-24 hours)

SSH User Level: 0 (0-15)

You must set the SSH authentication mode. In this example, set the authentication mode to Password.

SSH option (Note: Keep the default configuration of Console, Telnet, and FTP.)

Enabling STelnet and SFTP services.

Chapter 07

Device Management Using the Web UI

- Create administrator webuser and set the user level.

Add Administrator

Name: webuser

Authentication Type: ☒ Local authentication
☐ Server authentication
☐ Server authentication/Local authentication

Password: [masked] * (8-64 characters)
The password must contain at least three of the following character types: uppercase letters, lowercase letters, digits, and special characters. The password cannot contain two or more consecutive identical characters. The password cannot be the same as the administrator name or its reverse form.

Confirm Password: [masked]

Role: system-admin

Trusted Host 1: [empty]

A system administrator can not only configure the device but also manage the file system for software upgrade.

- Choose System > Administrator > Settings and set the HTTPS/HTTP service port. The device does not support disabling the HTTP or HTTPS service or changing its port number when you are logged in through HTTP or HTTPS, respectively.

Enable the HTTPS service and set the HTTPS service port.

Device Service Settings

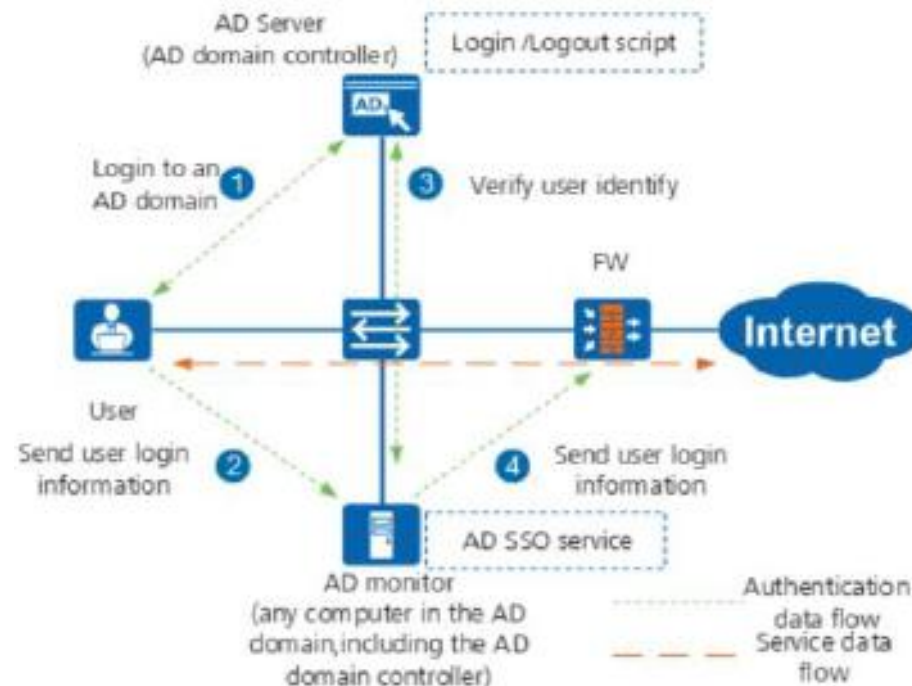
HTTPS Service	☒ Enable	
HTTPS Port	8443	1025-65535
Web Service Timeout	10	1-1440 minutes
Max. Online Web Users	200	1-200
Number of Consecutive Login Failures	3	1-5
Lockout Duration	30	1-60 minutes
Minimum Password Length	8	8-16

- **SSO refers to that the firewall obtains user login information from other authentication systems instead of authenticating users so that users can go online from the firewall.**
- **If users need to directly access network resources after being authenticated by an AD server, you can configure AD SSO to trigger authentication. AD SSO can be implemented in the following modes:**
 - ❑ **Install the SSO service program to receive messages from PCs.**
 - ❑ **Install the SSO service program to query AD server security logs.**
 - ❑ **The firewall monitors AD authentication packets.**
- **Users can use AD SSO to trigger authentication on the firewall. The firewall can have SSO enabled to identify the users that have been successfully authenticated by these authentication systems. In doing so, these users do not need to enter their usernames or passwords when accessing the network. The firewall supports multiple modes for obtaining user authentication success messages during AD SSO.**

Chapter
07

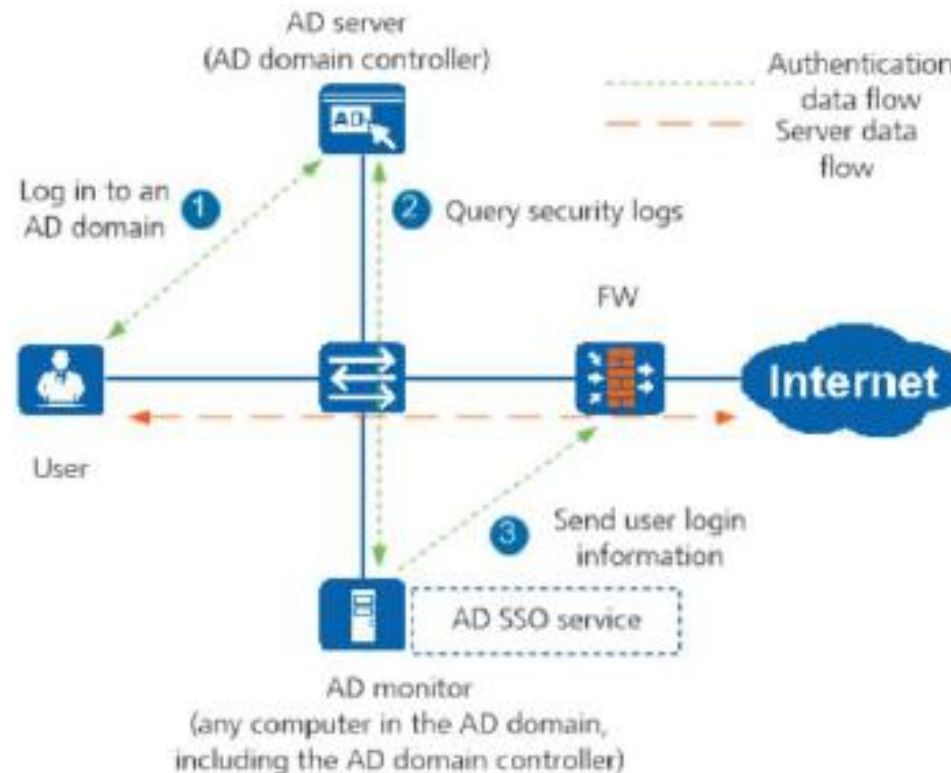
AD SSO (Receiving Message from the User PC)

- You need to deploy AD SSO service on the AD monitor (AD domain controller or other devices in the AD domain), configure login and logout scripts on the AD server (AD domain controller), and set AD SSO parameters on the firewall to receive the user login and logout information from the AD SSO service.



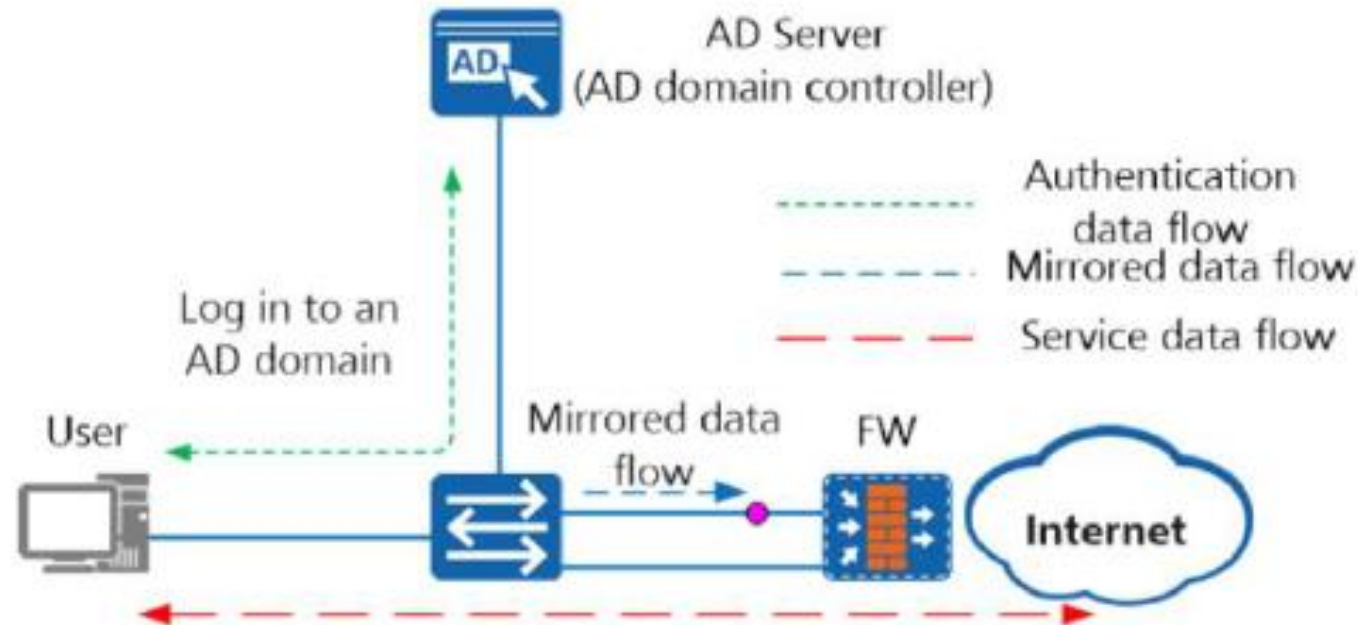
AD SSO (Querying Security Logs from the AD Server)

You need to deploy the AD SSO service on the AD monitor (this can be an AD domain controller or another device in the AD domain), set AD SSO parameters on the firewall to receive the user login and logout information from the AD SSO service.



AD SSO (with the Firewall Listening to AD Authentication Packets)

- In this mode, the program does not need to be installed on the AD server. The firewall listens to the authentication packets sent by users who log in to the AD server (AD domain controller) to obtain authentication results. If a user is authenticated, the firewall adds the mapping between the username and the user's IP address to the online user list.



Portal Authentication for Internet Access Users

- In portal authentication, the firewall or a third-party server provides a portal authentication page to authenticate users. you can trigger built-in portal authentication using the following methods:

- ☐ **Redirected authentication:**

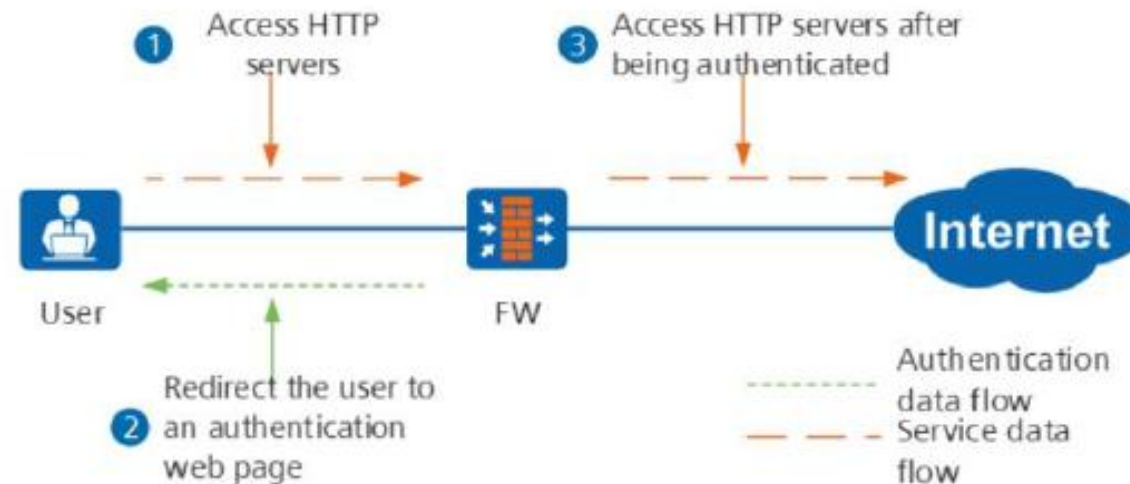
- Redirected authentication implements authentication for Internet access users when they attempt to access HTTP services.

- ☐ **User-initiated authentication:**

- User-initiated authentication indicates that Internet access users proactively access web pages for identity authentication before accessing network resources.

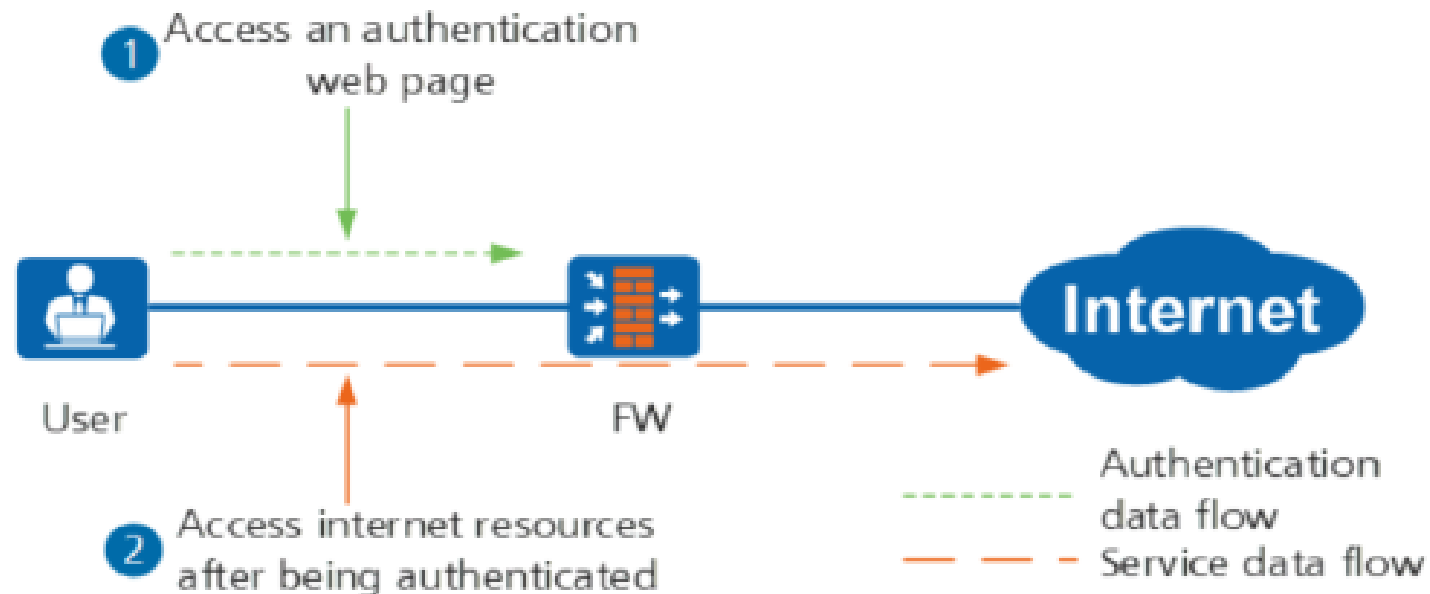
Built-in Portal Authentication Triggering Mode-Redirected Authentication

- When receiving the first HTTP service access data flow traffic from a user, the firewall redirects the HTTP request to the authentication page to trigger identity authentication. If authentication is successful, the user can access HTTP and other services.
- After receiving HTTP packets whose destination port is 80 from an Internet access user, a firewall redirects the user to an authentication web page and triggers identity authentication. The user can access network resources after being authenticated.



Built-in Portal Authentication Triggering Mode User-Initiated Authentication

- An Internet access user initiates an authentication request on the authentication web page hosted on the firewall. After receiving the authentication request, the firewall implements identity authentication for the user.
- The firewall supports user-defined Portal authentication. There are currently two types of user-defined Portal authentication.

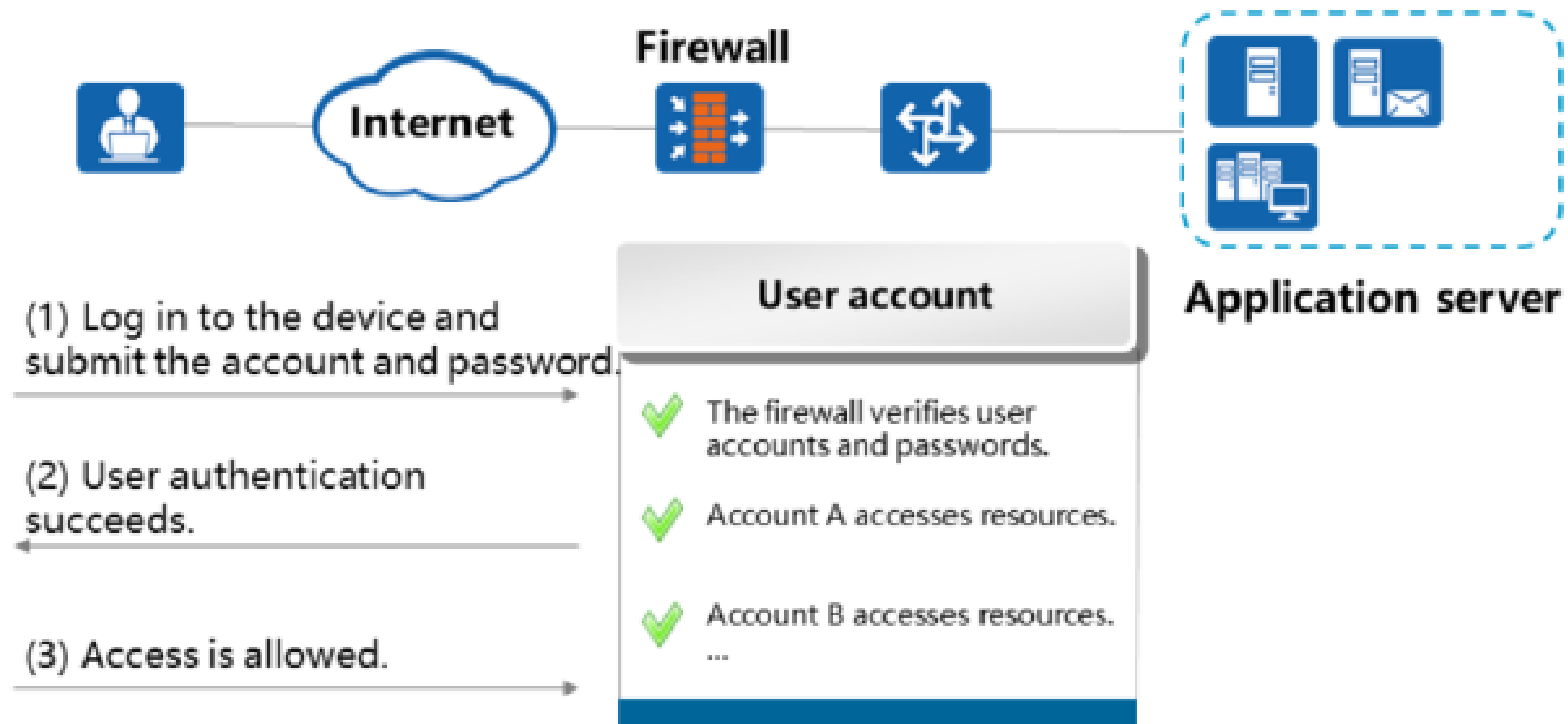


Remote Access User Authentication

- Remote access user authentication refers to the authentication of various VPN access users. The authentication triggering mode is determined by the access mode. Modes include:

- ☐ SSL VPN
- ☐ L2TPVPN
- ☐ IPSecVPN
- ☐ PPPoE

Example of SSL VPN Users Accessing Intranet Resources



Authentication Policy

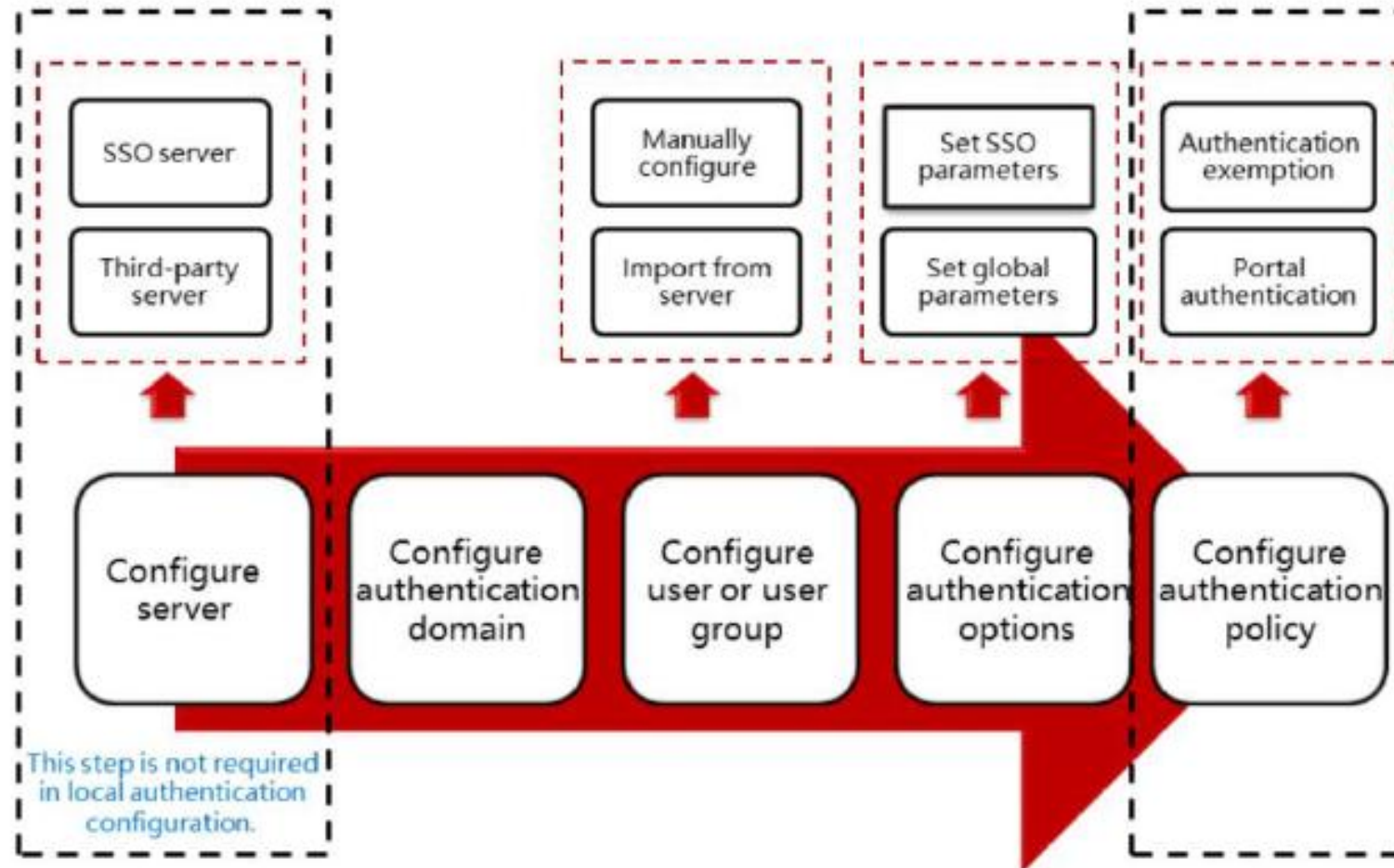
- Authentication policies determine which data flows need to undergo portal authentication and authentication exemption.
- The firewall does not authenticate passing-by data flows by default. Authentication policies are required to filter data flows that require authentication. An authentication policy takes effect on the following authentication modes:



Authentication Policy Explanation

- **An authentication policy is a set of authentication rules that determine whether to authenticate a data flow. An authentication rule consists of conditions and an action. The conditions used by a firewall to match packets are as follows:**
 - ☐ **Source/ Destination zone**
 - ☐ **Source/ Destination address/region**
- **An action indicates how a firewall processes packets. Possible actions are as follows:**
 - ☐ **Portal authentication**
 - ☐ **Authentication exemption**
 - ☐ **No authentication**
 - ☐ **SMS authentication**

Configuration Process



Chapter

07

Configuration a Server (RADIUS)

- Choose Object > Authentication Server > RADIUS and click Add to create a RADIUS server.

Add RADIUS Server

Name		Shared Key	
Primary Authentication Server IP Address		Port	1812 <1-65535> Outgoing Int
Secondary Authentication Server IP Address		Port	1812 <1-65535> Outgoing Int
Primary Accounting Server IP Address		Port	1813 <1-65535> Outgoing Int
Secondary Accounting Server IP Address		Port	1813 <1-65535> Outgoing Int

Advanced Settings

Retransmission Attempts: 3

Unit: [v]

Reply Timeout: [v]

User Name Format: [v]

NAS Port: ☒ New

Test OK Cancel

Set the RADIUS shared key, which is the same as that of the RADIUS server.

Generally, the RADIUS server uses port 1812 for authentication and port 1813 for accounting.

Chapter
07

Configuration a Server (AD)

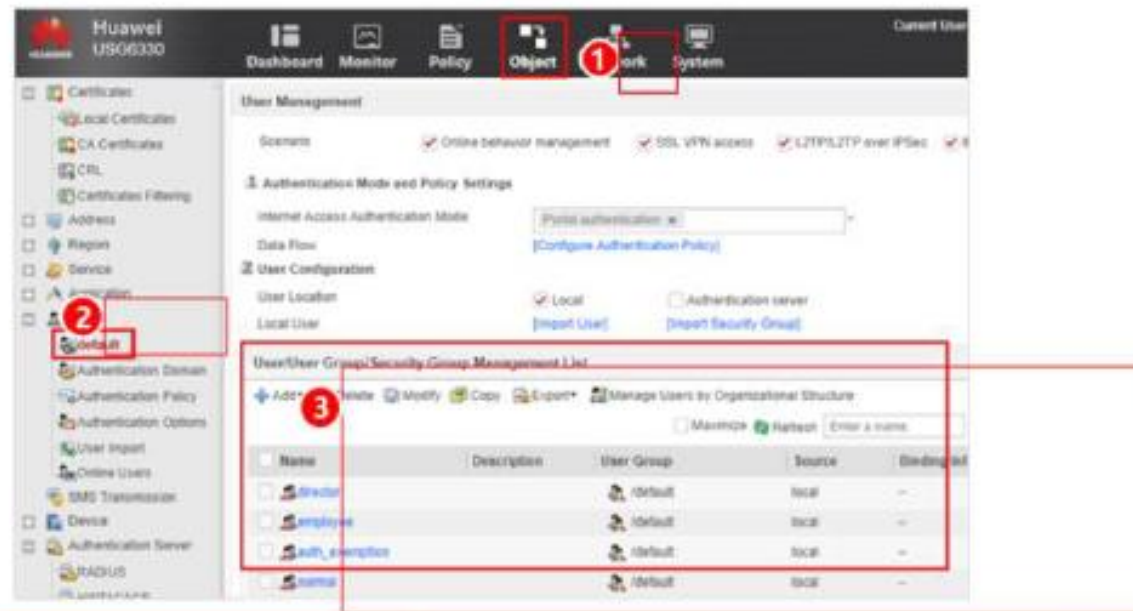
- Choose Object > Authentication Server > AD and click Add to create an AD server.
- During AD server configuration, the system time and time zone of the firewall must be the same as those on the AD server.

Set these parameters based on the settings on the AD server.

Chapter
07

Creating Users & User Groups

- Choose Object > User > default and create a user or user group.



 indicates a user group. The owning group and description of this user group are displayed on the list. The values of the other parameters are all --. The parameters valued -- do not apply to user groups and are unconfigurable.

 indicates a user. The list displays the owning group, binding information, account expiration time, description, and user status (editable).

Chapter
07

Configuring User Attributes

- For existing users, you can click Edit to modify their attributes.

The screenshot shows the 'Modify User' dialog box with the following fields and options:

- User Group:** /default/normal [Select]
- Security Group:** [Select]
- Password:** [Masked] *
- Confirm Password:** [Masked] *
- User Attributes:**
 - Expiration Time:**
 - ☒ Never
 - ☐ Specified Time
 - Account sharing:**
 - ☒ No binding
 - ☐ Unidirectional binding (The account can log in only to the bound address. Multiple users can use the address.)
 - ☐ Bidirectional binding (The account can log in only to the bound address. Only this user can use the address.)

Annotations in the image:

- A blue box on the left says: "Allows users to share this account to log in." with an arrow pointing to the 'Account sharing' section.
- A blue box on the right says: "Indicates the time when the account will expire." with an arrow pointing to the 'Expiration Time' section.

When Layer-3 devices exist between the user and the device, if the user is bidirectionally bound to a MAC address and is exempted from authentication, the user fails to log in. If the user is bound to a MAC address and the SSO authentication mode is used, the MAC binding attribute does not take effect.

Chapter
07

Configuring Authentication Options (Global Configuration)

- Choose Object > User > Authentication option > Global configuration/Local Portal and perform the configuration.

A user can change the password on the login authentication page, and this configuration is available only in this scenario.

This option indicates that a user must change their password upon the first login.

This area needs to be configured for pushing authentication web pages to Internet access users. The default authentication port is port 8887.

Global Configuration Local Portal User-defined Portal Resource Customization

Password Settings

Password Strength: ☒ High ☐ Medium ☐ Low

☐ Force Password Change upon First Login

Password Expiration: ☒ Never ☐ Expiration time

Global Configuration Local Portal User-defined Portal Resource Customization

Local Portal Authentication

☒ Enable ☐ Disable

Redirection Authentication Mode: ☐ HTTP ☒ HTTPS

Authentication Port: 8887

Lockout After Failed Login: ☒ Enable ☐ Disable

Maximum Failed Login Attempts: 3

Lockout Duration: 5

Authentication Conflict

The following action will be taken when account sharing is disabled and an account logs in a second time:

☒ Forcefully log out the original IP address and authenticate the new IP address.

☐ Allow the original IP address to continue using services and do not authenticate the new IP address.

Redirection after Authentication

☒ No redirection

☐ Redirect to the previous web page

☐ Redirect to a user-defined URL

Chapter
07

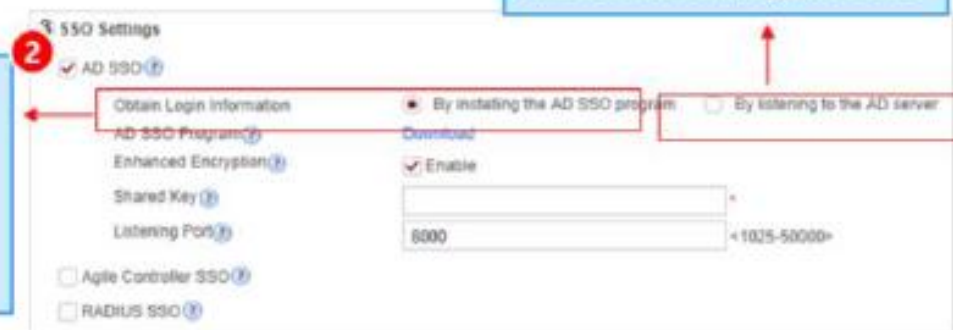
Configuring Authentication Options (SSO)

- Choose Object > User > default > Authentication Mode and Policy Settings and configure SSO.



Set the Internet access mode to SSO authentication.

To configure AD SSO in no-plug-in mode, you need to download the AD SSO program and decompress it. Then install **ADSSO_Setup.exe** on the AD monitor and set AD SSO service parameters.



AD SSO in no-plug-in mode

Chapter

07

Configuring an Authentication Policy

- Choose Object > User > Authentication Policy, click Add, and configure an authentication policy.

Select an action for the authentication policy.

Add Authentication Policy

Name:

Description:

Tag:

Source Zone: [Multiple]

Destination Zone: [Multiple]

Source Address/Region:

Destination Address/Region:

Action:

- ☒ Portal authentication
- ☐ SMS authentication
- ☐ Authentication exemption
- ☐ No authentication

Portal Authentication Template: ☐ Enable

OK Cancel

Chapter

07

Importing Users Locally or from a Server

- Choose Object > User > User Import.
- Local import: supports the import of user information in CSV files and database DBM files to the local device.
- Server import: Importing users from the authentication server in batches refers to importing user or user group information on the authentication server to the device based on the server import policy.

Download a CSV template, input required data, click **Browse**, and upload the data.

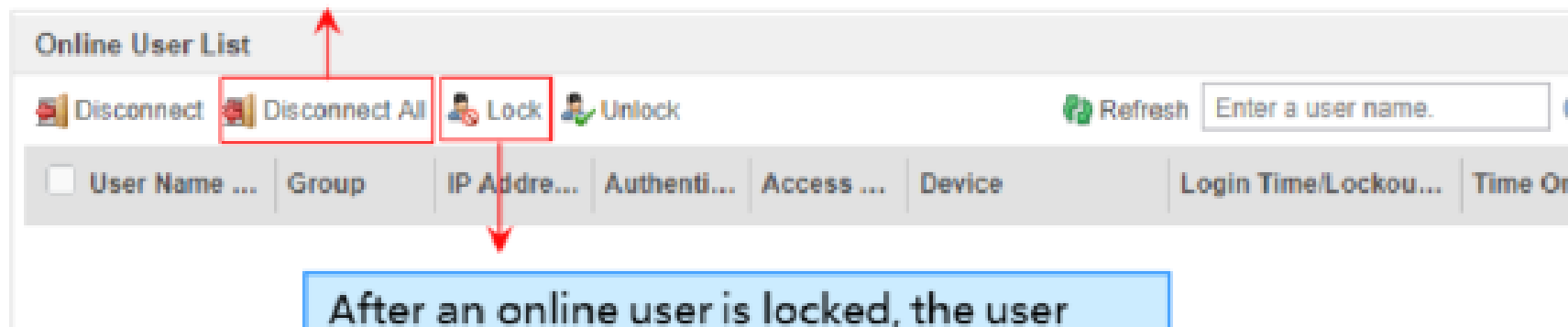
Chapter

07

Online User Management

- Choose Object > User > Online User and perform online user management.
- To restrict all Internet access behaviors of some users within a time segment, you can lock out these online users.
- You can also force some untrusted online users to log out.

Select a user to force the user out.



After an online user is locked, the user cannot access network resources, log out, or initiate another authentication request.



Thank You