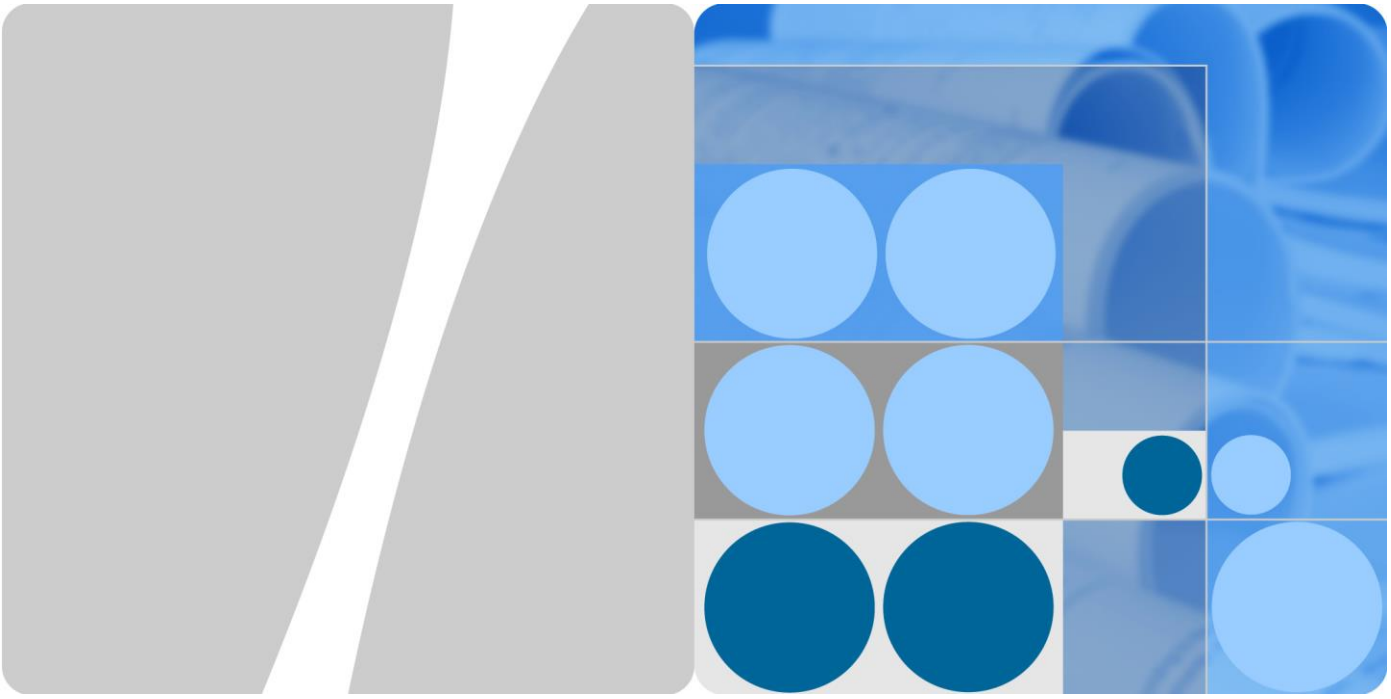


Agile Controller-Campus
V100R002C10

Security Technology White Paper

Issue 01

Date 2016-04-15

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

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

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

Notice

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

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

Huawei Technologies Co., Ltd.

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

Website: http://e.huawei.com

Contents

1 Overview

1.1 Introduction to the Agile Controller

Introduction

The Agile Controller, as the controller for enterprise campus network, implements policy control and security protection for the entire network. It uses a uniform policy engine to implement unified access policies and multi-dimensional authentication and authorization based on the user, device type, access time, access location, and access mode, meeting the multi-layer enterprise access and authentication requirements and access requirements of multiple terminals. It also supports full lifecycle guest management to allow guests to access the Internet anytime and anywhere. This improves guests' working efficiency and enterprises' brand image and reduces IT operation and maintenance (O&M) burdens.

The Agile Controller provides the following basic functions:

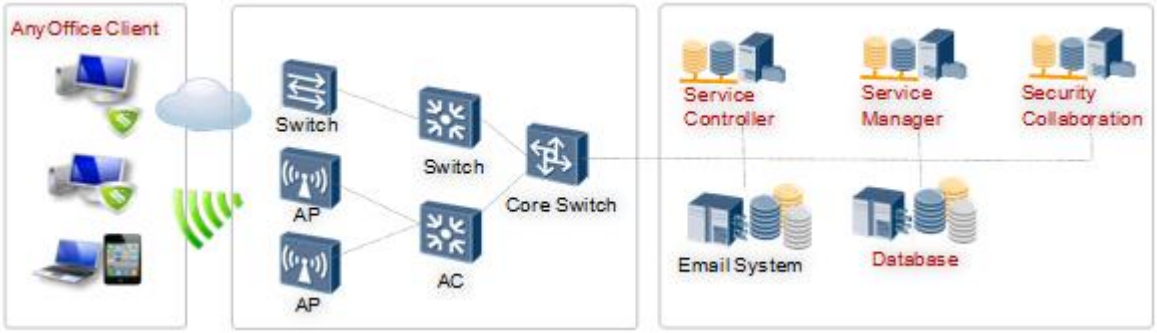
1. Network Access Control: provides multi-dimensional network access control functions and flexible network access authorization policies based on the combination of user identity, terminal type, access location, access time, and terminal compliance check results.
2. Guest Access Management: supports full lifecycle guest management to uniformly manage guest application, approval, distribution, authentication, and deregistration.
3. Free Mobility: provides a security group-based rights control model. Administrators can divide access users and server resources to different security groups and define users' resource access permissions based on the security group, guaranteeing experience of the VIP security group on the edge firewall.
4. Service Orchestration: defines service flows and service orchestration policies based on the IP zone and security group. Working with a Huawei agile switch, it can direct different network flows to different service devices to realize service-based flow control.
5. Terminal Management: provides the device identification function to determine the device type and its operating system based on data features obtained by the device identification probe.

6. User Management: supports department, user account, and role management, AD/LDAP authentication for external data sources, online users, account blacklist, and certificate authentication.
   a. Network Device Management: divides network devices into groups and manages the devices. Administrators can define and manage RADIUS access devices, free mobility devices, and service orchestration devices.

System Architecture

The Agile Controller is comprised of the service manager (SM), service controller (SC), client, and database.

The following figure shows the system components.



The Agile Controller can be deployed in a centralized or distributed manner. You can deploy the SM and SC on the same server, or deploy multiple SC servers separately.

- SM

The SM manages service configurations and the SC servers of the Agile Controller. The SM uses the Browser/Server (B/S) architecture and provides a web-based graphical user interface (GUI) for system administrators to perform service management tasks, such as managing users and configuring security policies. As a service management server, the SM also manages command delivery between each SC and the connected nodes to transmit various services.

- SC

The SC is responsible for access authentication and device configuration and management. The SC consists of the following components: RADIUS server, Portal server, authentication server, and network server.

RADIUS server: provides standard RADIUS services to implement unified access policies and multi-dimensional authentication and authorization based on the user, device type, access time, access location, and access mode.

Portal server: provides standard Portal authentication services and web-based authentication pages for connection with access devices through the Portal protocol.

Authentication server: provides the basic authentication service platform to control SACG access and terminal upgrade.

Network server: provides network device configuration functions and supports XMPP and Telnet protocols. You can implement device service configurations on the network server through free mobility and service orchestration.

- Client

The AnyOffice client is a user authentication access client and supports the Windows operating system only.

- Database

The database stores service data of the Agile Controller.

1.2 Security Threats to the Agile Controller

Management Layer

- Lack of security rules and regulations or strict implementation of them
- Weak sense of security
- Security vulnerability caused by untimely installation of security patches
- Account sharing, which makes liability tracing impossible
- Incomplete security documentation

Application Layer

- Access authentication: buffer overflow, cross-site scripting, and SQL injection
- Identity authentication: network interception, brute force, dictionary attack, cookie replay, and theft proof
- Authorization: privilege elevation, confidential data leak, data tempering, and temptation
- Configuration management: unauthorized access to the management interface, unauthorized access to the configuration storage device, retrieval of plain-text configuration data, lack of personal records, and unauthorized process and service accounts
- Sensitive data: access to the sensitive data in the storage device, network interception, and data tempering
- Session management: session hijacking, session replay, and man-in-the-middle (MITM) attack
- Encryption technology: vulnerable key generation or management, and weak or user-defined encryption technology
- Parameter operation: character string query, window field operation, cookie operation, and HTTP header operation
- Anomaly handling: information leak and denial of service (DoS)
- Security audit: users refusing to execute an operation, and attackers taking advantage of applications that do not leave traces

System Layer

- Virus, Trojan horse, and worm: A virus is a type of designed program, which maliciously breaks operating systems or applications. The Trojan horse is similar to the virus except that the former disguises malicious code with harmless data or executable programs. Similarly, a worm acts as the Trojan horse except that the former replicates itself from one server to another. Besides, the worm is hard to detect because it irregularly creates visible files. Generally, worms are noticed until they start to consume system resources, slowdown the system, or stop some applications.

- Footprint: Footprints include port scanning, ping scanning, and NetBIOS enumeration. With such footprints, attackers can collect system-level information and make severe attacks. Footprints reveal such potential information as account information, operating system and other software versions, server names, and database architectures.
- Password cracking: Due to the failure in establishing an anonymous connection to the server, the attacker attempts to establish the connection through authentication. In this regard, the attacker must know a valid user name and the user password. Using the default account leaves a chance for the attacker. Then, the attacker needs only to crack the account password. If you set no password or a weak one, the attacker makes the move easier.
- DoS: DoS attacks can be implemented in multiple modes towards several targets in the basic architecture. On the host, the attacker can interrupt services by forcibly attacking applications, or by attacking known vulnerabilities.
- Randomly executed code: If an attacker executes malicious code on your server, the attacker intends to damage server resources or to further attack downstream devices. If the process of the server that runs the attacker's code is executed without authorization, the risk brought by the randomly executed code increases. Common vulnerabilities are as follows: The server with no patch installed that allows path traversal and buffer overflow attacks is in use.
- Unauthorized access: Loose access control may allow unauthorized users to access restricted information or execute restricted operations.

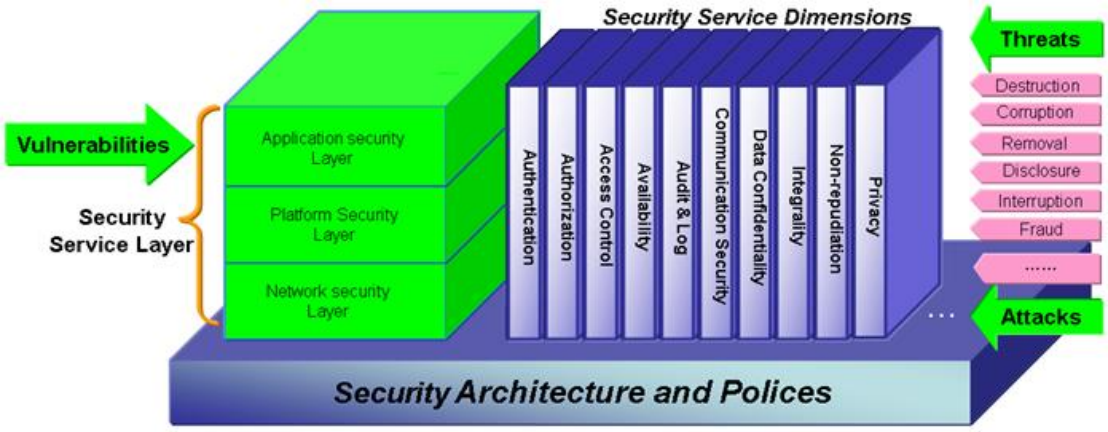
Network Layer

- Information collection: Attackers discover and analyze devices using the same method as other types of systems. Normally, the attackers scan the interface first. After identifying the open port, they obtain the device type, operating system, and application using title capture and enumeration. With such information, attackers exploit the known vulnerabilities whose security patches may not be updated.
- Network sniffing: indicates sniffing or intercepting the data, such as the plain text password and configuration information on the network. Using a simple packet probe, attackers can easily obtain all plain-text information, decrypt SHA-encrypted packets, and obtain the useful payload that you think is secure. To probe packets, attackers need to install the packet probe in the communication tunnel between the server and the client.
- Network spoofing: indicates a method of concealing user identity on the network. To create a fake identity, the attacker forges a source IP address. Using spoofing, the attacker conceals the real attack source, or bypasses the ACL that limits the access to the host based on the source address.
- Session hijacking (MITM attack): Session hijacking tricks the server or the client into believing that the upstream host is a legal one. In fact, the upstream host is of the attacker. It controls the network and makes the attacker's host look like the expected destination.
- DoS/DDoS: indicates the denial of user access to servers or services.

2 Security Architecture

2.1 Agile Controller Security Architecture

According to the communication system security model (ITU-T X.805), the Agile Controller security architecture consists of three layers and 10 dimensions, as shown in the following figure:



There are three Agile Controller security layers:

- Network security
- Platform security
- Application security

There are ten security service dimensions:

(Security requirements and security mechanisms are considered from these ten dimensions.)

- **Authentication:** Before a user accesses a network or a system, there must be a security mechanism to verify the user's identity, for example, to verify the user's login account.
- **Authorization:**Legitimate users can access network or system resources only after being authorized.

- **Access control:**prevents unauthorized access to or use of network resources. For example, the Untrust-Trust access to the system is protected against ill-intended behavior.
- **Availability:**indicates the degree to which a system or a resource is available during data processing. The availability measures, such as redundancy and backup, are important security protection methods. In the Agile Controller system, servers are in 1+1 redundancy, and the cold backup migration solution is available.
- **Audit and Log**: records and audits user behavior by using logs and audit policies.
- **Communication security**: secures data flows from ill-intended behavior including tempering and forgery, ensuring secure access between different systems or networks.
- **Data Confidentiality**: prevents information and data leaks. Encryption and decryption are used for data confidentiality.
- **Integrality**: identifies the integrity and accuracy of data and files, preventing malicious tempering and replacement.
- **Non-repudiation:** repudiates an individual or entity's denial of an operation with proofs. The proof includes the data source, proprietary, and source application. These proofs must be presented for a third-party to prove that some events occurred or operations were implemented. Non-repudiation is associated with security events including login, authentication, authorization, and access.
- **Privacy:**provides protection over the information of network operation observation. For example, when a user accesses a website, the geographical location, IP address, and DNS name of the user are protected. Agile Controller encrypts and stores user numbers.

Security risks

According to ITU-T X.805, the security risks and attacks of a telecommunication system are as follows:

- Destruction
- Corruption
- Removal
- Disclosure
- Interruption
- Fraud

2.2 Overview of the Agile Controller Security Solution

According to the security model, the Agile Controller security solution is designed from three aspects: network security, platform security, and application security.

- Network security: protects the Agile Controller system by using security networking, including security zone division and firewall isolation.
- Platform security: provides a secure and reliable environment for the Agile Controller system by enhancing the security level of the operating system through security hardening and patch installation.
- Application security: includes transmission security, user management, log management, and user data management. These security policies apply to corresponding services.

The following chapters are presented in the sequence of application security, platform security, and network security.

3 Application Security

3.1 User Data Security

3.1.1 User Data Protection

Personal data: indicates the data that can be used or referenced to identify a person, including the ultimate user name, account, call and callee numbers, communication record, communication time, and positioning data.

Sensitive data: varies with application scenarios and requires risk-oriented analysis and judgment. Sensitive data includes passwords, bank accounts, massive personal data, communication contents, and keys.

Personal data always involves user privacy. In many countries, the law poses certain requirements on personal data protection. The Agile Controller system protects the personal data.

System Compatibility

1. The Agile Controller system does not involve the bank accounts or passwords of enterprises and individual users.
2. The user login and logout logs collected by the Agile Controller terminals include the accounts such as email addresses and contact information, IP addresses, and MAC addresses of enterprises. Such private data is secured through security networking, login authentication, security protocol, permission control, and operation auditing.
3. The violation information collected by the Agile Controller compliance check function includes the accounts, IP addresses, MAC addresses, and department information of enterprises. Such private data is secured through security networking, login authentication, security protocol, and permission control.

4. The asset software and hardware information collected by the Agile Controller asset management function includes the accounts, IP addresses, MAC addresses, and PC software information of enterprises. Such private data is secured through security networking, login authentication, security protocol, and permission control.
5. The auditing reports collected by the Agile Controller employee behavior audit function includes the accounts, IP addresses, MAC addresses of individual users, and the department information and historical PC operation records (such as the use of USB disks and online records) of enterprises. Such private data is secured through security networking, login authentication, security protocol, and permission control.

User Data Content

1. Basic user data
   - User account
   - User name
   - User title
   - Phone number
   - Mobile phone number
   - Office address
   - Email address
   - Department
   - Auxiliary description (added by administrators)
2. Terminal users' login and logout logs
   - User account
   - User name
   - Department
   - IP address
   - MAC address
3. Compliance check data
   - User account
   - User name
   - Host name
   - IP address
   - MAC address
   - Department
   - Violation events collected by the compliance check, for example, a required patch is not installed, the antivirus software is not installed, and an illegitimate network share is created
4. Asset management data
   - Asset ID
   - IP address
   - Asset user
   - Asset owner
   - MAC address
   - PC software list

- PC hardware list

5. Employee behavior audit data
   - User account
   - User name
   - Host name
   - IP address
   - MAC address
   - Department
   - Events collected by the behavior audit function, for example, the use of USB disks and historical online records on PCs

Application Scenarios of User Data Content

User Information		Application Scenario (Example)
Basic user data	User account, user name, user title, phone number, mobile phone, office address, email address, department, and auxiliary information (added by administrators)	Administrators view users' accounts.
Terminal users' login and logout logs	User account, user name, department, IP address, and MAC address	Administrators view terminal users' login and logout records.
Compliance check data	User account, user name, department, IP address, MAC address, host name, and violation events collected by the compliance check	Administrators view the compliance check reports.
Asset management data	Asset ID, IP address, MAC address, asset owner, asset user, PC software list, and PC hardware list	Administrators view asset reports.
Employee behavior audit data	User account, user name, department, IP address, MAC address, host name, events collected by the behavior audit function	Administrators view employees' behavior audit reports.

User Data Retention Period

The Agile Controller stores the previous data for backup and after-event tracing based on enterprise service requirements. The retention period is stipulated by related laws and regulations.

User Data Security Solution

1. Technologies
   - Security networking: See section 5.1 Security Networking Modes"5.1 Security Networking Modes."
   - Security communication protocol: The Agile Controller supports secure communication protocols, including HTTPS.
   - Login authentication protection: The Agile Controller accesses personal data through the web UI. The user name and password are required for authentication when the Agile Controller logs in to the web and operating system where display and store personal data, as well as the database.
   - Permission control: The web UI supports role-based permission control. Unauthorized users cannot access personal data information or use related functions. In addition, permission control applies to accessing the operating system and database.
2. Audit
   - Non-query operations are logged.
3. Management
   - Logs and reports containing personal data can be sent out from the enterprise network only under the customer's permission.

3.2 Authentication and Authorization Management

3.2.1 Role-specific User Management

The authorization system is based on roles. Account- and role-based authorization uses the minimum authorization principle. That is, a role is authorized with only necessary permission, and an account is authorized to only necessary roles. The system supports data-level role control, which allows users with different roles to perform the same function, but not to query the sensitive information of the function.

In addition, based on roles and accounts, the operating system and database have separate management accounts, maintenance accounts, and application accounts. Therefore, the management, maintenance, and operations are separated.

Role Management

To protect personal data, the system adds a security administrator by default to perform security-related functions and view sensitive data.

User Management

Web applications provide a default system administrator. The system administrator has the rights of all functions. The Agile Controller can create different administrators and assigns roles (operation and maintenance permission) to corresponding administrators.

The groups and accounts of the operating system, database, and application system are properly planned. One user can have one account and accounts are audited. The audit policies vary with roles and accounts. User behavior is recorded for the audit on the condition that the system performance is not or slightly compromised.

Permission Management

The Agile Controller assigns different permissions to different users.

The system presents the permissions through the permission tree. The administrator can select permissions on the tree and assign them to a role. This indicates that the role and related rights of a user can be defined.

The system identifies the permission on sensitive information and grants the permission only to the security administrators.

3.2.2 Security Management

To prevent unauthorized users from logging in to the system illegitimately, the Agile Controller provides the login verification code and strict password security polices, ensuring the validity of the login users and securing the systems

User and Password Policies

1. Password strength

   A password must contain:

   - At least eight characters
   - At least one lower-case letter
   - At least one upper-case letter
   - At least one digit
   - At least one special character: `~!@#$%^&*()-_=+\|[{}];:'",<.>/? and a space
   - 密码不能包含超过两个连续相同字符,不能与帐号或者帐号的倒写一样

2. Password validity period

   A password is valid for 30 days by default. The period can be customized. A user is forced to change the password after the validity period expires.

3. Historical password restriction

   A used password cannot be employed again. You can configure the number of restricted history passwords.

4. Passwords cannot be stored in plain text

   Passwords, including the web password, FTP password, operating system account password, and database account password, cannot be stored in plain text. Passwords are encrypted in the scenarios where they do not need to be restored, whereas passwords are encrypted and decrypted in the scenarios where they need to be restored.

5. Password usage rules

   The passwords entered in the Agile Controller cannot be displayed in plain text or duplicated.

   Administrators can change only their own passwords with their old passwords authenticated.

   Administrators' operations of resetting other administrators' passwords are recorded in audit logs.

6. Verification code

Web applications use the disposable verification code.

Screen Lock

The web application client of the Agile Controller supports automatic screen lock. When the login user does not perform any operation for a specified period of time, the screen is locked. The user needs to re-enter the password for authentication again.

3.3 Data Transmission Security

3.3.1 Transmission Protocols

The Agile Controller uses a set of security protocols and applications to secure data transmission.

1. Web applications use HTTPS.
2. The authentication messages between the AnyOffice agent and the Agile Controller server use the TLS protocol for communication encryption.
3. The Agile Controller server uses the web service security framework and supports HTTPS to secure the web services provided to the external users.
4. The communication between the SM and SC components of the Agile Controller is encrypted using HTTPS to ensure communication security.
5. No security protocol is used for transmission of data between the Agile Controller server and database. To ensure communication security, the Agile Controller server and database must be deployed on the same trusted network, where a firewall is deployed. External users cannot access database resources.

3.3.2 Triple Isolation

The Agile Controller provides services at the control plane, such as terminal PC authentication and access control. This function is implemented by the authentication server and Portal server components of the SC server.

The Agile Controller also provides management services for administrators, such as the system management from the Agile Controller server. This function is implemented by the SM server.

The Agile Controller provides user-oriented services, such as user authentication. This function is implemented by the AnyOffice, Web, WebAgent, or built-in 802.1X client of the operating system.

Different components of the Agile Controller can run independently or be deployed on different servers to isolate from each other.

3.4 Security Management for Service Functions

The integrity check for software distribution and patch management prevents malicious use and secures system services.

The Agile Controller provides software distribution and patch management services for PCs. Before distributing software and patches, the Agile Controller server computes the integrity check values for the software and patches. The Agile Controller Agent installed on PCs

computes the integrity check values for the software and patches and compares the values with those computed by the Agile Controller server.

In addition, software distribution and patch management are enabled only when administrators implement policies.

3.5 Log Management

The Agile Controller records logs according to Huawei log standards. Each log contains the event time, user ID, event type, name of the accessed resource, and event result.

The Agile Controller also audits logs periodically to rule out security hazards.

3.5.1 Operation and System Logs

Operation Logs

An operation log records the operation initiated by the users on the Agile Controller web client and corresponding results. The log displays operation at a specific time period and therefore helps maintenance personnel to locate faults. The audit personnel can export and query the operation log through the web page to audit the operation of the maintenance personnel, discovering improper or malicious operations in a timely manner. Moreover, the log also serves as the evidence against repudiations.

The operation logs contain the following:

- User login events such as user login and logout
- User management events such as adding, deleting, or modifying a user, changing a password, and changing permission
- System management events such as adding, deleting, or modifying a system parameter

System Logs

System logs record the operating status of the system and servers, and are generated by different modules of the system. With the system logs, the maintenance personnel learn about and analyze the operating status of the system, and then locate and resolve anomalies in a timely manner. Moreover, the operation and maintenance personnel can export the system logs and send the logs to the technical support personnel for locating faults.

The system logs contain the following:

- Abnormal status and actions such as configuration failures
- Key events such as system startup and system shutdown

3.5.2 Operating System Logs

The Agile Controller runs the Windows Server operating system. The operating system records the following types of system logs:

- System logs
- Security logs
- Application program logs
- Performance logs and alarms

The operating system logs are reserved permanently. To manually delete a log, dump it first.

3.5.3 Database Logs

The Agile Controller runs the SQL Server database. The database logs contain the following:

- Operating logs: record the operating status of the database.
- Audit logs: record data operations.

4 Platform Security

4.1 Operating System Security

- Installation
  - Install only the required software packages and service components, reducing system vulnerabilities and risks of being attacked.
  - Use the latest or most stable operating system patch.
  - Configure security settings for the Windows/Suse Linux operating system during installation.
  - Install antivirus software for the Windows operating system to periodically scan viruses, preventing damages to the system.
- System logs
  - Record all authentication-related events.
- Enable network services and ports following the minimum principle.
  - Enable only service-related ports and other ports are disabled by default.
  - Bind network services only to the service related ports.
- Start up services following the minimum principle.
  - Only necessary services are started up.
- Security logs
  - Record authentication-related events, including login failures and authorization events, helping analyze user login status.
  - Record logs of scheduled tasks.
- System access, authentication, and authorization
  - Grant each user with the minimum permission for a task. Applications can be carried out only by the permitted accounts.
- Account and operating environment
  - The password of an account must have the required strength.

- The account is locked when your login attempts exceed the threshold.

4.2 Database Security

- Installation
  - Install only the required services and protocols.
  - Configure encrypted passwords in database files.
  - Use the latest or most stable database patch.
  - Harden the SQL server database and do not enable high-risk system storage processes to reduce security risks.
  - Start the SQL server database using a non-administrator account to authorize the minimum operation rights.
- Account management and password policies
  - Assign a specific usage for each account. Separate application accounts from management accounts.
  - Reserve only necessary default accounts provided by the database manufacture. Lock or delete unnecessary accounts. The default accounts apply only to given tasks, not to daily maintenance.
  - The password of the account has the required strength.
  - Do not specify individual accounts, R&D accounts, or test accounts.
  - Periodically audit the accounts.
- Permission control
  - Grant each account with the minimum permission for a task.
  - Do not grant authorization permission to application accounts.
  - Connect application programs to the SQL server database using a non-SA administrator account.
- Backup management
  - Provide maintenance plans for system service databases and back up data periodically to prevent data loss.
- Reliability
  - To ensure service availability, configure three database instances including the principal database, mirror database, and witness database instances on the SQL server database. The mirror database functions as a data backup to the principal database, and the witness database monitors the principal database. When a fault occurs, services are automatically switched to the mirror database to ensure service reliability.
  - To ensure service availability and reliability of Oracle databases, the Real Application Clusters (RAC) function is used to provide the hot backup solution.
- Access control

4.3 Web Service Security

Use the latest or most stable Tomcat web server version and perform security hardening on the server to ensure that the Agile Controller runs on secure web services.

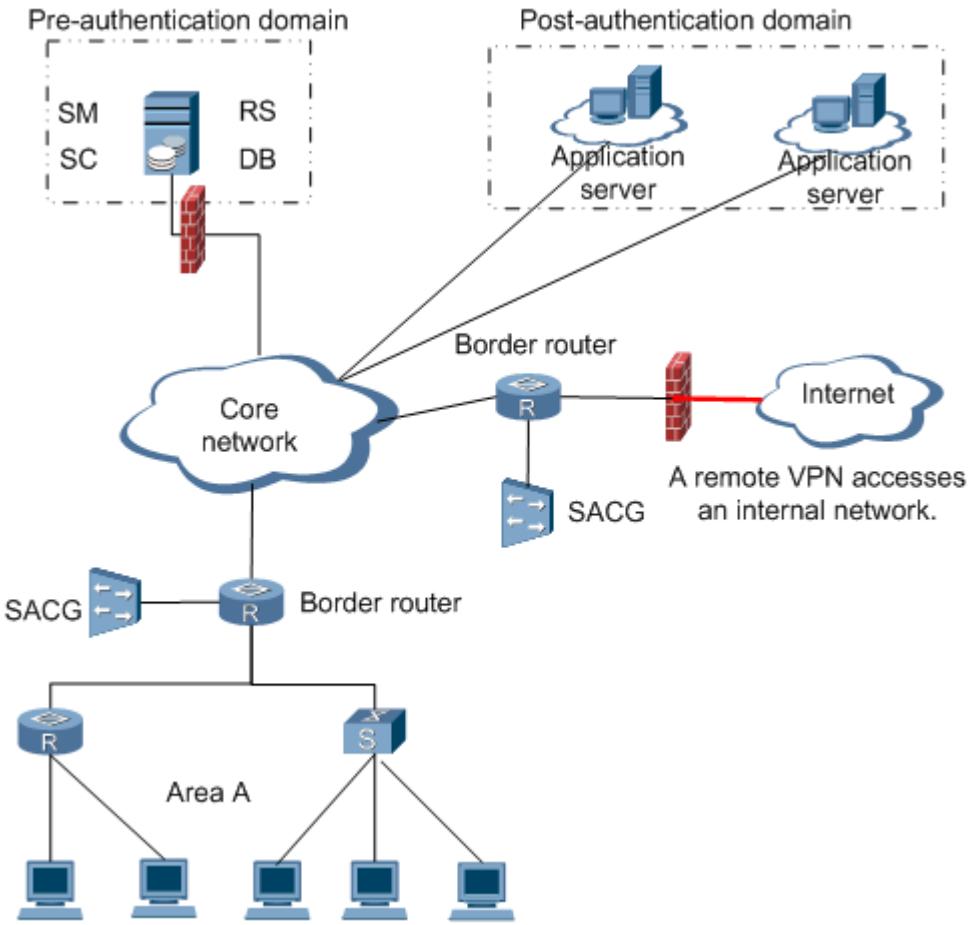
5 Network Security

5.1 Security Networking Modes

Networking Modes and Security Zones

Centralized networking mode

The centralized networking mode is a common practice. The following figure shows its networking diagram.

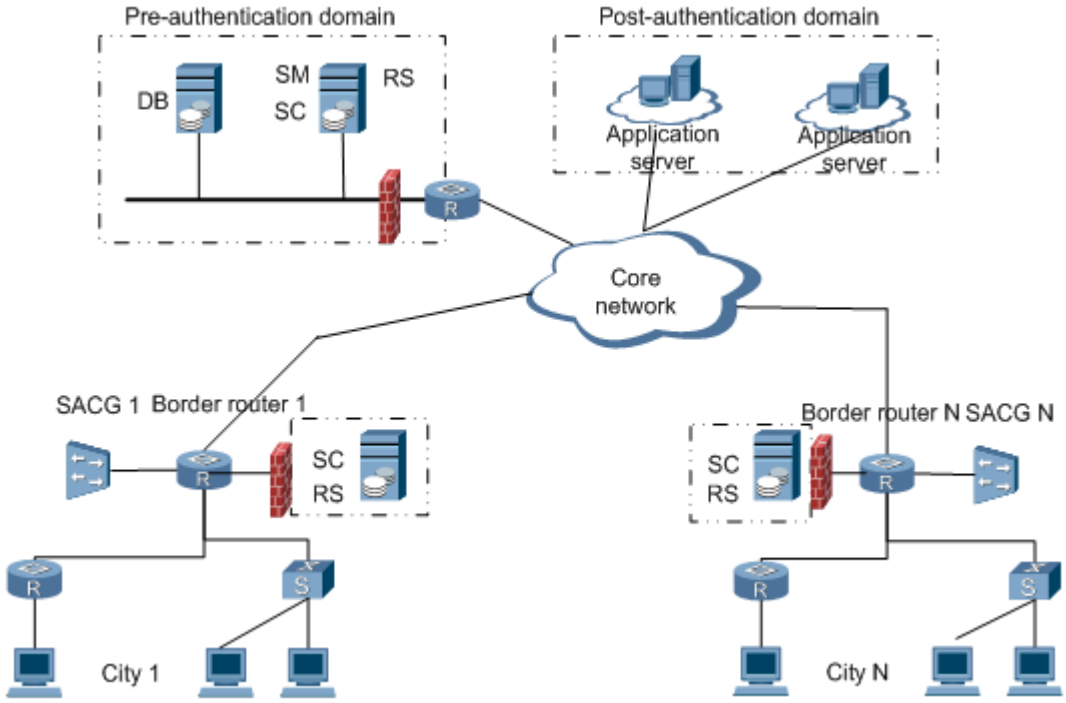


In this networking mode, the Agile Controller servers, including the SM server, SC server, RS server, and database server, are deployed in the same security zone. A firewall must be configured on the incoming path of the Agile Controller servers and firewall policies need to be configured based on the communication matrix of the system to prevent malicious attacks by terminals.

The Agile Controller servers can communicate with the access control device through a different network from the network of terminals. In this way, the user network and management network are separated.

Distributed networking mode

The distributed networking mode is applicable to large-scale networks. The following figure shows its networking diagram.



In this networking mode, there are several security zones: Agile Controller server zone in headquarters, Agile Controller server zones in branches, and terminal user zones.

A firewall must be configured between the Agile Controller server zone in headquarters and the Agile Controller server zone in each branch to prevent malicious attacks of terminals.

A VPN must be configured between the Agile Controller server zone in headquarters and the Agile Controller server zone in each branch. The IPSec is used to encrypt data transmission.

The Agile Controller servers can communicate with the access control device through a different network from the network of terminals. In this way, the user network and management network are separated.

Firewall Policy

The firewall must be deployed between a Trust zone and an Untrust zone.

Interface and Protocol

VPN/IPSec

5.2 Remote Maintenance

The Agile Controller is deployed inside an enterprise network; therefore, it does not provide a public network address for maintenance. If the Agile Controller needs to be remotely maintained, connect the maintenance terminal to the enterprise network through the VPN to access the Agile Controller.