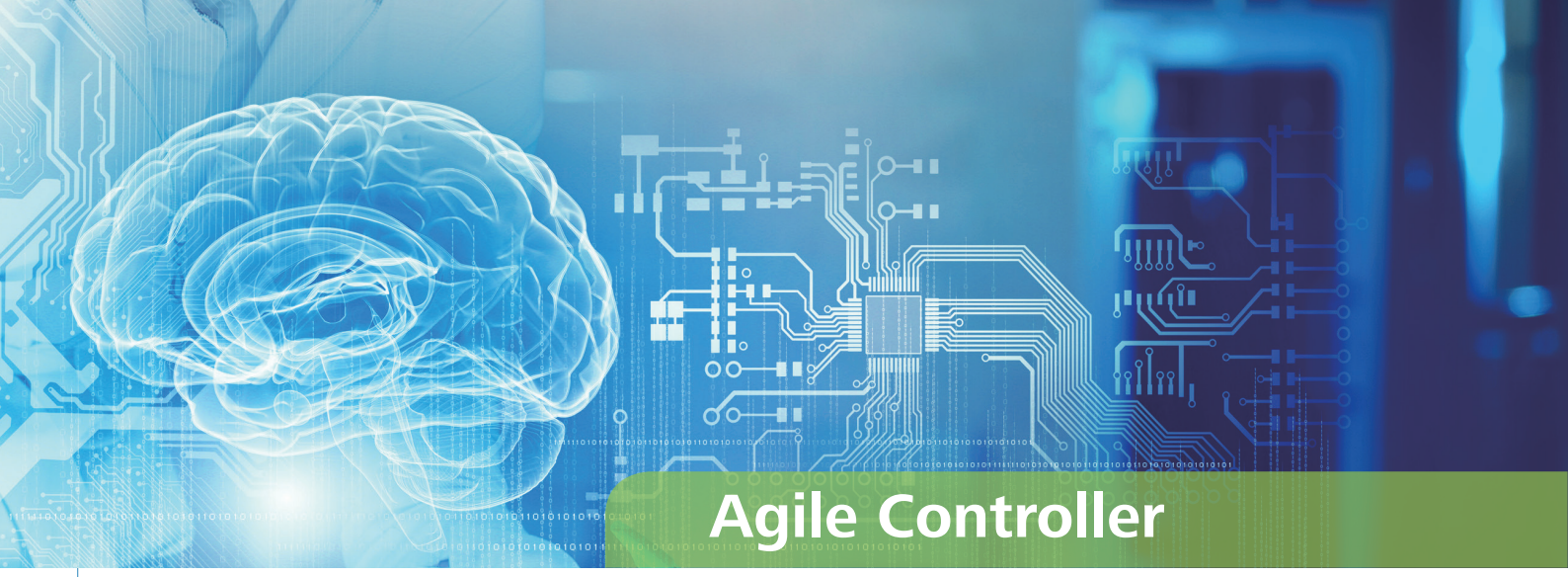
Huawei Agile Controller

HUAWEI TECHNOLOGIES CO., LTD.

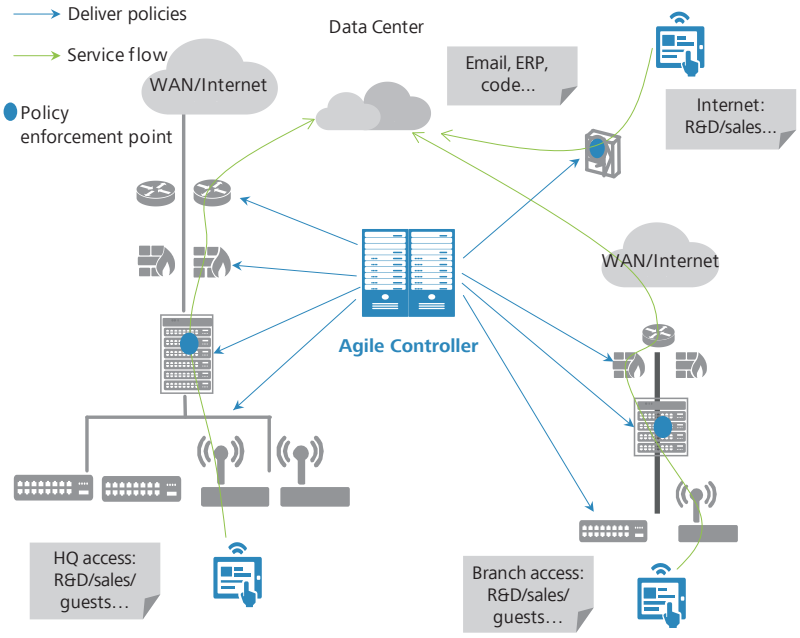
HUAWEI



Agile Controller

Product Overview

Agile Controller is the latest user- and application-based network resource auto control system offered by Huawei. Following the centralized control principle of software-defined networking (SDN), Agile Controller dynamically schedules network and security resources on the entire campus network, acting like the brain of the smart campus network. With Agile Controller, networks will be more agile for services.



Product Characteristics

Experience-centric Redefined Network

Agile Controller shifts customers' attention from technologies, equipment, and connectivity to users, services, and user experience, and freed customers from laborious manual configuration by providing natural-language network planning and automatic deployment.

- Agile Controller applies the SDN's centralized control idea into campus networks. It can dynamically schedule and adjust network and security resources in the entire campus network to meet requirements of frequently moving users, offering free mobility.
- Agile Controller can flexibly adjust user rights, QoS policies, and security policies on the entire network. This dynamic policy adjustment greatly reduces the service provisioning or network expansion period, allowing networks to keep in pace with fast changing services.
- Using Agile Controller, customers no longer need to pay attention to differences of various devices. They can use the natural language to configure network policies and deliver the configurations to all network devices by one click on Agile Controller.
- User-based QoS scheduling ensures preferential forwarding of VIP users' services when network resources are insufficient, delivering good experience to VIP users.

Network-wide united security

Agile Controller implements united security, replacing single single-point protection with network-wide protection.

- Agile Controller collects logs from network devices, security devices, and service systems, and employs Big Data analytics to discover potential attacks and threats that are difficult to detect through single-device protection.
- ecurity devices are virtualized into a security resource center. Traffic of users with certain characteristics is blocked or redirected to the security resource center to defend against attacks.
- Agile Controller provides comprehensive terminal security and desktop management functions, and has over 5000 predefined terminal security policies, ensuring terminal access security.

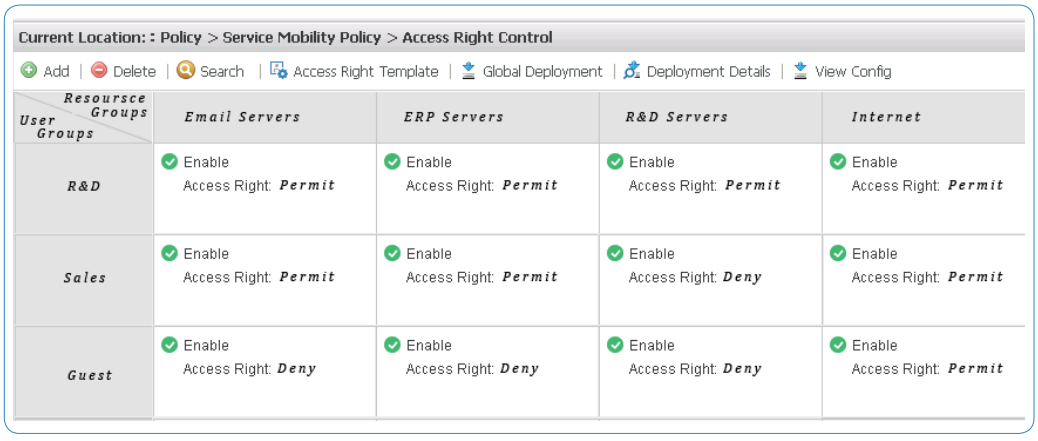
Openness and Interoperability

A fully programmable system enables transformation from hardware-defined networking to software-defined networking.

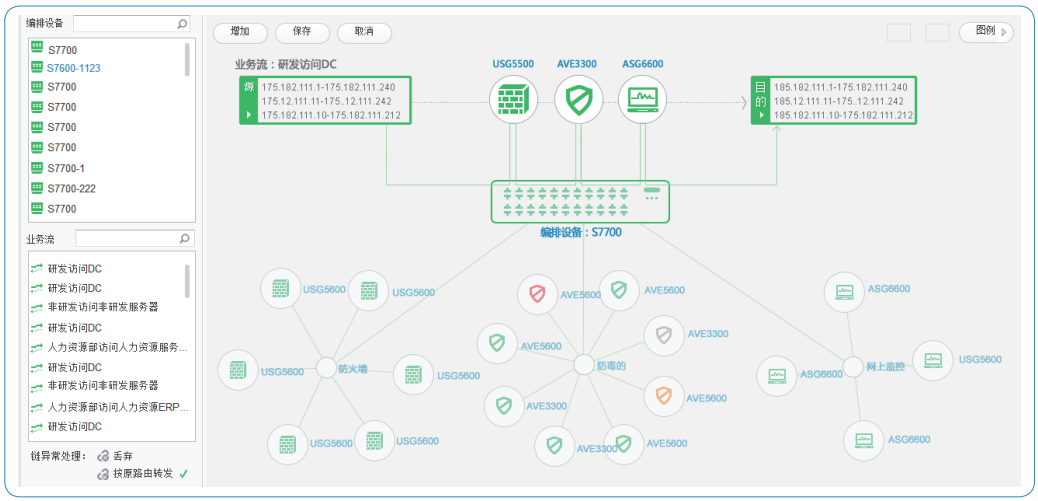
- Agile Controller provides various northbound and southbound interfaces and open APIs to make the forwarding plane and control plane programmable. It can interoperate with service systems of customers to improve end-to-end operation and maintenance efficiency, shorten new service provisioning time, and give customers a platform for innovation.
- Agile Controller is seamlessly interoperable with mainstream cloud platforms, including Huawei FusionSphere, VMware vSphere, Openstack, and Microsoft Hyper-v. The good interoperability makes Agile Controller an elastic, open platform integrating best practices of various fields, allowing customers to flexibly define their networks based on service requirements.

Core Functionalities

- Unified admission control policy engine: provides scenario awareness capability based on 5W1H (who, when, where, what device, why access, how to access). The 5W1H scenario awareness realizes unified authentication for wired/wireless, and internal/external users, allowing for access from various terminals.
- Security-group-based authorization: provides centralized policy configuration and network-wide automatic policy deployment and status monitoring. In this way, the same policy is applied to a user regardless of the user location, delivering consistent service experience for mobile users.



- User-group-based QoS policy configuration: ensures preferential forwarding of VIP users' data traffic when network resources are insufficient, delivering good service experience for VIP users.
- Guest management throughout the whole life cycle: enables customers to define Portal login pages according to their own needs. The self-defined Portal login pages can be pushed to users based on terminal types and locations, to help improve the enterprise image and reduce workload on IT operation and maintenance.
- Terminal security compliance check: checks the system configuration, software list, antivirus software, and local redundant accounts on terminals, and monitors user behaviors such as use of peripherals, network connection, unauthorized access to the Internet, and use of software.
- Service orchestration: abstracts all security devices into a security resource center and redirects user traffic to the security resource center for processing. The service orchestration capability improves resource efficiency and enhances network security protection capabilities.



- Big Data analytics: collects logs on the entire network and analyzes correlation between security events to show security status and trends of the network. Correlation analysis and security association help customers quickly identify network risks so that they can take proactive defense measures to protect the network.

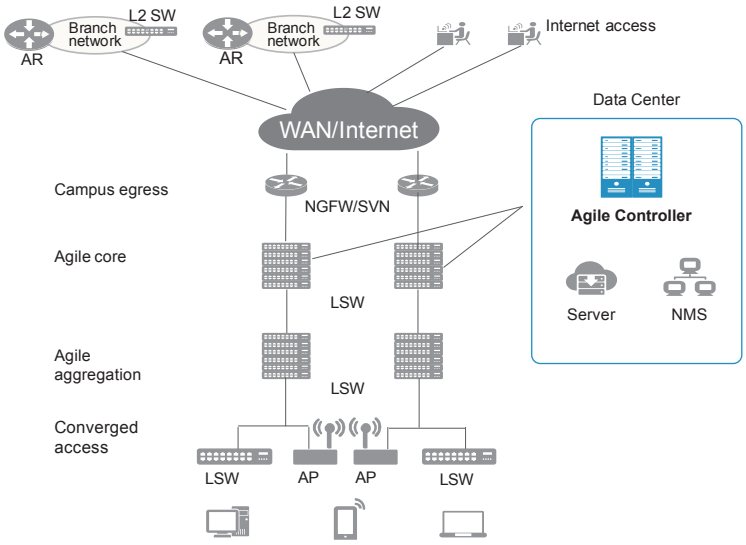
Operating Environment

Configuration	Service Management Server (SM & SC)	United Security Server (SV & iRadar)
CPU	2* hex-core processor, 2 GHz	2* hex-core processor, 2 GHz
Memory	16 GB	32 GB to 64 GB
Storage	600 GB	4 TB or higher

Note: The service management server (SM & SC) runs the Access Control, Guest Management, Free Mobility, and Service Orchestration components. The united security server (SV & iRadar) runs the United Security component.

Networking

Agile Controller can work as long as its physical servers and network devices have reachable routes to each other. It is usually deployed in a data center.



Specifications

Function	Description
Identity authentication	Internal account authentication
	Windows active directory (AD) authentication
	Third-party Lightweight Directory Access Protocol (LDAP) authentication
	Mobile certificate authentication
	Anonymous authentication: Administrators can configure anonymous authentication in specified zones, allowing users in this zone to be authenticated without entering a password.
Policy engine	Multi-dimensional authentication policies based on different rules Different authorization policies for different locations, departments, device types, access time, and access modes Different web authentication pages pushed based on conditions such as terminal locations, device types, and SSIDs
Network access control	Security compliance check (including security assessment and system configuration check): rejects access from security-incompliant terminals to protect network resources
	Automatic isolation and one-click repair of security-incompliant terminals
	User-based access authorization to deny unauthorized access
Guest management	Self-service guest account creation and registration
	Guest account notification (web, email, and SMS)
	APIs for guest account creation, deletion, and modification
	Customization of registration and authentication pages
Terminal identification	Identifying various terminals such as PCs, smart terminals (smartphones and tablet computers), IP phones, and network printers
	Identifying operating systems such as Windows, Linux, MAC OS, Android, IOS, and Windows Phone
	Multiple device identification modes, such as SNMP, User-Agent, DHCP, and MAC OUI
Free mobility	Unified policy configuration and management
	Configuration of intra-group policies and authorization rules
	Configuration of matrix policy templates

List of Specifications

功能	规格
Free mobility	Network-wide user group policy matrix
	Automatic policy deployment for new devices
	Network-wide policy status monitoring
	Experience guarantee for VIP users
Service orchestration	Service orchestration resource management
	Service flow definition
	Service chain orchestration
	Service chain monitoring
Terminal security management	Security hardening: including static configuration check (antivirus software, patch, suspected processes, and authorized software) and dynamic auditing (port usage check, minimum service, peripheral connection check, ARP inspection, and traffic monitoring), identifying and fixing potential risks
	Office behavior management: including web access, media downloading, and non-office software installation
	Information leak prevention: including peripheral and mobile storage management, unauthorized external network access control, and program control
	Network protection: isolates traffic of guests, security-incompliant terminals, and security-compliant terminals to prevent attacks from terminals
Desktop management	Patch management: one-stop automatic patch check and fix, patch deployment display on device and patch basis, association with Windows Server Update Services (WSUS)
	IP asset auto-discovery: automatically discovers unmanageable devices such as IP printers, IP phones, smartphones, cash registers, and barcode scanners
	Asset lifecycle management: helps enterprises prevent hardware and software assets and know about asset usages
	Bandwidth-conserving, high-speed software distribution through distributed storage and fast subnet forwarding of large-size files
	Remote desktop assistance
	Message announcement: pushes bulletin messages to specific users or departments and allows setting of bulletin validity period
United security	Security log collection from Huawei devices and third-party devices with standard interfaces, including Syslog, SNMP, FTP/SFTP, OPSEC, and ODBC interfaces
	Security event correlation analysis using predefined and user-defined correlation analysis policies
	Security event response: notifies administrators of security events quickly using emails or SMS messages
	Security trends display: shows security status and trends in the complete network topology, top N risky assets, and severity of security threats
Maintainable reports	Predefined report templates and security trend reports, such as online user information report
	User-defined reports or reports obtained from the security center
System management	System running status monitoring: provides alarms on server exceptions in dialog boxes or emails
	Online client fault diagnosis and centralized client fault handling
	Remote data backup
Networking	Centralized networking: applicable to networks with a small number of terminals and a clear network structure
	Distributed networking: applicable to networks with multiple branches or a large number of terminals

Ordering Information

Description	Quantity	Remarks
1.1 Software		
Agile Controller Access Control Component	1	Optional, providing user access control function
Agile Controller Terminal Count License for Access Control	Incremental	Incremental of 200, 500, 1000, 2000, 5000, 10000, and 50000
Agile Controller Guest Management Component	1	Optional, providing full-lifecycle guest management
Agile Controller Guest Account License	Incremental	Incremental of 200, 500, 1000, 2000, 5000, 10000, and 50000
Agile Controller Free Mobility Component	1	Optional, providing policy matrix and QoS policy deployment based on user groups
Agile Controller Service Orchestration Component	1	Optional, redirecting user traffic to the security resource center for processing
Agile Controller Terminal Security Management Component	1	Optional, providing terminal security management functions including terminal health check, peripheral management, unauthorized external network access control, asset management, patch management, software distribution, and bulletin message management
Agile Controller Terminal Account License for Terminal Security Management	Incremental	Incremental of 200, 500, 1000, 2000, 5000, 10000, and 50000
Agile Controller United Security Component	1	Optional, providing network-wide security event collection, correlation analysis, and security trend display
Agile Controller Event Count License for United Security	Incremental	Incremental of 500 EPS, 1000 EPS, 2500 EPS, and 5000 EPS EPS: Events Per Second
1.2 Hardware for centralized deployment (number of users ≤ 10000, number of logs ≤ 2500 EPS)		
Integrated service management server (SM & SC)	1	Used when number of users ≤ 10000
Integrated united security server (SV & iRadar)	1	Used when number of logs ≤ 2500 EPS
1.3 Hardware for distributed deployment (number of users > 10000, number of logs > 2500 EPS)		
SM server	Unlimited	Service Manager, managing SCs and sending real-time instructions to connected node to complete various services
SC server		Service Controller, completing tasks such as user authentication, security policy delivery, and data reporting
Database server		Can be deployed independently for database redundancy
SV server	Unlimited	Security View security trend management server, showing iRadar correlation analysis results and security status of the entire network
iRadar server		Log collection and correlation analysis server
iRadar-CA server		It is recommended that you deploy a correlation analyzer (CA) server when more than 15 correlation rules are configured on the iRadar server.
iRadar-CM server		An iRadar-CM log collector can be deployed when a branch has less than 2000 EPS logs, and an iRadar server is recommended when the number of logs is larger than 2000 EPS.
S2600T disk array		External disk array, configured when HA redundancy configuration is selected for SV and iRadar.

More Information

For more information about Huawei Agile Controller, please visit http://enterprise.huawei.com.

HUAWEI TECHNOLOGIES CO.,LTD.
Huawei Industrial Base
Bantian Longgang
Shenzhen 518129,P.R.China
Tel: +86 755 28780808

www.huawei.com