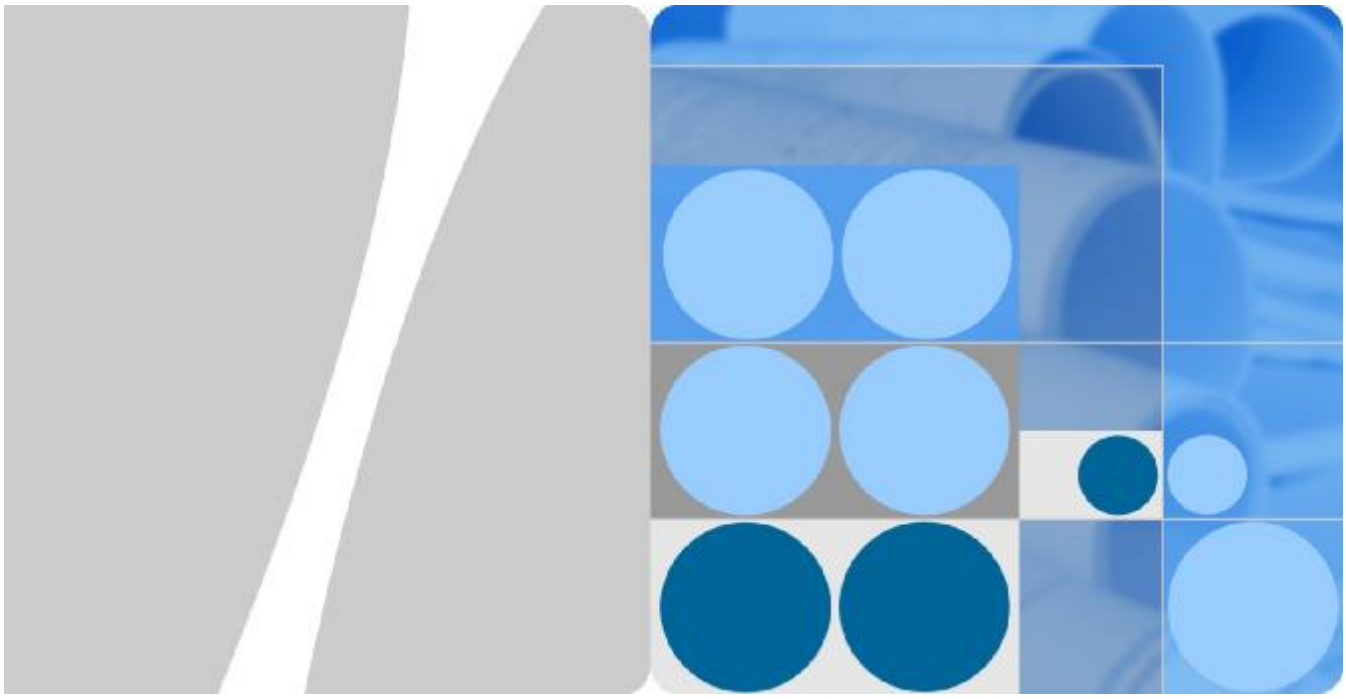


S Series Switches

Service Chain Technology White Paper

Issue 1.0

Date 2015-11-04

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://www.huawei.com

Email: support@huawei.com

Contents

Service Chain Technology White Paper

Abstract: To enable users to easily and flexibly deploy some advanced value-added service devices on a network, such as FWs, ASGs, AVEs, and IPSs, the Agile Controller delivers orchestration policies configured by users to the orchestration device (switch) using XMPP to control the forwarding of service flows. The service flows are directed to the FWs, ASGs, AVEs, and IPSs for processing according to the sequence defined in the policies. This solution is called Service Chain.

Keywords: Service Chain

1 Overview

1.1 Problems in Traditional Networking

In a traditional campus network, value-added service devices, such as firewalls (FWs), antivirus engines (AVEs), and application security gateways (ASGs), are usually deployed at borders of important service departments, demilitarized zones (DMZs), campus egresses, and data centers. These devices are connected to the network in inline or bypass mode.

1.1.1 Inline Networking of Service Devices

Figure 1-1 Traditional inline networking of service devices

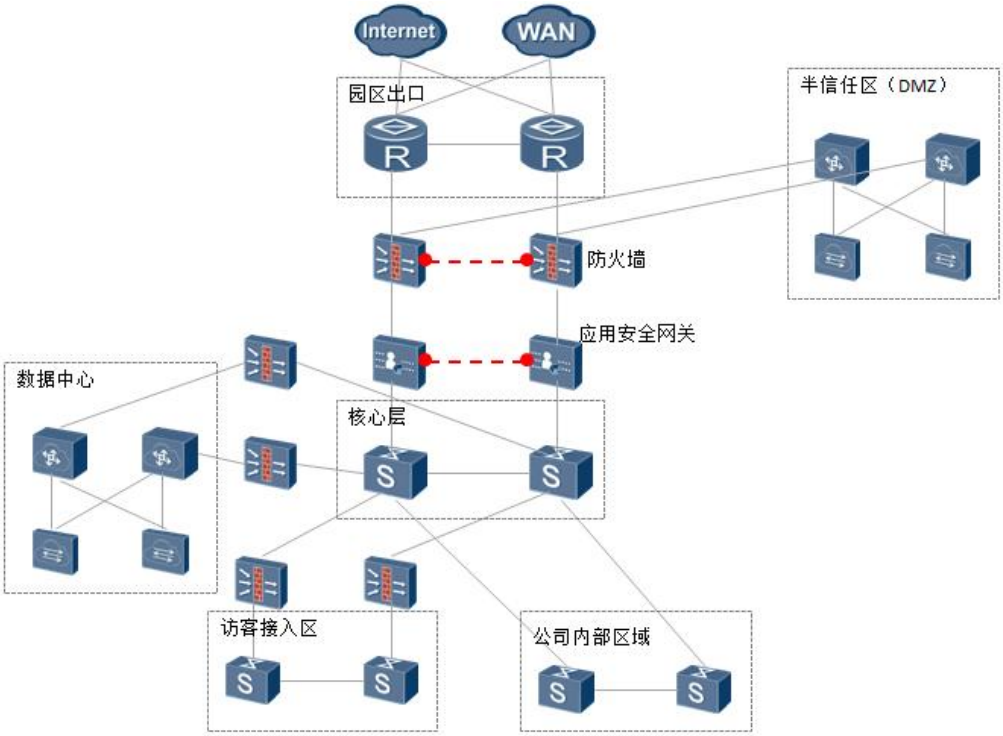


Figure 1-1 shows the traditional inline networking of service devices, which makes the network topology simple but faces the following problems:

- Performance bottleneck: Service devices have low performance. In inline networking, the device with the lowest performance becomes a bottleneck on the network.
- Difficulty in adding or removing service devices: Adding or removing service devices requires reconfiguration of IP addresses and routes, and network migration causes service interruption, which has great impact on the live network.
- High cost: Too many value-added service devices need to be deployed at borders of multiple areas, increasing investment.
- Low device usage: Service devices are deployed separately for each network area, causing low device usage and resource waste.

1.1.2 Bypass Networking of Service Devices

Figure 1-2 Bypass networking of service devices

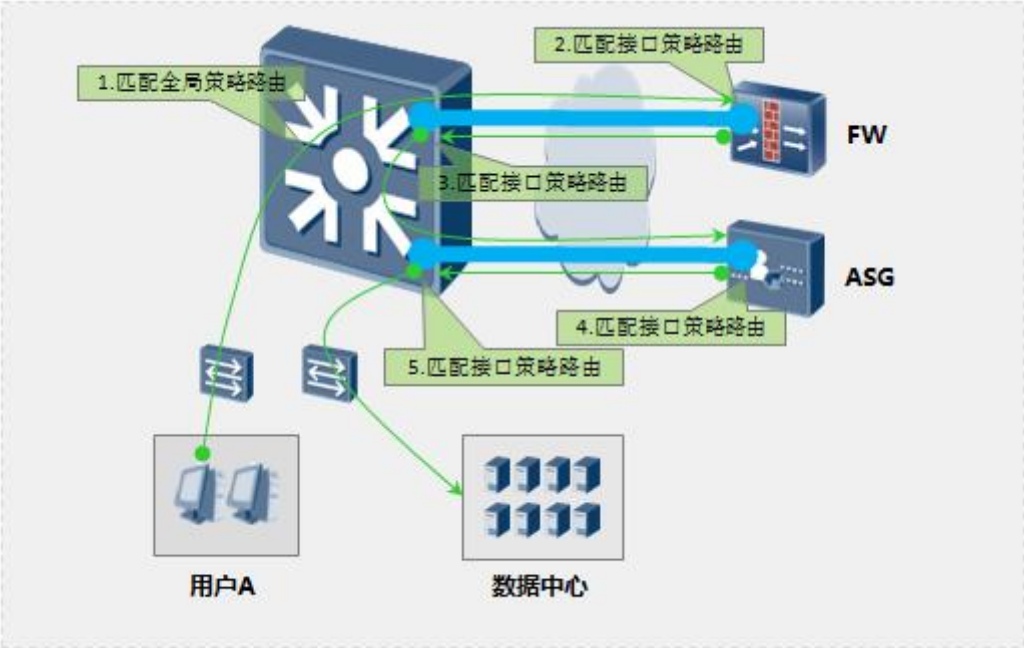
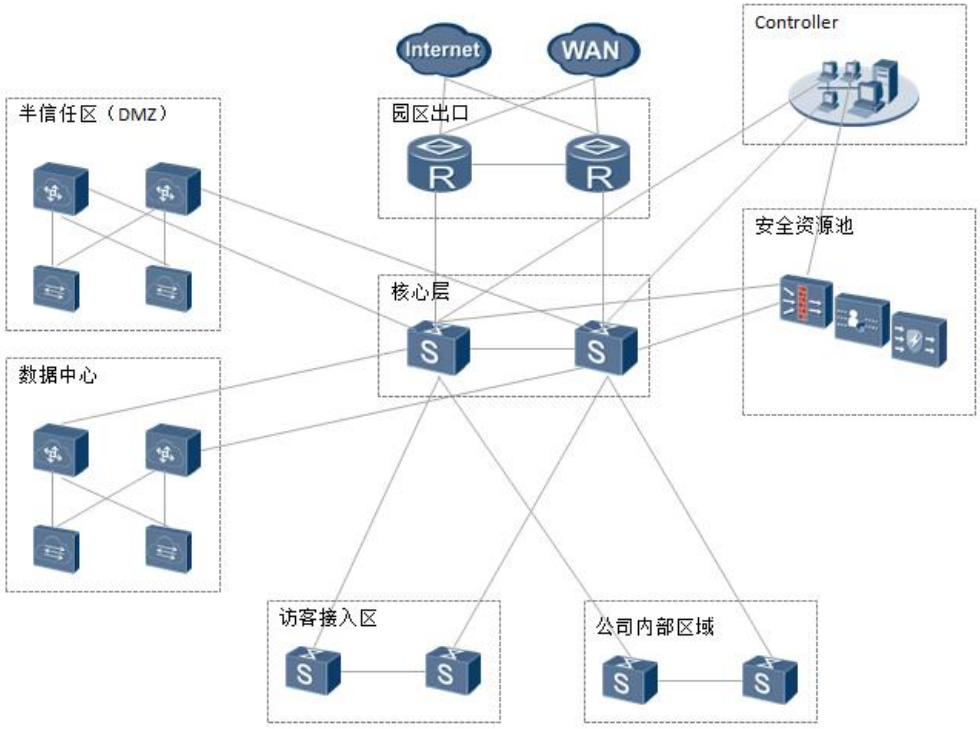


Figure 1-2 shows the bypass networking of service devices. In traditional bypass networking, traffic is redirected to service devices through policy-based routing. This method avoids problems in inline networking but has the following problems:

- Complex configuration: When two service devices are connected to a switch in bypass mode, at least five or six policies must be configured, including a global policy and several interface policies.
- Difficulty in understanding: Traffic directions, inbound interfaces, outbound interfaces, and next-hop addresses or outbound interfaces need to be analyzed.
- Insufficient reliability guarantee: Interfaces connecting two service devices are not correlated. When a link of one interface fails, the other interface is unaware of the fault. For example, if the link from the ASG to the switch fails, traffic is still forwarded to the switch through the FW and will be sent to the ASG. However, the link between the ASG and switch already fails, the service is therefore interrupted.

1.2 Huawei Service Chain Solution

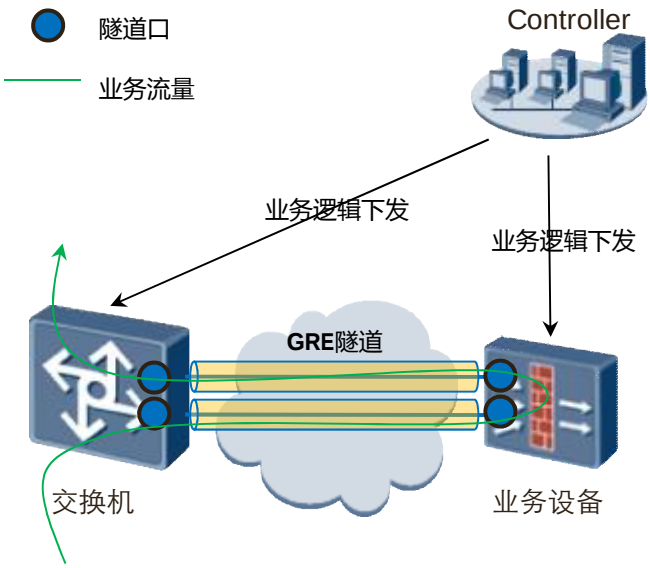
Figure 1-3 Campus networking diagram of Huawei Service Chain solution



Huawei offers the Service Chain solution to cope with the preceding problems.

As shown in Figure 1-3, the Service Chain solution consists of the policy controller (Controller), orchestration devices (switches), and security resource pool (including FWs, ASGs, and AVEs). On a campus network, the Service Chain solution allows value-added service devices to be concentrated in a physical zone.

Figure 1-4 Diagram of Huawei Service Chain solution



As shown in Figure 1-4, Huawei Service Chain solution has the following technical characteristics:

- Simple service logic: Service logic is abstracted on the Agile Controller. Only a few items need to be configured, and the configuration logic is simple and clear. On the Controller, users only need to define what traffic needs to be processed on which service devices by dragging service devices on the GUI. Interfaces on the service devices and configuration command lines are invisible to users. If the service logic is configured by running commands on devices, at least tens of commands need to be configured in the global view and interface view of the switch and service devices. The operations are labor-intensive and easily cause incorrect logic configurations.
- Uniform device connection: All service devices are connected to the switch through Generic Routing Encapsulation (GRE) tunnels. The service devices and switch do not need to be directly connected. Theoretically, service devices can be deployed at any physical locations where their IP addresses are reachable and can be interconnected with the switch.
- Service-chain-level reliability: The Service Chain solution provides two troubleshooting policies: escape policy and blocking policy. If a service chain node fails, traffic passing through this node can be forwarded through the escape link, preventing the failure of the entire service chain.
- Support for non-Huawei devices: The Controller has a third-party adaptation framework that supports various non-Huawei service devices, such as firewalls.

1.3 Customer Benefits

Huawei Service Chain solution brings the following benefits to customers:

- Easy to understand: This solution abstracts service logic to make the networking transparent to customers. Customers only need to define service flows and consider logic of service chains. Therefore, the solution is easy to understand and use.

- Flexible networking: Service devices are connected to a switch through Layer 3 GRE tunnels, allowing flexible service device networking and deployment locations.
- Easy expansion: When adding or deleting service devices, customers only need to add or delete GRE logical links and do not need to change routes or physical topology of the network.
- Simple management: Service device connection and configuration, as well as service policy adding or deletion are completed on the Agile Controller, greatly reducing workload on policy configuration. Adding or removing service devices only causes slight changes on the network, simplifying management of the basic network.
- Investment reduction: One security service device can be shared among multiple service areas to reduce the number of security service devices needed.

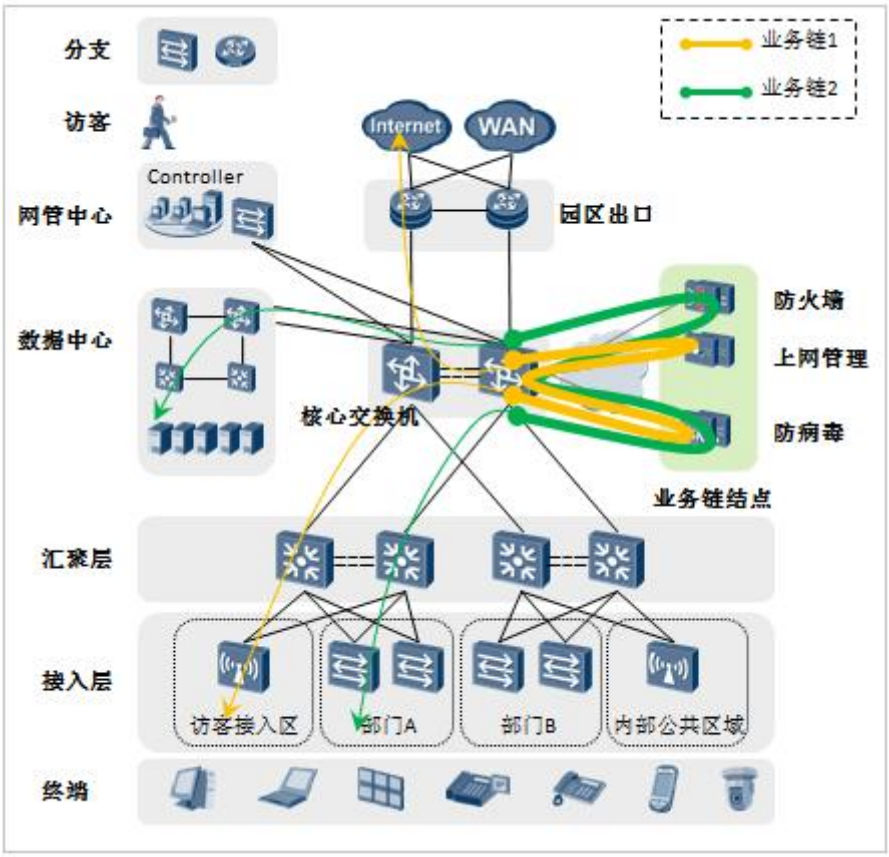
2 Solution Implementation

2.1 Basic Concepts

- Service flow: refers to a packet that has specific characteristics (for example, a packet carrying specific fields) or matches specific service policies (for example, specific IP address or port number).
- Service chain node: refers to a value-added service device (security device, for example, firewall or antivirus device) on a service chain. The service device can also be an independent service device or a value-added service card on a switch.
- Service chain: refers to a group of chain nodes that are deployed in a specific sequence providing a series of services.

2.2 Networking Architecture and System Functions

Figure 2-1 Networking architecture



As shown in Figure 2-1, the Service Chain solution involves three roles: Agile Controller, orchestration device (switch), and service device. They are deployed at Layer 3. Layer 3 GRE tunnels are established between the service devices and switch. The switch directs specified traffic to the service devices through GRE tunnels for processing based on access control lists (ACLs) or user control lists (UCLs).

The three roles in the Service Chain solution provide the following functions:

- Agile Controller: abstracts service logic and provides a GUI for customers to uniformly configure service logic for service chains.
- Orchestration device (switch): redirects IPv4 unicast traffic forwarded from routers to service devices by the Service Chain sequence based on the ACLs or UCLs delivered by the Agile Controller.
- Service device: interconnects with the switch through Layer 3 GRE tunnels and processes service flows.

NOTE

Currently, only firewalls can be used as service devices.

2.3 Overall Architecture and Process

As shown in Figure 2-2, the Service Chain solution consists of three subsystems:

- Service Chain subsystem: the Agile Controller, which completes service logic configuration for service chains.
- Service distribution subsystem: a switch, which identifies and redirects service flows.
- Service processing subsystem: a service device, which processes service flows that are redirected to it.

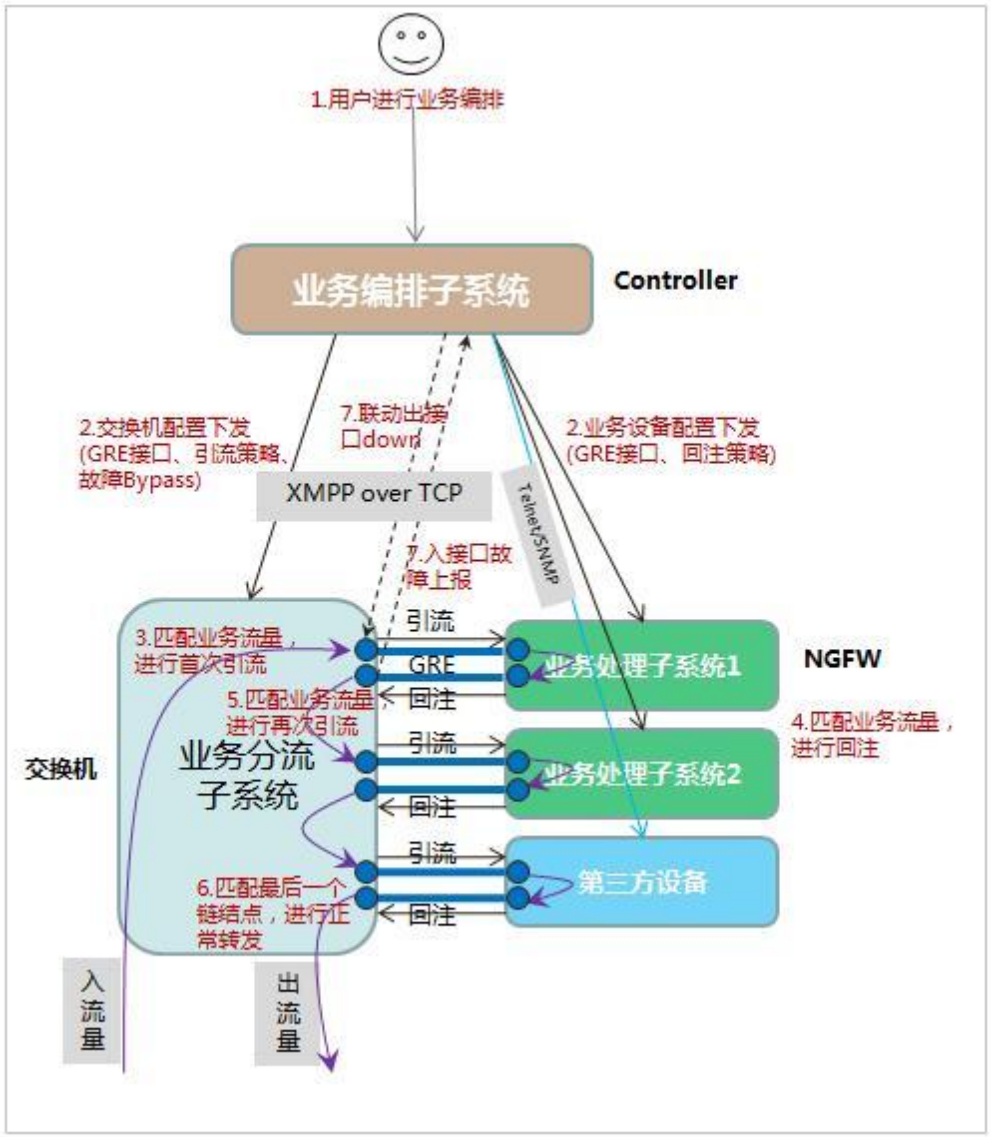
The solution uses the following technologies:

- Device-to-device interface protocols:

  Extensible Messaging and Presence Protocol (XMPP): used by Huawei orchestration devices and service devices to connect to the Agile Controller.

  Telnet/Simple Network Management Protocol (SNMP): used by third-party service devices to connect to the Agile Controller.
- Traffic diversion: policy-based routing based on GRE tunnels

Figure 2-2 Overall architecture and flowchart



As shown in Figure 2-3, the service interaction process is as follows:

1. A user configures Service Chain on the Agile Controller, including service flow definition, resource orchestration of the switch and service devices, and service chain orchestration.
2. The Agile Controller translates the service logic into machine language and uses XMPP to deliver the configurations to the switch and service devices.
3. When service traffic reaches the switch for the first time, the switch matches it with the global policy-based routing. If the traffic matches a service flow rule, the switch redirects the traffic to the first service device according to the traffic diversion policy.
4. The service device processes the traffic and re-injects the traffic to the switch according to the policy-based routing on the inbound interface.

5. When the service traffic reaches the switch again, the switch finds that it matches the interface policy-based routing with a higher priority, and then redirects the traffic to the second service device according to the matched traffic diversion policy.
6. When the service traffic is re-injected to the switch from the last service device, the switch finds that it matches the interface policy-based routing, and then takes the permit action to forward the traffic.
7. The switch checks the status of GRE tunnels through the GRE Keepalive mechanism. If a GRE tunnel between the switch and a service device fails, the switch reports the failure to the Agile Controller, which then shuts down the other GRE tunnel to prevent traffic forwarding exceptions.

2.4 Service Chain Implementation

In the Service Chain solution, different service flows are filtered and distinguished on the switch based on the ACLs or UCLs delivered by the Agile Controller.

- Service flows matching an ACL rule are redirected to the specified GRE tunnel.
- Service flows matching a UCL rule are redirected to the specified GRE tunnel. Users in the same user group use the same policies.

The Agile Controller delivers UCL rules and user group mapping relationships to the switch and service devices. The switch and service devices obtain the source user group number according to the source IP address of traffic and the destination user group number according to the destination IP address. Then, the service flow is redirected to the specified GRE tunnel based on the source and destination user group numbers. The following example describes the Service Chain process using a UCL:

1. On the Agile Controller, add the user **Marketing_User_A** to the marketing user group **Marketing_User_Group**, set the marketing server group to **Marketing_Server_Group,** and set the network segment of servers to **10.10.10.0/24**;
2. Configure a UCL rule to allow users in **Marketing_User_Group** to access **Marketing_Server_Group**, and redirect the access traffic to the specified GRE tunnel. The Agile Controller delivers the UCL rule and the mapping between **Marketing_Server_Group** and the network segment of servers to the switch and service devices.
3. When the user **Marketing_User_A** is authenticated, the Agile Controller delivers the mapping between dynamically obtained IP addresses and **Marketing_User_Group** to the switch.
4. Service devices need to obtain the user's IP address from service packets, query the mapping between the user's IP address and **Marketing_User_Group** from the Agile Controller, and request the Agile Controller to deliver the mapping.
5. When a service flow passes through the switch or a service device, the switch or service device obtains the user group number based on the source and destination IP addresses. The switch matches the service flow with the UCL rule and redirects the service flow matching the UCL rule to the specified GRE tunnel.

On a campus network, there are three types of service traffic according to traffic directions: service traffic from internal users to external networks, service traffic from external networks to internal users, and service traffic between internal users. In the Service Chain solution, Service Chain implementation is the same regardless of the traffic direction.

Figure 2-3 Path of traffic from an internal user to an external network

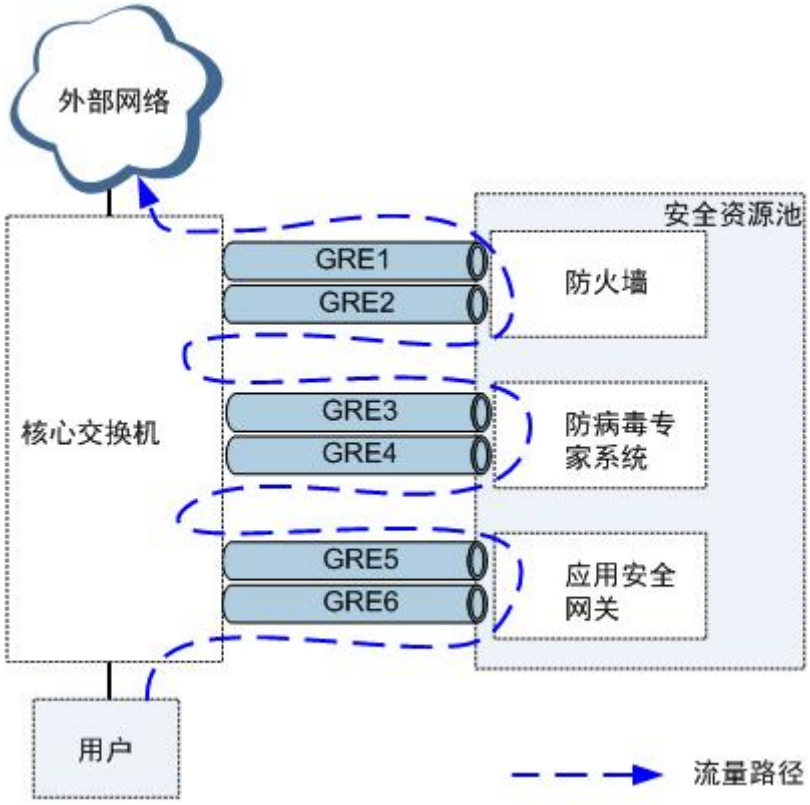


Figure 2-3 describes the Service Chain implementation of traffic that is sent from an internal user to an external network and needs to pass through the ASG, antivirus expert system, and firewall.

The Service Chain process is as follows:

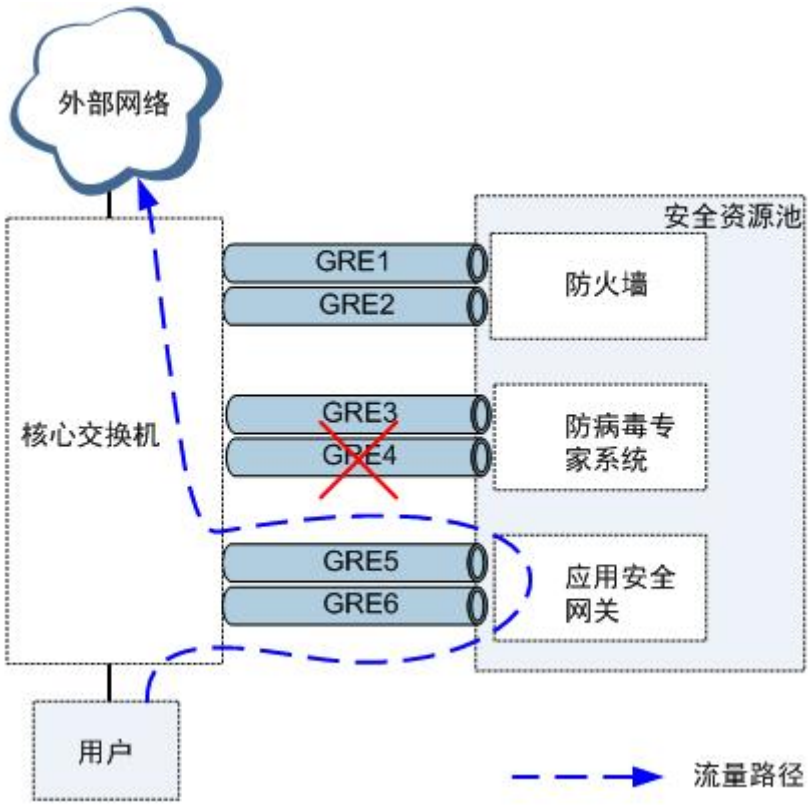
1. After traffic from the internal user to the external network is forwarded to the core switch, the core switch matches the traffic with an ACL or UCL rule and queries the global policy-based routing. If the traffic matches the rule, the core switch redirects the traffic to a specified tunnel interface, and then forwards the traffic to the ASG through GRE6.
2. After processing the traffic, the ASG redirects the traffic to a specified tunnel interface and returns the traffic to the core switch through GRE5.
3. The core switch matches the traffic received from GRE5 with the ACL or UCL rule and queries the policy-based routing on the GE5 interface. If the traffic matches the rule, the core switch redirects the traffic to the tunnel interface where GRE4 resides, and then forwards the traffic to the antivirus expert system. Similarly, the service traffic is processed by the antivirus expert system and firewall and then returned to the core switch.
4. The core switch receives the service traffic from GRE1 and forwards the traffic to the external network according to the routing table because the traffic does not need to be processed by other value-added service devices.

2.5 Measures Taken by a Service Chain to Respond to Network Faults

If a service device or the physical link between the core switch and a service device fails, the Agile Controller delivers configurations to the switch and service device to cancel the GRE tunnel configuration between them, and delivers a policy to discard or directly forward the traffic.

As shown in Figure 2-4, when a fault occurs on GRE4 tunnel between the core switch and antivirus expert system, the core switch sends the fault information to the Agile Controller, which then delivers configurations to the core switch and antivirus expert system to cancel GRE4 and GRE3 configuration. In this manner, the core switch discards the traffic received from the GRE5 tunnel or searches the routing table for a route and forwards it according to the specified policy. By default, the traffic is forwarded directly.

Figure 2-4 Traffic forwarding in the case of a fault



3 Application Scenarios

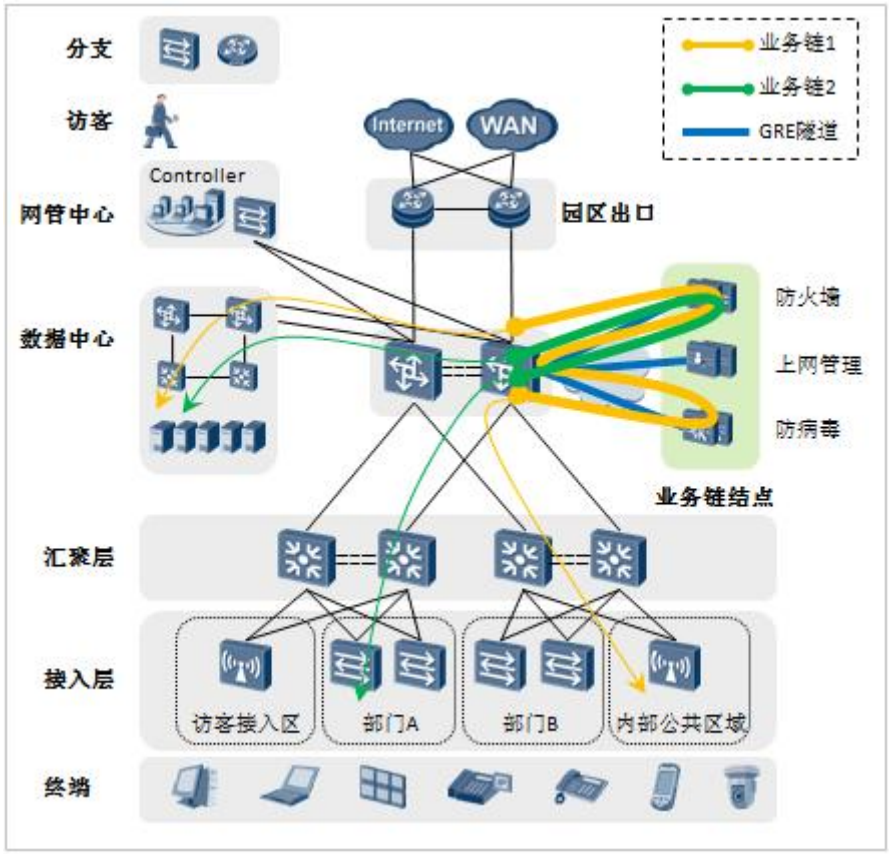
3.1 User Access to the Data Center

When a user accesses a data center, the uplink traffic passes through the access switch, aggregation switch, core switch, and finally reaches the data center. Any of the switches can be used as the orchestration device. Since service devices are deployed in a security zone to serve the entire network, the aggregation or core switch is usually used as the orchestration device.

Different departments in a campus face different security risks and have the following requirements:

- When users in the internal public area access the data center, access control and antivirus processing are required. Security level of users in the internal public area and their terminals is low. Viruses or Trojan horses may be brought into the campus network through USB flash drives or terminals of these users. In addition to the access control policy for traffic sent to the data center, an antivirus gateway is required to protect servers in the data center.
- When R&D users access the data center, only access control is required because the enterprise has applied strict host protection and security admission policies to users and terminals in the R&D department.

Figure 3-1 Access to the data center from Internet users



As shown in Figure 3-1, a core switch is used as the orchestration device and the service devices connect to the orchestration device through Layer 3 GRE tunnels.

Orchestration device:

- Traffic transmitted between campus users and the data center is forwarded by a core switch. To shorten the transmission path and reduce the forwarding delay, the core switch is used as the orchestration device.

Service device location:

- The service devices are deployed at the core layer to serve different service chains.

Service flow definition:

- Traditional switches support service flow definition based on the protocol type, source IP address, source port number, destination IP address, and destination port number in ACL rules.
- Agile switches serving as authentication nodes support service flow definition based on the protocol type, source security group number, source port number, destination security group, and destination port number in UCL rules.

Deployment description:

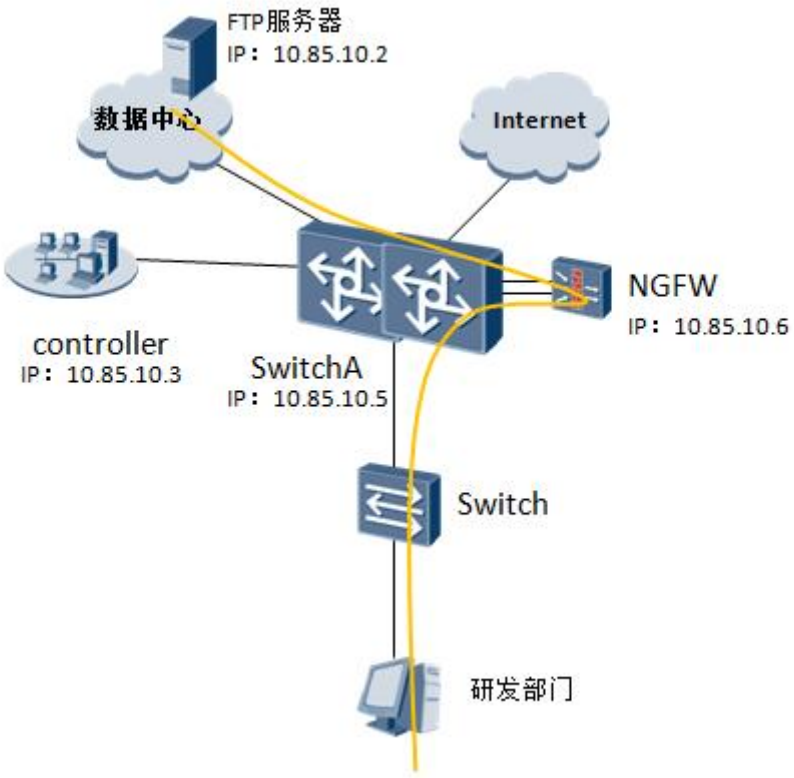
- Specify service chains to meet different requirements. In this example, two service chains are defined.

- For service flows from the internal public area to the data center, use service chain 1 (from the antivirus gateway to the firewall).
- For traffic from the data center to the internal public area, use the service chain 1-reverse (from the firewall to the antivirus gateway).
- For traffic from the R&D department to the data center, use service chain 2 (firewall).
- For traffic from the data center to the R&D department, use service chain 2 (firewall).

3.2 Service Chain Configuration Example on a Campus Network

As shown in Figure 3-2, traffic from employees in the R&D department of a company to the data center needs be checked by the firewall. An important FTP server is deployed in the data center with the IP address 10.85.10.2. It is planned that employees with IP addresses ranging from 10.85.100.11 to 10.85.100.15 are permitted to access the FTP server. ACL rules can be configured on the switch to match user traffic, and service traffic from employees to the FTP server can be redirected to the firewall for security check.

Figure 3-2 Service Chain networking diagram

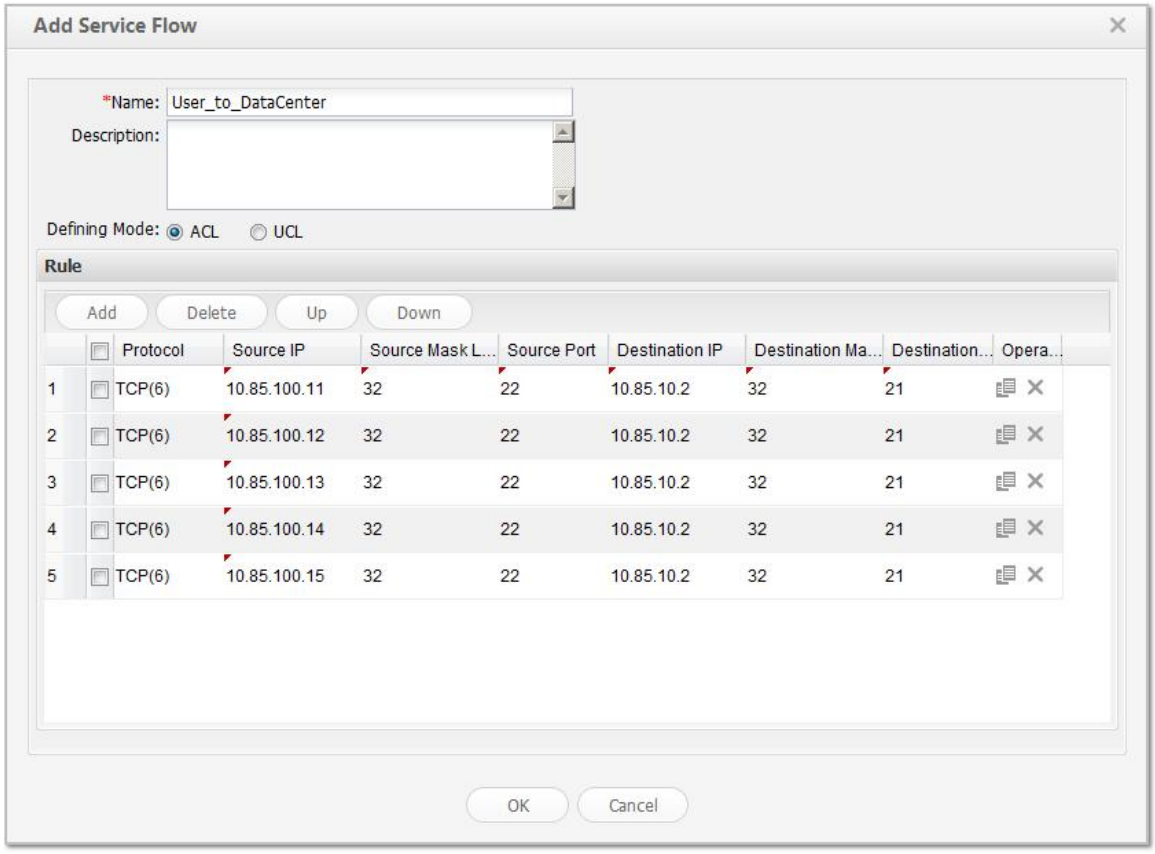


The visualized operations on the Agile Controller are as follows:

Step 1 Choose **Policy > Service Chain Configuration > Service Flow Defining** to define a service flow on the Agile Controller and configure an ACL rule to filter traffic based on the source IP

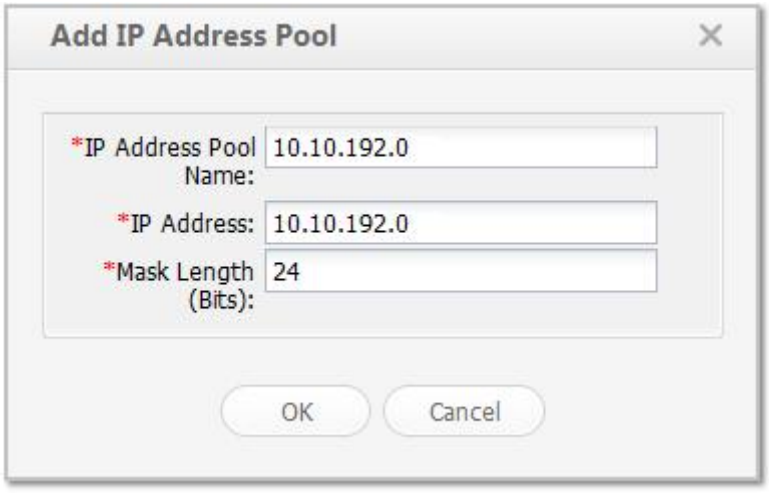
address, source port number, destination IP address, and destination port number, as shown in Figure 3-3.

Figure 3-3 Service flow parameter settings



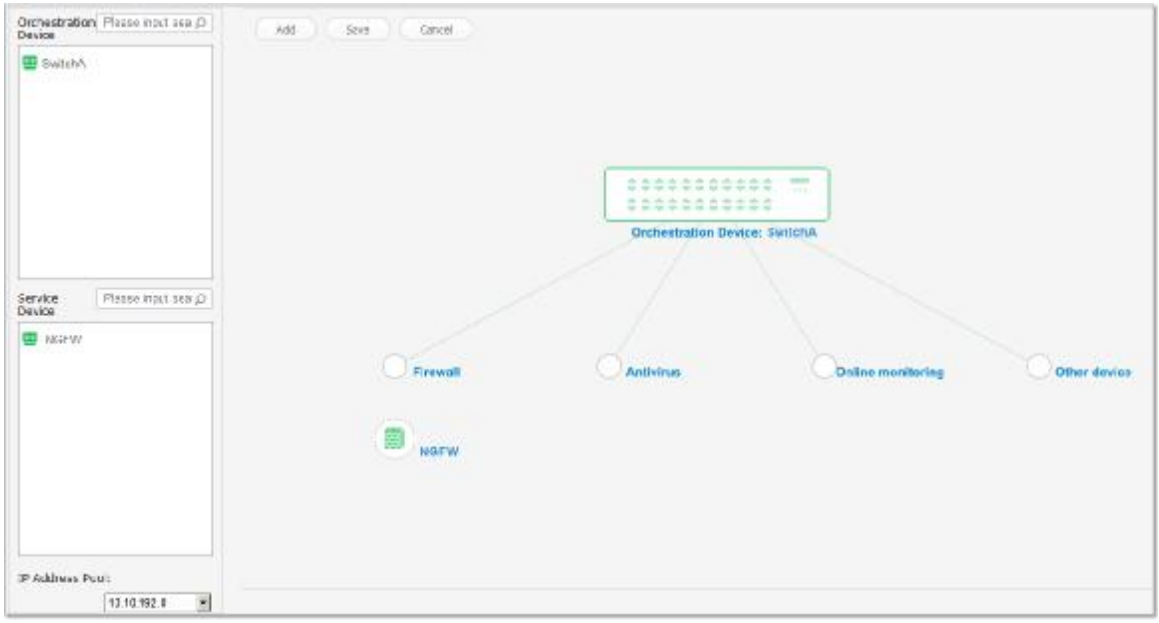
Step 2 Choose **Policy > Service Chain Configuration > IP Address Pool** to configure an IP address pool for establishing GRE tunnels between the orchestration device and service devices, as shown in Figure 3-4.

Figure 3-4 IP address pool parameter settings



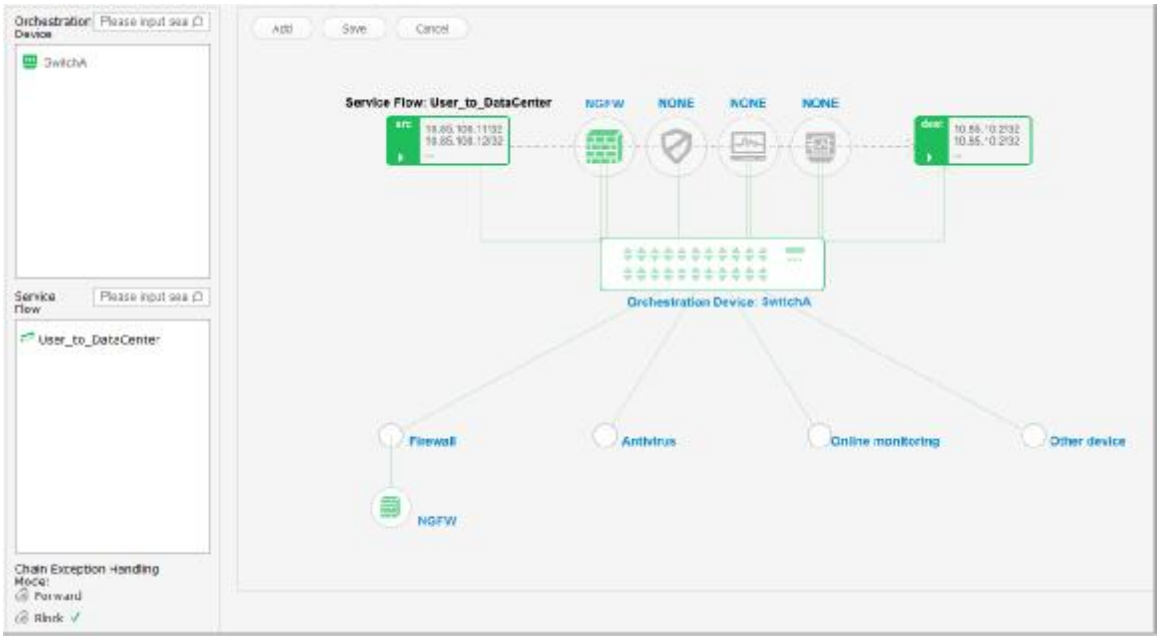
Step 3 Choose **Policy** > **Service Chain Configuration** > **Service Chain Resource** to configure a service chain, as shown in Figure 3-5. In the **Orchestration Device** area on the left, select and drag **SwitchA** to the **Orchestration Device** node on the right. In the **Service Device** area on the left, select and drag **NGFW** to the **Firewall** node on the right. Select **10.10.192.0** in the **IP Address Pool** area.

Figure 3-5 Service chain parameter settings



Step 4 Choose **Policy** > **Service Chain Configuration** > **Service Chain Configuration** to orchestrate and deploy a service chain, as shown in Figure 3-6. In the **Service Flow** area on the left, select and drag **User_to_Datacenter** to the **Service Flow** node on the right. In the **Orchestration Device** area on the left, select and drag **SwitchA** to the **Orchestration Device** node on the right. Drag **NGFW** to the upper **Firewall** node. In the **Chain Exception Handling Mode** area, select **Block**.

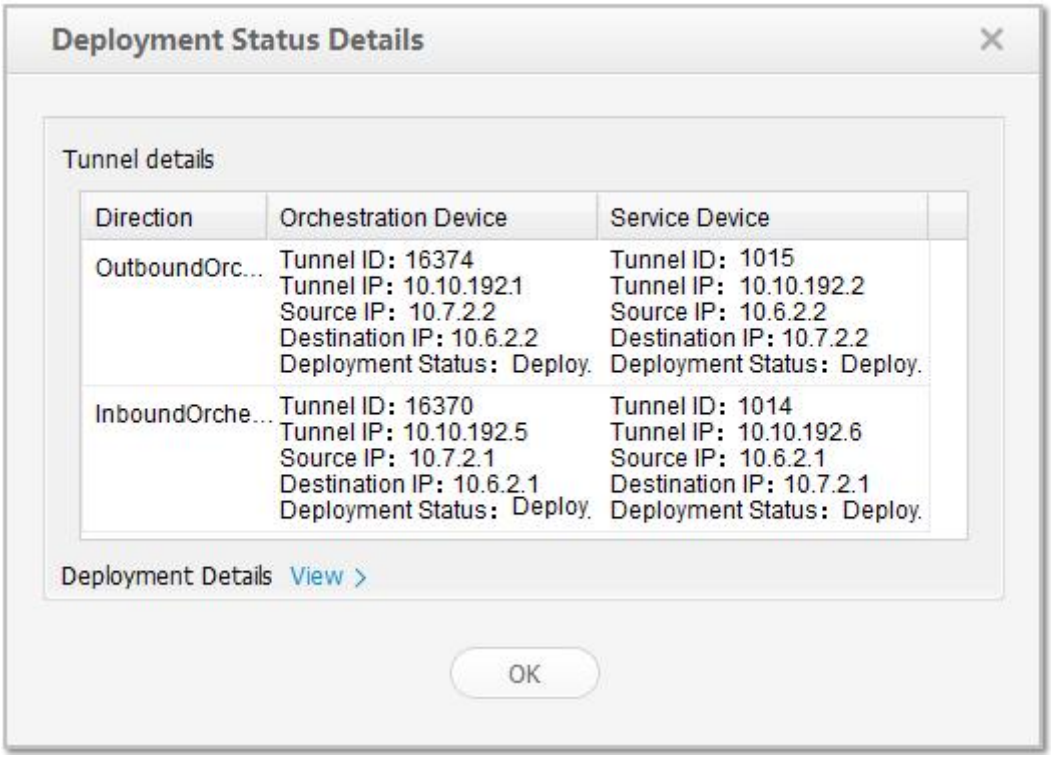
Figure 3-6 Service chain orchestration parameter settings



Verify the configuration. The commands used to configure Service Chain on the switch and firewall are automatically translated and delivered by the Agile Controller, without the need of manual operation. This improves deployment efficiency.

- Check whether a tunnel has been established between the switch and firewall on the Agile Controller, as shown in Figure 3-7.

Figure 3-7 Tunnel deployment results



- Run the **display acl all** command on the switch. The command output shows that the service flow rules have been delivered successfully.

```
[SwitchA] display acl all
 Total nonempty ACL number is 1
Advanced ACL S_ACL_20140401153202_B3E0 3998, 5 rules
Acl's step is 5
 rule 5 permit tcp source 10.85.100.11 0 source-port eq 22 destination 10.85.1
0.2 0 destination-port eq 21 (match-counter 0)
 rule 10 permit tcp source 10.85.100.12 0 source-port eq 22 destination 10.85.
10.2 0 destination-port eq 21 (match-counter 0)
 rule 15 permit tcp source 10.85.100.13 0 source-port eq 22 destination 10.85.
10.2 0 destination-port eq 21 (match-counter 0)
 rule 20 permit tcp source 10.85.100.14 0 source-port eq 22 destination 10.85.
10.2 0 destination-port eq 21 (match-counter 0)
 rule 25 permit tcp source 10.85.100.15 0 source-port eq 22 destination 10.85.
10.2 0 destination-port eq 21 (match-counter 0)
```

- Run the **display current-configuration | include traffic-redirect** command on the switch. The command output shows that the Service Chain configuration has been delivered successfully.

```
[SwitchA] display current-configuration | include traffic-redirect
traffic-redirect inbound acl name S_ACL_20140401153202_B3E0 3998 interface
Tunnel16370 <—When the service flow reaches the orchestration device for the first
time, the switch matches the traffic with the global policy-based routing and
redirects the traffic to the firewall.
SwitchA] interface Tunnel 16370
[SwitchA-Tunnel16370] display this
#
```

```
interface Tunnel16370
 description Controller_S_from_10.6.2.1
 ip address 10.10.192.13 255.255.255.252
 tunnel-protocol gre
 keepalive period 1
 source 10.7.2.1
 destination 10.6.2.1
 traffic-filter inbound acl name S_ACL_20140401153202_B3E0 3998<——The service flow
is filtered, returns to the orchestration device, and is forwarded based on normal
routes.
#
return
```

----End

4 Appendix

4.1 Acronyms and Abbreviations

Acronym/Abbreviation	Full Name
GRE	General Routing Encapsulation
ACL	Access control list
UCL	User control list
FW	Firewall
NGFW	Next-Generation Firewall
ASG	Application Security Gateway
AVE	Antivirus engine
IPS	Intrusion Prevention System
XMPP	Extensible Messaging and Presence Protocol