

# HUAWEI SecoManager Technical White Paper

**Issue**      V1.1  
**Date**        2020-09

**Copyright © Huawei Technologies Co., Ltd. 2020. All rights reserved.**

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

## **Trademarks and Permissions**



HUAWEI 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](mailto:support@huawei.com)

---

# About This Document

---

## Purpose

This document describes SecoManager security service orchestration technologies.





## Intended Audience


This document is intended for:

- Security planning engineers
- Network planning engineers
- Data configuration engineers
- System maintenance engineers

## Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
 <b>DANGER</b>	Indicates an imminently hazardous situation which, if not avoided, will result in death or serious injury.
 <b>WARNING</b>	Indicates a potentially hazardous situation which, if not avoided, could result in death or serious injury.
 <b>CAUTION</b>	Indicates a potentially hazardous situation which, if not avoided, may result in minor or moderate injury.
 <b>NOTICE</b>	Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance deterioration, or unanticipated results. NOTICE is used to address practices not related to personal injury.

Symbol	Description
 <b>NOTE</b>	Calls attention to important information, best practices and tips. NOTE is used to address information not related to personal injury, equipment damage, and environment deterioration.

---

# Contents

---

<b>About This Document</b> .....	<b>ii</b>
<b>1 Service Technologies</b> .....	<b>1</b>
1.1 Product Positioning .....	1
<b>2 Centralized Management of Infrastructure Security Services</b> .....	<b>2</b>
2.1 Device Management .....	2
2.2 Network Management .....	3
2.3 Object Management .....	3
2.4 Policy Management .....	3
<b>3 Infrastructure Security Service Orchestration</b> .....	<b>5</b>
3.1 Service Model .....	5
3.1.1 Protected Network Segment .....	5
3.1.2 Logical Partition .....	6
3.1.3 Application Program .....	7
3.2 Protected Network Segment .....	7
3.3 Security Management Based on Logical Partitions .....	7
3.4 Security Management Based on Applications .....	8
<b>4 Interworking with a Network Controller for Automatic Security Service Orchestration</b> .....	<b>9</b>
4.1 Overview .....	9
4.2 Feature Description .....	10
4.3 AC-DCN Service Model .....	10
4.3.1 Extranet .....	10
4.3.2 Tenant VPC .....	11
4.3.3 Public VPC .....	11
4.3.4 Logical Router .....	12
4.3.5 Logical Switch .....	12
4.3.6 Logical Port .....	12
4.3.7 Logical Firewall .....	12
4.3.8 Subnet .....	12
4.3.9 EPG .....	13
4.3.10 SFC .....	13

---

4.3.10.1 Background .....	13
4.3.10.2 Implementation .....	14
4.3.11 Object Relationship .....	15
4.4 Interworking with the AC-DCN for Automatic Security Service Orchestration .....	15
4.4.1 Solution Overview .....	15
4.4.2 System Administrator .....	15
4.4.2.1 Device Management .....	16
4.4.2.2 Resource Pool .....	16
4.4.3 Tenant Administrator .....	16
4.4.3.1 Security Policy Service .....	16
4.4.3.2 SNAT Service .....	17
4.4.3.3 EIP Service .....	18
4.4.3.4 IPSec Service .....	18
4.4.4 Application Example .....	19
4.4.4.1 Typical Networking .....	19
4.4.4.2 Traffic Model .....	19
<b>5 Interworking with the CIS for Closed-Loop Threat Handling and Intelligent Policy O&amp;M .....</b>	<b>21</b>
5.1 Automatic Closed-Loop Threat Handling in Data Center Scenarios .....	21
5.1.1 Overview .....	21
5.1.2 Feature Description .....	21
5.1.3 Key Technologies .....	21
5.1.4 Host Isolation .....	22
5.1.5 Quintuple-based Blocking .....	22
5.2 Application Policy Tuning .....	23
5.2.1 Overview .....	23
5.2.2 Key Technologies .....	23
5.3 Application Policy Simulation .....	24
5.3.1 Overview .....	24
5.3.2 Key Technologies .....	24

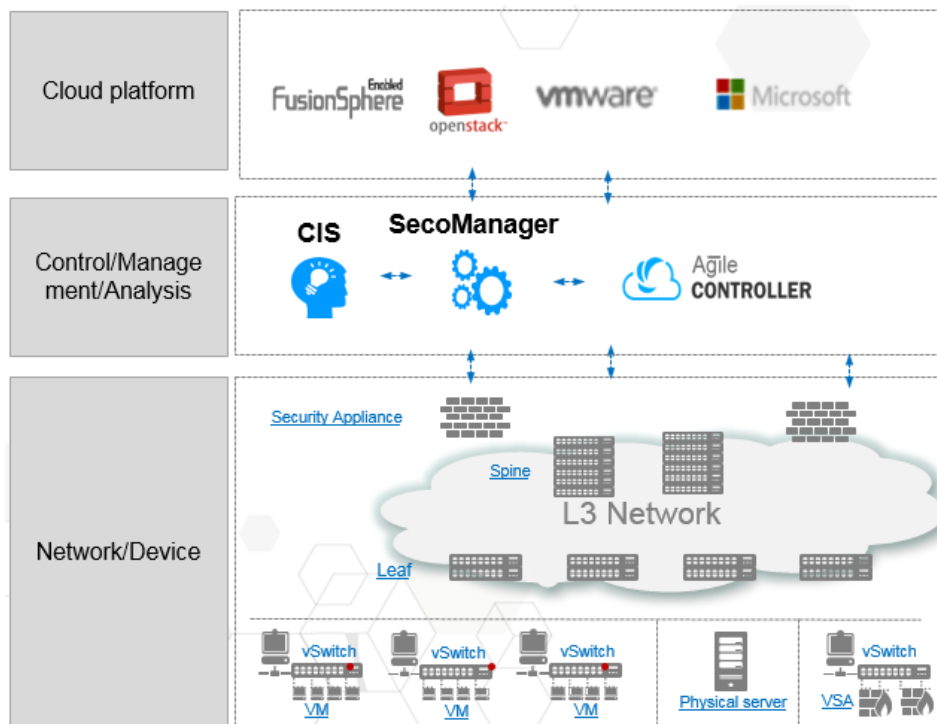
# 1 Service Technologies

## 1.1 Product Positioning

Huawei SecoManager is a new-generation security controller oriented for enterprise and carrier data centers and markets. As a centralized security control plane, the SecoManager automatically orchestrates and delivers security configurations to implement automatic service delivery.

The SecoManager can connect to a network controller (Agile Controller-DCN) and is compatible with a network management platform based on the Neutron service model. It provides diversified interconnection interfaces, including RPC and RESTful interfaces.

The SecoManager can also interwork with a security analyzer (CIS) to provide quick response to threats and implement traffic-based intelligent policy simulation and tuning.



# 2 Centralized Management of Infrastructure Security Services

---

This chapter describes the implementation mechanism of centralized management of infrastructure security services.

- ✧ [Device Management](#)
- ✧ [Network Management](#)
- ✧ [Object Management](#)
- ✧ [Policy Management](#)

## 2.1 Device Management

Device management provides the following basic device management capabilities: automatic device discovery, device and hot standby group addition, deletion, modification, and query, device group addition, deletion, modification, and query, device configuration consistency comparison, and device single sign-on (SSO).

To facilitate unified and routine management of two devices in hot standby mode, the SecoManager automatically identifies the two devices as a logical device.

**Device configuration consistency comparison:** The last SecoManager configuration is compared against the current device configuration. If the configurations are inconsistent, check the comparison result. You can synchronize device configuration changes to the controller or cancel the changes.

**Automatic hot standby identification:** After device discovery, the SecoManager automatically identifies devices' hot standby relationships and regards two physical devices in such a relationship as a logical device for management. This allows you to focus only on this logical device during policy configuration. Automatic hot standby identification takes several minutes. If the identification fails, you can also manually identify hot standby.

**Routine hot standby management:** You can perform configuration consistency check, active/standby consistency check, and version consistency check on the two devices in hot standby mode. If the configurations are inconsistent, you can manually adjust the configurations. In addition, you can manually perform active/standby switchover.



**Routine device O&M:** You can collect statistics on the CPU, memory, and disk usage of devices, device interface traffic statistics, and device license expiration time statistics, upgrade devices, and back up device configuration files.

Restrictions:

- The SecoManager can manage Huawei firewalls and provide relatively full-fledged functions, including hot standby management, consistency comparison and synchronization, and SSO.
- The SecoManager cannot manage third-party firewalls.
- WAF, vulnerability scanning, and DB audit support only the management and SSO capabilities.

## 2.2 Network Management

Currently, only the P2P IPSec policy function is supported.

IPSec policy configuration roadmap:

- Create a service group profile, in which you can specify the authentication mode, ID type, IKE algorithm, and IPSec algorithm.
- Based on the service group, you can create an IPSec policy (P2P), and specify the local and peer tunnel addresses, pre-shared key, and data flow to be encrypted. After that, IPSec is successfully created.

## 2.3 Object Management

Object management provides the security zone, address, service, time range, NAT address pool, intrusion prevention, URL filtering, AAPT, and antivirus capabilities.

These capabilities are basically the same as those of devices.

Security zones and address objects support device-level mapping, allowing different devices to have the same security zone and address name but different contents.

Configuration roadmap:

You can select an existing object from the policy module. If none of the existing objects meet your requirement, you can create one.

## 2.4 Policy Management

Currently, security and NAT policies are supported. The security policy function is mainly used for access control and content security check. You can set policy matching conditions, including the source/destination security zone, source/destination address, service, and time range, to perform control. The policy action can be permit or deny. In addition, you can also configure corresponding security profiles for content security protection.

Compared with the eSight in terms of the security policy function, the SecoManager has the policy group view and device group view added for quick policy management. In addition, it

also has policy change statistics, configuration consistency statistics, and deployment status statistics added.

**Policy group view and device group view for quick policy management:** You can check a single policy group or device group and quickly filter policies relevant to this policy group or device group. After you select a policy group or device group, new policies are automatically associated with this policy group or device group by default.

**Policy change statistics:** After the SecoManager configuration is changed, the policy status is identified as changed. You must deploy the changed policy to the corresponding device. The change status can be changed or not changed. You can click a state to quickly filter policies in this state.

**Configuration consistency statistics:** This function enables you to check whether the policies are the same as those on the associated devices, from a policy perspective. If any of the associated devices has inconsistent policy configurations, a message indicating the inconsistency is displayed. This function checks only whether the configuration of the last deployment is the same as the device configuration. The configuration consistency status can be consistent, inconsistent, and unknown (unchecked). You can click a state to quickly filter policies in this state.

**Deployment status statistics:** This function enables you to collect statistics on the policy deployment status, from a policy perspective. The deployment status can be not deployed, deployed, deploying, partially deployed, or deployment failed. This enables you to directly view the progress of policy deployment. You can click a state to quickly filter policies in this state.

**Configuration roadmap:**

- When creating a policy, you can select an existing object or directly create an object.
- After selecting an object, you can import it to the database or immediately deploy it to the corresponding device.
- If you only import it to the database, deliver the SecoManager configuration to the device through the subsequent unified deployment operation. Before the deployment, configuration comparison is performed. You can confirm the comparison result. If the comparison result is correct, deploy the configuration to the device.

**Configuration description:**

- If the current device configuration is inconsistent with the last configuration deployed to the device, a message indicating a conflict is displayed. Confirm the conflict first and then continue the deployment. You can perform either of the following operations to resolve the conflict: (1) Synchronize the device configuration to the SecoManager. (2) Discard the result of the device's proactive modification.
- You can back up a deployment task. If a fault occurs during device execution, you can perform rollback based on the deployment task.

# 3 Infrastructure Security Service Orchestration

---

This chapter describes the implementation mechanism of infrastructure security service orchestration.

- ✧ [Service Model](#)
- ✧ [Protected Network Segment](#)
- ✧ [Security Management Based on Logical Partitions](#)
- ✧ [Security Management Based on Applications](#)

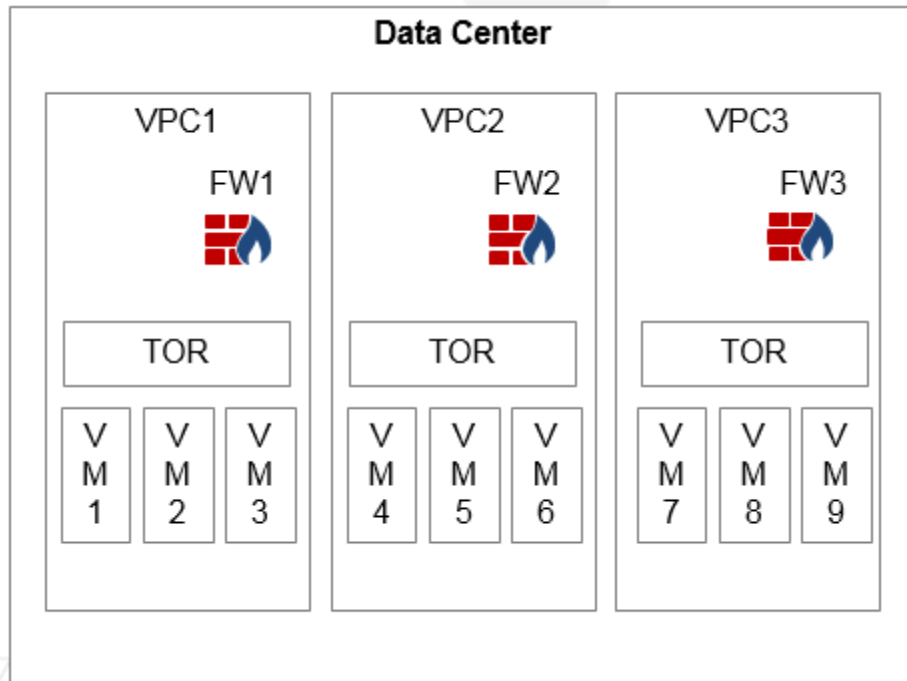
## 3.1 Service Model

This section describes the service orchestration models, including logical network, logical router, logical switch, subnet, and external network of the interworking network controller, and their relationship.

### 3.1.1 Protected Network Segment

As the basic model of security service orchestration, protected network segments specify the network segments that firewalls need to protect. Such a segment can be manually configured or automatically learned through collaboration with the AC-DCN. Through protected network segments, the SecoManager perceives relationships between IP addresses and firewall devices. During automatic policy orchestration, the SecoManager can then automatically find firewall devices that carry policies based on source and destination addresses of policies.

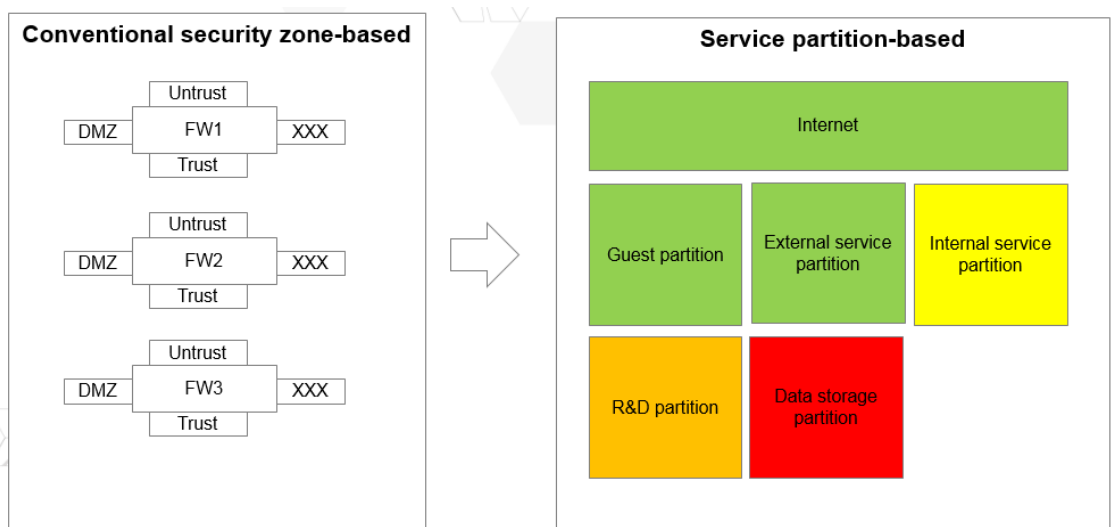
The following figure shows a data center scenario. Take VPC1 as an example. The protected network segment of FW1 covers the IP addresses of VM1, VM2, and VM3. Then the security policy for VM1 to access the Internet is automatically orchestrated to FW1. In this way, during the configuration of a policy, you need to pay attention only to service requirement configuration but not to which firewall will implement the policy.



In a data center scenario where an AC-DCN is deployed, the protected network of the SecoManager can automatically respond to changes. For example, if a VM is added to the network, the policy of the VM is automatically orchestrated to the firewall of the corresponding VPC.

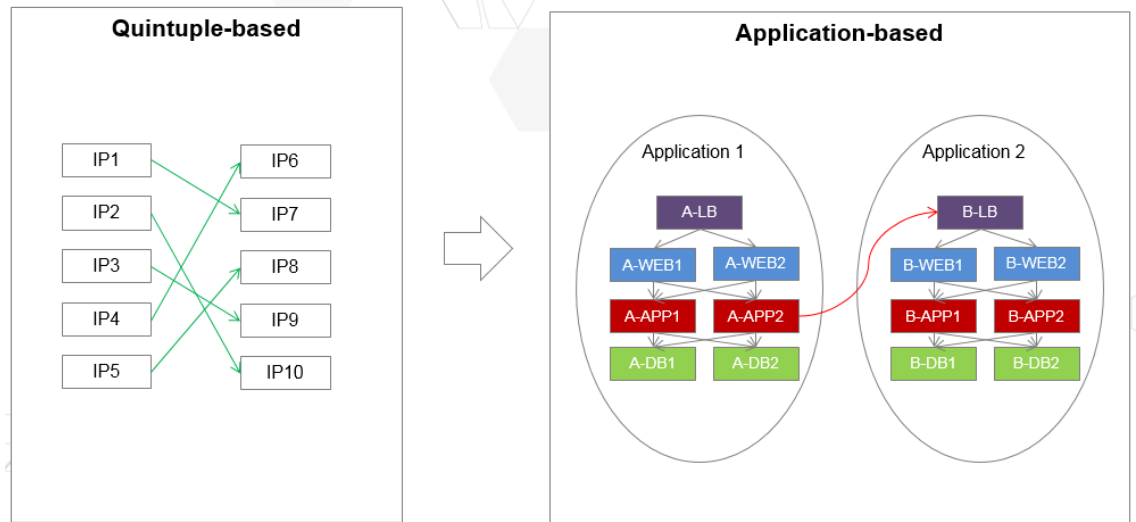
### 3.1.2 Logical Partition

Traditional security management is based on firewall security zones. However, this is too closely related to network deployment. When there are multiple firewalls, users' services cannot be restored. This issue can be addressed in a way that partitions are created based on services instead of physical networks and are automatically associated with firewalls.



### 3.1.3 Application Program

In a data center, there are many private application programs that are open to external systems, involving access requirements from IP addresses to applications and between applications. The application program model converts original IP address-IP address policies to application-related policies, making user maintenance easier and more direct and reducing the number of policies.



## 3.2 Protected Network Segment

#### Function description:

- You can import a protected network segment and create a device during the import.
- You can specify the security zone corresponding to the protected network segment. During policy orchestration, you can restore the corresponding security zone configuration.
- You can configure labels on the protected network segment, which can be used for policy orchestration (not supported in the current version).

#### Description of labels:

A label group is a group of labels of the same type. When configuring protected network segments, you can specify labels for them and group them according to the labels.

## 3.3 Security Management Based on Logical Partitions

#### Description of partition object management:

- The SecoManager supports the creation of logical partition objects. In a partition, you can specify an IP address range.
- You can also label a partition in the same way as you label a protected network segment.

- If the IP address range of a partition cannot be identified, the partition can be identified as a special partition. A system has one, and only one, special partition.

**Description of partition policies:**

- The SecoManager supports configuration of policies between partitions or within a partition using a matrix. In the policy matrix, you can view the number of common policies and the number of privilege policies (a privilege policy has a higher priority than a common policy) corresponding to partitions.
- You can click a matrix content item to view and configure corresponding policies between partitions or within a partition.
- The policies are configured basically in the same way.

**Configuration roadmap:**

- Configure or import a protected network segment.
- Configure the relationship between the partition and IP address range.
- Configure and deploy partition policies.

## 3.4 Security Management Based on Applications

**Description of application hosts:**

- An application host is a host where applications are deployed.
- If an application host has multiple IP addresses, you need to enter multiple IP addresses to the SecoManager.
- Multiple application host services can be deployed on an application host. Each host service usually consists of one or more processes, and can have one or more protocols and ports.

**Description of application policies:**

- The creation of application policies on the SecoManager involves defining application components, application host services contained in application components, and dependencies between components.
- Some application components depend on external application components and can be specified in application policies.
- Some application components need to open services externally, which can also be specified in application policies.

**Configuration roadmap:**

- Configure or import a protected network segment.
- Configure application host services.
- Configure and deploy application policies.

# 4 Interworking with a Network Controller for Automatic Security Service Orchestration

---

This chapter describes the implementation mechanism of network controller interworking for service orchestration.

- ✧ [Overview](#)
- ✧ [Feature Description](#)
- ✧ [AC-DCN Service Model](#)
- ✧ [Interworking with the AC-DCN for Automatic Security Service Orchestration](#)

## 4.1 Overview

In a conventional data center, application deployment often takes a long time. The application team relies on the network team to deploy a network; the network team needs to understand the application team's requirements to deploy a network that caters to the application service team. However, there are often some communication barriers between the application team and the network team, because they think differently. For the deployment of a new application, the network team needs to spend a large effort on requirement communications. In addition, it is difficult for network administrators to maintain subsequent network infrastructure adjustments.

This chapter describes how to use the Agile Controller-DCN and SecoManager to deploy an application. The Agile Controller-DCN maps applications to networks and implements fast network deployment of an application through simple GUI elements. The Agile Controller-DCN supports the basic requirement of Layer 2 and Layer 3 network interconnection and the advanced Layer 4 to Layer 7 network requirement. It provides a method of using the GUI to describe application requirements on networks to implement automatic service deployment. The SecoManager provides intra-application and inter-application security policy configurations to implement network visualization and improve network maintainability.

In this version, the SecoManager can be deployed in the Agile Controller-DCN as a service for efficient security and network collaboration.

## 4.2 Feature Description

The Agile Controller-DCN defines network orchestration models, such as VPC, EPG, and Subnet. EPG is essential for services, in that all policies are configured by EPG. The AC-DCN can connect to the vCenter and SystemCenter virtualization platforms.

The SecoManager automatically synchronizes information about the tenants, VPCs, network topology (including logical routers, logical switches, logical firewalls, and subnets), EPGs, and service function chains (SFCs) of the AC-DCN.

Independent security service orchestration based on AC-DCN interworking supports the following features:

- Device management
- Resource pool
- Security policy service
- SNAT service
- EIP service
- IPSec service

## 4.3 AC-DCN Service Model

This section describes the service orchestration models, including external network, tenant VPC, public VPC, logical router, logical switch, subnet, EPG, and SFC of the interworking AC-DCN, and their relationship.

### 4.3.1 Extranet

An extranet is connected to the Internet (the Internet can be replaced by other networks, such as an office network). This extranet provides a way for tenants' VMs to access the Internet or for the Internet to access VMs. The extranet has a subnet, which is a group of addressable IP addresses on the Internet. Generally, there is only one extranet (Neutron supports multiple extranets), and it is created by the administrator. Tenant networks can be created by tenants as they want. When a VM on the network of a tenant needs to communicate with the extranet and the Internet, the tenant needs a router. The router has two types of interfaces, namely, external gateway interface and internal interface. An internal interface is a gateway of the VM. There is only one external gateway interface that is connected to the extranet. This is how a path for the VM to access the Internet or for the Internet to access the VM is implemented.

The extranet can be used in the following scenarios:

- Mutual access between the intranet and Internet  
Enterprise devices are in the intranet and cannot obtain external information. To obtain external information, the intranet users need to access the Internet resources. For example, the railway ticketing system resides on the intranet. Railway staff can log in to the intranet to book tickets, but external personnel cannot access the ticketing system. If the intranet can communicate with the Internet, Internet users can also access the intranet to book tickets.
- Load balancing for traffic from the Internet. In scenarios where tenants' servers provide Internet services on intranets, LBs can be used to balance traffic from the Internet. VMs work in load balancing mode to balance heavy traffic on the Internet.

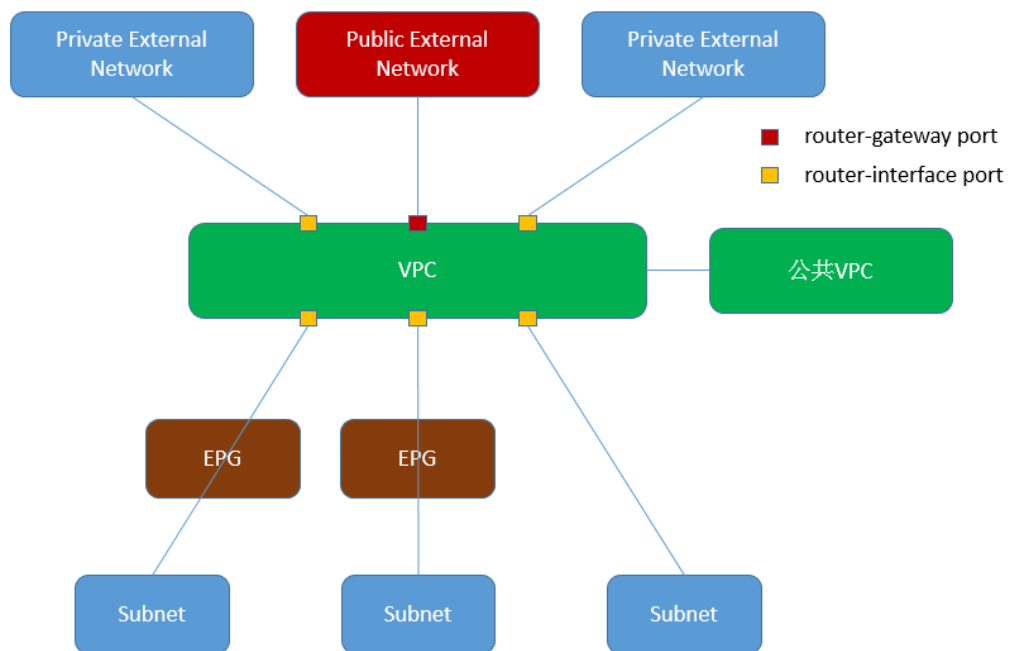


- Communication between an intranet and an external private network through IPSec VPN  
 During access between an intranet and an external private network, the non-encrypted connection is not secure, and the private IP address cannot be directly used for interconnection with the intranet and needs to be encapsulated through the VPN gateway. Therefore, access between an intranet and an external private network needs to be implemented through IPSec VPN.

### 4.3.2 Tenant VPC

Virtual Private Cloud (VPC) provides secure and reliable information processing, storage, and transmission services to tenants through the virtualization and encryption technologies based on network, storage, and computing resources. Multiple VPCs can be created for a tenant based on service requirements.

A VPC is the core of an application instance. It is a component for route selection and forwarding and a bridge between VMs and the Internet. A VPC can have an EPG, subnet, and port added internally and be associated with external networks and public VPCs externally. A VPC can be associated with a maximum of only one public external network that is connected to the Internet, but can be connected to multiple private external networks and public VPCs.



### 4.3.3 Public VPC

A public VPC is a public private network that can be accessed by all VPCs. It can be regarded as a public service in a POD, but is carried in the form of a VPC. The difference between the public VPC and public service lies in that the public service is outside the POD and not within the scope of AC-DCN service provisioning. Other systems or manual pre-configuration is required. The public VPC is a VPC provisioned by the AC-DCN.

If a Huawei firewall is deployed in the POD, the public VPC can have SNAT enabled. In addition, the VPC can access the public VPC and configure SNAT for address translation. In this way, VPCs with overlapping addresses can access the public VPC.

### 4.3.4 Logical Router

A logical router is virtualized from network devices running virtualization software such as the virtual system for Huawei CE switches to connect virtual machines (VMs) located on different networks to ensure that VMs can communicate with each other across a Layer 3 network.

A network device can have multiple logical routers virtualized for different tenants. Multiple tenants can share a network device. For each tenant, a logical router functions as an independent and real router, and has independent software and hardware resources and running space. Services of different logical routers do not affect each other. In terms of experience, there is no difference between a logical router and a real router.

One VPC has and only has one logical router.

### 4.3.5 Logical Switch

A logical switch is used to connect different virtual machines (VMs) to ensure that VMs can communicate with each other on a Layer 2 network.

A network device can have multiple logical switches virtualized for different tenants. Multiple tenants can share a network device. For each tenant, a logical switch functions as an independent and real switch, and has independent software and hardware resources and running space. Services of different logical switches do not affect each other. In terms of experience, there is no difference between a logical switch and a real switch.

### 4.3.6 Logical Port

A logical port is an access point for a VM to connect to a network. A physical port on a network device can be virtualized into multiple logical ports to be used by different tenants. Multiple tenants can share a port to access a network. For each tenant, a logical port functions as an independent and real port.

### 4.3.7 Logical Firewall

The firewall function can be provided by a physical or virtual firewall.

A firewall, as the border of a network, implements secure access control between extranets and an intranet, enhancing the network protection capability. It protects service data flows between the Untrust zone and Trust zone based on quintuple security control policies. It can also be used for access control between subnets.

The firewall is an optional component, depending on whether the tenant has an extranet. Deploy a firewall when a tenant is connected to an extranet for security.

A firewall can have multiple logical VASs virtualized for different tenants. Multiple tenants can share a firewall device. For each tenant, a logical VAS functions as an independent and real firewall, and has independent software and hardware resources and running space. Services of different logical VASs do not affect each other. In terms of experience, there is no difference between a logical VAS and a real firewall.

### 4.3.8 Subnet

In short, a subnet is an address pool consisting of a group of IP addresses. Communications between different subnets require the support of routers. Subnets on the network controller belong to the physical network.

Subnets fall into two types, namely subnets created in EPGs of VMM domains and subnets created in EPGs of physical domains.

The subnet VNI is allocated by the AC-DCN in the VNI resource pool of the POD, and the network segment is allocated in the IP resource pool of the tenant.

If a VLAN is created in the VMM domain, the VLAN is automatically allocated by the AC-DCN in the service VLAN resource pool of the POD. During application instance deployment, the subnet creates a network in the VMM selected by the EPG. For example, it invokes the vCenter interface to create a port group. If the subnet is a non-isolated network, the AC-DCN creates a VBDIF interface on the Border Leaf and binds it to the VRF of the VPC as the gateway of the subnet.

If a VLAN is created in the physical domain, the VLAN is allocated by the AC-DCN in the service VLAN resource pool of the tenant. During application instance deployment, if the subnet is a non-isolated network, the AC-DCN creates a VBDIF interface on the Border Leaf and binds it to the VRF of the VPC as the gateway of the subnet.

## 4.3.9 EPG

An End Point Group (EPG) is a set of devices that have the same attributes. Therefore, the EPG can be equivalent to the security group of the cloud platform on the network controller. On the AC-DCN, users can perform SFC traffic diversion based on the EPG.

## 4.3.10 SFC

### 4.3.10.1 Background

The SFC prototype is common in daily life. For example, to take the metro, passengers need to enter the station, purchase tickets, pass security check, and have their tickets verified under the guidance of metro staff. The process of entering the station can be regarded as an SFC, with the station entrance being the start point and the metro train the end point. Guiding passengers to enter the station, purchase tickets, pass security check, and have tickets verified is the major task.

On one hand, as the network size expands, an increasing number of devices are deployed in the network, and service data transmission paths gain in complexity. Network administrators need a tool to extract critical information from the complex service models and service logics, focusing on the function nodes involved in the service processing paths and summarizing a processing path for services of the same type.

On the other hand, an increasing number of services are carried in the network, and the services change more and more frequently. If network administrators need to manually configure devices for each service provisioning, the workload is heavy, and the working efficiency is low. The network administrators want to define the path for service processing. When the conditions are satisfied, the orchestration devices automatically redirect the traffic to the specified function devices for processing.

Eventually, when network administrators are using devices, devices cannot be shared because of network topology dependencies and physical device dependencies. Device resources cannot be fully used.

To solve the preceding problems, an abstract model is required, service provisioning workload needs to be reduced, and a resource pool of devices needs to be created for resource sharing. In response, SFCs appear.

### 4.3.10.2 Implementation

The core function of an SFC is to plan service data paths according to service objectives, determine the order and role of each node, and ensure that the data output from the SFC meets the requirements.



An SFC is composed of a consumer EPG, service nodes, and a producer EPG.

The consumer EPG is the entrance of the SFC, and the producer EPG is the exit. The service data to be processed enters the SFC from the consumer EPG, and the processing result is obtained from the producer EPG. The consumer EPG and producer EPG need to adopt Huawei CE series switches and are located at the network ingress and NVE nodes. The consumer EPG and the producer EPG can be the same device.

A service node has the following types of roles:

Role	Description
FW	A firewall is deployed at the network border and controls whether network access is allowed.
NAT	To solve the problems of public IP address shortage and private network server access to the Internet, NAT devices are used to map servers' private IP addresses to a public IP address so that multiple servers can share the same public IP address to access the Internet.
VPN	During interconnection between the headquarters and branches, data transmitted on the Internet is encrypted using VPN to ensure data transmission security.

Service nodes need to use Huawei Next Generation Firewalls (NGFWs) and third-party devices. For an NGFW, the preceding three roles are implemented on the basis of NGFW virtual systems.

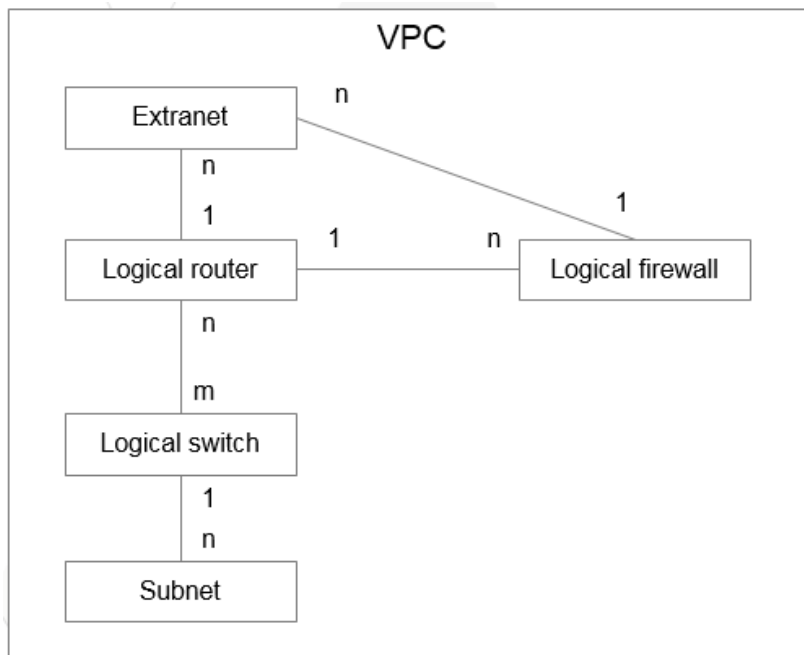
NGFWs fall into physical firewalls and software firewalls installed on X86 PC servers.

The support of the roles and AC-DCN varies with the service device model.

- If an NGFW is used, the NGFW supports not only the firewall, NAT, and VPN roles that the SFC needs to rely on but also the receiving of the network configuration parameters planned by the administrator from the AC-DCN.
- If a third-party device is used, the roles supported are subject to this third-party device. In addition, the AC-DCN does not support delivering network configuration parameters to the third-party device.

### 4.3.11 Object Relationship

For the preceding objects, multiple subnets can be created in a VPC logical network, and the subnets may be associated with a logical router through an internal router port, so that subnets on a logical router can communicate with each other. The logical router can be associated with an external network through an external gateway port, so that the subnets of the logical router can communicate with the external network.



## 4.4 Interworking with the AC-DCN for Automatic Security Service Orchestration

### 4.4.1 Solution Overview

This section describes how the SecoManager implements application-based independent service provisioning by role. The role can be system administrator and tenant administrator.

### 4.4.2 System Administrator

A system administrator manages devices and resource pools and allocates logical firewalls to tenants on demand.

This section describes key technical solutions unique to a system administrator.

- ✧ [Device Management](#)
- ✧ [Resource Pool](#)

### 4.4.2.1 Device Management

Device management provides the following basic device management capabilities: automatic device discovery, device and hot standby group addition, deletion, modification, and query, device group addition, deletion, modification, and query, device configuration consistency comparison, and device single sign-on (SSO).

To facilitate unified management of two devices in hot standby mode, the SecoManager automatically identifies the two devices as a logical device. In addition, you can perform configuration consistency check, active/standby consistency check, and version consistency check on the two devices in hot standby mode. If the configurations are inconsistent, you can manually adjust the configurations.

### 4.4.2.2 Resource Pool

After firewalls or hot standby groups are added to a resource pool, tenants can apply for logical firewalls as required. In this case, tenants no longer need to know which physical device in the resource pool carries a certain logical firewall, providing convenience.

The resource pool supports quota management for logical firewalls to limit the use of virtual firewalls and prevent multiple virtual firewalls of a physical firewall from preempting resources.

## 4.4.3 Tenant Administrator

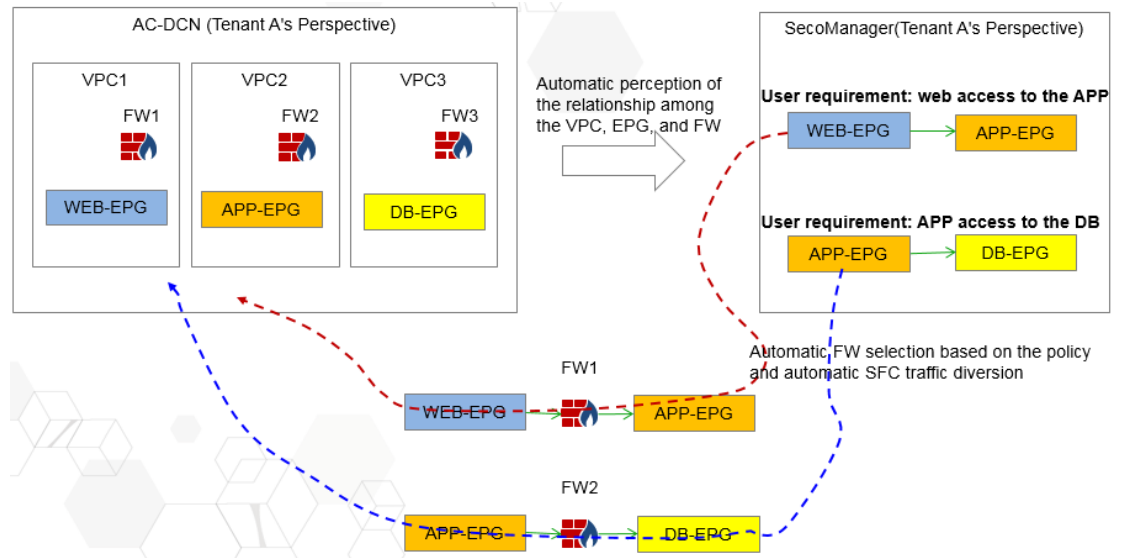
This section describes key technical solutions unique to a tenant administrator.

- ◇ [Security Policy Service](#)
- ◇ [SNAT Service](#)
- ◇ [EIP Service](#)
- ◇ [IPSec Service](#)

### 4.4.3.1 Security Policy Service

The SecoManager supports security policies within a VPC, between VPCs, and between a VPC and the Internet (both IPv4 and IPv6 are supported), and provides intrusion prevention and antivirus detection capabilities. After the AC-DCN's VPCs, external networks, and EPGs are synchronized to the SecoManager, the SecoManager allows the configuration of security policies based on the VPCs, external networks, and EPGs. Security policies can be configured between VPCs, between VPCs and external networks, and between EPGs to implement interworking or isolation.

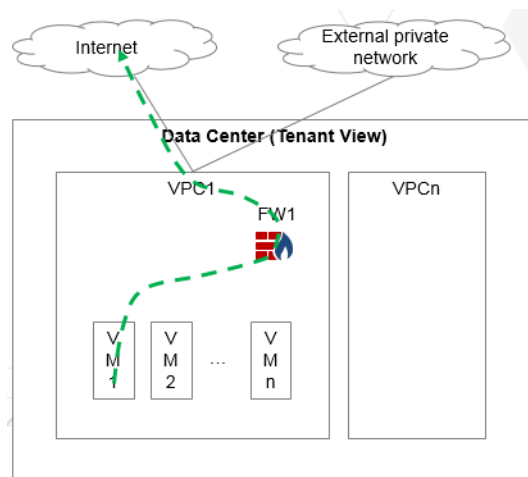
After a security policy service is configured, the SecoManager automatically determines the logical firewall that needs to carry the policy based on the service topology and whether to cooperate with the AC-DCN to implement on-demand SFC traffic diversion and scheduling and divert traffic to the firewall.



**Configuration roadmap:**

1. The tenant administrator creates a security policy service to allow secure access control between EPGs.
2. The SecoManager searches for the logical firewalls between the EPGs based on the existing configuration. If the logical firewalls can be found, select them. If no logical firewalls are found, a logical firewall is automatically specified.
3. The SecoManager orchestrates security policies to the corresponding logical firewalls.
4. The SecoManager checks whether traffic diversion is required. If yes, the AC-DCN is driven to perform SFC traffic diversion.

**4.4.3.2 SNAT Service**



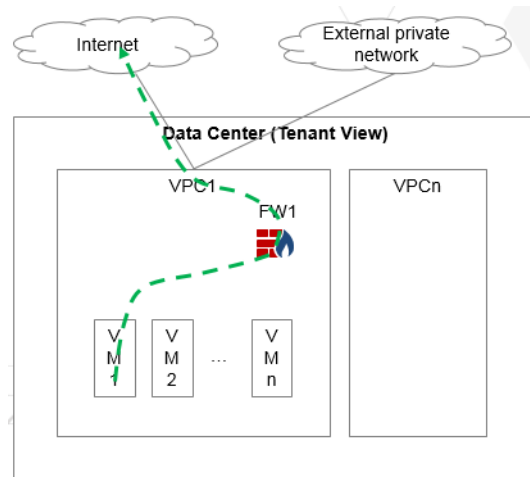
The SNAT service applies when VMs in a data center access the Internet or other private external networks (with overlapping addresses). In this case, the VMs must obtain a public IP address to access the external network.

The SecoManager supports the SNAT (including NAT and NAT64) service to be enabled on a specified logical firewall. Tenants can configure the SNAT service based on the VPC on

demand. An external network must be specified for the SNAT service. The addresses in the NAT address pool must be public IP addresses of external gateways.

The SecoManager can limit the bandwidth and control the number of connections based on the SNAT service.

### 4.4.3.3 EIP Service



The EIP service is used for a VM to provide services externally. A public IP address is required to allow external users to access the VM.

The SecoManager supports the EIP service to be enabled on a specified logical firewall. Tenants can configure the EIP service based on the VPC on demand. An external network must be specified for the EIP service. The external address of the EIP service must be the public IP address of an external gateway.

The SecoManager can limit the bandwidth and control the number of connections based on the EIP service.

### 4.4.3.4 IPSec Service

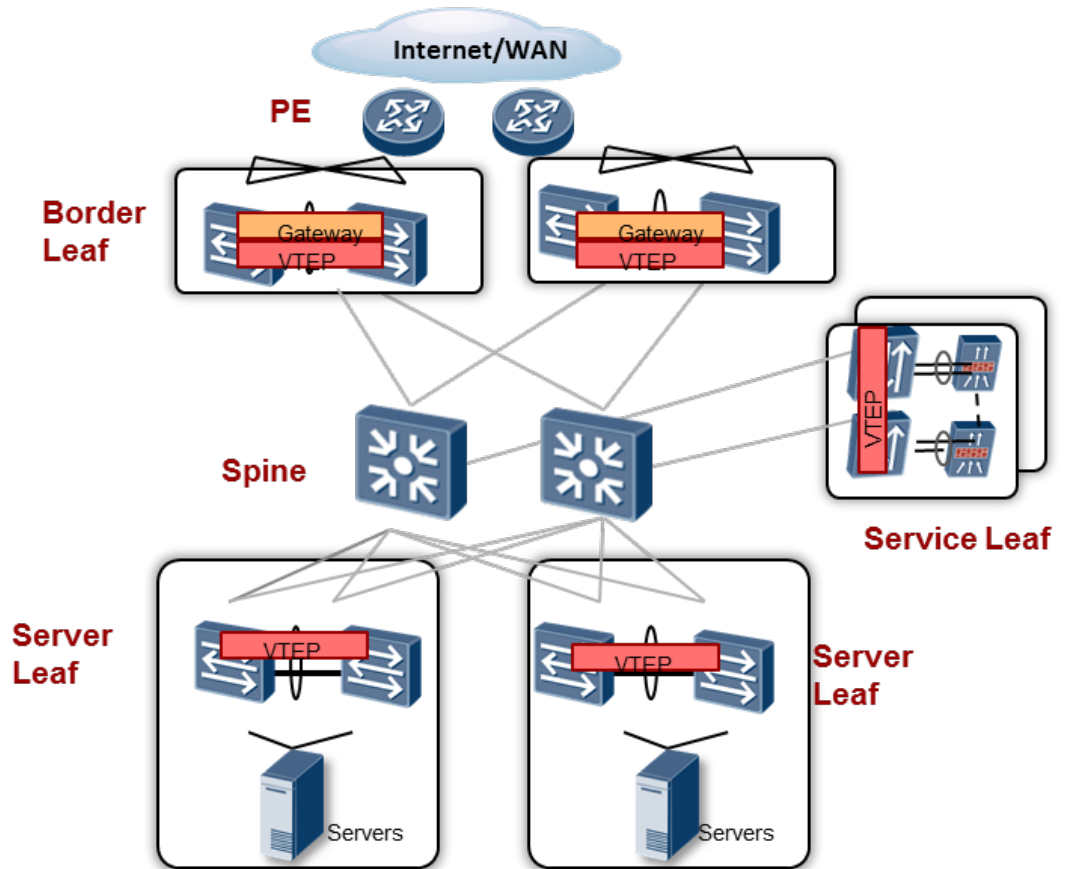
The IPSec service is used for the communication between a VPC and an external private network. When the VPC communicates with an external private network over the Internet, you can enable the IPSec service to solve this problem.

The SecoManager supports the IPSec service to be enabled on a specified logical firewall. Tenants can configure the IPSec service based on the VPC on demand. An external network must be specified for the IPSec service. The peer address of the IPSec service must be the public IP address of an external gateway.



## 4.4.4 Application Example

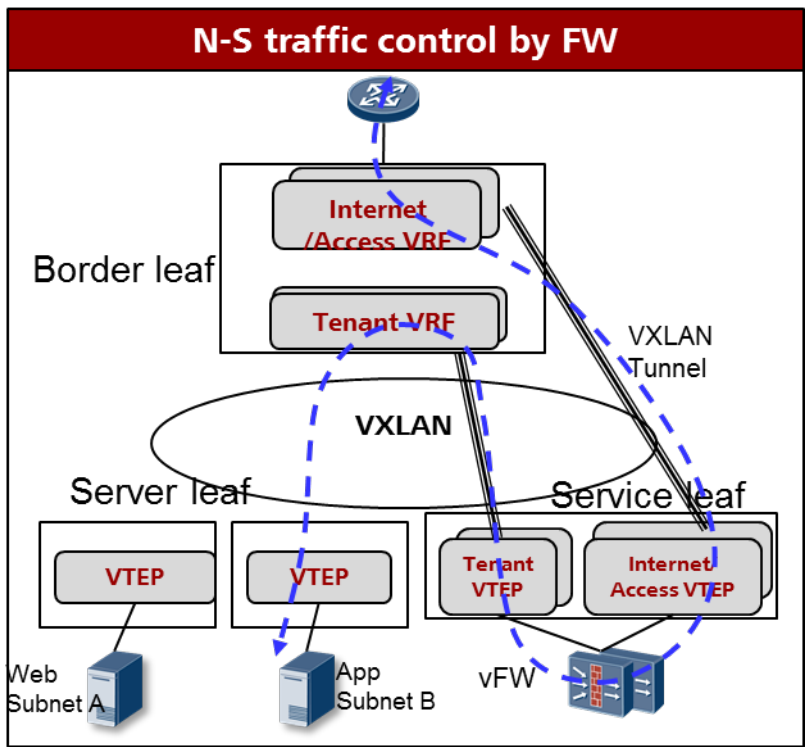
### 4.4.4.1 Typical Networking



As shown in the figure, the entire network consists of the PE, Spine, Border Leaf, Server Leaf, Service Leaf, server, and firewall. The Border Leaf, Server Leaf, and Service Leaf function as NVE nodes to encapsulate VXLAN packets. The firewall connects to the Service Leaf in bypass mode. The Border Leaf functions as a VXLAN gateway and connects to the PE as a network egress.

### 4.4.4.2 Traffic Model

The following figure shows a simple traffic model of a VM accessing the Internet.



When Subnet B accesses the external network, the following steps are involved:

The packet enters the Server Leaf, undergoes VXLAN encapsulation, and is sent to the Subnet B gateway on the Border Leaf through the VXLAN tunnel.

The Border Leaf is configured with the IP address for connecting to the firewall. The tenant searches for a route in the VRF and sends the packet to the firewall through the default route. The VXLAN tunnel is used to send the packet to the Service Leaf for decapsulation, and the VLAN packet is sent to the firewall.

After receiving the packet, the firewall matches it against some security policies. If Subnet B is allowed to access the Internet, VXLAN encapsulation is performed on the packet through the Service Leaf and then forwarded to the external VRF of the Border Leaf.

The Border Leaf searches for a route in the external VRF and sends the packet to the external network through the PE.

Till now, the entire forwarding process is complete.

# 5 Interworking with the CIS for Closed-Loop Threat Handling and Intelligent Policy O&M

---

This chapter describes the implementation mechanism of interworking with the network controller for service orchestration.

- ◇ [Closed-Loop Threat Handling](#)
- ◇ [Application Policy Tuning](#)
- ◇ [Application Policy Simulation](#)

## 5.1 Automatic Closed-Loop Threat Handling in Data Center Scenarios

### 5.1.1 Overview

As a security analyzer, the CIS can collect traffic and logs, and perform threat detection, threat identification, and threat handling based on Big Data analytics. After threat identification, threat handling requires the SecoManager to deliver the isolation or blocking policy to the firewall or AC-DCN.

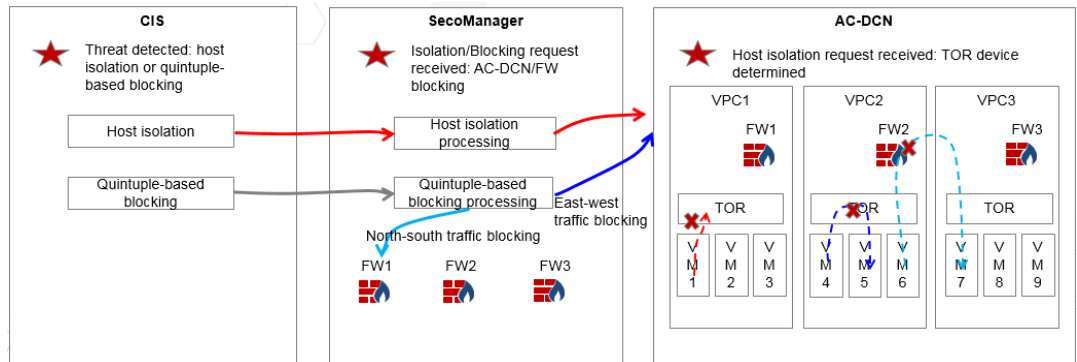
### 5.1.2 Feature Description

Automatic closed-loop threat handling supports the following features:

- Host isolation
- Quintuple-based blocking

### 5.1.3 Key Technologies

In a data center scenario, the SecoManager can collaborate with the CIS and AC-DCN to implement automatic closed-loop threat handling.



The overall implementation process is as follows:

- The CIS identifies threats, determines whether to perform host isolation or quintuple-based blocking according to the threat severity, and sends the request to the SecoManager.
- After receiving the host isolation request, the SecoManager directly distributes the request to the AC-DCN. After receiving the quintuple-based blocking request, the direction of the traffic to be blocked (east-west or north-south) is checked to determine whether the AC-DCN or the firewall shall block the traffic.
- If traffic isolation by the AC-DCN is required, the AC-DCN determines the TOR device and isolates the traffic.
- If traffic blocking by the firewall is required, the SecoManager orchestrates the policy to a specific firewall to perform quintuple-based blocking.

Restrictions: Currently, only scenarios where tenant IP addresses do not overlap are supported.

### 5.1.4 Host Isolation

For host isolation, refer to the preceding solution. The request is directly distributed to the AC-DCN for processing. On the AC-DCN, the corresponding TOR device is found based on the isolated VM-IP, and the corresponding isolation policy is delivered. If the TOR device changes due to VM migration, the AC-DCN automatically changes the policy and delivers the policy to the new TOR device.

### 5.1.5 Quintuple-based Blocking

The process of identifying whether east-west or north-south traffic is blocked is as follows:

- The SecoManager synchronizes the network topology information of the AC-DCN and identifies the association between the VPC subnet and the firewall in the network topology. The network segment corresponding to the subnet of the VPC serves as the protected network segment of the firewall.
- If both the source and destination IP addresses involved in quintuple-based blocking are on the protected network segment of a firewall, east-west traffic is to be blocked.
- If only the source or destination IP address involved in quintuple-based blocking is on the protected network segment of a firewall, north-south traffic is to be blocked.

## 5.2 Application Policy Tuning

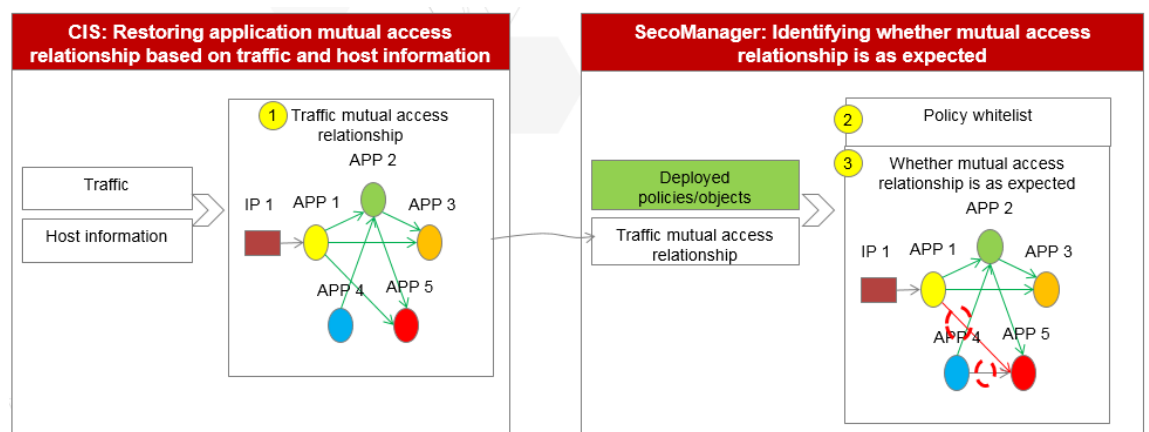
### 5.2.1 Overview

Application policy tuning has the following purposes:

- (1) Policy management is converted from the original IP address-IP address perspective to the IP address-application and application-application perspectives, making user maintenance more direct and reducing the number of policies to be maintained.
- (2) The access relationships between applications are complex and constantly changing. In addition, new applications constantly go online and offline. During routine O&M, you can identify newly discovered applications, offline applications, and changed applications by comparing application policies and application group mutual access relationships generated based on traffic.

### 5.2.2 Key Technologies

As a security analyzer, the CIS can collect traffic and host information, restore application groups and mutual access relationships based on traffic and host information, and assist the SecoManager in intelligent application policy tuning.



The overall implementation process is as follows:

- The SecoManager creates a tuning task and distributes the task to the CIS for application grouping and mutual access relationship learning.
- The CIS collects traffic and host information and generates application groups and mutual access relationships based on learning algorithms.
- The SecoManager receives information about the application groups and mutual access relationships and compares the information with the mutual access relationships generated by the deployed policies or objects.
- If a policy but not a mutual access relationship is found, the policy is considered redundant.

- If a mutual access relationship is found and a traditional IP policy is used, you can convert the traditional IP policy to an application-based policy, that is, generate an application whitelist.

Instructions:

- A tuning task supports both one-time and periodic task delivery.
- You can specify a traffic time range for application learning. By default, traffic of the last 15 days is learned.

Restrictions: Only an infrastructure administrator can perform application policy tuning.

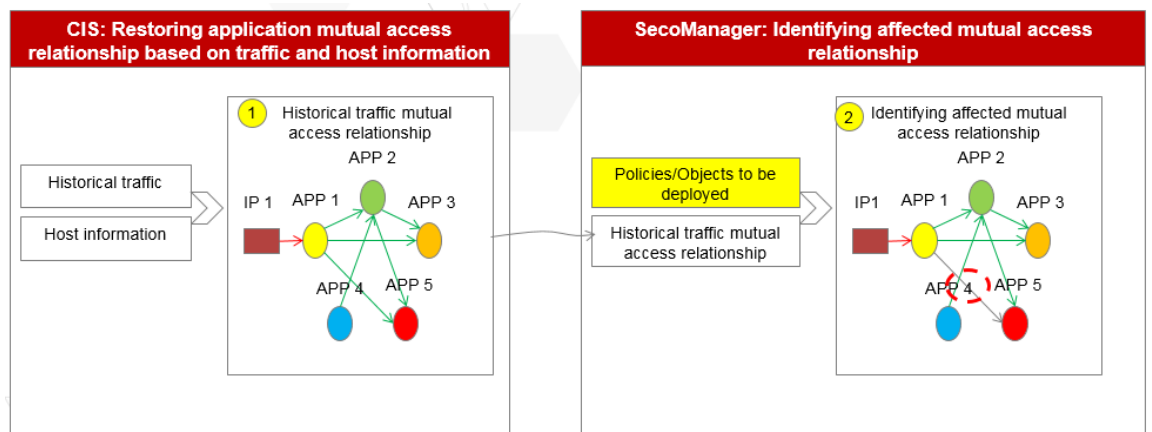
## 5.3 Application Policy Simulation

### 5.3.1 Overview

When a large number of policies are changed or a key period such as a major holiday is around, policy simulation can be used to evaluate the impact of policies before their deployment to devices. If the simulation result is as expected, you can determine that the policies can be deployed based on the simulation result. If the simulation result is not as expected, you can modify the policies, perform simulation again, and check whether the simulation result is as expected.

### 5.3.2 Key Technologies

As a security analyzer, the CIS can collect traffic and host information, restore application groups and mutual access relationships based on traffic and host information, and assist the SecoManager in application policy simulation.



The overall implementation process is as follows:

- The SecoManager creates a simulation task and distributes the task to the CIS for application grouping and mutual access relationship learning.
- The CIS collects traffic and host information and generates application groups and mutual access relationships based on learning algorithms.

- The SecoManager receives information about the application groups and mutual access relationships and matches them against all policies or objects to be deployed.
- If the matching action is permit, the application mutual access relationship does not change.
- If the matching action is block, the application mutual access relationship is blocked. You need to confirm with the customer whether the result is as expected.

Instructions:

- The simulation task can only be a one-time task but not a periodic one.
- During the simulation, the changed device list is automatically selected.
- The simulation can be performed based on the application discovery learning result or on the application mutual access relationship that is learned based on the traffic.

Restrictions: Only an infrastructure administrator can perform application policy simulation.