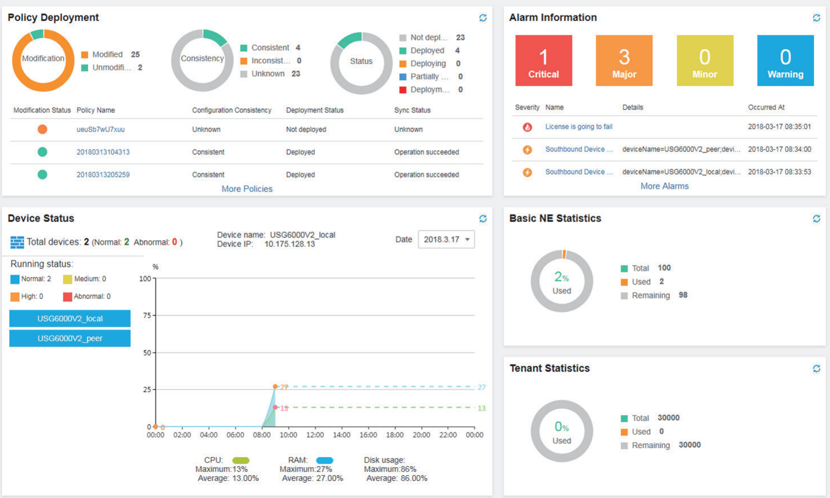
Huawei SecoManager Security Controller

In the face of differentiated tenant services and frequent service changes, how to implement automatic analysis, visualization, and management of security services, security policy optimization, and compliance analysis are issues that require immediate attention. Conventional O&M relies on manual management and configuration of security services and is therefore inefficient. Security policy compliance check requires dedicated personnel for analysis. Therefore, the approval is usually not timely enough, and risky policies may be omitted. The impact of security policy delivery on services is unpredictable. That is, the impact of policies on user services cannot be evaluated before policy deployment. In addition, as the number of security policies continuously increases, it becomes difficult for security O&M personnel to focus on key risky policies. The industry is in urgent need of intelligent and automated security policy management across the entire lifecycle of security policies to help users quickly and efficiently complete policy changes and ensure policy delivery security and accuracy, thereby effectively improving O&M efficiency and reducing O&M costs.

The SecoManager Security Controller is a unified security controller provided by Huawei for different scenarios such as DCs, campus networks, Branch. It provides security service orchestration and unified policy management, supports service-based and visualized security functions, and forms a proactive network-wide security protection system together with network devices, security devices, and Big Data intelligent analysis system for comprehensive threat detection, analysis, and response.

Product Appearances



Policy Deployment

Modification		Consistency		Status	
Modified	25	Consistent	4	Not depl...	23
Unmodifi...	2	Inconsist...	0	Deployed	4
		Unknown	23	Deploying	0
				Partially ...	0
				Deploym...	0

Modification Status	Policy Name	Configuration Consistency	Deployment Status	Sync Status
●	ueuSb7wU7xuu	Unknown	Not deployed	Unknown
●	20180313104313	Consistent	Deployed	Operation succeeded
●	20180313205259	Consistent	Deployed	Operation succeeded

More Policies

Alarm Information

1	3	0	0
Critical	Major	Minor	Warning

Severity	Name	Details	Occurred At
●	License is going to fail		2018-03-17 08:35:01
●	Southbound Device ...	deviceName=USG6000V2_peer;devi...	2018-03-17 08:34:00
●	Southbound Device ...	deviceName=USG6000V2_local;devi...	2018-03-17 08:33:53

More Alarms

Device Status

Total devices: 2 (Normal: 2 Abnormal: 0)

Device name: USG6000V2_local
Device IP: 10.175.128.13

Date 2018.3.17

Running status:
Normal: 2 Medium: 0
High: 0 Abnormal: 0

USG6000V2_local
USG6000V2_peer

CPU: Maximum:13% Average: 13.00%
RAM: Maximum:27% Average: 27.00%
Disk usage: Maximum:86% Average: 86.00%

Basic NE Statistics

2% Used

Total	100
Used	2
Remaining	98

Tenant Statistics

0% Used

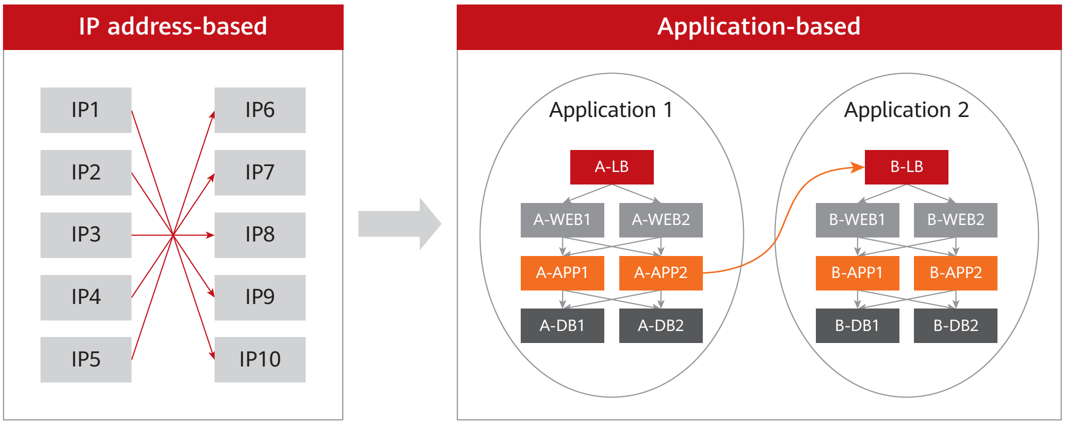
Total	30000
Used	0
Remaining	30000

HUAWEI

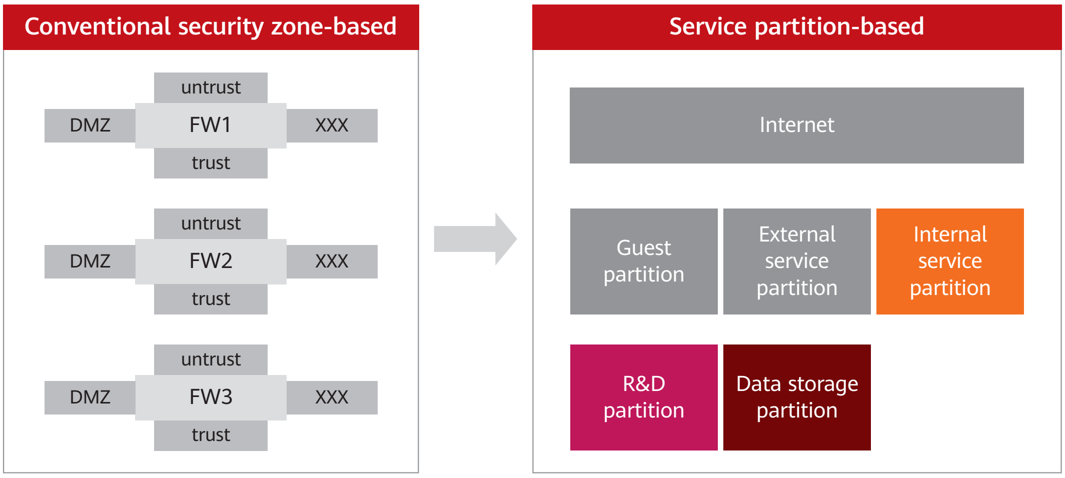
Product Highlights

Multi-dimensional and automatic policy orchestration, security service deployment within minutes

- **Application mutual access mapping and application-based policy management:** Policy management transitions from the IP address-based perspective to the application mutual access relationship-based perspective. Mutual-access relationships of applications on the network are abstracted with applications at the core to visualize your application services so that you can gain full visibility into the services, effectively reducing the number of security policies. The model-based application policy model aims to reduce your configuration workload and simplify network-wide policy management.



- **Policy management based on service partitions:** Policy management transitions from the security zone-based perspective to the service partition-based perspective. Conventional network zones are divided into security zones, such as the Trust, Untrust, DMZ, and Local zones. In a scenario with a large number of security devices and a large network scale, factors of security zone, device, policy, service rollout, and service change are intertwined, making it difficult to visualize services and to effectively guide the design of security policies. However, if security policies are managed, controlled, and maintained from the perspective of service partitions, users need to pay attention only to service partitions and security services but not the mapping among security zones, devices, and services, which effectively reduces the complexity of security policy design.



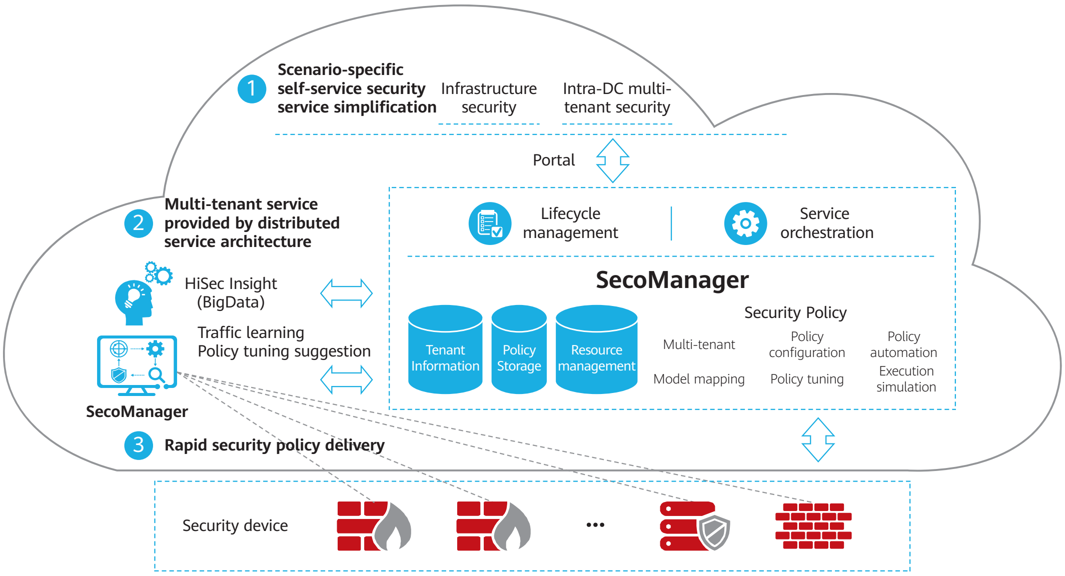
- **Management scope of devices and policies defined by protected network segments to facilitate policy orchestration:** A protected network segment is a basic model of security service orchestration and can be considered as a range of user network segments protected by a firewall. It can be configured manually or through network topology learning. The SecoManager Security Controller detects the mapping between a user service IP address and a firewall. During automatic policy orchestration, the SecoManager Security Controller automatically finds the firewall that carries a policy based on the source and destination addresses of the policy.
- **Automatic security service deployment:** Diversified security services bring security assurance for data center operations. Technologies such as protected network segment, automatic policy orchestration, and automatic traffic diversion based on service function chains (SFCs) enable differentiated tenant security policies. Policies can be automatically tiered, split, and combined so that you can gain visibility into policies.

Intelligent policy O&M to reduce O&M costs by 80%

- **Policy compliance check:** Security policy compliance check needs to be confirmed by the security approval owner. The average number of policies to be approved per day ranges from several to hundreds. Because the tool does not support all rules, the policies need to be manually analyzed one by one, resulting in a heavy approval workload and requiring a dedicated owner to spend hours in doing so. The SecoManager Security Controller supports defining whitelists, risk rules, and hybrid rules for compliance check. After a policy is submitted to the SecoManager Security Controller, the SecoManager Security Controller checks the policy based on the defined check rules and reports the check result and security level to the security approval owner in a timely manner. In this way, low-risk policies can be automatically approved, and the security approval owner needs to pay attention only to non-compliant policy items, improving the approval efficiency and avoiding the issues that the approval is not timely and that a risky policy is omitted.
- **Policy simulation:** Based on the learning result of service mutual access relationships, the policies to be deployed are compared, and their deployment is simulated to assess the impact of the deployment, effectively reducing the risks brought by policy deployment to services.
- **Redundant policy deletion:** After a policy is deployed, redundancy analysis and hit analysis are performed for policies on the entire network, and the policy tuning algorithm is used, deleting redundant policies and helping you focus on policies closely relevant to services.

Network collaboration and security association for closed-loop threat handling within minutes

- **Collaboration with network for threat handling:** In a conventional data center, application deployment often takes a long time. The application service team relies on the network team to deploy the network; the network team needs to understand the requirements of the application service team to deploy a network that is suitable for the application service team. The SecoManager Security Controller learns mappings between service policies and security policies based on the network topology, and collaborates with the data center SDN management and control system (IMaster NCE-Fabric) or campus SDN management and control system to divert tenant traffic to corresponding security devices based on SFCs on demand. The SecoManager Security Controller automatically synchronizes information about the tenants, VPCs, network topology (including logical routers, logical switches, logical firewalls, and subnets), EPGs, and SFCs from the SDN management and control system and combines the learned application service mutual access relationships to automatically orchestrate and deliver security policies, implementing security-network synergy.



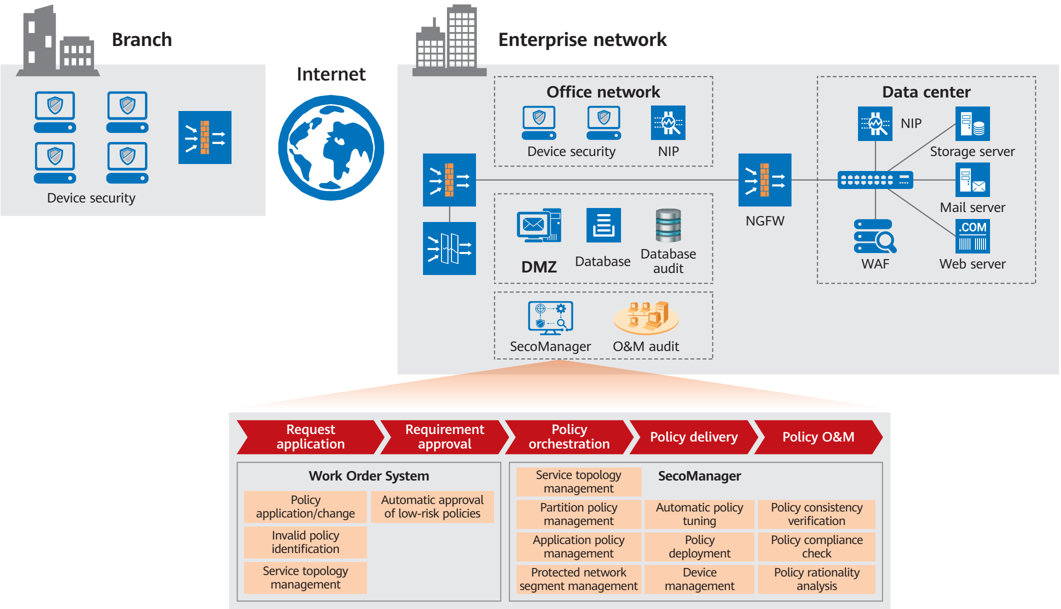
- **Collaboration with security:** Advanced persistent threats (APTs) threaten national infrastructure of the finance, energy, government, and other sectors. Attackers exploit 0-day vulnerabilities, use advanced evasion techniques, combine multiple attack means such as worm and ransomware, and may remain latent for a long period of time before they actually initiate attacks. The Big Data security product HiSec Insight can effectively identify unknown threats based on network behavior analysis and correlation analysis technologies. The threat handling method, namely isolation or blocking, is determined based on the threat severity. For north-south threats, the SecoManager Security Controller delivers quintuple blocking policies to security devices. For east-west threats, isolation requests are delivered to the network SDN management and control system to control switches or routers to isolate threatened hosts.

Product Deployment

- **Independent deployment:** The SecoManager Security Controller is deployed on a server or VM as independent software.
- **Integrated deployment:** The SecoManager Security Controller and SDN management and control system are deployed on the same physical server and same VM.

Typical Applications

Conventional network: Centralized management of security policies on the entire network



Request application → Requirement approval → Policy orchestration → Policy delivery → Policy O&M

Work Order System

Policy application/change	Automatic approval of low-risk policies
Invalid policy identification	
Service topology management	

SecoManager

Service topology management		
Partition policy management	Automatic policy tuning	Policy consistency verification
Application policy management	Policy deployment	Policy compliance check
Protected network segment management	Device management	Policy rationality analysis

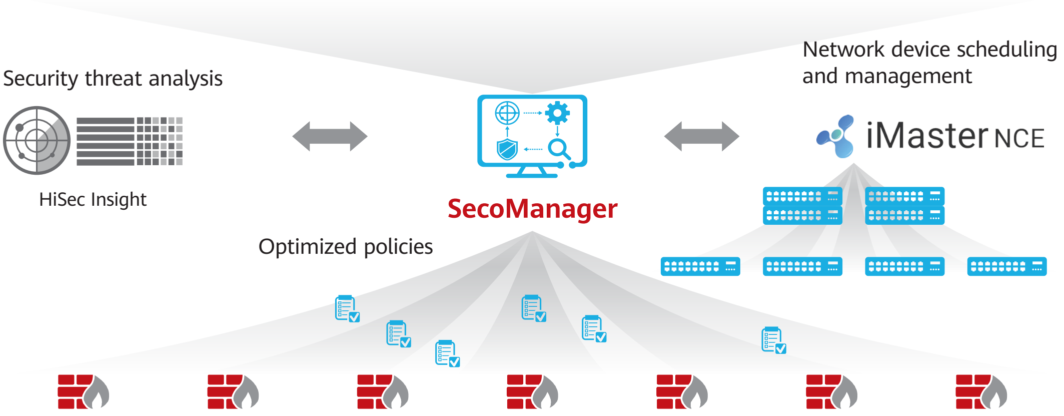
- For organizations with a large number of branches, such as large-scale retail chains, large-scale logistics enterprises, and finance business outlets, the SecoManager Security Controller can centrally manage a large number of security NEs.
- The SecoManager Security Controller can connect to an enterprise's work order system for automated policy compliance check, policy orchestration, and policy delivery.
- The SecoManager Security Controller can analyze the reasonability of deployed policies and improve O&M efficiency through policy compliance check, policy redundancy analysis, and policy consistency comparison.

SDN network: Unified management of network-wide security policies and multi-dimensional threat prevention

Security Controller

Automatic service orchestration	Security policy simulation	Security policy tuning	Intelligent network-wide collaboration
FW/IPS/AV security policy services Service topology Lifecycle management	Predeployment impact analysis Dynamic simulation execution	Redundancy, risk, and hit analysis Application policy tuning	HiSec Insight collaboration Data center SDN management and control system Collaboration

Basic NE management (policy, device, and cluster management)



- Collaboration with the SDN management and control system to detect network topology changes and implement tenant-based automatic security service deployment.
- North-south threat blocking, east-west threat isolation, and refined SDN network security control through SFC-based traffic diversion.
- Interworking with the cloud platform to automatically convert service policies to security policies.

Product Specifications

Major Functions		
Category	**Sub-Category**	**Description**
Basic NE management	Device management	Device discovery, device management (firewall and IPS), (three-level) device group management, virtual system management, configuration consistency check, device SSO, HSB management, customized rights- and domain-based management, system template, device monitoring, and global monitoring
	Resource pool management	Resource pool adding, deletion, modification, and query
	Object management	Address, service, time range, NAT address pool, URL category, IPS, antivirus, URL filtering, APT, application host, network partition management, and application group
	Policy management	Security policy, NAT policy, VPC policy, IPSec policy, security service, and task deployment
Policy collaboration	Big Data security collaboration	Receiving threat handling requests from the big data security analysis system and sending them to threat blocking devices
	Controller collaboration	Network topology awareness and SFC-based traffic diversion policy delivery
Policy orchestration	Automatic delivery of security policies based on network partitions, application mutual access relationships, security services, and VPCs	
Policy tuning	Policy tuning based on redundancy analysis results	
Policy simulation	Analysis of policy change impacts on application services based on simulation results before policy changes	
Operating Environment		
X86 hardware requirements	• CPU: 2.4GHz, 16-core • Memory: 64 GB • Hard disk: 2 x 600G RAID1 • Network: 6 x GE	
ARM hardware requirements	• CPU: 2.6GHz, 2*32-core • Memory: 128G • Hard disk: 2 x 1200G RAID1 • Network: 4 x GE + 4 x 10GE	
Software requirements	Operating system: • X86: Euler OS 2.0 SP5 • ARM: Euler OS 2.0 SP8 Virtualization software (If the SecoManager Security Controller is deployed on a VM, the virtualization software must be prepared.) • FusionCompute KVM 6.5 • FusionSphere 6.3	

Ordering Information

BOM Number	Description
Rack Server	
SCM-AC-01	Function Module, SecoManager, SCM-AC-01, SecoManager AC Typical Configuration 01 (2*10Core/2.2GHz CPU, 2*32GB Memory, 2*600GB-SAS 3.5inch, 2*4GE+2*10GE SFP+, 2*900W AC, RAID Card, Guide rail)
SCM-AC-02	Function Module, SecoManager, SCM-AC-02, SecoManager AC Typical Configuration 02 (2*10Core/2.2GHz CPU, 2*32GB Memory, 2*600GB-SAS 3.5inch, 2*4GE+2*10GE SFP+, 2*900W AC, RAID Card, Guide rail)
SCM-AC-03	Function Module, SecoManager, SCM-AC-03, SecoManager AC Typical Configuration 03 (2*10Core/2.2GHz CPU, 2*32GB Memory, 2*600GB-SAS 3.5inch, 2*4GE+2*10GE SFP+, 2*900W AC, RAID Card, Guide rail)
SCM-AC-04	Function Module, SecoManager, SCM-AC-04, SecoManager AC Typical Configuration 04 (2*10Core/2.2GHz CPU, 2*32GB Memory, 2*600GB-SAS 3.5inch, 2*4GE+2*10GE SFP+, 2*900W AC, RAID Card,Guide rail)
SCM-AC-05	Function Module, SecoManager, SCM-AC-05, SecoManager AC Typical Configuration 05 (2*10Core/2.2GHz CPU, 2*32GB Memory, 2*600GB-SAS 3.5inch, 2*4GE+2*10GE SFP+, 2*900W AC, RAID Card, Guide rail)
SCM-TS-02	Function Module, TaiShan 200(Model 2280), SCM-TS-02, SecoManager AC High Configuration(2*32Core@2.6GHz CPU, 4*32G Memory, 2*1200GB SAS, 4*GE+4*10G SFP+, 2*900W AC)
Software	
SCMPLF01	Software Charge, SecoManager, SCMPLF01, SecoManager Software Platform, Electronic
SCMDM	Software Charge, SecoManager, SCMDM, Firewall Device Management License, per device, Electronic
SCMPO	Software Charge, SecoManager, SCMPO, Firewall Security Policy Orchestration License, per devices, Electronic
SCMDMVAS	Software Charge, SecoManager, SCMDMVAS, Firewall Device Management License, per VAS, Electronic
SCMPOVAS05	Software Charge, SecoManager, SCMPOVAS05, Firewall Security Policy Orchestration License, per 5 VAS, Electronic
SCMPOVAS10	Software Charge, SecoManager, SCMPOVAS10, Firewall Security Policy Orchestration License, per 10 VAS, Electronic
SCMPOVAS50	Software Charge, SecoManager, SCMPOVAS50, Firewall Security Policy Orchestration License, per 50 VAS, Electronic
SCMPOVAS100	Software Charge, SecoManager, SCMPOVAS100, Firewall Security Policy Orchestration License, per 100 VAS, Electronic
SCMPOVAS500	Software Charge, SecoManager, SCMPOVAS500, Firewall Security Policy Orchestration License, per 500 VAS, Electronic

BOM Number	Description
SCMPOVAS1000	Software Charge, SecoManager, SCMPOVAS1000, Firewall Security Policy Orchestration License, per 1000 VAS, Electronic
SCMADAT	Software Charge, SecoManager, SCMADAT, SCM third party platform adaption license, Electronic
SCMPLFSNS01	Software annual fee, SecoManager, SCMPLFSNS01, SecoManager Software Platform, 1 Year Subscription and Support, Electronic
SCMDMSNS1Y	Software annual fee, SecoManager, SCMDMSNS1Y, Firewall Device Management, 1 Year Subscription and Support, per device, Electronic
SCMPOSNS1Y	Software annual fee, SecoManager, SCMPOSNS1Y, Firewall Security Policy Orchestration, 1 Year Subscription and Support, per device, Electronic
SCMDMVASSNS1Y	Software annual fee, SecoManager, SCMDMVASSNS1Y, Firewall Device Management, 1 Year Subscription and Support, per VAS, Electronic
SCMPOVAS05SNS1Y	Software annual fee, SecoManager, SCMPOVAS05SNS1Y, Firewall Security Policy Orchestration, 1 Year Subscription and Support, per 5 VAS, Electronic
SCMPOVAS10SNS1Y	Software annual fee, SecoManager, SCMPOVAS10SNS1Y, Firewall Security Policy Orchestration, 1 Year Subscription and Support, per 10 VAS, Electronic
SCMPOVAS50SNS1Y	Software annual fee, SecoManager, SCMPOVAS50SNS1Y, Firewall Security Policy Orchestration, 1 Year Subscription and Support, per 50 VAS, Electronic
SCMPOVAS100SNS1Y	Software annual fee, SecoManager, SCMPOVAS100SNS1Y, Firewall Security Policy Orchestration, 1 Year Subscription and Support, per 100 VAS, Electronic
SCMPOVAS500SNS1Y	Software annual fee, SecoManager, SCMPOVAS500SNS1Y, Firewall Security Policy Orchestration, 1 Year Subscription and Support, per 500 VAS, Electronic
SCMPOVAS1000SNS1Y	Software annual fee, SecoManager, SCMPOVAS1000SNS1, Firewall Security Policy Orchestration, 1 Year Subscription and Support, per 1000 VAS, Electronic
SCMPLFSNS02	Software annual fee, SecoManager, SCMPLFSNS02, SecoManager Software Platform, 3 Years Subscription and Support, Electronic
SCMDMSNS3Y	Software annual fee, SecoManager, SCMDMSNS3Y, Firewall Device Management, 3 Years Subscription and Support, per device, Electronic
SCMPOSNS3Y	Software annual fee, SecoManager, SCMPOSNS3Y, Firewall Security Policy Orchestration, 3 Years Subscription and Support, per device, Electronic
SCMDMVASSNS3Y	Software annual fee, SecoManager, SCMDMVASSNS3Y, Firewall Device Management, 3 Years Subscription and Support, per VAS, Electronic
SCMPOVAS5SNS3Y	Software annual fee, SecoManager, SCMPOVAS5SNS3Y, Firewall Security Policy Orchestration, 3 Years Subscription and Support, per 5 VAS, Electronic
SCMPOVAS10SNS3Y	Software annual fee, SecoManager, SCMPOVAS10SNS3Y, Firewall Security Policy Orchestration, 3 Years Subscription and Support, per 10 VAS, Electronic
SCMPOVAS50SNS3Y	Software annual fee, SecoManager, SCMPOVAS50SNS3Y, Firewall Security Policy Orchestration, 3 Years Subscription and Support, per 50 VAS, Electronic
SCMPOVAS100SNS3Y	Software annual fee, SecoManager, SCMPOVAS100SNS3Y, Firewall Security Policy Orchestration, 3 Years Subscription and Support, per 100 VAS, Electronic

BOM Number	Description
SCMPOVAS500SNS3Y	Software annual fee, SecoManager, SCMPOVAS500SNS3Y, Firewall Security Policy Orchestration, 3 Years Subscription and Support, per 500 VAS, Electronic
SCMPOVAS1000SNS3Y	Software annual fee, SecoManager, SCMPOVAS1000SNS3Y, Firewall Security Policy Orchestration, 3 Years Subscription and Support, per 1000 VAS, Electronic

Note: This product ordering list is for reference only. For product subscription, please consult Huawei representatives.

GENERAL DISCLAIMER

The information in this document may contain predictive statement including, without limitation, statements regarding the future financial and operating results, future product portfolios, new technologies, etc. There are a number of factors that could cause actual results and developments to differ materially from those expressed or implied in the predictive statements. Therefore, such information is provided for reference purpose only and constitutes neither an offer nor an acceptance. Huawei may change the information at any time without notice.