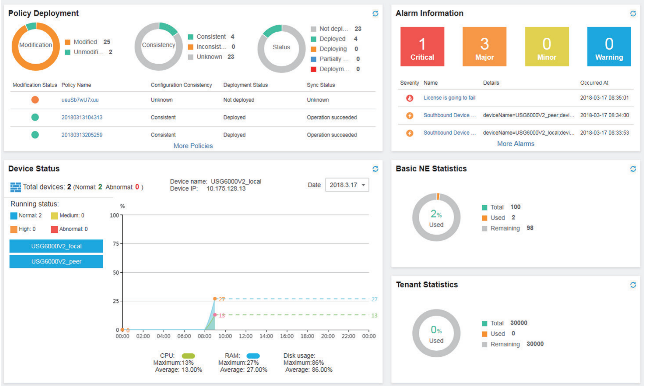
# Huawei SecoManager Security Controller



**Policy Deployment**

| | |
|---|---|
| 🟧 Modified | 25 |
| 🟩 Unmodifi... | 2 |

| | |
|---|---|
| 🟩 Consistent | 4 |
| 🟧 Inconsist... | 0 |
| ⬜ Unknown | 23 |

| | |
|---|---|
| ⬜ Not depl... | 23 |
| 🟩 Deployed | 4 |
| 🟧 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 Critical | 3 Major | 0 Minor | 0 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 |

## Product Overview

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 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.
- **Policy management based on service partitions:** Policy management transitions from the security zone-based perspective to the service partition-based perspective.
- **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.
- **Automatic security service deployment:** Diversified security services bring security assurance for enterprise 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.

### 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 policy approval items that need to be processed per day ranges from several to hundreds. After a policy is submitted to the SecoManager Security Controller, the SecoManager Security Controller checks the policy based on the defined compliance 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.
- **Policy redundancy analysis:** 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:** 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 to divert tenant traffic to corresponding security devices based on SFCs on demand.
- **Collaboration with security:** 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 controller are deployed on the same physical server and same VM.

HUAWEI

# Huawei SecoManager Security Controller

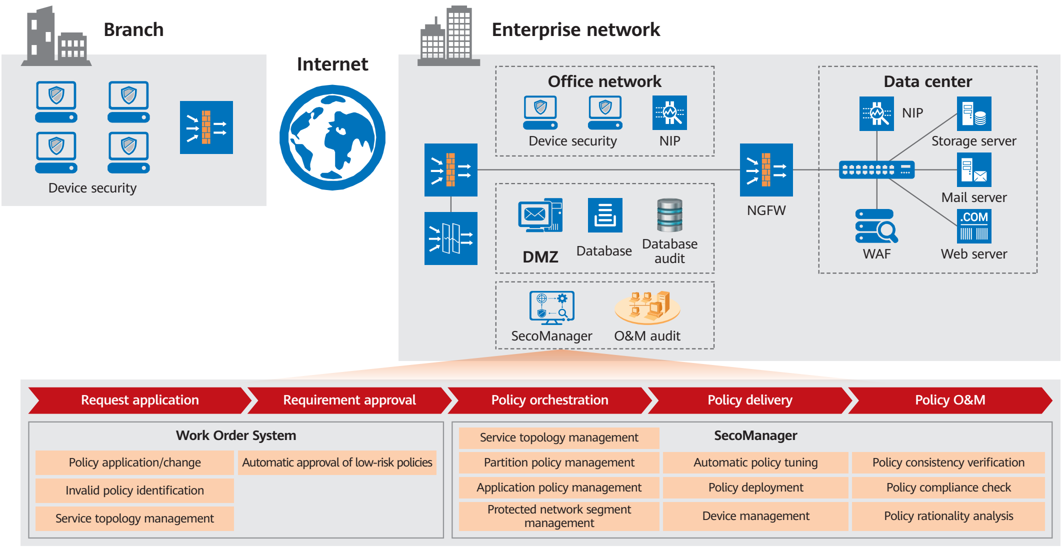
## Typical Applications

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

- 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.

- 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<br>• Memory: 64 GB<br>• Hard disk: 2 x 600G RAID1<br>• Network: 6 x GE | |
| ARM hardware requirements | • CPU: 2.6GHz, 2*32-core<br>• Memory: 128G<br>• Hard disk: 2 x 1200G RAID1<br>• Network: 4 x GE + 4 x 10GE | |
| Software requirements | Operating system:<br>• X86: Euler OS 2.0 SP5<br>• ARM: Euler OS 2.0 SP8<br>Virtualization software (If the SecoManager Security Controller is deployed on a VM, the virtualization software must be prepared.)<br>• FusionCompute KVM 6.5<br>• FusionSphere 6.3 | |

**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.

**Copyright © 2020 HUAWEI TECHNOLOGIES CO., LTD. All Rights Reserved.**