1.1 IDC (Internet DateCenter)Security

1.1.1 Overview

With the IT development, for example, as Web2.0, service oriented architecture (SOA), and cloud computing technologies are emerging and mobile devices, remote access devices, browsers, plug-ins of various applications, intelligent terminals, and cloud hosts come into being, information security faces new challenges. Attacks from the intranet and extranet and system vulnerability are major threats to information security. Based on IDC service characteristics, we must consider whether security technologies and products meet IDC security requirements, and how to use various software and hardware security products to construct an IDC security solution to meet various IDC service security requirements.

The IDC functioning as an information hub contains servers, storage devices, network devices, and applications. With the emergence of the cloud computing, new elements, such as virtualization, are added in the IDC. Therefore, the IDC security solution must be designed with consideration of all IDC elements. Using traditional security technologies only cannot ensure IDC security.

The Huawei IDC security architecture is designed based on the best practice in the industry and Huawei's expertise and experience. The security architecture is designed to meet service security, reliability, and data integrity requirements. The Huawei IDC security architecture supports the following features:

- Reliability

  Security devices and key components in security systems adopt high-reliability design. That is, dual-node hot backup is implemented to meet long-term running requirements of data center services.

- Modularization

  The Huawei IDC security architecture is designed based on eight modules: physical security, network security, host security, application security, virtualization security, user security, security management, and security services. A security architecture can be quickly formed based on customer requirements to provide a customized security system.

- E2E security

  The Huawei IDC security solution provides E2E protection from user access, use, and exit. Technologies such as the authentication technology based on dual factors, rights control technology for privileged users, VPN, application protection technology, and event auditing technology are used to control user access to IT resources, ensure data communication security and secure application access, and audit operations.

- Scalability

  The Huawei IDC security architecture is a guiding framework. Users can implement security construction based on the guiding framework and security requirements, which protects investment while meeting security requirements.

1.1.2 IDC Security Architecture

According to the ideas of layered and in-depth defense, the Huawei IDC security architecture is divided into physical device security, network security, host security, application security, virtualization security, data security, user management, and security management layers. The

IDC security architecture meets different security requirements. Figure 1-1 shows the IDC security architecture.

Figure 1-1 Security architecture

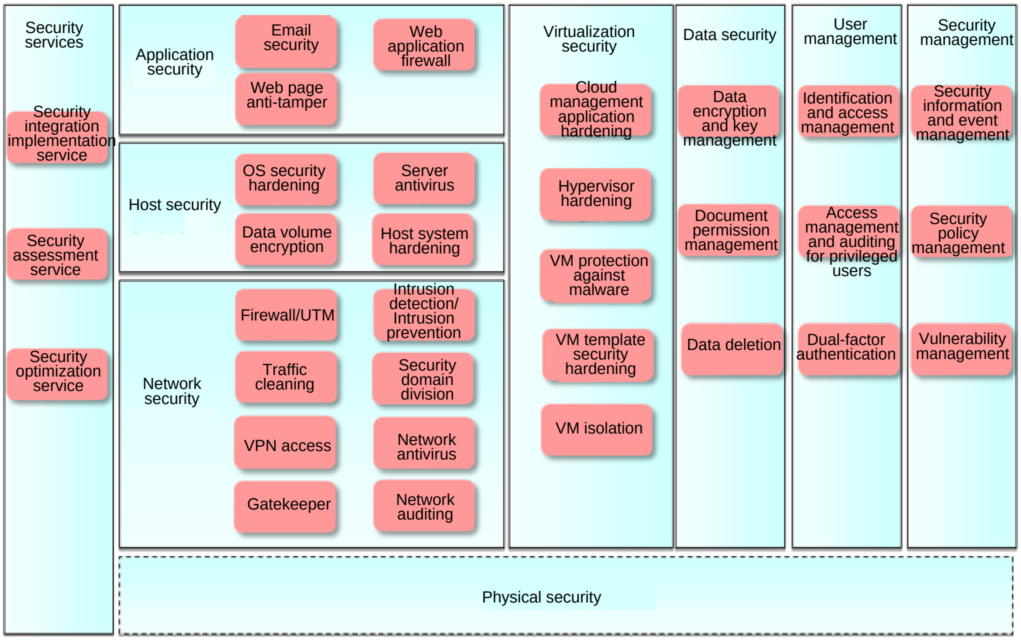
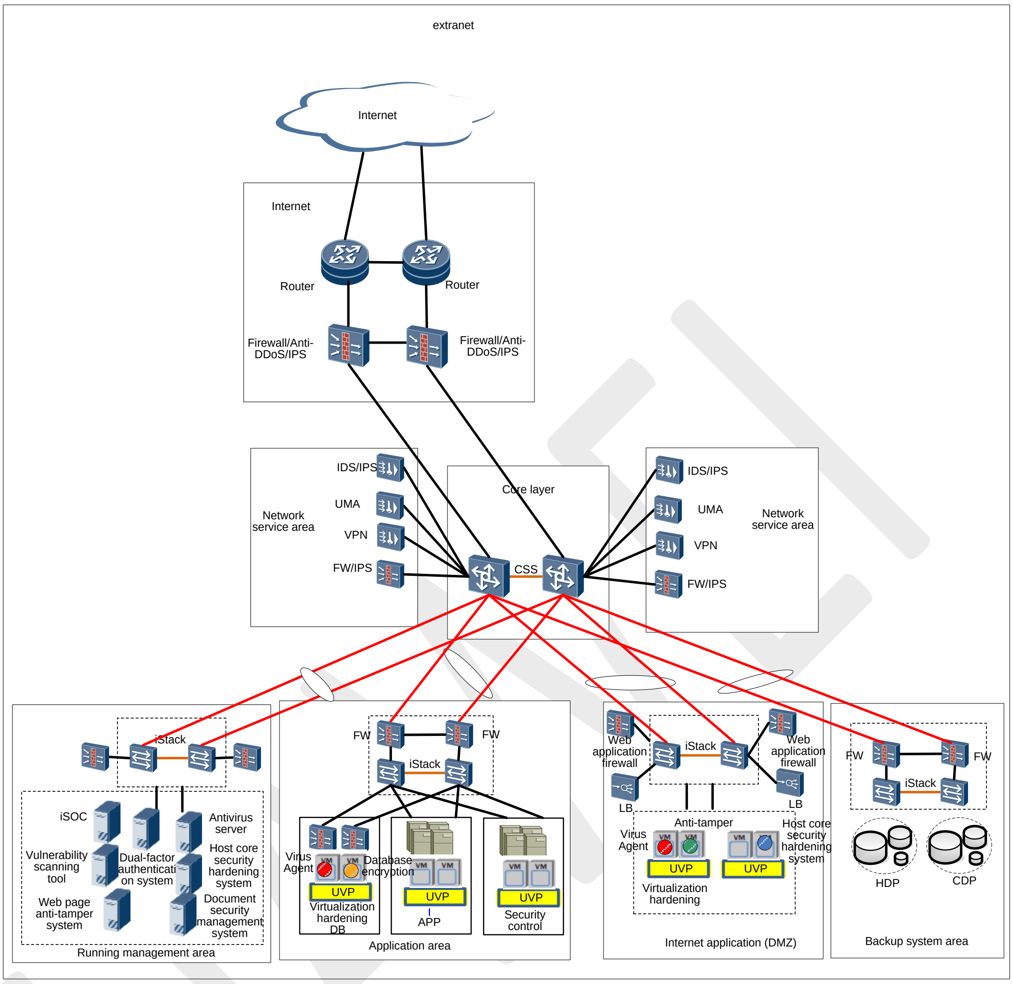

Security services
Security integration implementation service
Security assessment service
Security optimization service
Application security
Email security
Web application firewall
Web page anti-tamper
Host security
OS security hardening
Server antivirus
Data volume encryption
Host system hardening
Network security
Firewall/UTM
Intrusion detection/ Intrusion prevention
Traffic cleaning
Security domain division
VPN access
Network antivirus
Gatekeeper
Network auditing
Virtualization security
Cloud management application hardening
Hypervisor hardening
VM protection against malware
VM template security hardening
VM isolation
Data security
Data encryption and key management
Document permission management
Data deletion
User management
Identification and access management
Access management and auditing for privileged users
Dual-factor authentication
Security management
Security information and event management
Security policy management
Vulnerability management
Physical security

Figure 1-2 IDC security integration design



Different security components are deployed on different network areas based on component functions to ensure security.

- Firewalls and traffic cleaning devices are deployed on the network border.
- Antivirus software and host core security hardening system software are deployed on service hosts.
- Web application firewalls are deployed on the Internet application area.
- Service backup systems are deployed on the backup system area.

1.1.3 IDC Security Layer Design

Physical Security

The physical security is ensured by deploying the access control system, video surveillance system, and environment surveillance system. The access control system allows only the authorized personnel to enter the IDC. The video surveillance system and environment surveillance system facilitate subsequent auditing. In addition, the following aspects must be considered to further ensure physical security:

- Anti-theft and anti-sabotage

- Anti-lightning
- Fire prevention
- Waterproofing and moisture proof
- Electrostatic discharging
- Humidity control
- Power supply protection
- Electromagnetic shielding

Network Security

The firewall, IPS, SSL VPN, anti-DDoS, and data ferry technologies are used to protect systems and communication data. These technologies prevent data from being damaged, changed, or disclosed accidentally or intentionally. With these technologies, systems are reliable, secure, and able to run continuously without service interruption.

Host Security

Client antivirus protection, HIPS protection, HIDS protection, VM security hardening are used to prevent VMs from being threatened by intranet and extranet viruses, hackers, and security vulnerability. This ensures VM security and enables user services to run stably in the long term.

Application Security

Mail security protection and web application security protection are used to protect key applications, such as emails, web applications, and portal networks in the IDC, and prevent data from being damaged, changed, or disclosed accidentally or intentionally.

Virtualization Security

The virtualization layer and cloud management application layer are hardened, and VMs are isolated to prevent the virtualization environment from being threatened by viruses and hackers. Even if one VM is attacked, other VMs are not affected.

Data Security

The remaining data destruction mechanism ensures the security of the data stored in the storage of the cloud computing platform. User data stored on physical storage devices is deleted so that the user data is not disclosed when the storage devices are leased to other users. This helps dispel users' worries about data security of cloud services.

High-security encryption algorithms are used to encrypt data. This ensures data integrity and data security.

Distributed file systems are used in the storage system. Data is segmented and distributed on different cloud hard disks on storage nodes. Data cannot be restored by using a single hard disk. When a hard disk is faulty, the hard disk can be discarded without data deletion.

User Management

A unified O&M access control solution is provided to control and manage accounts, authentication, authorization, and auditing of IT resources (such as OSs of core services and network devices). The unified security control and management center collects operation logs to perform event association analysis and discover security risks in a timely manner. Logs and related analysis results provide evidence for information security events.

Security Management

Security management involves the technologies, methods, and products that support security policies and security management regulations. A unified security control and management center collects IDC security logs to perform association analysis and discover security risks in a timely manner. These security logs include firewall logs, intrusion detection logs, intrusion prevention logs, traffic cleaning logs, VPN access logs, junk mail gateway logs, Hypervisor logs, and auditing logs.

To protect services without interrupting services and affecting efficiency, obey the following rules to configure security policies for IDC network devices, security devices, and security software:

- Minimum authorization rule
- Service relativity rule
- Policy maximization rule
- Ensure that security policies are not exclusive with each other.

Security Service

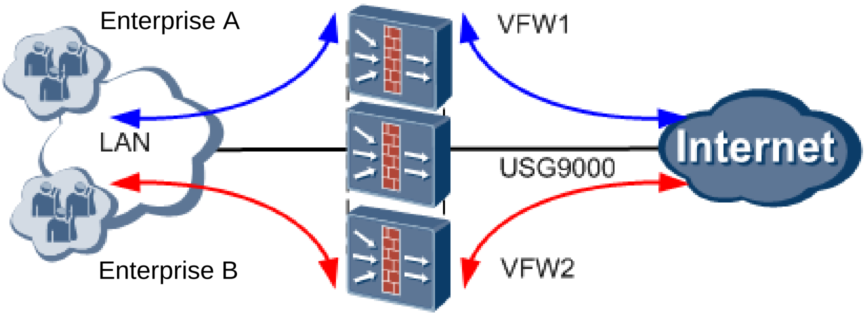
Security services not only include integration services, such as end-to-end IDC devices, software installation, and software configuration, but also include professional security assessment and optimization services. These services help users know about their existing and potential security threats and take measures in a timely manner.

1.1.4 IDC Security Features

VFW

A firewall is logically divided into multiple VFWs to provide independent security insurance for enterprises and maximize resource utilization of physical firewalls.

Figure 1-3 VFW



Each VFW is a complex of a VPN instance, security instance and configuration instance. It can provide private routing services, security services, and configuration management services for users.

- VPN instance

  The VPN instance provides isolated VPN routes that correspond to VFWs for VFW users. These VPN routes support routing for packets received by VFWs.

- Security instance

  The security instance provides isolated security services that correspond to VFWs for VFW users. These security instances consist of private interfaces, security areas, security domains, ACL, and NAT address pools and can provide private security services such as blacklists, package filtering, ASPF, and NAT.

- Configuration instance

  The configuration instance provides isolated configuration management services that correspond to VFWs for VFW users. These configuration instances allow VFW users to log in to their VFWs and manage and maintain preceding private VPN routers and security instances.

VM Isolation

VM isolation refers to the resource isolation of different VMs on the same physical machine. VM isolation is a basic feature of virtualization applications. VM isolation includes the isolation of CPUs, memory, internal networks, and disk I/O.

Account Management, Authentication and Authorization

The Huawei Operation and Maintenance Management (OMM) System supports account period management. A super administrator named admin is provided by default. Users can log in to the system as user **admin**, create other accounts, and assign rights to these accounts.

The OMM System supports role management and role-based authorization. The OMM System supports three types of roles: super administrator, O&M administrator, and guest. Different roles are assigned with different rights.

Tailoring and Hardening of the Cloud Platform OS

The Huawei cloud platform OS is tailored and hardened, and is implemented security configuration.

- OS tailoring

  This solution simplifies the cloud platform OS based on the rule of installing systems with minimum configurations. Only required components are installed. The quantity of OS software is substantially reduced. This lowers the possibility of systems from being attacked.

- Security configuration

  This solution implements the security settings for OSs on nodes by referring to the Center for Internet Security (CIS) Linux benchmark. For example, insecure services are disabled; account and password complexity policies, and permissions for files and directories are correctly configured.

- Security patch management

Huawei implements a strict process for managing security patches and regularly releases tested OS patch packages on the Huawei support website. O&M personnel regularly download and install OS patches.

Protection Against Malicious VMs

- Protection against address spoofing

  vSwitch (bridge) of the Hypervisor binds the IP address of each VM to the MAC address of the VM, so that each VM can send packets only using the local address. This prevents VM IP address spoofing and address resolution protocol (ARP) address spoofing.

- Protection against malicious sniffing

  The vSwitch is only for switching but not for sharing. When packets of different VMs are forwarded to the specified virtual port, a VM cannot receive packets of other VMs even on the same physical host. This prevents malicious sniffing.

1.2 Security Threats to Cloud Computing Systems

1.2.1 Traditional Security Threats

Traditional security threats are as follows:

- Security threats from external network include:
  - IP attacks

    The IP attacks include port scans, IP address spoofing, land attacks, Routing Information Protocol (RIP) routing attacks, source routing spoofing, IP fragment packet attacks, and teardrop attacks.
  - OS and software loopholes

    There are numerous security bugs on the software including third-party software, commercial software and free software. Hackers can control the OS of a computer to do what they want by exploiting programming defects or the contexts. Common OS and software loopholes include buffer overflow, abusing privilege operations, and downloading code without integrity verification.
  - Virus

    Virus includes Trojan horses and worms.
  - SQL injection

    Structured Query Language (SQL) injection is a technique often used to attack databases through a website. This is done by including portions of SQL statements in a web form entry field or query character strings of a page request in an attempt to get server to execute malicious SQL statements. The primary form of SQL injection consists of direct insertion of code into user-input variables that are concatenated with SQL commands and executed. A less direct attack injects malicious code into strings that are destined for storage in a table or as metadata. When the stored strings are subsequently concatenated into a dynamic SQL command, the malicious code is executed.
  - Phishing

    Phishing is the act of attempting to acquire information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity in an electronic communication. Communications purporting to be from popular social web sites, auction sites, online payment processors or IT administrators are commonly used to lure the unsuspecting public. Phishing is typically carried out by e-mail spoofing or instant messaging.

  - Zero-day attacks

    In the past, it usually takes several months for a software vulnerability to be discovered and exploited. Nowadays, the vulnerability will be exploited within 24 hours after it is discovered to implement attacks. These types of vulnerabilities are called zero-day vulnerabilities and these attacks are called zero-day attacks. It is difficult for original vendors to provide patches at the time when system loopholes are detected, because it takes time to check whether the loopholes exist, assess the risks of loopholes, find the methods to fix the loopholes, and verify, assess as well as inspect these methods found. The absence of a patch and users' prevention awareness for a zero-day vulnerability presents great threats to the system security. What's worse, the duration between a vulnerability is discovered and that is exploited is shortened, facilitating the generation of zero-hour attacks.

- Security threats from intranet include:
  - Ever-changing attacks pose difficulties for prevention

    Address Resolution Protocol (ARP) spoofing and malicious plug-ins are the new security threats. The hosts in an intranet are attacked and become zombie hosts inserted with Trojan or malicious programs. The zombie hosts are used to attack other devices in the intranet to steal commercial secrets or used to implement DDoS attacks to consume large network bandwidth. If employees browse web pages inserted with Trojan or virus, or open emails with malicious codes, attackers can take these opportunities to implement attacks.

  - Worms and viruses are spread through loopholes if patches and virus database are not upgraded to the latest version, causing tremendous security threats.

    If the latest patches are not installed to fix security loopholes or bugs in platforms or devices within a network and the virus databases are not upgraded to the latest version or do not contain the new virus, attackers may take advantages of these vulnerabilities to spread viruses and worms. Large number of worms may paralyze the intranet of an enterprise, interrupting all services.

  - Confidential information disclosure happens frequently because of unauthorized Internet access activities.

    Employees access the Internet directly using the Asymmetric Digital Subscriber Line (ADSL), virtual private network (VPN) or general packet radio service (GPRS) without passing through the firewall, which leads to the exposure of IT resources to attackers and viruses. In addition, employees can also disclose commercial secrets through the Internet without being monitored, bringing economic losses for enterprises.

  - Convenient mobile device access challenges intranet security.

    The notebook computers, pocket PCs, and other mobile devices of employees or temporary visitors are used in various network environments. If these devices access the intranet without being scanned, they may bring viruses and Trojan into the intranet and threaten the network security.

  - Device abuse threatens asset security.

    CPUs, memory modules and hard disks can be freely replaced but cannot be traced. Employees can change IP addresses of their office computers, causing trouble for implementing unified management and for identifying trouble-makers once attack action and security incidents occur.

  - Network applications spread viruses.

The instant messaging tools such as Tencent QQ, MSN messenger and ICQ messenger have become the latest agents to spread viruses. The downloading tools such as BitTorrent and eMule are commonly used to download files such as movies, games, and software so that the network bandwidth of important service application systems cannot be guaranteed.

- Data leakage and virus spreading occurs due to the lack of peripheral management.

  Peripherals such as the USB flash drive, CD-ROM drive, printer, Infrared Data Association (IrDA), and serial and parallel ports are widely used for data exchange and also become important ways of data disclosure and virus spreading. The peripherals, especially the USB flash drives cannot be managed flexibly by sealing the ports or introducing regulations. Therefore, technical measures must be implemented to manage and control the peripherals.

- Security regulations cannot be put into practice.

  The existing security regulations cannot eliminate security incidents. The management mechanisms, such as sealing ports and periodic inspection cannot ensure the implementation of the regulations as they lack effective assurance measures.

1.2.2 Security Threats of Cloud Computing

The utilization and management modes of computing resources in the cloud computing system bring new risks and threats for both operators and end users.

Risks and threats for operators include:

- The virtualization management layer becomes the new high-risk area.

  The cloud computing system provides computing resources for large number of users using the virtualization technology. Therefore, the virtualization management layer becomes the new high-risk area.

- It is difficult to track and isolate malicious users.

  The on-demand and self-service allocation of resources makes it much easier for malicious users to launch attacks in the cloud computing system.

- Open interfaces make the cloud computing system vulnerable to external attacks.

  Users use open interfaces to access the cloud computing system through networks, which makes the system vulnerable to attacks from external networks.

Risks and threats for end users include:

- Risks cannot be controlled as data are stored in the cloud.

  All risks brought by computing resources and data are controlled and managed by cloud computing service providers. These risks are as follows: Operator administrators may invade the user system illegally. Data security after the computing resource or storage space is released. No laws and regulations can be used for data processing.

- Multi-tenant resource sharing causes data leakage and attacks.

  Resource sharing among multiple tenants poses the following security risks: User data may leak out because of inappropriate isolation methods. Users may be attacked by other users within the same physical environment.

- Open network interfaces cause security risks.

  In the cloud computing environment, users operate and manage computing resources through the Internet. The openness of network interfaces brings more security risks.

1.3 Security Advantages

The security advantages include:

- The cloud computer provides comprehensive and unified security management for computing resources.

  The centralized management of computing resources makes it easier to deploy boundary protection. Comprehensive security management measures, such as security policies, unified data management, security patch management, and unexpected event management, can be taken to manage computing resources. In addition, professional security expert teams can protect resources and data for users.

- Security costs are low.

  Because security measures are taken for all computing resources shared among many users, security costs per user are low.

- Security protection is provided efficiently.

  Able to allocate resources fast and elastically, the cloud computing system can efficiently provide security protection for processes, such as filtering, traffic shaping, encryption, and authentication.

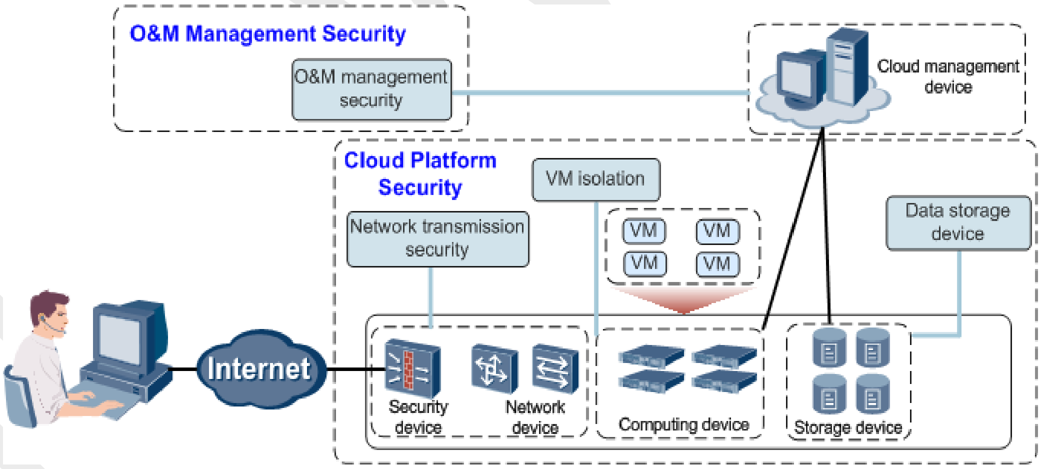
2 FusionSphere Security Solution

2.1 Solution Structure

Huawei provides the virtualization platform security solution to face the threats and challenges posed to the cloud computing system.

Figure 2-1 shows the structure of the virtualization platform security solution.

Figure 2-1 Structure of the virtualization platform security solution



Each layer of the security structure is described as follows:

- Cloud Platform Security
  - Data storage security

    The integrity and confidentiality of user data are ensured using user data isolation, data access control, residual information protection, VM disk encryption, and data backup.
  - VM isolation security

    VMs running on the same physical machine are isolated to prevent data theft and malicious attacks. Users can only use VMs to access resources belonging to their own VMs, such as hardware and software resources and data.

- Network transmission security

  Network plane isolation, firewalls, and data transfer encryption are used to ensure the security of service operation and maintenance.

- Operating and Management (O&M) Security

  Security is ensured from aspects of user accounts, passwords, user permissions, logs, and data transmission.

In addition, the security of each physical host is ensured by repairing web application loopholes, hardening the system and database, and installing patches and antivirus software.

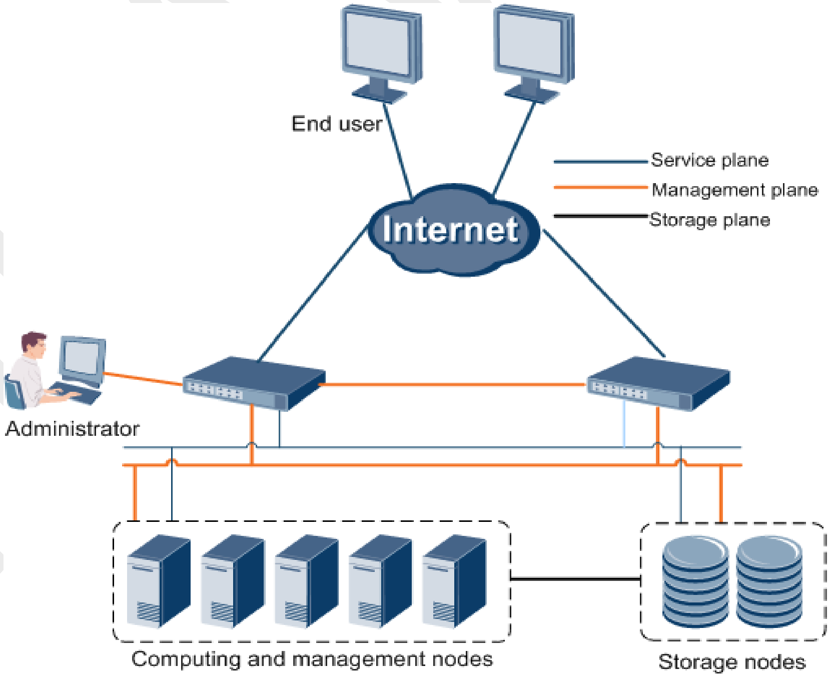
2.2 Network Security

2.2.1 Network Plane Isolation

The FusionSphere solution provides three network communication planes: the service plane, storage plane, and management plane. These planes are isolated from each other so that users cannot damage basic platforms and administrators cannot access the service plane.

Figure 2-2 shows the plane isolation provided by the FusionSphere solution.

Figure 2-2 Plane isolation provided by the FusionSphere solution



- Service plane

  The service plane provides service channels for users and works as the communication plane of the virtual network interface cards (NICs) of VMs to provide services.

- Storage plane

  The storage plane works as the communication plane for storage over the Internet Small Computer Systems Interface (iSCSI) storage devices and provides storage resources for VMs. The storage plane communicates with VMs over the virtualization platform.

- Management plane

  The management plane works as the communication plane for cloud computing system management, service deployment, and system loading.

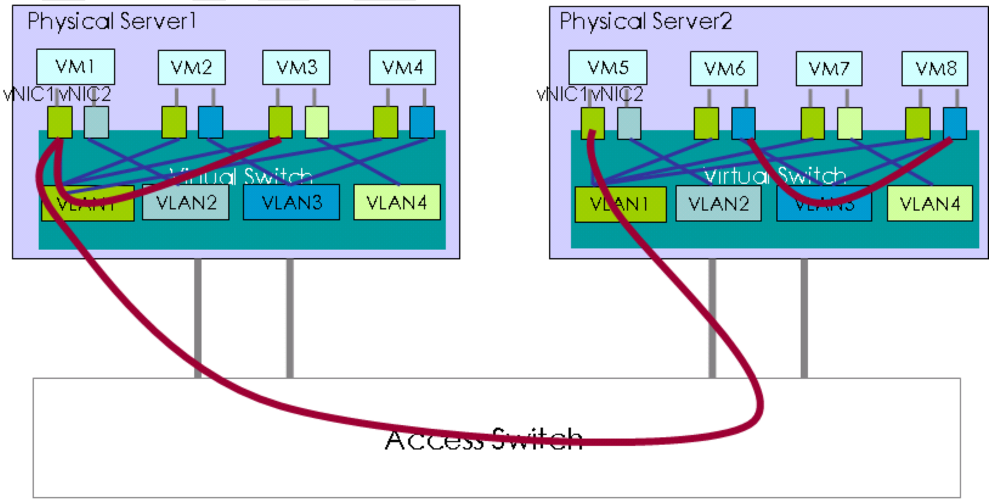
2.2.2 VLAN Isolation

This function enables a virtual network bridge to serve as a virtual switch, that is, to provide the virtual LAN (VLAN) tagging function to isolate VLANs for VM security.

A virtual bridge connects all VMs running on the same physical server. The front-end interface refers to VM NICs such as eth0 and eth1. The back-end interface is the vif that connects to a virtual bridge. In this way, the uplink and downlink traffic of a VM is forwarded by the virtual bridge. The virtual bridge forwards packets based on the mapping between the MAC address and vif interface.

The virtual bridge supports the VLAN tagging function. VMs of a security group running on different hosts tag data frames. Switches and routers in the network forward and route the frames based on the VLAN tag, and thereby isolating the virtual network.

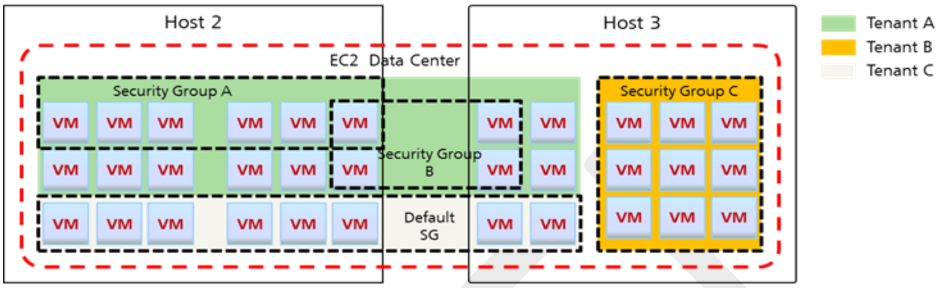
Figure 2-3 VLAN networking



As shown in Figure 2-3, the VMs distributed on different physical servers can be deployed on the same LAN using the VLAN technology. The VMs on a VLAN of a server communicate with each other through the virtual switch; while the VMs on a VLAN of different servers communicate with each other through the physical switch, ensuring that the VMs of different LANs are isolated and cannot exchange data.

2.2.3 Security Group

Figure 2-4 Security group



Users can create security groups based on VM security requirements. Each security group provides a set of access rules. VMs that are added to a security group are protected by the access rules of the security group. Users can add VMs to security groups when creating VMs.

VMs in the same security group can be distributed on different physical servers. The VMs in a security group can communicate with each other, while those in different security groups are not allowed to communicate with each other. However, the VMs in different security groups, when configured, can also communicate with each other.

2.2.4 IP-MAC Address Spoofing Prevention

IP-MAC address binding prevents IP address or MAC address spoofing initiated by changing the IP address or MAC address of a vNIC, thereby enhancing network security of user VMs. With this feature enabled, an IP address is bound to an MAC address using the DHCP snooping feature, and then the packets from untrusted sources are filtered using IP Source Guard and dynamic ARP inspection (DAI).

2.2.5 DHCP Quarantine

DHCP quarantine blocks users from unintentionally or maliciously enabling the DHCP server service for a VM, ensuring common VM IP address assignment.

2.2.6 Broadcast Packet Suppression

In the FusionSphere and FusionCloud scenarios, the broadcast packet suppression function is enabled for distributed virtual switches (DVSs) so that network exceptions due to broadcast packet attacks, such as network attacks or virus attacks, can be prevented.

A DVS provides the suppression function for ARP broadcast packets and IP broadcast packets at the VM sending direction and also provides the suppression threshold setting function. You can enable the broadcast packet suppression function for the port group to which vNICs belong to set the suppression threshold, reducing the consumption of layer 2 network bandwidth by excessive broadcast packets.

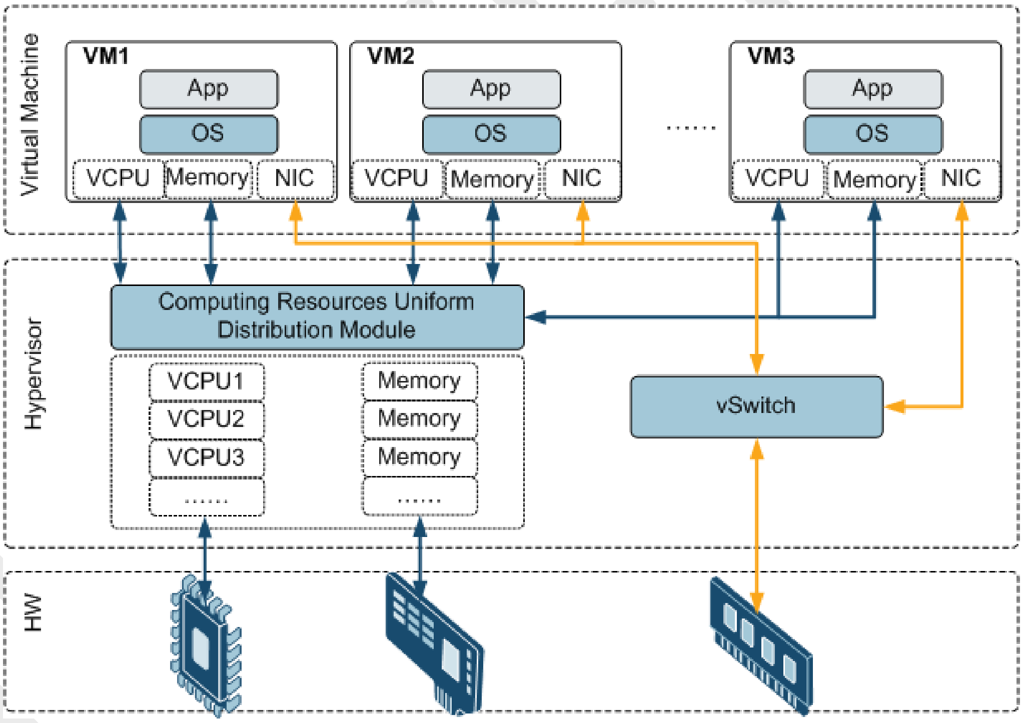
Administrators can configure the broadcast packet suppression function and set the ARP broadcast packet suppression threshold and IP broadcast packet suppression threshold for DVS port group objects on the system portal.

2.3 Virtualization Security

The hypervisor isolates VMs running on the same physical machine to prevent data theft and malicious attacks. Users can only use VMs to access resources belonging to their own VMs, such as hardware and software resources and data.

Figure 2-5 shows VM isolation.

Figure 2-5 VM isolation



2.3.2 vCPU Scheduling Isolation

Huawei cloud computing platform uses x86 architecture servers. The x86 architecture offers 4 privilege levels ranging from ring 0 which is the most privileged, to ring 3 which is the least privileged. OS core runs in ring 0. OS services run in ring 2, and user applications run in ring 3. The Hypervisor schedules instructions to be executed and manages resources to prevent conflicts from occurring. The Hypervisor prevents the Guest OS of VMs from executing all the privileged instructions and isolates the OS from applications.

2.3.3 Virtual Memory Isolation

The VM uses the Memory Virtualization technology to virtualize the physical memory and isolate the virtual memory. This technology introduces a new address concept, physical address, based on the existing mapping between virtual addresses and the machine addresses of clients. The OS on a VM translates the virtual address into the physical address. The Hypervisor first translates the physical address of a client into a machine address, and then sends the machine address to the physical server.

2.3.4 Internal Network Isolation

The Hypervisor provides the abstraction of Virtual Firewall-Router (VFR). Each guest VM has one or more virtual interfaces (VIFs) logically associated with the VFR. Data packets sent from a VM first reach domain 0. Domain 0 filters the data packets, checks the integrity of the data packets, adds or deletes rules, includes certificates, and sends the data packets to the destination VM. Then the destination VM checks the certificates to determine whether to accept the data packets.

2.3.5 Disk I/O Isolation

The Hypervisor intercepts and processes all input/output operations of a VM to ensure that a VM only visits the allocated hard disks.

2.3.6 DHCP Quarantine

The FusionSphere security solution provides the Dynamic Host Configuration Protocol (DHCP) quarantine function for VMs. If the DHCP software is installed on a VM, the VM assigns IP addresses to other VMs, thereby affecting the proper running of other VMs. However, enabling the DHCP quarantine function for the port group can prevent this problem from occurring.

2.4 Data Security

2.4.1 User Data Isolation

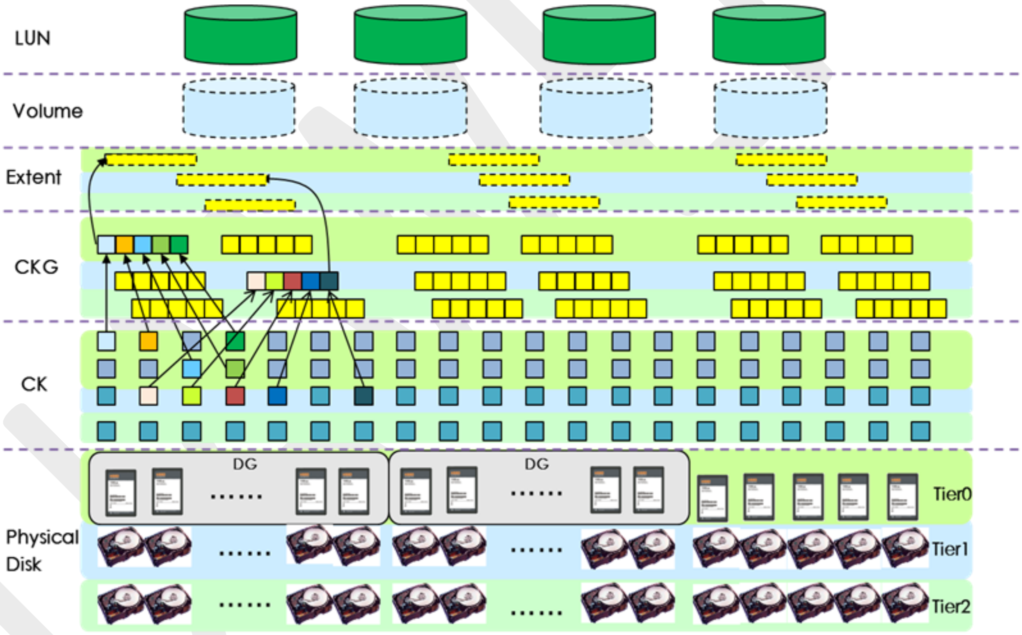
Huawei unified virtualization platform (UVP) implements the virtualization of I/O by dividing the device drive model into three parts: front-end driver, back-end driver and native driver. The latter two run in Domain 0 while the front-end driver runs in Domain U. The front-end driver transfers I/O requests from Domain U to the back-end driver in Domain 0. The back-end driver parses the requests, maps them to the physical devices, and sends them to the corresponding device driver to control hardware I/O operations. In short, VMM intercepts and processes all I/O activities. It ensures that the VMs only access the appointed space, thereby implementing the hard disk isolation of multiple VMs.

2.4.2 Data Access Control

Volume storage: In the FusionSphere, access to each volume is controlled. Only users have the access permission can access a volume, and different volumes are isolated from each other.

2.4.3 Residual Information Protection

With the Redundant Array of Independent Disks (RAID) technology applied to data storage, the system divides the storage pool into multiple small data blocks and constructs a RAID group using these data blocks. This enables data to be evenly distributed on all the hard disks in the storage pool, and resource management is implemented on a data block basis. The size of a data block is adjustable and ranges from 256 KB to 64 MB. Its default value is 4 MB.



When a VM or a data volume is deleted, the system reclaims resources, and a linked list of small data blocks is released to the resource pool. These small data blocks are reorganized for storage resources reuse. In this way, the possibility of restoring original data from the reallocated virtual disks is low.

In high security scenario, when the system reclaims resources, it allows the physical bits of logical volumes to be formatted to ensure data security. In scenario where the security requirements are not high, the system allows the first 10 MB of logical volumes to be formatted by default.

After the physical disks of the data center are replaced, the system administrator of the data center degausses them or physically destroys them to prevent data leakage.

2.4.4 Data Backup

In the FusionSphere solution, one or more copies of backup data are stored so that data is not lost and services are not affected even if storage devices such as hard disks become faulty.

The system performs a bit- or byte-based verification on data stored in disks, and distributes verification information to each disk in a disk array. During the distribution, the system makes sure that a data block and its verification information are stored on different disks. In this way, damaged data can be reconstructed based on other data blocks and corresponding verification information after a disk is damaged.

2.5 Access Security

In cloud computing environment, users usually access their computing and storage resources through network. To prevent malicious users from accessing the resources illegally, Huawei cloud computing system adopts powerful measures for user access, authentication, and authorization to ensure that only authenticated and authorized users can access the computing and storage resources in the cloud computing system. In this way, damages to the cloud computing system from malicious terminals or users can be minimized.

2.6 O&M Management Security

Security threats in O&M management include:

- Fine-grained control of administrator rights is not supported.
- Weak passwords are used and are not changed for a long time, leading to password theft.
- Malicious activities of administrators cannot be monitored and reviewed.

2.6.1 Rights- and Domain-Based Management for Administrators

Administrators log in to portals to manage the cloud system, including viewing resources and allocating VMs.

The system supports the access control of portal users. Functions such as rights- and domain-based management are provided to ensure the orderly maintenance of the system.

2.6.2 Account and Password Security

The system supports password policies to protect administrator's passwords. For example, the password policies can specify the minimum password length, password validity period, and whether special characters are allowed.

Passwords are stored in ciphertext.

2.6.3 Log Management

Logs managed by the FusionSphere are as follows:

- Operation logs

  Operation logs recording the operations performed by the O&M engineers contain information sufficient for audit purposes. The logs contain operator name, operation type, client IP address, operation time, and operation result to locate malicious operations in a timely manner. Operation logs can also serve as non-repudiation evidence.

- Process Logs

  Process logs record the running status of each node. The system can be controlled to generate logs only of a certain level.

  Process logs consist of log level, thread name, and log information. O&M engineers understand and analyze the running status of the system by viewing the process logs to detect and handle abnormalities.

- Black box logs

  Black box logs record location information about serious system faults and are used to locate and handle severe system faults. Black box logs generated on computing nodes are exported to specified directories on the log server. Black box logs generated on management nodes and storage nodes are stored in local directories.

2.6.4 Transmission Encryption

Administrators access management systems using Hypertext Transfer Protocol Secure (HTTPS), and data transfer channels are encrypted using secure socket layer (SSL).

2.6.5 Database Backup

To ensure data security, databases must be backed up periodically to prevent loss of important data. The LDAP and PostgreSQL databases support the following backup modes:

- Local backup: Backup scripts are executed at scheduled time every day to back up data.
- Remote backup: Data is backed up to a third-party server.

2.7 Infrastructure Security

Infrastructure security refers to the security of the devices and nodes in the FusionSphere, as well as the security of the OSs and databases of FusionSphere components. Common software such as the OS and database (DB) in the cloud computing environment is vulnerable to virus attacks, hacker attacks, Trojan virus, and DoS. Therefore, system operation may be affected. Infrastructure security is the basis to ensure the proper running of the system and secure network building and application security.

2.7.1 OS Hardening

In the FusionSphere solution, computing nodes and management nodes use the SUSE Linux OS. To ensure their security, basic security configurations are required. The basic security configurations are as follows:

- Stop unnecessary or risky processes and services, such as email agent service, graphics desktop, and Telnet service.
- Harden the secrete shell (SSH) and Xinetd services.
- Modify kernel parameters to enhance OS security by disabling IP forwarding, system responses to broadcast requests, and Internet Control Message Protocol (ICMP) redirection receiving and forwarding functions.
- Control access permission on files and directories.
- Enhance account and password security by enabling password complexity check and configuring password validity and number of unsuccessful login attempts.
- Restrict system access permission.
- Record and audit process logs.

2.7.2 Web Security

These Web service platforms provide the following security functions:

- Automatically redirects users' access requests to Hypertext Transfer Protocol Secure (HTTPS) links.

  The web service platform automatically redirect users' access request to HTTPS links. When users access a web service platform using HTTP, the web service platform automatically redirects the users' access requests to HTTPS links to enhance access security.
- Prevents cross-site scripting.

  Cross-site scripting is a type of computer vulnerability typically found in web applications, which enables attackers to inject client-side scripts into web pages viewed by other users.
- Prevents SQL injection.

  SQL injection is done by including portions of SQL statements in a web form entry field in an attempt to get the website to pass a newly formed rogue SQL command.
- Prevents cross-site request forgery.

  Cross-site request forgery is a type of malicious exploit of a website whereby unauthorized commands are transmitted from a user that the website trusts. For example, a user logs in to website A and concurrently logs in to website B that contains attack programs, before the session times out. In this case, attackers can obtain the session ID of website A and then log in to website A to intercept private information.
- Protects sensitive information.

  The web service platform can protect sensitive information from being obtained by attackers.
- Restricts file upload and download.

The web service platform can restrict file uploading or downloading to prevent high-security files and insecure files from being uploaded or downloaded.

- Prevents uniform resource locator (URL) from overriding.

  Certain rights are granted to each type of users to prevent users from performing unauthorized operations on systems.
- A graphic verification code is used on the login page.

  On the login page of each web service platform, the system generates verification code randomly. Users can log in to the system only when the username, password, and verification code entered are all entered correctly.
- Account password security

  The Web account and password meet system account and password security rules.

2.7.3 Database Hardening

In the FusionSphere solution, databases have the following types:

- Lightweight Directory Access Protocol (LDAP) database
- PostgreSQL database

Basic security configurations are required for databases to ensure their secure operation. The security configurations for each type of database are as follows:

- LDAP database
  - Accounts and passwords are encrypted before being stored.
  - Security parameters of the LDAP database are configured to impose a connection timeout limit and prohibit anonymous access.
  - Logs recording operations performed on the LDAP database are kept.
- PostgreSQL database
  - Strong passwords are required.
  - Logs recording operations performed on the PostgreSQL database are kept.

2.7.4 Security Patch

Software design defects may cause many system loopholes. System security patches can eliminate system loopholes and prevent viruses, worms, and hackers from using these loopholes to attack the system. The FusionSphere solution provides the following security patches:

- Virtualization platform security patches

  A patch server is deployed on the management node of the virtualization platform to automatically install patches and perform tests.
- User VM security patches

  The FusionSphere solution does not provide any additional security patch for user VMs. You are advised to obtain OS security patches from the official OS website and install patches for user VMs.

2.7.5 Antivirus Software(additional license and services required)

Antivirus software is deployed on management nodes or VMs to protect components of the FusionSphere from being attacked.

- Management node

  The management node runs the reinforced Linux OS. Therefore, the virus infection risk is under control, although the management node provides an O&M portal to interact externally. It is still recommended that you deploy antivirus software on the management nodes.

  You can deploy antivirus software which is compatible with SUSE Linux 11.

NOTE

1. A compatibility test must be performed for the antivirus software before being deployed on a management node.

2. Management nodes are the nodes where the FusionManager and Virtualization Resource Management are located.

3. You are not advised to install any antivirus software on a computing node, such as the Computing Node Agent, because the tailored and hardened Linux OS running on a computing node can effectively reduce virus infection.

- User VM

  The antivirus software products Symantec SEP12.0 and McAfee Move2.5 are the best choice for Huawei virtualization platform. The deployment of these two antivirus software products for user VMs contributes to improving virus scan efficiency, reducing resource occupation by virus scan operation, and increasing VM density, thereby protecting user VMs from virus attacks.