Guideline on Effectively Managing Security Service in the Cloud

CSA cloud security alliance®

Acknowledgements

Initiative Lead

Kai Chen

Key Contributors

Renato Jose Delatorre
Zhenyu Wang
Xinmei Shi
Zhiliang Zhang
Yixin Jin
Bin Luo
Heng Liang
Theo Dimitrakos
Sabri Khemissa
Vani Murthy
Andrea Knoblauch
Atul Bahl
Diego Fernandez

CSA Staff

Hing-Yan Lee
Haojie Zhuang
Victor Chin
Courtney Keogh
Jane Chow

Abstract

Based on the shared security responsibility model, specific security responsibilities are divided between the cloud service provider and cloud customer in different cloud service deployment environments (e.g. IaaS, PaaS, and SaaS) and, where applicable, cloud security service providers offering Security-as-a-Service (SecaaS) for cloud platforms. For each security responsibility there are one or more security features or functions defined to support it. This document provides guidance on how to fulfill cloud controls (based on CCM) by using third-party security products and services. Appendix A provides a case study using examples of commercially available security products and services (no vendor will be referred) to illustrate exemplary cases of supporting those security features in practice.

1 Summary

1.1 Background of This Document

The shared security responsibility model is well recognized. Every leading cloud service provider (CSP) has published whitepapers or statements on shared security responsibility, explaining their roles and responsibilities in cloud provisioning. The reality is that, given the same concept of shared responsibility, there are different interpretations and different implementations among different CSPs. There are many cloud security standards and/or specifications developed for CSPs in fulfilling their security responsibilities, but for the cloud customer it is still difficult to design, deploy, and operate a secure cloud service. This document provides easy-to-understand guidance to cloud customers on how to design, deploy, and operate a secure cloud service with respect to different cloud service models. There are some standards and best practices[1,2,3] providing useful guidance to cloud customers from different aspects and these are helpful references.

1.2 How to Use This Document

This document provides guidance for organizations that intend to use cloud services before they plan to build their service systems on the cloud or to move existing systems to the cloud. This guidance can help these organizations ensure the secure running of service systems and help them clearly understand security responsibilities of their own and of CSPs, what security assurance features should be provided to bear these security responsibilities, existing gaps, and how to develop related capabilities to address these gaps. This document can also provide guidance for CSPs building cloud platform security assurance systems and can be used by cloud service security integrators or by cloud customers.

This document applies to private cloud, public cloud, hybrid cloud, and community cloud.

1.3 Glossary

CSP: Cloud Service Provider
O&M: Operations and Maintenance

[1] Cloud Customer Architecture for Securing Workloads on Cloud Services, **https://www.omg.org/cloud/deliverables/CSCC-Cloud-Customer-Architecture-for-Securing-Workloads-on-Cloud-Services.pdf**.

[2] Cloud Computing Security for Tenants, **https://acsc.gov.au/publications/protect/Cloud_Computing_Security_for_Tenants.pdf**.

[3] ISO/IEC 27018:2014 — Information technology — Security techniques —Code of practice for protection of Personally Identifiable Information (PII) in public clouds acting as PII processors.

2 Security Role and Responsibility of CSPs, Security Service Providers, and Cloud Customers

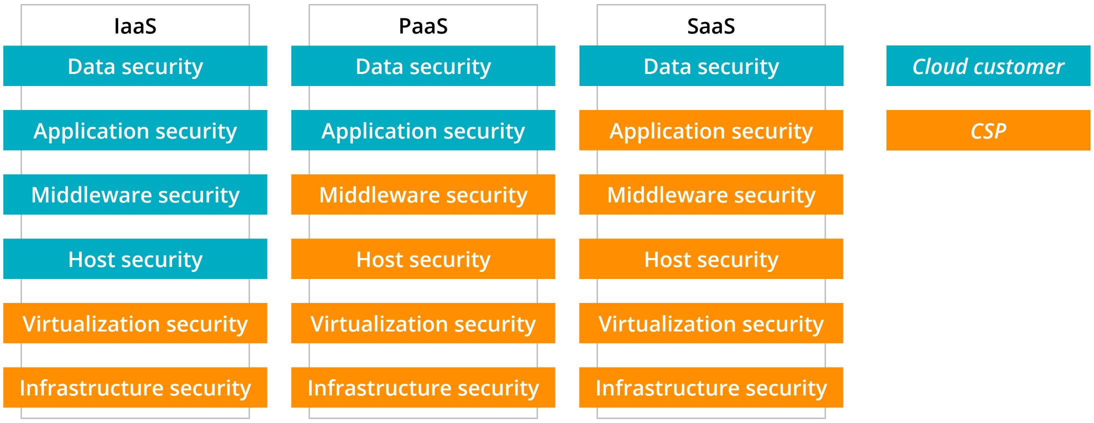
2.1 Shared Security Responsibility Model

It is well recognized that security in the cloud is a shared responsibility between CSPs and customers. Understanding the shared responsibility model requires understanding the three different tiers of cloud computing, and many organizations use a mix of these services as they build their cloud computing strategies. The three tiers of cloud computing are Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). In each of these environments, the security responsibility division between vendors and customers differs significantly.

The leading CSPs have published white papers to explain their shared security responsibility models, such as Microsoft Azure,[4] Amazon AWS,[5] and Huawei.[6]

Here, we refer to Gartner's shared security responsibility model[7] to develop the below shared security responsibility figure. It illustrates the security handoff points for IaaS, PaaS, and SaaS cloud models. The handoff point moves up the stack across the models. The IaaS CSP offers the most control, with the commensurate security responsibility left to customers. The SaaS customer offers the least control, with the CSP taking on most of the security responsibility.

Figure 2-1 Security responsibility division between CSPs and cloud customers in different cloud service modes



IaaS	PaaS	SaaS
Data security	Data security	Data security
Application security	Application security	Application security
Middleware security	Middleware security	Middleware security
Host security	Host security	Host security
Virtualization security	Virtualization security	Virtualization security
Infrastructure security	Infrastructure security	Infrastructure security

[4] Shared Responsibilities for Cloud Computing, Microsoft Azure, **https://gallery.technet.microsoft.com/Shared-Responsibilities-81d0ff91**.

[5] AWS Shared Responsibility Model, **https://aws.amazon.com/compliance/shared-responsibility-model**.

[6] Huawei Cloud Security Whitepaper, **https://static.huaweicloud.com/upload/files/pdf/20171123/20171123171541_66845.pdf**.

[7] Staying Secure in the Cloud Is a Shared Responsibility, Gartner, **https://www.gartner.com/doc/3277620/staying-secure-cloud-shared-responsibility**.

2.2 Common Security Responsibilities of CSPs and Cloud Customers

Some security responsibilities of CSPs and cloud customers are common for all cloud service models. In order to make it straightforward, they are listed here and will not be repeated in each service model.

2.2.1 CSPs' Common Security Responsibilities

- Physical security of the infrastructure, including but not limited to: equipment room location selection; power supply assurance; cooling facilities; protection against fire, water, shock, and theft; and surveillance (for details about the security requirements, see related standards)
- Security of computing, storage, and network hardware
- Security of basic networks, such as anti-distributed denial of service (Anti-DDoS) and firewalls
- Cloud storage security, such as backup and recovery
- Security of cloud infrastructure virtualization, such as tenant resource isolation and virtualization resource management
- Tenant identity management and access control
- Secure access to cloud resources by tenant
- Security management, operating monitoring, and emergency response of infrastructure
- Formulating and rehearsing service continuity assurance plans and disaster recovery plans for infrastructure

2.2.2 Cloud Customers' Common Security Responsibilities

- User identity management and access control of service systems
- Data security (in European GDPR mode, cloud customers control the data and should be responsible for data security while CSPs only process the data and should take security responsibilities granted by data controllers)
- Security management and control of terminals that access cloud services, including hardware, software, application systems, and device rights

2.3 IaaS

For the IaaS deployment model, a cloud customer leases computing, storage, and network infrastructure from a CSP to build its own service systems. Therefore, the customer takes most of system security responsibilities. The CSP is responsible for the security of infrastructure and basic resources in cloud data centers.

2.3.1 CSP's Security Responsibilities

The CSP should take the common security responsibilities defined in section 2.2.1.

2.3.2 Cloud Customer's Security Responsibilities

The cloud customer should take the following security responsibilities in addition to those common ones in section 2.2.2:

- The security assurance capability of the infrastructure provided by a CSP—the cloud customer can check the service description and security responsibility commitment of the CSP or ask the CSP to provide a security certificate issued by a third party, and, if necessary, the customer can check the CSP's security assurance capabilities on site
- Security of the data transfer
- Security of virtual networks
- Security of the platform layer, such as the security of operating systems (OSs) and databases
- Security of application systems
- Security configuration, security management, and monitoring of system resources
- Formulation and rehearsal of business continuity assurance plans and disaster recovery plans
- Security configuration, management, operating monitoring, and emergency response of infrastructure

2.4 PaaS

For the PaaS deployment model, a CSP provides a cloud customer with computing, storage, and network infrastructure as well as platform services such as OSs and databases to support the customer in developing and deploying service application systems. Their security responsibilities are described as follows.

2.4.1 CSP's Security Responsibilities

Apart from the CSP's common security responsibilities, the CSP should also take the following responsibilities:

- Security configuration, management, operating monitoring, and emergency response of infrastructure
- Security of virtual networks
- Security of the platform layer, such as the security of OSs and databases
- Security of application systems

2.4.2 Cloud Customer's Security Responsibilities

The cloud customer should take the following security responsibilities in addition to those common ones in section 2.2.2:

- The security assurance capability of the infrastructure provided by a CSP—the cloud customer can check the service description and security responsibility commitment of the CSP or ask the CSP to provide a security certificate issued by a third party, and, if necessary, the customer can check the CSP's security assurance capabilities on site
- Security configuration, management, and monitoring of the platform
- A written agreement with the CSP to audit their network whenever required
- Security of service application systems
- Formulation and rehearsal of business continuity assurance plans and disaster recovery plans
- Serverless Architectures Security

2.5 Saas

For the SaaS deployment model, a CSP provides the application and underlying components security. The customer is responsible for its data security and end-point device protection.

2.5.1 CSP's Security Responsibilities

Apart from requirements in 2.4.1 CSP's Security Responsibilities, the CSP should also take the following responsibilities:

- Security configuration, management, running monitoring, and emergency response of the platform
- Security of service application systems

2.5.2 Cloud Customer's Security Responsibilities

The cloud customer should take the following security responsibilities in addition to those common ones in section 2.2.2:

- The security assurance capability of the infrastructure provided by a CSP—the cloud customer can check the service description and security responsibility commitment of the CSP or ask the CSP to provide a security certificate issued by a third party, and, if necessary, the customer can check the CSP's security assurance capabilities on site
- Security configuration, management, and monitoring of service application systems
- Secure access

2.6 Roles of Third-Party Security Service Providers

With the rapid development of the cloud computing industry, third-party security service providers play an increasingly important role in cloud service security assurance. These security service providers will take partial security responsibilities of CSPs or cloud customers (responsibility transfer) based on business contracts and agreements.

As cloud computing services become popular, the cloud computing platform does not only carry multiple service systems of cloud customers. The secure and reliable running of cloud services has an important impact on a country's social and economic stability. Therefore, governments and industry organizations should monitor the security of cloud service platforms provided by CSPs and of application systems built by cloud customers and then provide guidance for customers. This process requires security authentication, audit, and inspection services from professional third-party security service providers.

Organizations have different security capabilities. When migrating their service systems to the cloud, they are struggling to design, plan, and deploy security solutions based on the shared security responsibility model on the cloud service platform. Therefore, they probably need consulting, integration, and construction services from professional third-party service providers. In addition, they will also require security management and O&M services after systems go online, such as security vulnerability scanning and fixing for the cloud platform and systems deployed.

3 Technical Requirements and Implementation Guide of Cloud Security Assurance Capabilities

This chapter describes the technical requirements for the security assurance of cloud service systems and provides the implementation guide based on the existing security technologies, products, and services. It also illustrates security assurance technologies, products, and services that CSPs and customers should provide in different cloud service modes according to section 2 Security Role and Responsibility of CSPs, Security Service Providers, and Cloud Customers.

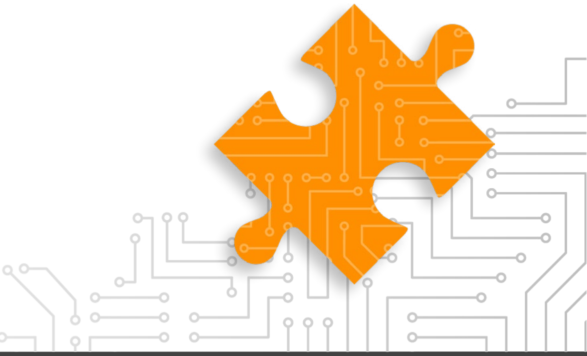
3.1 Responsibility Division of Security Technologies in Different Cloud Service Modes

Figure 3-1 Security responsibilities between CSPs and cloud customers

Category	Major Security Technology Requirement	IaaS	PaaS	SaaS
Infrastructure security	Physical and network security	🟧	🟧	🟧
Virtualization security	Virtualization platform, virtual storage, and API security	🟧	🟧	🟧
	Virtual network	🟦	🟧	🟧
Host security	Antivirus, intrusion prevention, host security hardening, and patch management of OS, firmware updates	🟦	🟧	🟧
Middleware security	Container, API, database, and resource management platform security	🟦	🟧	🟧
Application system security	Web vulnerability scanning, web tamper protection (WTP), anti-DDoS, application firewall, Identity and access management (IAM), and API security, DLP solutions	🟦	🟦	🟧
Data security	Data transmission and storage security, integrity protection, backup, and recovery	🟦	🟦	🟦
Security management	Network audit, network behavior management, traffic control management, key and certificate management, IAM, database audit, cloud log audit, host security management	🟦 🟧	🟦 🟧	🟦 🟧
Security O&M	Security operations center (SOC), security situation awareness (SSA), web vulnerability scanning, system vulnerability scanning, security event monitoring, baseline configuration check, and security audit	🟧	🟧	🟧

🟦 Cloud customer

🟧 CSP



3.2 Security Technology Requirements and Implementation Measures for Cloud Service Systems

3.2.1 Infrastructure Security

3.2.1.1 Physical Security

Security technology requirements:

- Environment security requires protection against related physical damage threats and physical access risks. Device security requires protection of systems, buildings, and related infrastructure.

Implementation guide:

- Comprehensive physical security control measures, management, and risk control are implemented to prevent service interruptions and data loss caused by natural disasters (such as floods and earthquakes) and force majeure.
- Infrastructure protection includes physical location selection; physical access control; protection against thefts, damages, lightning strokes, fires, water, moisture, and static electricity; temperature and humidity control; power supply; and electromagnetic protection.
- For details about the physical security implementation guide, see *TIA-942 Telecommunications Infrastructure Standard for Data Centers*.[8]

3.2.1.2 Network Security

Security technology requirements:

- For network border protection, the system should filter information entering or exiting the cloud network, limit the maximum traffic of the management network and the number of network connections per user of the cloud computing platform, control administrators' access to the management network, and detect and block invalid links of service and management networks. The system should also automatically update access control lists (ACLs) or traffic flow policies on managed interfaces of border management devices, isolate malicious virtual machines (VMs), defend against DDoS attacks, monitor traffic, and detect attacks and intrusion on borders.

[8] TIA-942.org, About Data Centers, **http://www.tia-942.org/content/162/289/About_Data_Centers**.

- For network communication security, the system should support secure transmission between areas of different security levels to enable data transmission confidentiality, integrity protection, and trusted access protection. Users can be authenticated and authorized before accessing cloud computing resources. Direct access to the physical network of the cloud computing platform through the internet is forbidden. Open interfaces should be provided to allow access of trusted third-party security products.

Implementation guide:

- Security devices such as firewalls, IDS/IPS, traffic control, security gateways, and anti-DDoS devices are deployed at the border of the security zone based on the structure of security and security zone division. Security policies are configured to manage the security zone to protect the network border. In addition, core switches and border security devices are deployed in redundancy mode and load balancers are also deployed. This approach ensures that key network devices provide redundant service processing capabilities to meet service demands during peak hours.
- A security access platform is built to deploy VPN systems between users and cloud computing resources to ensure that all users access the resources through the VPN. The encrypted communication protects data transmission confidentiality and integrity. The VPN and access authentication management system are deployed to provide remote access and encrypted data transmission for remote access users to prevent data tampering and data eavesdropping.

3.2.2 Virtualization Security

3.2.2.1 Virtualization Platform Security

Security technology requirements:

- For virtualization platform security, the platform should support API security and tenant isolation of VMs/containers. Security hardening is required to ensure the integrity and confidentiality of resource data on the virtualization platform.

Implementation guide:

- API security policy set configuration is supported. Open interfaces or security services should be provided to allow cloud customers to access third-party security products or select third-party security services on the cloud platform.
- Virtualization layer security technology is used to ensure the security of the cloud virtualization environment including virtual resource isolation, cloud platform security hardening, VPC, VDC, and security group.

- Security information and event management (SIEM), security compliance management, and vulnerability management should be strengthened to enable secure operating management of the cloud platform and address network threats and vulnerabilities in the cloud environment.

3.2.2.2 Virtual Network Security

Security technology requirements:

- Secure isolation of multi-tenant network services is required. Network resources and network topology can be updated and monitored centrally. The system should provide protection against DDoS attacks. Secure transmission is supported during communication between areas with different security levels.

Suggested implementation solution:

- A comprehensive network border security protection solution is provided to protect all applications on the cloud platform. To ensure secure and reliable running of the cloud system network, divide the system network into multiple independent security zones and select different protection measures based on the features of each security zone. Secure isolation between north-south traffic and east-west traffic is implemented to ensure normal network communication and security of information transmitted through the network.
- The virtual network resources of multi-tenant are isolated through virtual local area network (VLAN)/Virtual Extensible LAN (VXLAN) and VPC after switch VLAN and firewall isolation configuration. In addition, the quota and QoS are configured on the switch or virtual switch to prevent excessive network resource usage. A secure access platform is built to deploy the VPN system, access authentication management system, mobile security management system, and firewall system. The platform provides remote access and encrypted data transmission for remote access users to prevent data tampering and data eavesdropping.
- Antivirus gateways are deployed to provide antivirus capabilities. The gateway detects and clears viruses based on common application protocols such as HTTP, FTP, and email. It effectively prevents viruses from accessing the cloud platform through internet access and remote O&M and from spreading on the cloud platform.
- The firewall enables flexible configuration of access control policies between multi-tenant and between different services of the same tenant.

- The intrusion prevention system (IPS) is deployed at the egress to perform in-depth detection on the traffic to prevent north-south and east-west intrusions. The IPS also performs in-depth analysis and detection of application traffic. Together with the attack feature knowledge base and user rules, the IPS can effectively detect and block viruses, attacks, and abuse in mass network traffic in real time. In addition, it can manage various traffic distributed in the network to protect the network application layer.
- Data leakage/detection prevention (DLP) is deployed to detect and prevent any sensitive data misusage and leakage.
- Anti-DDoS devices are deployed at the egress of the internet to detect and defend against traffic-based DDoS attacks (such as UDP flood and TCP SYN flood), application-based DDoS attacks (such as CC, DNS flood, and slow-rate connection exhaustion), DoS attacks (such as LAND, teardrop, and Smurf), and illegal protocol attacks (such as IP flow, TCP packet without flag, FIN bit with no ACK bit, and Christmas tree).

3.2.2.3 Virtual Storage Security

Security technology requirements:

- User data on different VMs is isolated at the virtualization layer to prevent data theft and ensure data security. The system manages data location and home location and supports backup and service continuity.

Implementation guide:

- Data isolation, access control, data reliability, and residual information protection are used to ensure data storage security in the virtualization environment.
- User data on different VMs is isolated at the virtualization layer to prevent data theft and ensure data security.
- The hypervisor ensures that the VMs only access the allocated space, thereby implementing the hard disk isolation of multiple VMs.
- Volume storage security: The system specifies an access policy for each volume. Only authorized users can access a specified volume. Volumes are isolated from each other.
- Residual information protection: When the data enhancement technology is applied to data storage, the system will divide the storage pool into multiple small data blocks and construct a redundant array of independent disks (RAID) group using these data blocks. This enables data to be evenly distributed on all hard disks in the storage pool and resource management is implemented on a data block basis.

- 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 when storage resources are reused. Therefore, the possibility of restoring original data from the reallocated virtual disks is lower, which helps residual information protection.
- When the system reclaims resources, it allows the physical bits of logical volumes to be formatted to ensure data security.
- After physical disks of the data center are replaced, the system administrator degausses or physically destroys them to prevent data leakage.
- The one-way hash algorithm is used to ensure the integrity of image and snapshot data.
- Reliability assurance of stored data: The reliability mechanism is adopted. 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.

3.2.3 Host Security

Cloud host security protection: The host security service module is preset on the cloud platform and can be purchased and used as required in security as a service (SECaaS) mode. Carriers and users do not need to purchase any external systems and resources and can quickly deploy host security services and develop security capabilities.

Security technology requirements:

- Host antivirus and malicious code prevention
- Host intrusion detection and prevention
- Host security hardening and patch management

3.2.3.1 Host Antivirus

Implementation guide:

- The antivirus engine caches and shares the scanning results of VMs and servers and performs incremental scanning to improve the scanning efficiency. In addition, the local antivirus engine can enhance the antivirus effects without connecting to extranets, optimizing the local virtualization environment.

3.2.3.2 Host Intrusion Prevention

Security technology requirements:

- Common denial of service (DoS) attacks, buffer overflow attacks, backdoor Trojan horses, and web attacks from external systems can be detected and prevented. System and application vulnerabilities of cloud hosts are protected against external attacks.

Implementation guide:

- As a cloud host security protection component, the cloud host firewall provides stable and effective protection policies when the cloud host drifts to any host machine in the resource pool. The firewall also controls the access of a cloud host to other cloud hosts. Based on customers' service requirements, fine-grained access control policies are formulated for firewalls between cloud hosts based on IP addresses, ports, protocols, and directions, and then delivered to cloud hosts in batches based on security standards in security zones.

3.2.3.3 Host Security Hardening

Implementation guide:

- Vulnerabilities, insecure user accounts or passwords, improper configurations and operations, and insecure services bring potential security threats in the form of viruses, horses, and worms. The following OS hardening methods are provided to prevent hacker attacks through vulnerabilities:
  - Disabling unused communication ports
  - Disabling unnecessary service processes
  - Restricting system access permission
  - Strictly controlling rights of accounts
  - Enabling the security log audit function
  - Hardening of the OS and databases as per the best practices from SANS, NIST, or the OS developer themselves
- OS security requires security hardening for virtual resources such as identity authentication of the computing environment, access control, security audit, virtualization security, data confidentiality and integrity, data backup and recovery, image and snapshot security, object security reuse, intrusion detection, and malicious code prevention.

3.2.4 Middleware Security

3.2.4.1 Container Security

Security technology requirements:

- The security of underlying physical infrastructure (computing, network, and storage) and manager should be ensured. The container repository should be properly protected and located in a secure location where appropriate access control is configured.

Implementation guide:

- Security capabilities are developed based on the applications/tasks/codes running in the container. Vulnerable software may run in a container in some cases, which may expose OSs or data from other containers. The container environment including network and image/container must be configured securely.

3.2.4.2 API Security

Security technology requirements:

- The system should support API lifecycle and security policy management, API request management, IAM, validity verification of API requests by background services, and security analysis of monitoring and log data.

Implementation guide:

- API authentication: The purpose is to ensure that users accessing the system are authorized users. This function can be applied to real users and computer systems or applications that need to use the capabilities provided by the API. For OpenAPI authentication, the relationship between user roles must be considered, including third-party App system, App developer, App user, and system administrator.
- API security monitoring: The system shall enable the monitoring of the indicators such as the number of API invoking times, delay, and error rate.
- API log and audit:
    - Management plane logs, such as operation logs of API life status management and App subscription logs, which must be recorded.
    - Key API invoking logs on the data plane, such as invoking of payment and charging APIs, which must be recorded by the service party.
    - Common API invoking logs on the data plane, which occupy a large ratio and should be recorded based on the actual situation.

- API data security: Leakage of sensitive data or personal privacy data may lose customers, impact services, and leak personal privacy. Therefore, during API development protection of sensitive information or personal privacy data is a priority, including data protection and secure data storage during transmission.
- API data transmission security: To ensure the security of sensitive data and personal privacy data during transmission, the system usually encrypts the transmitted content, that is, to use Hypertext Transfer Protocol Secure (HTTPS).
- API security policy management: Through security policy management, users can modify APIs and monitor API behavior to enhance API access conflict control, performance, and security capabilities.
- API security analysis: The API invoking logs are analyzed to detect and defend against potential intrusion operations.

3.2.4.3 Database Security

The database audit can parse the traffic entering and exiting the core database at the packet field level, completely restore the operation details, and provide detailed operation return results. In this way, all access is presented to the administrator in a visualized manner so that databases can be controlled and data threats can be quickly detected and handled. Database audit has the following capabilities: pre-event security risk evaluation, real-time behavior monitoring, fine-grained protocol parsing and two-way audit, web service audit, application three-layer association audit, flexible audit rules, abundant alarm methods, efficient behavior retrieval, report system, and session-based playback of actual scenarios.

3.2.4.4 Resource Management Platform Security

Security technology requirements:

- The system should support code security test and defect rectification.
- The system should support security hardening.
- The system should monitor attack behavior and generates alarms. When detecting an attack, the system can record the IP address, attack type, purpose, and time.
- The system should detect and handle malicious codes.
- The system should control administrators' access to the management network and detect and block invalid links.
- Software coding best practices need to be enforced during the development stage of the coding.
- Preferably, the codes should be validated/audited by third-party vendors.

- The system should dynamically enable instances that are created based on images, deployed in containers, and automatically extended. When these instances are not needed, they can be disabled and will not break the application stack.
- Running systems should not be patched. Instead, they can be replaced by new official versions.
- The system should securely isolate service resources among multi-tenants. The tenant can only access and operate their own service resources.
- The system should securely isolate multi-tenant data. The tenant can access and operate only their own data.
- Tenant can define and set data backup, data export, and data reset permissions.

Implementation guide:

- The resource management platform evaluates, detects, and responds to unauthorized and suspicious events, monitors cloud environment compliance, and manages security patch applications. SIEM, security compliance management, and vulnerability management should be strengthened to enable secure operating management of the cloud platform.
- The virtualization layer isolates VMs from hosts and other VMs. Traditional security protection devices cannot meet security requirements of the virtualization layer because they cannot prevent malicious attacks between VMs. The virtualization layer security technologies are used to ensure the security of the cloud virtualization environment. The technology measures are implemented by the virtualization platform, including virtual resource isolation, cloud platform security hardening, VPC, VDC, and security group.

3.2.5 Application System Security

Security technology requirements:

- The system should support user management identity authentication, account management, role authentication, API access security, service management plane isolation, web security, and behavior audit. The cloud security service provider can provide web attack defense, cloud WAF, cloud WTP, and two-factor authentication services.

Implementation guide:

- IAM: The application system platform needs to perform management identity authentication, account management, role authentication, API access security, and service management plane isolation for users of the application.

- Web code security protection: The web code security mechanism is supported, including the validity check on input and output and measures to prevent authentication, permission, session, web service, and injection vulnerabilities. The system also controls user access to resources through the web and supports secure transmission of remote web access.
- Web attack defense: The web attack defense capabilities are developed to implement the overall web security lifecycle solution covering pre-event detection, in-event protection, and post-event analysis. Cloud monitoring is used to monitor user website vulnerabilities before an event and the zero-deployment cloud protection solution is used during the event.
- Prevention against DDoS and CC attacks: There are two types of DDoS attack defense. One is a dedicated protection device deployed locally, which can directly defend against DDoS attacks with heavy traffic. When the DDoS attack traffic exceeds the local protection limit, the cloud scrubbing center from a professional security service provider can be used to solve the problem. The anti-DDoS/CC algorithm is used to solve the availability issue of DDoS attacks and enhance the SSA system to ensure stable operations.
- WAF system: Rule-based protection provides accurate and detailed defense against a large number of known attacks, including SQL injection, cross-site scripting, OS command injection, remote file inclusion, local file inclusion, directory traversal, HTTP violation, and WebShell attacks. This approach protects websites.
- WTP system: If web pages are changed by hackers or staff incorrectly, the WTP software can recover the changed web pages in real time to ensure normal running of the website. Moreover, the software records information about the tampering event, which can be used as proof during investigation by the security department.

3.2.6 Data Security

Security technology requirements:

- Data security is important. Key or sensitive data (static and dynamic) must be protected and risks of data leakage and damage must be minimized to ensure the reliability and security of service systems on the cloud. During network transmission, data integrity, confidentiality, and validity must be ensured to prevent interruption, replication, tamper, forgery, interception, and monitoring.

Implementation guide:

- To prevent data leakage, data must be encrypted during storage and transmission. The cloud should ensure data isolation and secure sharing between different tenants. Transmission security, data storage security, disaster recovery and backup, and other technical measures are used to enhance data security. The database audit system audits the behavior of accessing database servers. Data isolation, access control, data reliability, and residual information protection are used to ensure data storage security in the virtualization environment. If supported, the ability for customers to retain access to keys is preferred.
- Data transmission security: HTTPS is used for pages that contain sensitive data and SSL/TLS-based transmission paths are used for system administrators to access the management system. When users log in to VMs, SSH and RDP are adopted. When customers access the remote cloud O&M, SSL VPN is used. Login using encryption protocols enables encrypted transmission and identity authentication, ensures that data is sent to the correct client and server, prevents data theft during transmission, and guarantees data integrity. HTTPS certificates can be replaced and managed. The application platform system deployed by the tenant in IaaS mode can generate and manage certificates by itself or purchase the certificate management service from the CSP. The application platform can also enable client-side encryption, such as HTTPS during data transmission into or out of CSP Storage. If the web application may be the target of determined attackers (a common threat model for internet-accessible applications handling sensitive data), it is strongly advised to use TLS services that are provided by well recognized crypto modules.
- Data storage security: The application platform system deployed by the customer in IaaS mode can generate and manage keys by itself or purchase the key management service from the CSP. The sensitive data of key/authentication credentials is reversibly encrypted, and passwords are irreversibly encrypted. This approach ensures data security when data is stored in files, data volumes, or system volumes.
- Data integrity verification: The system identifies key/sensitive data service scenarios that require integrity verification. Data is digitally signed during storage, and integrity check is performed before the data is used.
- Data backup and restoration capabilities: Refer to the disaster recovery and backup measures for database security and infrastructure security in the module of middleware security.

3.2.7 Security Management

3.2.7.1 Network Audit

Security technology requirements:

- If cloud users affect network efficiency by performing irrelevant operations or using hosts to set up irrelevant services, technical capabilities need to be developed to record and restore network resource usage for audit.

Implementation guide:

- To restore content in real-time traffic, the network audit system is deployed in off-line mode by mirroring traffic on the core switches at the internet border and extranet border. The system identifies traffic of multiple common application protocols such as HTTP, SMTP, POP3, RDP, FTP, and NFS, and restores content and behavior audit records to detect security risks in a timely manner and to optimize network resource usage. In addition, the device provides the traffic analysis capability to help O&M personnel locate and analyze network bandwidth usage to quickly locate problems and optimize the network.

3.2.7.2 Network Behavior Management

Security technology requirements:

- If users transfer sensitive information through the network, publish inappropriate comments in forums, and conduct behavior that supervisors forbid, related technical capabilities should be built to record and restore network resource usage and network behavior.

Implementation guide:

- The online behavior management mechanism is set at the border of the security zone. The security management center manages behavior in a centralized manner and generates alarms once violations are confirmed. Utilizing cloud access security broker (CASB) provides cloud application visibility, risk intelligence, data governance, user behavior analytics (UBA), and policy controls for sanctioned cloud apps, and provides real-time UBA, data security, and threat protection for unsanctioned cloud apps including cloud data encryption and tokenization for regulatory compliant use of cloud apps.

3.2.7.3 Traffic Control Management

Security technology requirements:

- Web servers in the cloud internet area carry websites. Within a given time window, a great number of normal access requests may be initiated and a single host may fail to handle mass volumes of concurrent requests quickly, reliably, and securely. For the website, a key application on the cloud, the system should eliminate service interruption risks caused by single point of failures (SPOFs). Similarly, applications such as the OA system carried by the extranet area are also facing risks caused by host overload and server SPOFs.

Implementation guide:

- Application load balancers are deployed on the core switch in bypass mode to provide flow control at layers L2 through L7. This solution effectively addresses the problems of high data traffic and network overload and prevents data traffic loss caused by SPOFs. The load balancer supports multiple discontinuous load balance algorithms such as polling, weighted round robin (WRR), minimum connection, and shortest response time, and multiple continuous load balance algorithms such as IP keepalive, persistent cookie, QoS cookie, QoS URL, and QoS Hostname. It adopts various application acceleration modes (including TCP connection reuse, hardware SSL acceleration, high-speed data cache, HTTP compression, asymmetric TCP acceleration, and high-speed protocol stack technology) to efficiently and rapidly allocate application requests to appropriate servers and conducts health checks to monitor the server status in real time.

3.2.7.4 Key and Certificate

Security technology requirements:

- The system limits the administrator login address of network devices (including virtualization network devices), handles device login failures, and uses two or more authentication technologies to authenticate the identity of administrators of these network devices. It also implements secure transmission of the devices in remote management, restricts privileged commands, minimizes administrator rights, and supports log records and audit reports.

Implementation guide:

- Accounts, authentication, authorization, and audit of cloud platforms, security products, network devices, servers, and storage resources are controlled and managed centrally. The system provides O&M rights management and comprehensive log auditing and supports graphic terminals, character terminals, database applications, and file transmission. It also provides real-time video surveillance and screen recording to block high-risk operations such as deletion and restart in a timely manner. The system also implements strong two-factor authentication by use of mobile phone tokens or hardware tokens and passwords, ensuring the security of system O&M personnel accounts and privileged accounts.

3.2.7.5 Identity Authentication Management Platform

Security technology requirements:

- The identities of system users are managed in a unified manner. According to the service division, personnel are classified into different types or groups and different access rights to modules are assigned. The rights can be set by the role, such as the common user, system administrator, security administrator, and audit administrator.

Implementation guide:

- The unified network management system (NMS) is deployed to configure, control, and manage the resources and running of the system.

3.2.7.6 Database Audit

Security technology requirements:

- Data security is important. Key or sensitive data (static and dynamic) must be protected and risks of data leakage and damage must be minimized to ensure the reliability and security of service systems on the cloud. Data isolation and security sharing between different tenants should be ensured. The database audit system is used to audit the behavior of accessing database servers.

Implementation guide:

- The database audit system provides multiple functions including static audit, real-time monitoring and risk control, real-time audit, bidirectional audit, auditing rules, behavior search, association audit, auditing reports, security event review, auditing object management, warning management, and system configuration management. It can audit all database access traffic through data flow mirroring.

- The database audit system helps detect database violation operations. It collects, analyzes, and identifies network data, monitors all network database access operations in real time, and supports user-defined content keywords, user-defined protocol monitoring, and user-defined port monitoring to deliver content monitoring and identification in operations.
- In response to unauthorized database access, the database audit system can report alarms in various forms in a timely manner and restore the entire process of unauthorized access. This helps accurately trace and locate security events throughout the whole process and ensures security of the database system. With capabilities for integrated analysis and comprehensive and systematic reporting, the database audit system provides users with comprehensive database access security analysis reports.

3.2.7.7 Cloud Log Audit

Security technology requirements:

- The log audit system is deployed to centrally manage security audit mechanisms of components in the system. The log audit system classifies audit records based on security audit policies, enables or disables the corresponding security audit mechanism by time segment, and stores, manages, and queries audit records. It also conducts strict identity authentication on the security auditor and allows the auditor to perform security audit operations only through specific commands or interfaces.

Implementation guide:

- Log monitoring: The system monitors the status of received events in real time, such as the latest log list and system risk status. It also monitors the running parameters of devices to determine the status of devices and networks. Real-time and graphical monitoring of log traffic, system risks, and other change trends is also supported.
- Log management: The system manages multiple log formats in a unified manner. SNMP, Syslog, or other log interfaces are used to collect log information about managed objects. The logs are then converted into a unified format for management, analysis, and alarm reporting. The system automatically parses and classifies log data and supports data storage, backup, recovery, deletion, import, and export operations. Distributed log cascading management is also supported. The log data of the lower-level management center can be sent to the upper-level management center for centralized management.
- Security event analysis: The centralized audit can integrate various security events and provide customized reports to users based on unified audit results. The reports comprehensively reflect the overall network security status and are easy to understand with highlighted key points.

- The system collects statistics on and analyzes packet filtering logs, proxy logs, intrusion attack events, and virus intrusion events and generates analysis reports. It implements statistical analysis on security device management information based on device running status and device management operations. It supports statistical analysis based on multiple conditions such as access traffic, intrusion attacks, mail filtering logs, source addresses, and user access control logs. Moreover, intrusion attack logs can be analyzed based on intrusion attack events, source addresses, and attacked hosts to generate various trend analysis charts.

3.2.7.8 Host Security Management (Bastion Host)

Security technology requirements:

- The cloud platform needs to provide centralized and unified access control policies, which can perform identity authentication and authorization, audit operation behavior, and record user operations to prevent adverse impact on the production system due to incorrect operations, permission abuse, and misoperations of O&M personnel. The operation records can be used for troubleshooting and fault recovery.

Implementation guide:

- The O&M bastion host is deployed in the management area to centrally control and manage accounts, authentication, authorization, and audit of cloud platforms, security products, network devices, servers, and storage resources. The system provides O&M rights management and comprehensive log audit and supports graphic terminals, character terminals, database applications, and file transmission. It also provides real-time video surveillance and screen recording to block high-risk operations such as deletion and restart in a timely manner. The bastion host can be deployed to audit O&M logs.

3.2.8 Security O&M

3.2.8.1 SOC

Security technology requirements:

- Plan the overall architecture of the security management platform and design compliance analysis, event response, vulnerability analysis, threat intelligence, event correlation analysis, and event handling functions.

Implementation guide:

- The SOC has situation awareness (visualized large-screen display), vulnerability management, SIEM, threat intelligence, and event response modules. Process IT/GSC capability and security operation practice are introduced to facilitate use case design.

3.2.8.2 SSA

Security technology requirements:

- To ensure the security of the cloud customers' service systems, the out-of-band big data cloud security monitoring system, namely the SSA system, can automatically check vulnerabilities of mass cloud applications as scheduled to ensure that security issues of cloud systems can be detected as soon as possible and to improve the security management and service capabilities of cloud systems. The SSA system can also build a good cloud environment to support secure and reliable cloud operations.

Implementation guide:

- Uninterrupted service quality monitoring is implemented on all important sites and applications on the cloud to ensure that the site is available and can provide services normally. In addition, scheduled website security monitoring services are provided for these sites and applications to quickly detect and locate network security problems and events. Network security issue and event detection capabilities include website vulnerability detection, website availability monitoring, website Trojan horse monitoring, website link monitoring, website security event monitoring, website sensitive content monitoring, and network host monitoring.

3.2.8.3 Web Vulnerability Scanning

Security technology requirements:

- The vulnerability scanning system is deployed on the cloud platform to detect security vulnerabilities of specified web servers through scanning and to provide timely security protection.

Implementation guide:

- The web vulnerability scanning system helps detect vulnerabilities of web applications, including SQL injection, command injection, CRLF injection, LDAP injection, XSS cross-site script, path traversal, information leakage, URL redirection, file inclusion, application program, and file uploading (website malicious code detection and dark chain detection). The system also verifies vulnerabilities, monitors website security, and detects survival availability.

3.2.8.4 System Vulnerability Scanning

Security technology requirements:

- The vulnerability scanning system is deployed on the cloud platform to detect security vulnerabilities (which are exploited in initiating attacks such as penetration attacks) of specified VMs or physical machines through scanning and to provide timely security protection.

Implementation guide:

- The vulnerability scanning system cooperates with the firewall and intrusion detection system. By scanning the network, the platform administrator can know the security settings and running application services, detect security vulnerabilities in a timely manner, and objectively evaluate the network risk level.
- Based on the scanning result, the platform administrator can correct network security vulnerabilities and error settings in the system to defend against hacker attacks, including vulnerability scanning, analysis, fixing, and audit, risk alarm, policy management, and statistical analysis.

3.2.8.5 Security Event Monitoring

Security technology requirements:

- The system can dynamically dispatch monitoring devices deployed in all systems and local monitoring engines deployed in the private cloud system to scan all online information systems on the private cloud and provide basic fingerprint data for various systems.

Implementation guide:

- Uninterrupted service quality monitoring is implemented on all important sites and applications on the cloud to ensure that the site is available and can provide services normally. In addition, scheduled website security monitoring services are provided for these applications and sites to quickly detect and locate network security problems and events.

3.2.8.6 Baseline Configuration Check

Security technology requirements:

- A large number of servers, storage devices, network devices, and security devices are deployed on the cloud. The configuration files of these devices may contain security threats such as weak passwords, backdoors, and risky ports. The security configuration check system automatically checks the configuration files of servers, storage devices, network devices, and security devices on the cloud platform, detects security threats, and notifies users in a timely manner. CASB solutions can support many of these functionalities including real-time response to changes in configurations that impact security and compliance.

Implementation guide:

- The security configuration check system supports security baseline check on the following items:
    - OSs such as Windows Server 2012/Windows Server 2008/Windows Server 2003/ Windows 7, Linux RH5 or later, CentOS 5 or later, and SUSE Enterprise 9
    - Network devices and security devices from Huawei, Cisco, Juniper, and other vendors
    - Databases such as Oracle 9i, MySQL, SQL Server, and Informix
    - Middleware such as Tomcat, IIS, WebSphere, Apache, and BIND

3.2.8.7 Security Audit

Security technology requirements:

- The log audit system is deployed to centrally manage security audit mechanisms of components in the system. The log audit system classifies audit records based on security audit policies, enables or disables the corresponding security audit mechanism by time segment, and stores, manages, and queries audit records. It also conducts strict identity authentication on the security auditor and allows the auditor to perform security audit operations only through specific commands or interfaces.

Implementation guide:

- Log monitoring: The system monitors the status of received events in real time, such as the latest log list and system risk status. It also monitors the running parameters of devices to determine the status of devices and networks. Real-time and graphical monitoring of log traffic, system risks, and other change trends is also supported.

- Log management: The system manages multiple log formats in a unified manner. SNMP, Syslog, or other log interfaces are used to collect log information about managed objects. The logs are then converted into a unified format for management, analysis, and alarm reporting. The system automatically parses and classifies log data and supports data storage, backup, recovery, deletion, import, and export operations. Distributed log cascading management is also supported. The log data of the lower-level management center can be sent to the upper-level management center for centralized management.
- Security event analysis: The centralized audit can integrate various security events and provide customized reports to users based on unified audit results. The reports comprehensively reflect the overall network security status and are easy to understand with highlighted key points. The system collects statistics on and analyzes packet filtering logs, proxy logs, intrusion attack events, and virus intrusion events, and generates analysis reports. It implements statistical analysis on security device management information based on device running status and device management operations. It also supports statistical analysis based on multiple conditions such as access traffic, intrusion attacks, mail filtering logs, source addresses, and user access control logs. Moreover, intrusion attack logs can be analyzed based on intrusion attack events, source addresses, and attacked hosts to generate various trend analysis charts. The system can generate multiple types of audit reports in tables or charts. Users can use Internet Explorer to access and export audit results. The system can be set to generate log reports as scheduled and automatically save them for review or automatically send them to specified recipients through emails, enabling process-based security audits.
- O&M security audit: Important security events in the system are audited, such as O&M personnel behavior, abnormal use of network device and system resources, and use of important system commands. The audit record should contain the event date, event time, event type, subject identity, object identity, and result. In addition, record data is analyzed to generate audit reports. The audit process should be protected from unexpected disruption and the audit record should be protected from unexpected deletion, modification, or overwriting. The cloud platform enables tenants to collect and view audit information related to their own resources through SECaaS extension capabilities.

3.3 Security Assurance Capabilities Offered by Third-Party Security Service Providers

In 2.6 Roles of Third-Party Security Service Providers, third-party security service providers can offer security services for CSPs and customers and provide security assurance capabilities for service buyers through commercial contracts. 3.1 and 3.2 provide suggestions on security technology requirements and corresponding implementation measures for the security assurance system of a specified service system deployed in cloud-based mode. Although these security capabilities should be provided by CSPs or customers, they can be deployed, implemented, managed, and maintained by third-party security service providers in practice.

A third party can provide various security services through separate products or services or through packages. Some examples are as follows:

- Situation awareness: The out-of-band-based big data cloud security monitoring system can automatically check vulnerabilities of mass cloud applications as scheduled to ensure that the security issues of cloud systems can be detected as soon as possible and to improve the security management and service capabilities of cloud systems.
- Web code security protection: The web code security mechanism is supported, including the validity check on input and output and measures to prevent authentication, permission, session, web service, and injection vulnerabilities. The system also controls user access to resources through the web and supports secure transmission of remote web access.
- WAF system: Rule-based protection provides accurate and detailed defense against a large number of known attacks including SQL injection, cross-site scripting, OS command injection, remote file inclusion, local file inclusion, directory traversal, HTTP violation, and WebShell attacks.
- WTP system: This service can restore website files in real time to ensure the normal running of websites and to record information about tamper events.
- SOC: The integrated management platform integrates various security services and provides service platforms such as WTP, cloud host protection, cloud bastion, cloud WAF, log audit, database audit, and situation awareness.

APPENDIX A

A Building a Secure B2B Cloud Solution - A Case Study

A.1 Requirement Analysis and Key Assumptions

A.1.1 Requirements for Information Security Protection

The following are requirements for an information security protection program:

- Evaluate the existing network infrastructure of the B2B cloud, analyze features of various applications, specify requirements for information security, and clarify objectives and overall guidelines for the future information security construction.
- Considering actual conditions of the B2B cloud and relevant technologies for information security devices, formulate a security construction solution for the B2B cloud based on the status and development trends of security technologies.
- Build a complete information security infrastructure system to secure the normal running of the B2B cloud.

Based on the security requirements on cloud computing and in compliance with the Cloud Controls Matrix Version 3.0.1, the Cloud Security Alliance (CSA) cloud controls matrix (CCM) is a security controls framework designed for cloud security.

CSA CCM consists of 16 control domains and provides security guidance about technologies, personnel, management, and processes on the tenant and cloud platform layers from the prospects of physical security; identity and access management (IAM); infrastructure and virtualization; security incident management, e-discovery and cloud forensics; and threat and vulnerability management.

The following provides compliance requirement analysis:

- **Security technology requirement analysis**
  - **Requirements for physical security** Physical security risks mainly refer to unavailable network devices and cables caused by the surrounding environment and physical features, which may cause an unavailable network system or breakdown of the entire network. An available physical layer is the premise for the entire network system security. It enables the entire network availability and improves the network resistance to risks including:
    - Equipment rooms not under personnel access control, which brings risks.
    - Stolen or damaged network devices.
    - Aged or intentionally or unintentionally damaged cables.
    - Unexpectedly faulted or powered off devices.
    - Natural disasters such as earthquake, flood, fire, and lightning.
    - Electromagnetic interference.
  - **Requirements for IAM**
    - **Identity authentication** Identity authentication applies to hosts and applications.
    - **Access control** Access control applies to hosts and applications.
    - **Identity and account management** Authorized users must have access to appropriate assets at the right time. The assets consist of infrastructure, data, information, and services.
      - **Unified account management** As for dispersed and multi-point access requests, set up a centralized O&M account management system to record user information and generate O&M personnel IDs. This system performs identification and authentication before users' access to resources, preventing unauthorized users or unauthorized access of authorized users.
      - **Anti-spoofing** Provide the dual-factor authentication, consisting of complex passwords and other strong authentication credentials, to prevent brute-force cracking and hackers from performing unauthorized operations as authorized users.
      - **Non-repudiation** Manage O&M administrator accounts for various systems of the data center in a centralized manner and record various operations of O&M accounts such as system changes and account changes to trace malicious behavior.

- **Requirements for infrastructure and virtualization security**
  - **System audit** The system audit includes the host audit and application audit.
  - **Intrusion prevention** Host OSs face various targeted intrusion threats. Common OSs have various security vulnerabilities, which are much easier to be detected and exploited. These vulnerabilities bring huge risks to the entire system. Therefore, during installation, use, and maintenance of host OSs, intrusion must be prevented.
  - **Border access control** A basic security requirement on various borders is access control, which means to control data that enters and exits security area borders and to prevent unauthorized access.
  - **Border intrusion prevention** Various network attacks may come from either well-known external networks, such as the internet, or the internal network. Security measures must be taken to actively prevent various attacks against the information system, such as viruses, Trojan horses, spyware, suspicious codes, port scanning, and DoS and DDoS attacks. This will protect the network layer, the service system, and core information assets against attacks.
  - **Border security audit** An auditing mechanism on the security area border must be set up to record and audit network behavior, such as entering and exiting borders. This audit mechanism works with host audit, application audit, and network audit to form a multi-level auditing system. This auditing system can be managed by the security management center.
  - **Backup and restoration** A backup mechanism must be established for key data, and redundancy configurations must be applied to key network devices and cables. Backup and restoration are necessary measures for emergency events.
  - **Data security** Data security mainly refers to data integrity and confidentiality. Data is the information asset. All measures are taken to guarantee service data security. Therefore, data backup is important and must be considered. Measures must be taken to ensure data integrity and confidentiality during transmission.
  - **Reasonable resource control** Reasonable resource control applies to hosts and applications.

        - **Residual information protection** Host OSs and databases in normal use usually need to temporarily or permanently store user authentication information, files, directories, and database records. Reallocating them without deleting the original user information will lead to information leakage risks. Therefore, user authentication, files, directories, and database records in the system should be deleted before their storage space is released or reallocated to other users.

          Original user information should be deleted before allocating dynamic resources in dynamic management and use to prevent information leakage.

- **Security incident management, e-discovery, and cloud forensics requirement analysis** “30% technology and 70% management” shows the importance of the management layer in the security system. In addition to technical management, security management effectively ensures functions of security technologies.
    - **Security management processes** Security O&M scenarios of the cloud include maintenance of cloud platforms, B2B cloud personnel, and service suppliers. Maintenance is divided into local and remote maintenance. Because maintenance scenarios are complex, a data center security management system must be established to provide security management, risk management, and compliance management. In addition, security policies, plans, and processes must be developed for various scenarios to support security O&M of cloud data center and to meet security compliance requirements.
    - **Security audit** Security logs of various security products, network devices, hosts, and databases record user operations. To prevent non-standardized operations, rights abuse, or disoperation of O&M personnel from interrupting the production system, it is necessary to audit operation behavior, predict and manage security events, and treat their security risks.
- **Threat and vulnerability management requirement analysis**
    - **Vulnerability management** Utilize vulnerability detection methods such as vulnerability scanning, application scanning, and manual evaluation to develop a vulnerability library. This library is used to assess vulnerabilities of assets and services; therefore, system security hardening and security patches can be adopted to protect the system.
    - **Malicious code prevention** Viruses now tend to combine with hacker programs, and worms are increasingly flooding. The spreading path of computer viruses has greatly changed. In most cases, they spread in networks, including the internet, WANs, and LANs. It is therefore necessary to find new ways to face challenges. Gateway products urgently need to scan and remove viruses at the network level.

A.1.2 Requirements for Information Security Services

- **Requirements for access security of B2B clouds**
  - The data center must support all kinds of services. The data center network must therefore support multiple security access modes, such as IPsec VPN and SSL VPN, and it must ensure the following users have access to the data center:
    - Enterprise users (office network users, remote office users, and mobile users): Users who have access to core services of the data center.
    - O&M personnel: personnel responsible for cloud platform maintenance and management, including system, database, network, storage, and application administrators, as well as contingency O&M personnel of security vendors.
  - Requirements for network interconnection among multiple data centers: Multiple data centers must be interconnected with each other on the B2B cloud.
- **Requirements for operation audit of O&M personnel from cloud service providers**
  - O&M personnel of cloud service providers have access to tenants' service systems and data stored on the B2B cloud. As a result, stealing of data and tampering of system logs might occur. It is therefore necessary to record and audit operations of O&M personnel to prevent risks or perform post-event tracing.

A.1.3 Requirements for Complete Security Monitoring, Analysis, and O&M System

Cloud data centers have much greater security monitoring and O&M coverage and complexity than traditional data centers. Security devices deployed in traditional data centers are separated systems and cannot face security risks as a whole. In addition, each system generates a large number of logs and repeated alarms. O&M personnel cannot view and process all the logs and alarms, so they are not clear about cloud security and performance. As a result, security risks in enterprises cannot be detected in time.

To immediately detect and handle security risks in the cloud environment, a security information and event management (SIEM) system must be deployed to provide centralized security management. This system integrates distributed security resources to show the overall security status. The intelligent association analysis of logs quickly exposes security risks and threats, enhancing overall security and improving O&M efficiency.

A.2 Cloud Security Solution Design

A.2.1 Network Security Design

The B2B cloud involves access from multiple networks such as internet and intranet. The network security design should focus on the protection of service and data security. According to the service differences, internal and external networks associated with the B2B cloud are divided and designed by partition and domain and these networks are isolated by the firewall. Incoming and outgoing data in these network zones need to be restricted based on the actual situation.

Because the B2B cloud is accessed by multiple external networks, measures should be taken to defend against intrusion, virus, worm, and DoS attacks from external networks. Additionally, secure and reliable SSL encryption channels must be provided for the O&M personnel to further ensure data transmission security and prevent maintenance data from being interrupted, replicated, tampered with, forged, intercepted, or monitored during transmission.

The B2B cloud provides internet-based services; therefore, it faces multiple security risks such as hacking, viruses, network attacks, and internal management issues. A complete border security solution must be provided to protect all services and applications on the cloud platform. This project aims to utilize existing security resources and security facilities of the cloud platform to protect boundaries. The design covers the following aspects:

Core firewall

Two firewalls connect to core switches in bypass mode and the core switches work in active/standby mode. Security zones are divided to provide basic security isolation. The core firewall creates a virtual firewall (vFW) for each service to flexibly configure access control policies between different services and different applications of the same service. Additionally, it provides functions such as anti-ARP spoofing, malformed packet attack defense, and NAT.

Anti-DDoS

Two anti-DDoS devices are deployed at the internet egress of the B2B cloud. The two devices work in detection and cleaning modes, respectively. The device in detection mode monitors and analyzes traffic in real time by traffic mirroring. The device in cleaning mode dynamically advertises and reinjects the traffic by using the Border Gateway Protocol (BGP) and static routes. The anti-DDoS system can effectively detect and defend against traffic-based DDoS attacks (such as UDP flood and TCP SYN Flood), application-based DDoS attacks (such as CC, DNS Flood, and low-rate connection exhaustion), DoS attacks (such as Land, Teardrop, and Smurf), and illegal protocol attacks (such as IP flow, TCP without labels, unconfirmed FIN, and Christmas tree).

Intrusion prevention system

Each of the two core firewalls is equipped with an intrusion prevention system (IPS) card, which performs in-depth detection on the traffic passing by the firewall to provide north-southbound and east-westbound intrusion prevention capabilities for the cloud. The IPS performs in-depth analysis and detection of application traffic and works with the attack feature knowledge base and user rules to effectively detect and immediately block hidden viruses, attacks, and traffic abuses. Additionally, the IPS can effectively manage the traffic distributed on the network to protect the application layer.

Anti-virus gateway

Two anti-virus gateways connect to the core switches in bypass mode to provide anti-virus capabilities on the gateway. Anti-virus gateways detect and clear viruses using common application protocols such as HTTP, FTP, and emails, effectively prevent viruses from accessing the B2B cloud platform through internet access and remote O&M, and prevent viruses from spreading on the cloud platform.

VPN

A security access platform is set up at the internet ingress. On this platform, the VPN system, access authentication management system, mobile security management system, and firewall system are deployed. Additionally, the platform provides remote access and encrypted data transmission functions for remote access administrators, which avoids data tampering, data eavesdropping, and other risks.

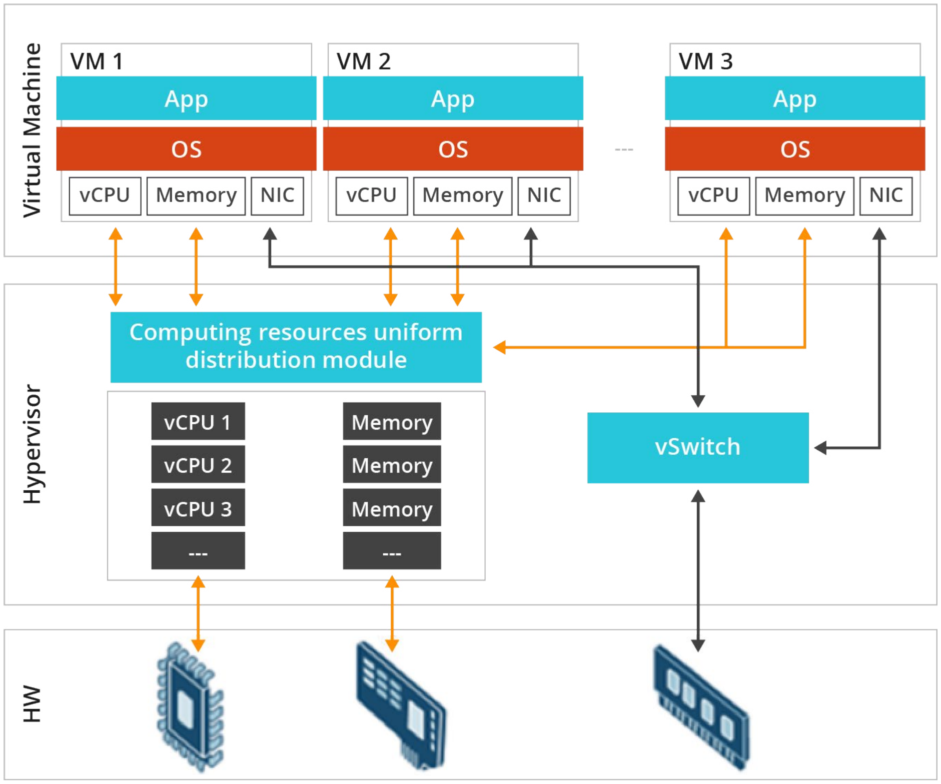
A.2.2 Virtualization Security

Resource virtualization involves certain risks. To ensure VM security, the virtualization layer must separate hosts from VMs and separate a VM from another VM. In response to the threats and challenges in the cloud computing field, this provides security solutions covering VM isolation, network isolation security, data storage security, and cloud platform system hardening for the B2B cloud.

A.2.2.1 VM Isolation

The hypervisor isolates VMs running on the same physical machine to prevent data theft and malicious attacks. End users can only access resources allocated to their own VMs, such as hardware and software resources and data, ensuring secure VM isolation. The following figure illustrates VM isolation.

Figure A-1 Isolation between physical and virtual resources



The hypervisor centrally manages physical resources and ensures that each VM obtains independent physical resources. It also masks faults of virtual resources. As a result, if a VM becomes faulty the hypervisor and other VMs are not affected.

vCPU scheduling isolation security

The cloud platform uses x86 architecture servers. The x86 architecture offers 4 privilege levels ranging from ring 0 (the most privileged) to ring 3 (the least privileged). The OS kernel runs in ring 0. OS services run in ring 1 and ring 2 and user applications run in ring 3. The operations for each level can be performed only within the ring. 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.

Memory isolation

The VM uses 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 client OS translates the virtual address into the physical address. The hypervisor first translates the physical address of the client into a machine address and then sends the machine address to the physical server.

Internal network isolation

The hypervisor provides the function of virtual private network (VPN) routing and forwarding (VRF). Each guest VM has one or more virtual interfaces (VIFs) logically associated with the VRF. 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. The destination VM then checks the certificates to determine whether to accept the data packets.

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.

A.2.2.2 Network Isolation Security

VPC

The solution provides the virtual private cloud (VPC) function. A VPC is regarded as a LAN. Users can configure different VPCs to isolate communications between VMs to enhance VM security.

Security group

The solution provides the security group feature. The security group feature allows users to control interconnection and isolation between VMs to enhance VM security. Security group rules are used to achieve interconnection or isolation between VMs. The default security group rules are as follows:

- VMs in the same security group can communicate with each other.
- VMs in different security groups are isolated from each other.
- Only requests allowed by a security group can access VMs in the security group.

Users can configure security group rules as follows:

- Inter-group authorization: specifies the security groups that can access a specific security group.
- VM authorization rule: defines peer network devices that can access a specific VM.

DHCP quarantine
DHCP quarantine 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.

DHCP snooping
DHCP snooping is a security feature that filters messages from untrusted sources by setting up and maintaining the DHCP snooping binding database. The DHCP snooping feature performs the following activities:

- Intercepts and parses DHCP ACK messages received from virtual ports.
- Saves the IP addresses assigned by DHCP servers to the IP-MAC address binding table that is associated with virtual ports.
- The IP-MAC address binding function is enabled by intelligent network interface cards (iNICs) or elastic virtual switches (EVSs).

A.2.2.3 Data Storage Security

The B2B cloud solution should provide data storage security in the virtualization environment in terms of data isolation, access control, data reliability, and residual information protection.

User data isolation
User data on different VMs is isolated at the virtualization layer to prevent data theft and ensure data security. The hypervisor implements I/O virtualization by dividing the device driver model into the following three parts:

- Front-end driver: Runs in Domain U and transfers I/O requests of Domain U to the end driver in Domain 0.
- Back-end driver: Runs in Domain 0, parses I/O requests, maps them to physical devices, and hands them to the device driver controlling hardware.
- Original driver: Runs in Domain 0.

The hypervisor intercepts and processes all I/O activities, allowing VMs to use only the allocated disk space, thereby implementing the hard disk isolation of multiple VMs.

Data access control
Volume storage: Different access policies are configured for different volumes. Only users who have the access permission can access a volume, and different volumes are isolated from each other.

Residual information protection
With data enhancement technology applied to data storage, the system divides the storage pool into multiple small data blocks and constructs a Redundant Array of Independent Disks (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.

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. Therefore, the possibility of restoring original data from the reallocated virtual disks is low, protecting residual information from being illegally obtained.

When the system reclaims resources, it allows the physical bits of logical volumes to be formatted to ensure data security.

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

Data storage reliability
In the B2B cloud 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.

A.2.2.4 Cloud Platform OS Hardening

In the B2B cloud solution, compute nodes and management nodes use the SUSE Linux OS. The following basic security configurations must be performed to ensure OS security on these nodes:

- Minimum services: Disable unnecessary services, such as Telnet and FTP services.
- Service hardening: For example, harden the SSH service.
- Kernel parameter modification: For example, modify kernel parameters to disable the kernel forwarding function.
- Permission configuration for files and directories: Control access permissions on files and directories.
- System authentication and authorization: Restrict system access permissions.
- Account and password security: Manage user passwords.
- Operation log recording: For example, enable the system log function.

The following security hardening configurations apply to the web middleware:

- Delete irrelevant resources: For example, sample applications provided during the middleware pre-installation.

- Prevent platform information leakage by shielding the middleware version displayed on the client.
- Protect key ports: For example, disable the shutdown port.
- Protect key configuration files: For example, control the permissions on key configuration files.
- Record logs: For example, create your own log files.
- Conduct connector security configuration: For example, configure the SSL protocol.

A.2.3 VM Security

In the B2B cloud, a large amount of common application software is applied, such as OSs, databases, and webs. Therefore, hosts are vulnerable to virus attacks, vulnerability attacks, and Trojan horses, affecting system operations. VM security is ensured by system hardening and host security protection.

A.2.3.1 Host Security Protection System

In the B2B cloud, enterprise-level antivirus products are deployed on physical machines and VMs for integrated management and monitoring.

Hackers can intrude on VMs by accessing the external applications involved in the B2B cloud to implant malicious code like Trojan horses and viruses. In addition, the VM and host machine have external interfaces, such as the USB interface and the interface formed by bridging the vNIC and physical NIC of the host machine, which increases the possibility that VMs are infected with Trojan horses and viruses.

In this project, the virtualization security management system is deployed and a virtualization security management and control center is built to safeguard VMs against malicious code, considering potential risks such as virtualization storms, host machine security, high client resource percentage, attacks between VMs, and security zone chaos caused by a failover.
In the host security protection system, agent programs are installed on the OS of the virtual host and virtual server resources are managed in a unified manner to achieve the real-time anti-virus purpose. The system provides innovative methods to solve the resource consumption problem caused by anti-virus programs. It adopts the anti-virus scanning and caching mechanism and scheduled tasks to prevent anti-virus database update storms. This project also provides the following malicious code prevention services:

Access control
Traditional firewall technologies are implemented using hardware for access control at the physical network layer and security zone division. However, after computing resources are virtualized, a majority of information exchanges can be implemented within a server. The most basic security issue is how to implement access control and virus propagation suppression within a virtual system.

The host firewall enables comprehensive fine-grained access control based on status detection and implements port-based virtual switch access control and logical isolation between regions of virtual systems. It also helps identify and intercept various flood attacks.

Host intrusion prevention
Based on deep packet inspection (DPI), the host security protection system checks all communications that do not comply with protocols to protect the system against possible application-layer attacks, SQL injection, cross-site program code rewriting, and vulnerability attacks. In addition, intelligent defense rules are used to provide zero-day protection. The system can detect abnormal and infected protocol data code to prevent attacks by unknown vulnerabilities.

Virtual patch protection
With the emergence of new vulnerabilities, carriers are struggling to install patches. It may be a very rocky time for them to go through the maintenance period when important security patches are being installed. In addition, OS and application vendors do not provide patches for vulnerabilities of some versions or the patch release time lags behind. If there are no sufficient IT personnel and time, the system is vulnerable to risks during the review, test, and installation of official patches.

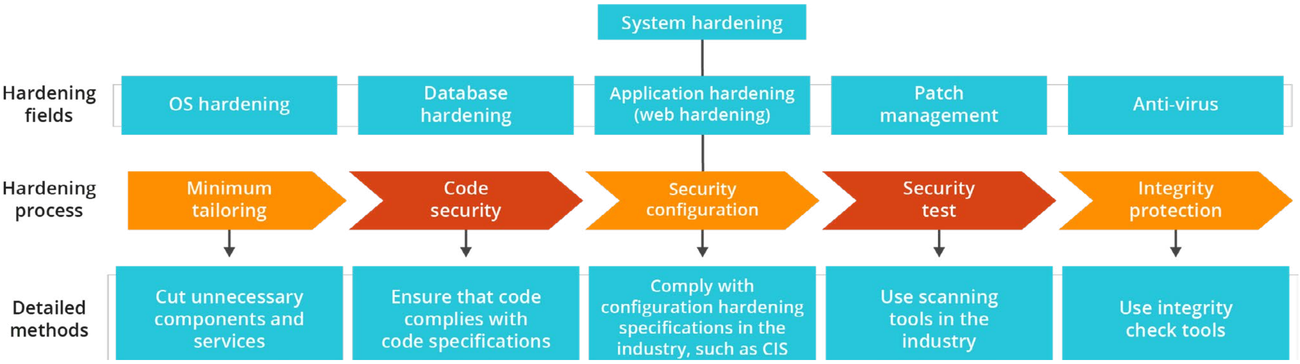
The host security protection system adopts the virtual patch technology to solve patch-specific issues. It evaluates the virtual host system through the interface of the virtual system and automatically repairs vulnerabilities for each virtual host. This technology helps block loophole attacks before the OS is patched, saving a lot of time for IT personnel.

A.2.3.2 Host Security Hardening

Vulnerabilities, insecure user accounts or passwords, improper configurations and operations, and insecure services bring potential security threats in the form of viruses, horses, and worms. To reduce these risks, security configurations are required. 80% to 90% of known security risks can be eliminated by basic security configurations. In addition, security hardening is more effective than anti-virus software or patches.

This project formulates a series of uniform security regulations for developing and testing OSs, databases, and web applications. System security customization and check tools are also provided to meet industry CIS benchmarks.

Figure A-2 System hardening


System hardening
Hardening fields
OS hardening
Database hardening
Application hardening (web hardening)
Patch management
Anti-virus
Hardening process
Minimum tailoring
Code security
Security configuration
Security test
Integrity protection
Detailed methods
Cut unnecessary components and services
Ensure that code complies with code specifications
Comply with configuration hardening specifications in the industry, such as CIS
Use scanning tools in the industry
Use integrity check tools

The following OS hardening methods are provided to prevent hacker attacks through vulnerabilities:

- Disable unused communication ports.
- Disable unnecessary service processes.
- Restrict system access permission.
- Strictly control rights of accounts.
- Enable the security log audit function.

Software design defects cause many loophole risks. Regular installation of system security patches can fix system loophole risks and prevent viruses, worms, and hackers from using these loophole risks to attack the system. This is an effective way to fix system loophole risks.

A.2.4 Application Security

A.2.4.1 Application Security Protection

An application security protection scheme has been designed for the SaaS platform BES/IES based on the service attributes of the BES/IES application system to effectively defend the BES/IES application system against security threats caused by malicious code or virus access to the web application, malicious code or virus input in to external files, and application code bugs.

B2B cloud applications carry carriers' services and core operation services. Therefore, measures must be taken to avoid service interruptions caused by heavy load or single point of failure (SPOF). To ensure normal running of services, security protection must be performed on the application systems. Detailed security protection designs are as follows:

WAF

The security protection products deployed at the network layer can defend against most attacks generated by tools but cannot handle attacks at the application layer. To defend against severe web attacks, two web application firewalls (WAFs) are deployed in bypass mode on the core switch of the B2B cloud. Policy-based routing is used to divert the traffic destined for the web server to the WAFs to protect the web application layer.

The WAF provides two engines: rule-based detection and active defense.

- The rule-based detection engine provides intensive and detailed protection for the application system against a great number of known attacks, including SQL injection, cross-site scripting, OS command injection, remote file inclusion, local file inclusion, directory traversal, HTTP violation, and WebShell attacks.
- The active defense engine provides self-learning modeling to protect web sites. For the URI and POST forms, the active defense engine can learn the number of parameters as well as the type and length of each parameter. After learning of one to two weeks, a forwarding model for all dynamic pages of the target server can be established. In this case, if the proactive defense policy is applied, all parameters that do not comply with the forwarding model are blocked, which effectively defends against unknown threats and zero-day attacks.

Load balance system

For the B2B cloud that carries core systems and services for carriers such as convergent billing, customer relationship management, and operation support, service interruptions caused by SPOFs need to be avoided. Within a given time window a great number of normal access requests may be initiated and a single host may fail to handle massive volumes of concurrent requests quickly, reliably, and securely.

In this project, application load balancers are deployed on the core switch in bypass mode to provide flow control at layers L2 through L7. This solution effectively addresses the problems of high data traffic and network overload and prevents data traffic loss caused by SPOFs.

The load balancer supports multiple discontinuous load balance algorithms such as polling, weighted round robin (WRR), minimum connection, and shortest response time as well as multiple continuous load balance algorithms such as IP keepalive, persistent cookie, QoS cookie, QoS URL, and QoS Hostname. It adopts various application acceleration modes (including TCP connection reuse, hardware SSL acceleration, high-speed data cache, HTTP compression, asymmetric TCP acceleration, and high-speed protocol stack technology) to efficiently and rapidly allocate application requests to appropriate servers and conducts health check to monitor the server status in real time.

A.2.4.2 Identity and Access Management

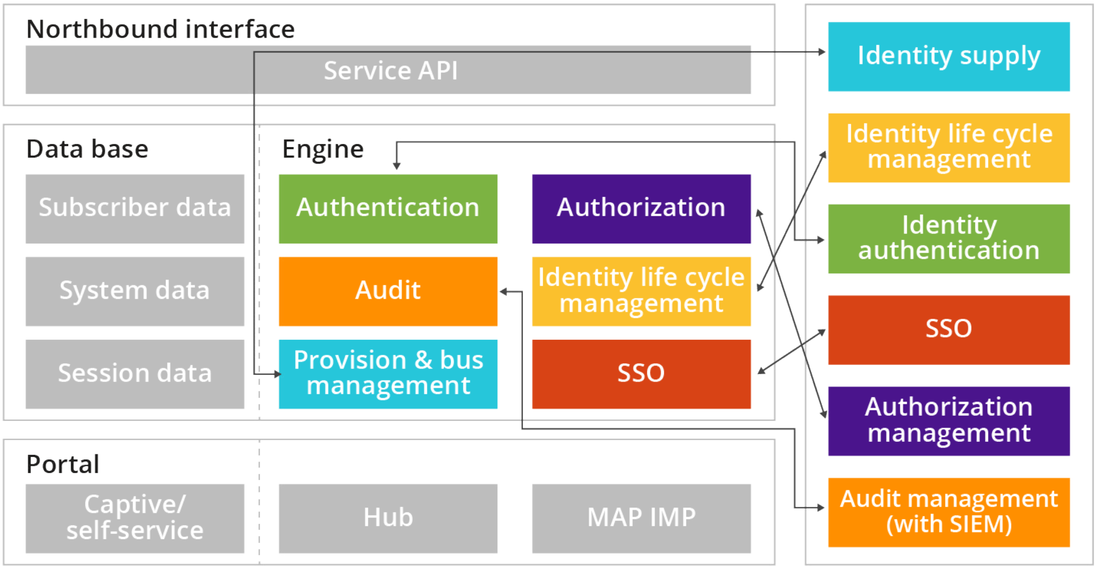
To implement unified IAM for the network management system on the PaaS/IaaS, this solution provides an identity and access management system to enable unified registration, authentication, identification, read/write authorization, and life cycle management for internal and external user identities.

The following figure shows the overall architecture of IAM.

- North API: Serves as the IT interface adapter of IAM and interconnects with OA system and other VAS systems of users.
- Database: Stores the account data, user data, identity information, system management data, and log files of IAM of various types.
- Engine: Serves as the core module of IAM and implements authentication, Single Sign On (SSO), authorization management, life cycle management of user identities, and audit management (only simple log audit for interface adaptation with SIEM).
- Portal: Serves as the web page of IAM and is responsible for allowing users to log in to IAM and for transferring information to other internal modules of IAM.

In Southbound Interface, HUB provides multiple interface access modes such as RADIUS or Diameter. It serves as the CT-side interface adapter of IAM to interconnect with NEs such as the BRAS, AC, and WAG. IMP serves as the protocol conversion module between IAM and HLR to convert the MAP protocol into the Diameter protocol.

Figure A-3 Identity and access management



A.2.5 Data Security

Key or sensitive data (static and dynamic) must be protected and risks of data leakage and damage must be minimized to ensure the reliability and security of service systems on the cloud. Data isolation and secure sharing between different service systems must be ensured. Data security is enhanced by using various technologies, such as transmission security, data storage security, and disaster recovery (DR). The database audit system is used to audit the behavior of accessing database servers.

A.2.5.1 Transmission Security

Data transmission may be interrupted and data may be replicated, modified, forged, intercepted, or monitored during transmission. Therefore, it is necessary to ensure the integrity, confidentiality, and validity of data during network transmission. This solution ensures transmission security as follows:

- When accessing a management system, administrators browse data-sensitive pages using Hypertext Transfer Protocol Secure (HTTPS) and data transfer channels are encrypted using Secure Socket Layer (SSL).
- When users log in to VMs using Virtual Network Computing (VNC), SSH and RDP are adopted.
- When users access the DC for remote O&M, the SSL VPN mode is used.

Login using encryption protocols helps achieve encrypted transmission and identity authentication, ensures that data is sent to the correct client and server, and prevents data theft during transmission, ensuring data integrity.

A.2.5.2 Database Audit

The database audit system mainly provides the following functions:

- Static audit
- Real-time monitoring and risk control
- Real-time audit
- Bidirectional audit
- Audit rules
- Behavior search
- Association audit
- Audit reports
- Security event review
- Audit object management
- Warning management

System configuration management
The database audit system connects to the core switch in bypass mode. Data flow mirroring is used to audit all database access traffic.

The database audit system helps detect database violation operations. It collects, analyzes, and identifies network data, monitors all network database access operations in real time, and supports user-defined content keywords, user-defined protocol monitoring, and user-defined port monitoring to deliver content monitoring and identification in operations.

In response to unauthorized database access, the database audit system can report alarms in various forms in a timely manner and restore the entire process of unauthorized access. This helps accurately trace and locate security events throughout the whole process and ensures security of the database system. With the capabilities of integrated analysis and comprehensive and systematic reporting and analysis, the database audit system provides users with comprehensive database access security analysis reports.

A.2.6 Security Management

To implement security management on devices and systems on the entire network, a security O&M management zone is designed for unified security management on devices and systems of the B2B cloud. A complete system for O&M audit and vulnerability management has been established. The B2B cloud needs to comprehensively analyze the security situation of the cloud platforms (SaaS, PaaS, and IaaS), virtualization, networks, data, applications, and identity access rights. Currently, SIEM tools are commonly used for security situation awareness. To use SIEM tools, perform investigations and analysis, formulate use cases based on the overall technical architecture of SIEM tools, and perform integrated deployment on the B2B cloud platform according to use cases.

A.2.6.1 SIEM

In the B2B cloud security system a great number of security devices have been deployed, covering border network security, virtualization security, host security, application security, data security, and management security. However, there is a lack of a unified monitoring and management platform. As a result, independent security products and data bring great management burdens to management personnel and cause low monitoring and management efficiency.

To address the problems above, this solution provides the SIEM platform, which integrates and centrally manages existing security resources in the cloud platform and implements closed-loop management of security warning, protection, and response through a combination of association analysis and intelligent response. In addition, it helps cloud service providers learn the security situation of the cloud platform in a timely and accurate manner.

Intelligent collection
Continuous connection check, integrity check, and customized cache ensure that the platform can receive all data and can monitor the entire transmission link. Filtering and aggregation functions can be configured to eliminate irrelevant data and combine duplicate device logs. The powerful data compression function saves bandwidth.

Standardized logs
Standardized logs include the following: security event logs (attacks, intrusion, and exceptions), behavior event logs (internal control and violation), vulnerability scanning logs (vulnerabilities and loopholes), and status monitoring logs (availability, performance, and status).
The description about a security event includes the following information: event target object, event behavior, event feature, event result, attack type, and detection device.

Log parsing
Parsing rules are activated only when the corresponding logs are received. Unrecognized logs are watermarked. Multi-level parsing and dynamic planning algorithms are used to flexibly process non-parsed logs. Multiple parsing methods (such as the regular expression, separator, and MIB information mapping configuration) are supported. Log parsing performance is irrelevant to the number of connected log devices.

Association analysis
The system association engine adopts in-memory computing to ensure high-efficiency and real-time performance in event analysis. Compared with the log audit function that provides association analysis through SQL query, the system association engine is superior in terms of the analysis speed, analysis dimension, flexibility, and resistance to I/O compression. The SIEM platform supports standardized association rules, complex association based on logical expressions, and association based on almost all fields of common events. The platform features strong customization and time sequence tolerance.

Security event standards
The SIEM platform adopts the universal standard security event normalization format and classification architecture and can process the following logs in a standard manner: security event logs (attacks, intrusion, and exceptions), behavior event logs (internal control and violation), vulnerability scanning logs (vulnerabilities and loopholes), and status monitoring logs (availability, performance, and status).

The description about a security event includes the following information: event target object, event behavior, event feature, event result, attack type, and detection device.

A.2.6.2 O&M Bastion Host

The B2B cloud needs to provide centralized and unified access control policies, which can perform identity authentication and authorization, audit operation behavior, and record user operations to prevent adverse impact on the production system due to incorrect operations, permission abuse, and misoperations of O&M personnel. The operation records can be used for troubleshooting and fault recovery.

The O&M bastion host is deployed in the management area to centrally control and manage accounts, authentication, authorization, and audit for various resources in the ITC, including the cloud platform, security products, network devices, servers, and storage resources. The system provides O&M rights management and comprehensive log audit and supports graphic terminals, character terminals, database applications, and file transmission. It also provides real-time video surveillance and screen recording to block high-risk operations, such as deletion and restart, in a timely manner. The bastion host can be deployed to audit O&M logs.

All resources in the B2B cloud will be exposed when the administrator account is stolen. This solution provides a two-factor authentication system, which interconnects with bastion hosts to implement two-factor strong authentication by use of the mobile phone tokens or hardware tokens and passwords, ensuring the security of O&M personnel accounts of O&M bastion hosts.

A.2.6.3 Vulnerability Scanning System

The vulnerability scanning system is deployed on the cloud platform to detect security vulnerabilities of specified VMs or physical machines by means of scanning and provide timely security protection.

The vulnerability scanning system cooperates with the firewall and intrusion detection system. By scanning the network, the platform administrator can learn the security settings and running application services, detect security vulnerabilities in a timely manner, and objectively evaluate the network risk level.

Based on the scanning result, the platform administrator can correct network security vulnerabilities and error settings in the system to defend against hacker attacks.

Vulnerability scanning is an active preventive measure, which can effectively prevent hacker attacks.

Potential risk scanning
The vulnerability scanning system scans network devices, OSs, and databases, identifies related network security vulnerabilities and weak points of the tested system, provides detailed monitoring reports, and offers corresponding measures and security suggestions based on the detected potential network security risks.

Vulnerability analysis
The vulnerability scanning system uses the authoritative risk assessment model in the industry to assess the risks of the target system.

Vulnerability repair
The vulnerability scanning system provides a vulnerability fixing solution and offers secondary development interfaces for third-party patch management products, assisting platform administrators in rectifying vulnerabilities in a timely and efficient manner.

Vulnerability audit
The vulnerability scanning system urges related security management personnel to repair vulnerabilities through email and starts a scheduled scanning task to audit the vulnerabilities.

Warning upon risks
The vulnerability scanning system classifies the detected risks and vulnerabilities according to the risk level, sends different warnings to the platform administrator, submits the risk assessment report, and provides a detailed solution.

Policy management
The vulnerability scanning system predefines various scanning policies. Administrators can select corresponding detection scripts after loading corresponding scanning policies.

Statistical analysis
The vulnerability scanning system analyzes the scanning results in the form of reports and graphics to facilitate security performance evaluation and check on users. You can pre-define the display format of analysis results and customize the items for analysis.

A.2.6.4 Web Vulnerability Scanning

The web vulnerability scanning system is deployed on the B2B cloud platform to detect security vulnerabilities of specific web servers by means of scanning. It helps detect vulnerabilities of the web application system in time and provides timely security protection.

The web vulnerability scanning system helps detect vulnerabilities of web applications in the following aspects: SQL injection, command injection, CRLF injection, LDAP injection, XSS cross-site script, path traversal, information leakage, URL redirection, file inclusion, application program, and file uploading,

The following detection functions are adopted: Trojan horse detection on networks, detection of dark chains in web pages, verification on detected web application vulnerabilities, website security monitoring (involves Trojan horse detection, sensitive word monitoring, and application vulnerability monitoring), and website service survival availability detection.