

SAP

Security White Paper

Issue 01
Date 2018-11-30



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

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

Trademarks and Permissions



HUAWEI and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Contents

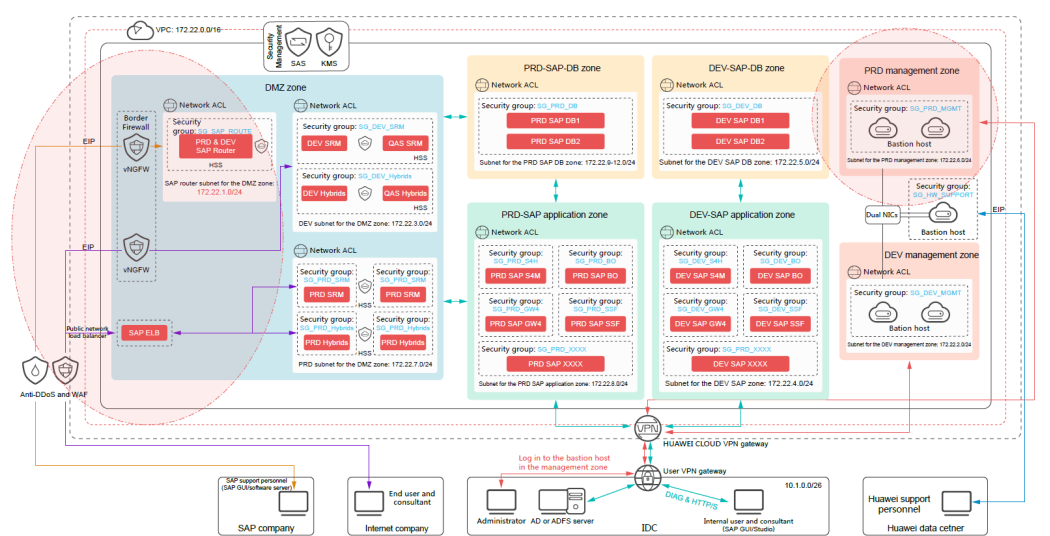
1 Production Environment Security Solution.....	1
1.1 Network Isolation and Access Control.....	1
1.2 Network Border Security.....	14
1.2.1 Service Border.....	14
1.2.2 O&M Border.....	19
1.2.3 Border Between the Production Environment and the Development and Test Environment.....	20
1.3 Security Management.....	24
1.4 Host Security.....	25
2 Development and Test Environment Security Solution.....	26
2.1 Network Isolation and Access Control.....	26
2.2 Network Border Security.....	32
2.2.1 Border Between the Development and Test Environment and the Production Environment.....	33
2.2.2 Service Border.....	35
2.2.3 O&M Border.....	39
2.3 Security Management.....	42
2.4 Host Security.....	43
3 Huawei Technical Support Channel Security Solution.....	44
4 Other Security Solutions.....	46
5 Security Solution Mapping Table.....	47
A Change History.....	50

1 Production Environment Security Solution

1.1 Network Isolation and Access Control

Figure 1-1 shows the SAP production environment security solution.

Figure 1-1 Production environment security solution



After service characteristics and enterprise security practices are taken into consideration, it is recommended that you divide the cloud-based system (production environment and development and test environment) into zones of different security levels, including the management, application, SAP DB, and demilitarized zone (DMZ) zones. The zones are isolated from each other using subnets.

The DMZ zone is special because it interacts with the Internet and is shared by the production system and the development and test system. It is recommended that you configure specific security policies for each zone to control inter-zone access and access from external networks.

- **DMZ zone:** This zone directly interconnects with the Internet. All service system access requests from public network users and SAP support personnel are processed in the zone. The DMZ zone has a low security level and a high security risk.
- **Application zones:** SAP applications are deployed in the zones for integrated data center (IDC) users (enterprise internal users) to use and for interconnection with systems including the AD server. The zones have a higher security level than the DMZ zone.
- **SAP DB zones:** SAP databases are deployed in the zones. The zones allow limited access from the internal network application and management zones and have the highest security level.
- **Management zones:** Operations and maintenance (O&M) bastion hosts are deployed in the zones. The zones are the intermediary areas through which system O&M personnel (in an enterprise) manage, operate, and maintain Elastic Cloud Servers (ECs) and systems in other zones.

Configure specific security policies for each zone using security groups and network access control lists (ACLs) to control inter-zone access and access from external networks. Configure security policies according to the "deny by default" and "minimum permission" principles, allowing only access from specified sources to required IP addresses and ports.

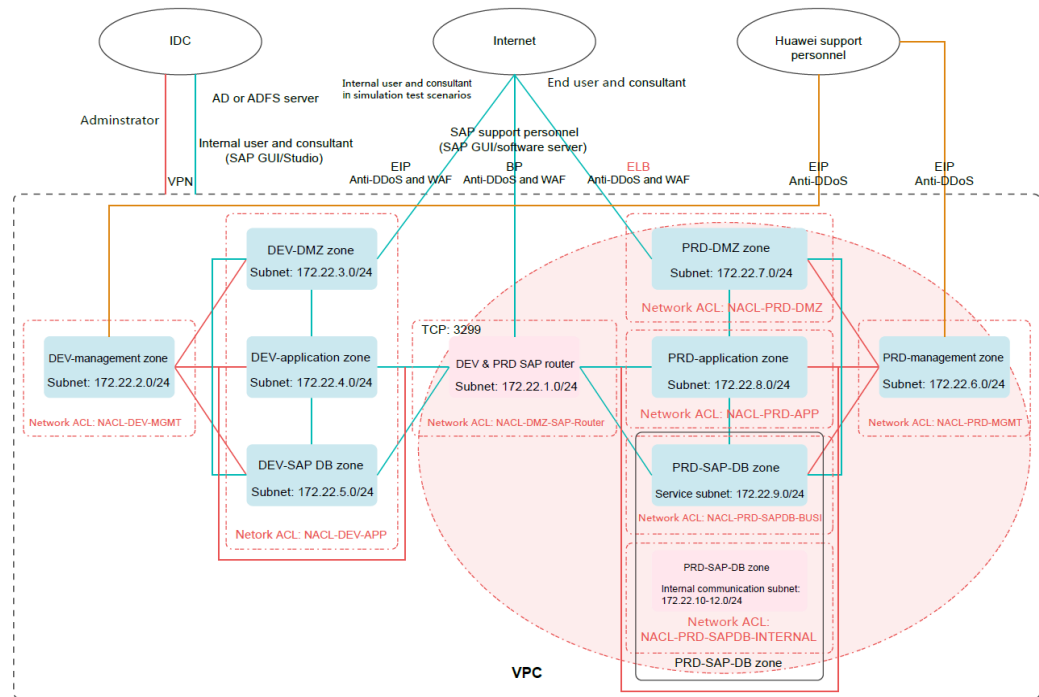
For example, only administrators in an enterprise are allowed to access the remote access port of the bastion host in management zones. Common users and internal systems are not allowed to access the port. Common users in an enterprise should be allowed to access only SAP service ports in internal network application zones. Network ACLs are used to deny traffic between all zones (isolated using subnets) in the system by default. Necessary services must be allowed by adding ACL rules.

This section describes the access control policies between the zones in a production environment. This section also provides suggestions on network ACL and security group configuration according to the "deny by default" and "minimum permission" principles. (The development and test environment is special. To ensure that IDC users can efficiently access the internal resources and that networking is flexible, looser access control policies are configured for the development and test environment than for the production environment. For details, see [Development and Test Environment Security Solution](#).)

Security Policies

As shown in [Figure 1-2](#), the production environment has eight subnets. It is recommended that you create an independent network ACL for each subnet. These network ACLs include **NACL-DMZ-SAP-Router**, **NACL-PRD-DMZ**, **NACL-PRD-APP**, **NACL-PRD-SAPDB-BUSI**, **NACL-PRD-SAPDB-INTERNAL**, and **NACL-PRD-MGMT**.

Figure 1-2 Subnet and network ACL layout in the production environment



Network ACL **NAACL-DMZ-SAP-Router** is associated with the subnet for the DEV&PRD-SAP router shared by the production environment and the development and test environment. Configure outbound rules of network ACL **NAACL-DMZ-SAP-Router** to allow access to specified service ports of the SAP application zone and SAP-DB zone in the production environment through the SAP router. Configure inbound rules of network ACL **NAACL-DMZ-SAP-Router** to allow access to management ports (such as port 22) of servers in the subnet through the bastion host in the management zone.

NOTE

IP addresses and ports in this section are only used as examples. If there are other management ports, you can add ACL rules as required. This section describes only network ACLs for the production environment.

Table 1-1 Outbound rules of network ACL **NACL-DMZ-SAP-Router**

Rule	Destination IP Address	Protocol	Destination Port	Allow or Deny	Description
For the PRD-application zone	172.22.8.0/24	TCP	234	Allow	Allows the SAP-Router server to access service port 234 of servers in the PRD-application zone.
For the PRD-SAP-DB zone	172.22.9.0/24	TCP	345	Allow	Allows the SAP-Router server to access service port 345 of servers in the PRD-SAP-DB zone.
*	0.0.0.0/0	Any	Any	Deny	Denies all inbound traffic that is not processed based on preset rules.

Table 1-2 Inbound rules of network ACL **NACL-DMZ-SAP-Router**

Rule	Source IP Address	Protocol	Destination Port	Allow or Deny	Description
For the PRD-management zone	172.22.6.0/24	TCP	22	Allow	Allows the bastion host in the management zone in the production environment to access the SSH ports of servers in the zone.
*	0.0.0.0/0	Any	Any	Deny	Denies all inbound traffic that is not processed based on preset rules.

Network ACL **NACL-PRD-MGMT** is associated with the subnet for the PRD-management zone in the production environment. Configure outbound rules of network ACL **NACL-PRD-MGMT** to allow access to management ports (such as port 22) of servers in other zones through the bastion host in the management zone and deny access from other zones to the bastion host in the management zone.

Table 1-3 Outbound rules of network ACL **NACL-PRD-MGMT**

Rule	Destination IP Address	Protocol	Destination Port	Allow or Deny	Description
For the PRD-DMZ zone	172.22.7.0/24	TCP	22	Allow	Allows the bastion host in the management zone in the production environment to access the SSH ports of servers in the PRD-DMZ zone.
For the PRD-application zone	172.22.8.0/24	TCP	22	Allow	Allows the bastion host in the management zone in the production environment to access the SSH ports of servers in the PRD-application zone.
For the PRD-SAP-DB zone	172.22.9.0/24	TCP	22	Allow	Allows the bastion host in the management zone in the production environment to access the SSH ports of servers in the PRD-SAP-DB zone.

Rule	Destination IP Address	Protocol	Destination Port	Allow or Deny	Description
For the DEV&PRD SAP router	172.22.1.0/24	TCP	22	Allow	Allows the bastion host in the management zone in the production environment to access the SSH port of the DEV&PRD-SAP-Router server.
*	0.0.0.0/0	Any	Any	Deny	Denies all outbound traffic that is not processed based on preset rules.

Table 1-4 Inbound rules of network ACL **NACL-PRD-MGMT**

Rule	Source IP Address	Protocol	Destination Port	Allow or Deny	Description
*	0.0.0.0/0	Any	Any	Deny	Denies all inbound traffic that is not processed based on preset rules.

Network ACL **NACL-PRD-DMZ** is associated with the subnet for the PRD-DMZ zone in the production environment. Configure inbound rules of network ACL **NACL-PRD-DMZ** to allow access to management ports (such as port 22) of servers in the zone through the bastion host in the management zone. Configure outbound rules of network ACL **NACL-PRD-DMZ** to allow access to required service ports in the PRD-application zone and PRD-SAP-DB zone through this subnet.

Table 1-5 Outbound rules of network ACL **NACL-PRD-DMZ**

Rule	Destination IP Address	Protocol	Destination Port	Allow or Deny	Description
For the PRD-application zone	172.22.8.0/24	TCP	8080	Allow	Allows hosts in the DMZ zone in the production environment to access service port 8080 of servers in the PRD-application zone.
For the PRD-application zone	172.22.8.0/24	TCP	8443	Allow	Allows hosts in the DMZ zone in the production environment to access service port 8443 of servers in the PRD-application zone.
For the PRD-SAP-DB zone	172.22.9.0/24	TCP	345	Allow	Allows hosts in the DMZ zone in the production environment to access service port 345 of servers in the PRD-SAP-DB zone.

Rule	Destination IP Address	Protocol	Destination Port	Allow or Deny	Description
*	0.0.0.0/0	Any	Any	Deny	Denies all outbound traffic that is not processed based on preset rules.

Table 1-6 Inbound rules of network ACL **NACL-PRD-DMZ**

Rule	Source IP Address	Protocol	Destination Port	Allow or Deny	Description
For the PRD-management zone	172.22.6.0/24	TCP	22	Allow	Allows the bastion host in the management zone in the production environment to access the SSH ports of servers in the zone.
*	0.0.0.0/0	Any	Any	Deny	Denies all inbound traffic that is not processed based on preset rules.

Network ACL **NACL-PRD-APP** is associated with the subnet for the PRD-application zone in the production environment. Configure inbound rules of network ACL **NACL-PRD-APP** to allow access to management ports (such as port 22) of servers in the zone through the bastion host in the management zone and allow access to service ports of servers in this subnet through the SAP router and PRD-DMZ zone. Configure outbound rules of network ACL **NACL-PRD-APP** to allow access to required service ports in the PRD-SAP-DB zone through this subnet.

Table 1-7 Outbound rules of network ACL **NACL-PRD-APP**

Rule	Destination IP Address	Protocol	Destination Port	Allow or Deny	Description
For the PRD-SAP-DB zone	172.22.9.0/24	TCP	345	Allow	Allows hosts in the application zone in the production environment to access service port 345 of servers in the PRD-SAP-DB zone.
*	0.0.0.0/0	Any	Any	Deny	Denies all outbound traffic that is not processed based on preset rules.

Table 1-8 Inbound rules of network ACL **NACL-PRD-APP**

Rule	Source IP Address	Protocol	Destination Port	Allow or Deny	Description
For the PRD-management zone	172.22.6.0/24	TCP	22	Allow	Allows the bastion host in the management zone in the production environment to access the SSH ports of servers in the zone.
For the DEV&PRD SAP router	172.22.1.0/24	TCP	234	Allow	Allows the SAP-Router server to access service port 234 of servers in the PRD-application zone.
For the PRD-DMZ zone	172.22.7.0/24	TCP	8080	Allow	Allows hosts in the DMZ zone in the production environment to access service port 8080 of servers in the PRD-application zone.

Rule	Source IP Address	Protocol	Destination Port	Allow or Deny	Description
For the PRD-DMZ zone	172.22.7.0/24	TCP	8443	Allow	Allows hosts in the DMZ zone in the production environment to access service port 8443 of servers in the PRD-application zone.
*	0.0.0.0/0	Any	Any	Deny	Denies all inbound traffic that is not processed based on preset rules.

Network ACL **NACL-PRD-SAPDB-BUSI** is associated with the service subnet (172.22.9.0/24) for the PRD-SAP-DB zone in the production environment. Configure inbound rules of network ACL **NACL-PRD-SAPDB-BUSI** to allow access to management ports (such as port 22) of servers in the zone through the bastion host in the management zone and allow access to service ports of servers in this subnet through the SAP router, PRD-DMZ zone, and PRD-application zone.

Table 1-9 Outbound rules of network ACL **NACL-PRD-SAPDB-BUSI**

Rule	Destination IP Address	Protocol	Destination Port	Allow or Deny	Description
*	0.0.0.0/0	Any	Any	Deny	Denies all outbound traffic that is not processed based on preset rules.

Table 1-10 Inbound rules of network ACL **NACL-PRD-SAPDB-BUSI**

Rule	Source IP Address	Protocol	Destination Port	Allow or Deny	Description
For the PRD-management zone	172.22.6.0/24	TCP	22	Allow	Allows the bastion host in the management zone in the production environment to access the SSH ports of servers in the zone.
For the DEV&PRD SAP router	172.22.1.0/24	TCP	345	Allow	Allows the SAP-Router server to access service port 345 of servers in the PRD-SAP-DB zone.
For the PRD-DMZ zone	172.22.7.0/24	TCP	345	Allow	Allows hosts in the DMZ zone in the production environment to access service port 345 of servers in the PRD-SAP-DB zone.
For the PRD-application zone	172.22.8.0/24	TCP	345	Allow	Allows hosts in the application zone in the production environment to access service port 345 of servers in the PRD-SAP-DB zone.
*	0.0.0.0/0	Any	Any	Deny	Denies all inbound traffic that is not processed based on preset rules.

Network ACL **NACL-PRD-SAPDB-INTERNAL** is associated with the internal communication subnet (172.22.10-12.0/24) for the PRD-SAP-DB zone in the production environment. The internal communication subnet is used for only internal communication within a subnet and requires a network ACL to deny all inbound and outbound traffic.

Table 1-11 Outbound rules of network ACL **NACL-PRD-SAPDB-INTERNAL**

Rule	Destination IP Address	Protocol	Destination Port	Allow or Deny	Description
*	0.0.0.0/0	Any	Any	Deny	Denies all outbound traffic that is not processed based on preset rules.

Table 1-12 Inbound rules of network ACL **NACL-PRD-SAPDB-INTERNAL**

Rule	Source IP Address	Protocol	Destination Port	Allow or Deny	Description
*	0.0.0.0/0	Any	Any	Deny	Denies all inbound traffic that is not processed based on preset rules.

Security groups, such as **SG_PRD_MGMT** and **SG_PRD_DB** (which do not interact with the public network), are associated with Elastic Cloud Servers (ECSs) in the subnets in the production environment. The security groups must be configured according to the "minimum permission" principle so that a minimum number of ECS ports are opened. **Figure 1-3** shows an example for configuring the security groups. You need to configure them based on your own ports. Network ACLs are used for IP address access control. Other security groups in the production environment (for details, see **Figure 1-1**) that do not interact with the public network can be configured similarly.

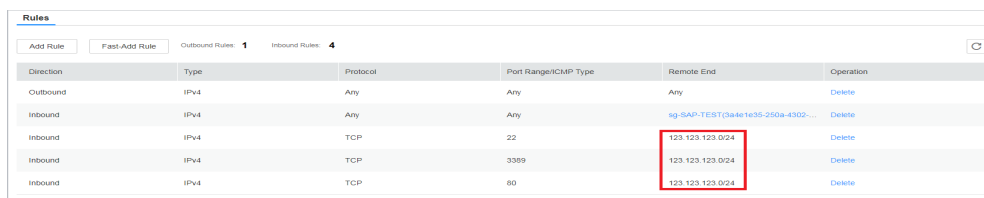
Figure 1-3 Security group rule example

Direction	Type	Protocol	Port Range/ICMP Type	Remote End	Operation
Outbound	IPv4	Any	Any	Any	Delete
Inbound	IPv4	Any	Any	SG_MGMT_TEST_DEV047c996-ar...	Delete
Inbound	IPv4	TCP	22	0.0.0.0/0	Delete
Inbound	IPv4	TCP	3389	0.0.0.0/0	Delete
Inbound	IPv4	TCP	80	0.0.0.0/0	Delete
Inbound	IPv4	TCP	443	0.0.0.0/0	Delete
Inbound	IPv4	TCP	3306	0.0.0.0/0	Delete

Security groups, such as **SG_SAP_ROUTER** (which interacts with the public network), are associated with ECSs in the subnets in the production environment. The security groups must be configured according to the "minimum permission"

principle so that a minimum number of ECS ports and source IP addresses are opened. If the public IP address is fixed, you can refer to [Figure 1-3](#) for configuring the security groups. You need to configure them based on your own ports.

Figure 1-4 Security group rule example

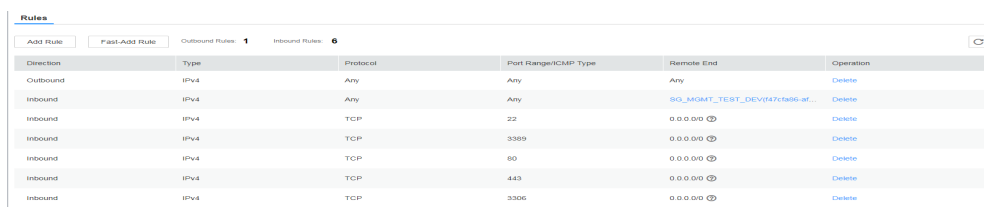


Direction	Type	Protocol	Port Range/ICMP Type	Remote End	Operation
Outbound	IPv4	Any	Any	Any	Delete
Inbound	IPv4	Any	Any	sg-SAP-TEST(3a4e1e35-250a-4302-...	Delete
Inbound	IPv4	TCP	22	123.123.123.0/24	Delete
Inbound	IPv4	TCP	3389	123.123.123.0/24	Delete
Inbound	IPv4	TCP	80	123.123.123.0/24	Delete

If the public IP address is not fixed, you can create a security group rule to allow access from a specified public source IP address to meet your service requirements (such as the simulation test or technical support) and then delete the rule when it is not required.

Security groups, such as **SG_PRD_SRM** and **SG_PRD_Hybrids** (which interact with the public network), need to open their service ports to the entire network. [Figure 1-5](#) shows an example for configuring the security groups. You need to configure them based on your own ports. Network ACLs are used for source IP address access control on management ports, such as ports 22 and 3389, so that only access through the bastion host in the management zone is allowed. Service ports, such as port 80, are opened to the entire Internet and will not be configured with source IP address access control. It is recommended that you use proper security products to protect these ports. For details, see [Service Border](#).

Figure 1-5 Security group rule example



Direction	Type	Protocol	Port Range/ICMP Type	Remote End	Operation
Outbound	IPv4	Any	Any	Any	Delete
Inbound	IPv4	Any	Any	sg_MGMT_TEST_DEV(47cfa86-af...	Delete
Inbound	IPv4	TCP	22	0.0.0.0/0	Delete
Inbound	IPv4	TCP	3389	0.0.0.0/0	Delete
Inbound	IPv4	TCP	80	0.0.0.0/0	Delete
Inbound	IPv4	TCP	443	0.0.0.0/0	Delete
Inbound	IPv4	TCP	3306	0.0.0.0/0	Delete

1.2 Network Border Security

1.2.1 Service Border

The production environment needs to provide services for the public network and interconnect with other IDCs. Therefore, set up virtual private network (VPN) channels between the production environment and enterprise intranets (IDCs).

Configure access control policies between the cloud and the on-premises system and between the cloud and the Internet.

Take border protection measures in the DMZ, internal network application, and management zones because they can be accessed from external networks.

VPN

Static connections are usually used by enterprise intranets. When security and latency are taken into consideration, the recommended priority is as follows: Direct Connect > Internet Protocol security virtual private network (IPsec VPN) > virtual private network over Secure Sockets Layer (SSL VPN).

NOTE

Currently, the HUAWEI CLOUD VPN service supports only Direct Connect and IPsec VPN. If you need to use SSL VPN, you can deploy it using a third-party image.

Security Policies

The production environment needs to communicate with enterprise intranets and allow access from the Internet. Therefore, network ACLs are used for access control.

Network ACL **NACL-DMZ-SAP-Router** is associated with the subnet for the DEV&PRD SAP router in the production environment. Configure inbound rules of network ACL **NACL-DMZ-SAP-Router** to strictly control access from the Internet, allowing access from only specified external network segments to specified IP addresses and ports.

NOTE

IP addresses and ports in this section are only used as examples. If the public IP address is not fixed, you can create an ACL rule to allow access from a specified public source IP address to meet your service requirements (such as technical support) and then delete the rule when it is not required. If there are other services, you can add ACL rules as required.

Table 1-13 Outbound rules of network ACL **NACL-DMZ-SAP-Router**

Rule	Destination IP Address	Protocol	Destination Port	Allow or Deny	Description
*	0.0.0.0/0	Any	Any	Deny	Denies all inbound traffic that is not processed based on preset rules.

Table 1-14 Inbound rules of network ACL **NACL-DMZ-SAP-Router**

Rule	Source IP Address	Protocol	Destination Port	Allow or Deny	Description
For SAP technical support personnel (SAP GUI or software server)	123.123.123.0/24	TCP	3299	Allow	Allows Internet SAP technical support personnel (SAP GUI or software server) from specified source IP addresses to access the DEV&PRD SAP router and then access backend services.
*	0.0.0.0/0	Any	Any	Deny	Denies all inbound traffic that is not processed based on preset rules.

Network ACL **NACL-PRD-DMZ** is associated with the subnet for the PRD-DMZ zone in the production environment. Configure inbound rules of network ACL **NACL-PRD-DMZ** to strictly control access from the Internet and IDCs, allowing access from external networks to only specified IP addresses and ports in the production environment.

Table 1-15 Outbound rules of network ACL **NACL-PRD-DMZ**

Rule	Destination IP Address	Protocol	Destination port	Allow or Deny	Description
For AD or ADFS servers	IP address of an AD or ADFS network in the IDC	TCP	AD or ADF port	Allow	Allows access to AD or ADFS servers in IDCs.
*	0.0.0.0/0	Any	Any	Deny	Denies all outbound traffic that is not processed based on preset rules.

Table 1-16 Inbound rules of network ACL **NACL-PRD-DMZ**

Rule	Source IP Address	Protocol	Destination Port	Allow or Deny	Description
For Internet users	0.0.0.0/0	TCP	80	Allow	Allows Internet users and IDC users to access web services in the production environment.
For Internet users	0.0.0.0/0	TCP	443	Allow	Allows Internet users and IDC users to access web services in the production environment.
*	0.0.0.0/0	Any	Any	Deny	Denies all inbound traffic that is not processed based on preset rules.

Network ACL **NACL-PRD-APP** is associated with the subnet for the PRD-application zone in the production environment. Configure inbound rules of network ACL **NACL-PRD-APP** to strictly control access from IDCs, allowing access from only specified IDC networks to specified IP addresses and ports in the production environment. Configure outbound rules of network ACL **NACL-PRD-APP** to strictly control access to IDCs, allowing access from the production environment to only specified IDC networks.

Table 1-17 Outbound rules of network ACL **NACL-PRD-APP**

Rule	Destination IP Address	Protocol	Destination Port	Allow or Deny	Description
For AD or ADFS servers	IP address of an AD or ADFS network in the IDC	TCP	AD or ADF port	Allow	Allows access to AD or ADFS servers in IDCs.
*	0.0.0.0/0	Any	Any	Deny	Denies all outbound traffic that is not processed based on preset rules.

Table 1-18 Inbound rules of network ACL **NACL-PRD-APP**

Rule	Source IP Address	Protocol	Destination Port	Allow or Deny	Description
For IDC users and consultants	A subnet (subnet b) in an IDC	TCP	8080	Allow	Allows internal users and consultants in a subnet (subnet b) in an IDC to access service port 8080 in the application zone in the production environment.
For IDC users and consultants	A subnet (subnet b) in an IDC	TCP	8443	Allow	Allows internal users and consultants in a subnet (subnet b) in an IDC to access service port 8443 in the application zone in the production environment.
*	0.0.0.0/0	Any	Any	Deny	Denies all inbound traffic that is not processed based on preset rules.

The PRD-SAP-DB zone does not need to communicate with external networks. Therefore, configure only internal rules of network ACLs **NACL-PRD-SAPDB-BUSI** and **NACL-PRD-SAPDB-INTERNEL** by referring to [Network Isolation and Access Control](#).

For security group rule configuration, see the related content in [Network Isolation and Access Control](#).

Security Services

- Anti-DDoS

The production environment needs to access the public network. Therefore, you need to deploy Anti-DDoS on SAP router, SRM, and Hybrids servers. It is recommended that you use HUAWEI CLOUD Anti-DDoS to protect elastic IP addresses (EIPs).

- Web application firewall (WAF)

The production environment needs to provide web applications for the Internet. Therefore, you need to install WAF to defend against OWASP TOP10 and other web attacks. It is recommended that you use the HUAWEI CLOUD WAF service to create WAF instances to protect EIPs and load balancers.

- Virtual next-generation firewall (vNGFW)

The SAP router will be used by a third-party system to connect to the internal system. SRM and Hybrids in the development and test environment will be

available for simulation tests. These points are subject to network attacks, and it is recommended that you install vNGFW on them.

1.2.2 O&M Border

The management zone does not need to communicate with the public network. Therefore, you only need to configure ACL rules between the management zone and IDCs.

Security Policies

As shown in [Figure 1-2](#), network ACL **NACL-PRD-MGMT** is associated with the subnet for the management zone in the production environment. Configure inbound rules of network ACL **NACL-PRD-MGMT** to control access from IDCs to the production environment, allowing access to management ports (such as ports 22 and 3389) in the management zone.

NOTE

IP addresses and ports in this section are only used as examples. If there are other management ports, you can add ACL rules as required.

Table 1-19 Inbound rules of network ACL **NACL-PRD-MGMT**

Rule	Source IP Address	Protocol	Destination Port	Allow or Deny	Description
For the administrator	A subnet (subnet a) in an IDC	TCP	22	Allow	Allows the administrator of a subnet (subnet a) in an IDC to access VMs in the management zone in the production environment.
For the administrator	A subnet (subnet a) in an IDC	TCP	3389	Allow	Allows the administrator of a subnet (subnet a) in an IDC to access VMs in the management zone in the production environment.
*	0.0.0.0/0	Any	Any	Deny	Denies all inbound traffic that is not processed based on preset rules.

Table 1-20 Outbound rules of network ACL **NACL-PRD-MGMT**

Rule	Destination IP Address	Protocol	Destination Port	Allow or Deny	Description
1	0.0.0.0/0	Any	Any	Allow	Allows all outbound traffic from the management zone.
*	0.0.0.0/0	Any	Any	Deny	Denies all outbound traffic that is not processed based on preset rules.

Security Services

With enterprise security practices considered, bastion hosts are used to free O&M and operations personnel from using system usernames and passwords (usernames and passwords for all system components are stored in the bastion host system). The rights of O&M operations performed through bastion hosts are controlled. The rights of high-risk operations are limited. The whole process of O&M operations is recorded and audited so that each event is monitorable and traceable. Bastion hosts are deployed in the form of ECSs in the subnet for the management zone.

1.2.3 Border Between the Production Environment and the Development and Test Environment

The development and test environment has a low security level and a high security risk. If you need to connect the production environment to the development and test environment, configure strict ACL rules for their border. Use ACL rules to strictly control (deny by default) access from the development and test environment to the production environment, allowing access to only required IP addresses and ports in the production environment. You can configure relatively loose ACL rules for access from the production environment to the development and test environment.

Security Policies

Network ACLs **NACL-PRD-DMZ**, **NACL-PRD-APP**, and **NACL-PRD-SAPDB-BUSI** are associated with subnets in the production environment, respectively. Configure inbound rules of these network ACLs to strictly control access from the development and test environment according to the "minimum permission" principle, allowing access to only specified IP addresses and ports in the

production environment. You can configure relatively loose outbound ACL rules for access from the production environment to the development and test environment.

 **NOTE**

Stronger, securer, and complexer ACL rules mean higher deployment and configuration and O&M costs. You can configure looser ACL rules based on your actual enterprise requirements.

Network ACLs configured between the production environment and the development and test environment are mainly used in the DEV-DMZ, DEV-application, and DEV-DB zones. For details, see [Table 1-21](#), [Table 1-22](#), [Table 1-23](#), [Table 1-24](#), [Table 1-25](#) and [Table 1-26](#).

 **NOTE**

IP addresses and ports in this section are only used as examples. If there are other services, you can add ACL rules as required. This section describes only network ACLs configured between the production environment and the development and test environment.

Table 1-21 Inbound rules of network ACL **NACL-PRD-APP**

Rule	Source IP Address	Protocol	Destination Port	Allow or Deny	Description
For the DEV-application zone	172.22.4.0/24	TCP	2433	Allow	Allows VMs in the DEV-application zone in the development and test environment to access port 2433 of servers in the application zone in the production environment for software and codes update pushing.
*	0.0.0.0/0	Any	Any	Deny	Denies all inbound traffic that is not processed based on preset rules.

Table 1-22 Outbound rules of network ACL **NACL-PRD-APP**

Rule	Destination IP Address	Protocol	Destination Port	Allow or Deny	Description
For the DEV-application zone	172.22.8.0/24	TCP	Any	Allow	Allows VMs in the PRD-application zone in the production environment to access any TCP port of servers in the DEV-application zone.
*	0.0.0.0/0	Any	Any	Deny	Denies all outbound traffic that is not processed using preset fixed rules.

Table 1-23 Inbound rules of network ACL **NACL-PRD-DMZ**

Rule	Source IP Address	Protocol	Destination Port	Allow or Deny	Description
For the DEV-DMZ zone	172.22.3.0/24	TCP	1433	Allow	Allows VMs in the DMZ zone in the development and test environment to access port 1433 of servers in the PRD-DMZ zone in the production environment for software and codes update pushing.
*	0.0.0.0/0	Any	Any	Deny	Denies all inbound traffic that is not processed based on preset rules.

Table 1-24 Outbound rules of network ACL **NACL-PRD-DMZ**

Rule	Destination IP Address	Protocol	Destination Port	Allow or Deny	Description
For the DEV-DMZ zone	172.22.4.0/24	TCP	Any	Allow	Allows VMs in the PRD-DMZ zone in the production environment to access any TCP port of servers in the DEV-DMZ zone.
*	0.0.0.0/0	Any	Any	Deny	Denies all outbound traffic that is not processed using preset fixed rules.

Table 1-25 Inbound rules of network ACL **NACL-PRD-SAPDB-BUSI**

Rule	Source IP Address	Protocol	Destination Port	Allow or Deny	Description
For the DEV-SAP DB zone	172.22.5.0/24	TCP	3433	Allow	Allows VMs in the DEV-SAP DB zone in the development and test environment to access port 3433 of servers in the PRD-SAP-DB zone in the production environment for software and codes update pushing.
*	0.0.0.0/0	Any	Any	Deny	Denies all inbound traffic that is not processed based on preset rules.

Table 1-26 Outbound rules of network ACL **NACL-PRD-SAPDB-BUSI**

Rule	Destination IP Address	Protocol	Destination Port	Allow or Deny	Description
For the DEV-SAP DB zone	172.22.5.0/24	TCP	Any	Allow	Allows VMs in the PRD-SAP DB zone in the production environment to access any TCP port of servers in the DEV-SAP DB zone in the development and test environment.
*	0.0.0.0/0	Any	Any	Deny	Denies all outbound traffic that is not processed using preset fixed rules.

1.3 Security Management

Security Evaluation

It is recommended that you regularly perform security evaluation (provided by Huawei Security Assessment Service) on websites and key hosts in order to discover and mitigate security risks.

- Check items include:
 - For websites: structured query language (SQL) injection, cross-site scripting (XSS), file inclusion, any file upload, any file download, web weak password, and service weak password.
 - For hosts: remote vulnerability scanning, weak password scanning, high-risk port identification, high-risk service identification, and baseline check.
- The Huawei security expert team will review the security evaluation reports submitted by professional organizations and direct the professional organizations to improve service quality for better customer experience.
- Security evaluation identifies vulnerabilities accurately and provides information about how to fix them. Customized overall solutions are available for users to build a comprehensive security system.

Website Monitoring

- Unauthorized tampering detection (monitoring web page tampering, especially unauthorized tampering and hidden link tampering)
- Broken link detection (detecting links whose target pages were deleted or removed, invalid links whose associated websites were migrated, and unreachable article links that were static links)
- Vulnerability check (detecting SQL injection, XSS, file inclusion, sensitive information disclosure, and any file download)

- Availability check (monitoring network availability through nationwide availability and domain name service (DNS) monitoring sites)
- Unnecessary service check (regularly checking whether a website provides unnecessary services)
- Sensitive content audit (regularly checking whether a website provides sensitive content and generating alarms for pages with sensitive content)
- Collaborative prewarning (assisting the technical team to provide prewarning concerning newly-detected vulnerabilities and threats)

Key Management

If a service in the system requires data encryption, it is recommended that you use HUAWEI CLOUD Key Management System (KMS) for key management on the service to meet security and compliance requirements.

1.4 Host Security

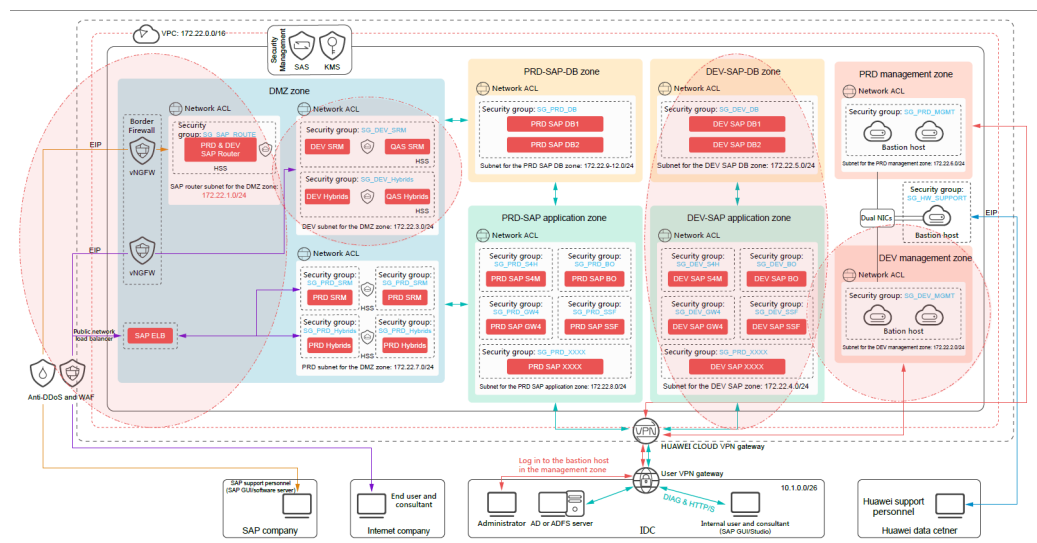
- It is recommended that you perform security hardening on ECSs that communicate with the public network by referring to HUAWEI CLOUD **Brute Force Attack Prevention for Cloud Hosts**. Host security protection includes operating system (OS) security hardening and the use of host security products, such as host-based intrusion detection system (HIDS) and antivirus (AV).
- To ensure the running reliability of key ECSs, you can add key similar nodes (when creating ECSs) to an ECS group and allocate ECSs in an ECS group to different physical servers using anti-affinity policies. For example, you can add backend ECSs monitored by ELB listeners to an ECS group and add SAP DB ECSs to an ECS group.

2 Development and Test Environment Security Solution

2.1 Network Isolation and Access Control

Figure 2-1 shows the SAP development and test environment security solution.

Figure 2-1 Development and test environment security solution



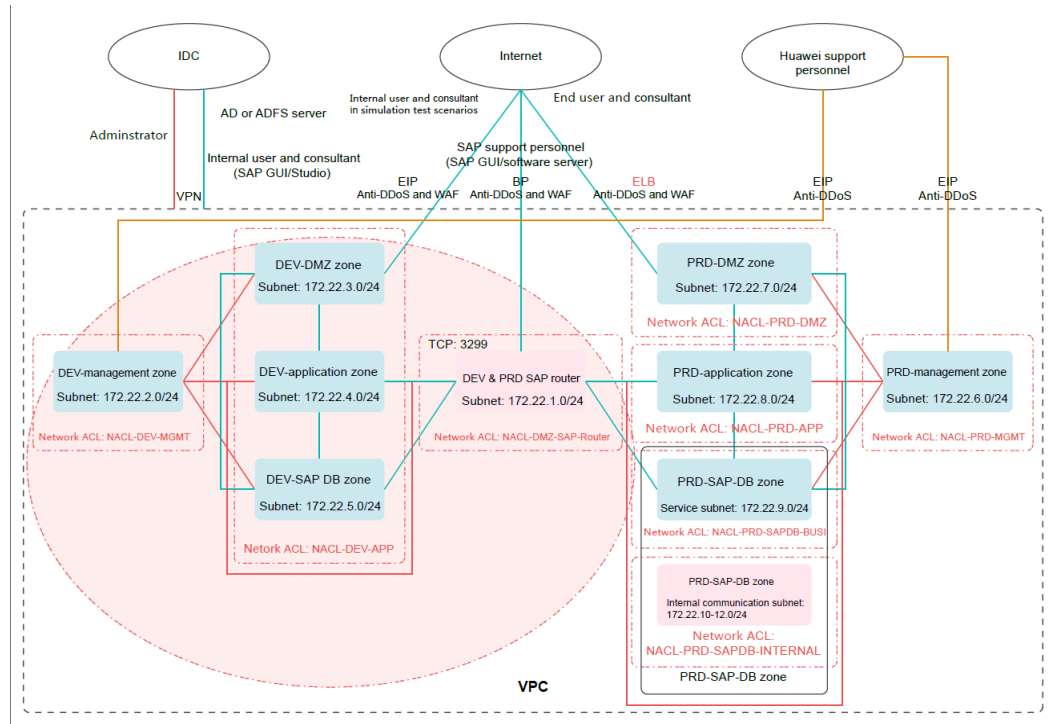
The development and test environment is only used for service development and tests in an enterprise. When this characteristic and enterprise security practices are taken into consideration, you can configure relatively loose network isolation and access control policies for the development and test environment, thereby ensuring network deployment flexibility.

The development and test environment has a low security level and a high security risk. Therefore, if you need to connect the development and test environment to the production environment, configure relatively tight access control policies for the border between the two environments.

In addition, configure security groups to specify open ports according to the "minimum permission" principle. Source IP address access control is performed using network ACLs instead of security groups.

Figure 2-2 shows the subnet and network ACL layout in the SAP development and test environment.

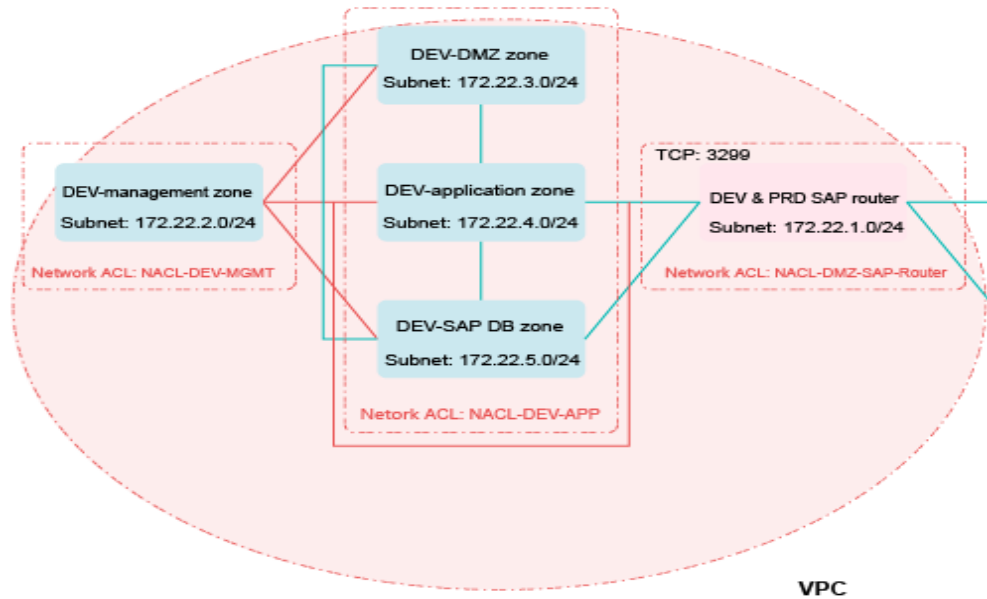
Figure 2-2 Subnet and network ACL layout in the development and test environment



Security Policies

Network ACLs for the development and test environment are **NACL-DEV-MGMT**, **NACL-DEV-APP**, and **NACL-DMZ-SAP-Router**. Each network ACL is associated with a subnet, as shown in **Figure 2-3**. By default, a network ACL denies all access ("deny by default"). If you need to enable communication across network ACLs, add ACL rules to allow required access ("minimum permission").

Figure 2-3 Network ACL layout in the development and test environment



Network ACL **NACL-DEV-MGMT** is associated with the subnet for the DEV-management zone in the development and test environment. Configure rules of network ACL **NACL-DEV-MGMT** to allow access to management ports (such as port 22) of servers in other zones through the bastion host in the management zone and deny access from other zones to the bastion host in the management zone.

NOTE

IP addresses and ports in this section are only used as examples. If there are other management ports, you can add ACL rules as required. This section describes only access control policies for the development and test environment.

Table 2-1 Outbound rules of network ACL **NACL-DEV-MGMT**

Rule	Destination IP Address	Protocol	Destination Port	Allow or Deny	Description
For the DEV-DMZ zone	172.22.3.0/24	TCP	22	Allow	Allows the bastion host in the management zone in the development and test environment to access the SSH ports of servers in the DEV-DMZ zone.

Rule	Destination IP Address	Protocol	Destination Port	Allow or Deny	Description
For the DEV-application zone	172.22.4.0/24	TCP	22	Allow	Allows the bastion host in the management zone in the development and test environment to access the SSH ports of servers in the DEV-application zone.
For the DMZ-SAP-DB zone	172.22.5.0/24	TCP	22	Allow	Allows the bastion host in the management zone in the development and test environment to access the SSH ports of servers in the DEV-SAP-DB zone.
For the DEV&PRD SAP router	172.22.1.0/24	TCP	22	Allow	Allows the bastion host in the management zone in the development and test environment to access the SSH port of the DEV&PRD-SAP-Router server.
*	0.0.0.0/0	Any	Any	Deny	Denies all outbound traffic that is not processed based on preset rules.

Table 2-2 Inbound rules of network ACL **NACL-DEV-MGMT**

Rule	Source IP Address	Protocol	Destination Port	Allow or Deny	Description
*	0.0.0.0/0	Any	Any	Deny	Denies all inbound traffic that is not processed based on preset rules.

Network ACL **NACL-DEV-APP** is associated with the subnets for the DEV-DMZ, DEV-application, and DEV-SAP-DB zones. Configure inbound rules of network ACL

NACL-DEV-APP to allow access to management ports (such as port 22) of servers in the zones through the bastion host in the management zone and allow access to service ports of servers in the zones through the SAP router.

Table 2-3 Outbound rules of network ACL **NACL-DEV-APP**

Rule	Destination IP Address	Protocol	Destination Port	Allow or Deny	Description
*	0.0.0.0/0	Any	Any	Deny	Denies all outbound traffic that is not processed based on preset rules.

Table 2-4 Inbound rules of network ACL **NACL-DEV-APP**

Rule	Source IP Address	Protocol	Destination Port	Allow or Deny	Description
For the DEV-management zone	172.22.2.0/24	TCP	22	Allow	Allows the bastion host in the management zone in the development and test environment to access the SSH ports of servers in the zone.
For the DEV&PRD SAP router	172.22.1.0/24	TCP	234	Allow	Allows the SAP-Router server to access service port 234 of servers in the DEV-application zone.
For the DEV&PRD SAP router	172.22.1.0/24	TCP	345	Allow	Allows the SAP-Router server to access service port 345 of servers in the DEV-SAP-DB zone.
*	0.0.0.0/0	Any	Any	Deny	Denies all inbound traffic that is not processed based on preset rules.

Network ACL **NACL-DMZ-SAP-Router** is associated with the subnet for the DEV&PRD-SAP router. Configure inbound rules of network ACL **NACL-DMZ-SAP-**

Router to allow access to management ports (such as port 22) of servers in the zone through the bastion host in the management zone. Configure outbound rules of network ACL **NACL-DMZ-SAP-Router** to allow access to specified service ports in the application zone and SAP-DB zone in the development and test environment through the SAP router.

Table 2-5 Outbound rules of network ACL **NACL-DMZ-SAP-Router**

Rule	Destination IP Address	Protocol	Destination Port	Allow or Deny	Description
For the DEV-application zone	172.22.4.0/24	TCP	234	Allow	Allows the SAP-Router server to access service port 234 of servers in the DEV-application zone.
For the DEV-SAP-DB zone	172.22.5.0/24	TCP	345	Allow	Allows the SAP-Router server to access service port 345 of servers in the DEV-SAP-DB zone.
*	0.0.0.0/0	Any	Any	Deny	Denies all inbound traffic that is not processed based on preset rules.

Table 2-6 Inbound rules of network ACL **NACL-DMZ-SAP-Router**

Rule	Source IP Address	Protocol	Destination Port	Allow or Deny	Description
For the DEV-management zone	172.22.2.0/24	TCP	22	Allow	Allows the bastion host in the management zone in the development and test environment to access the SSH ports of servers in the zone.
*	0.0.0.0/0	Any	Any	Deny	Denies all inbound traffic that is not processed based on preset rules.

Security groups, such as **SG_DEV_MGMT** and **SG_DEV_DB** (which do not interact with the public network), are associated with ECSs in the subnets in the development and test environment. The security groups must be configured according to the "minimum permission" principle so that a minimum number of ECS ports are opened. **Figure 2-4** shows an example for configuring the security groups. You need to configure them based on your own ports. Network ACLs are used for IP address access control. Other security groups in the development and test environment (for details, see **Figure 2-1**) that do not interact with the public network can be configured similarly.

Figure 2-4 Security group rule example

Direction	Type	Protocol	Port Range/ICMP Type	Remote End	Operation
Outbound	IPv4	Any	Any	Any	Delete
Inbound	IPv4	Any	Any	SG_DEV_MGMT_TEST_DEV(47c1a86-af...	Delete
Inbound	IPv4	TCP	22	0.0.0.0/0	Delete
Inbound	IPv4	TCP	3389	0.0.0.0/0	Delete
Inbound	IPv4	TCP	80	0.0.0.0/0	Delete
Inbound	IPv4	TCP	443	0.0.0.0/0	Delete
Inbound	IPv4	TCP	3306	0.0.0.0/0	Delete

Security groups, such as **SG_DEV_SRM**, **SG_DEV_Hybrids**, and **SG_SAP_ROUTER** (which interact with the public network), are associated with ECSs in the subnets in the development and test environment. The security groups must be configured according to the "minimum permission" principle so that a minimum number of ECS ports and source IP addresses are opened. If the public IP address is fixed, you can refer to **Figure 2-5** for configuring the security groups. You need to configure them based on your own ports.

Figure 2-5 Security group rule example

Direction	Type	Protocol	Port Range/ICMP Type	Remote End	Operation
Outbound	IPv4	Any	Any	Any	Delete
Inbound	IPv4	Any	Any	sg-SAP-TEST(3a4e1e35-250a-4302-...	Delete
Inbound	IPv4	TCP	22	123.123.123.0/24	Delete
Inbound	IPv4	TCP	3389	123.123.123.0/24	Delete
Inbound	IPv4	TCP	80	123.123.123.0/24	Delete

If the public IP address is not fixed, you can create a security group rule to allow access from a specified public source IP address to meet your service requirements (such as the simulation test or technical support) and then delete the rule when it is not required.

2.2 Network Border Security

2.2.1 Border Between the Development and Test Environment and the Production Environment

The development and test environment has a low security level and a high security risk. If you need to connect the development and test environment to the production environment, configure strict access control policies for this border. Use the access control policies to strictly control ("deny by default") access from the development and test environment to the production environment, allowing access to only required IP addresses and ports ("minimum permission") in the production environment. You can configure relatively loose access control policies for the access from the production environment to the development and test environment.

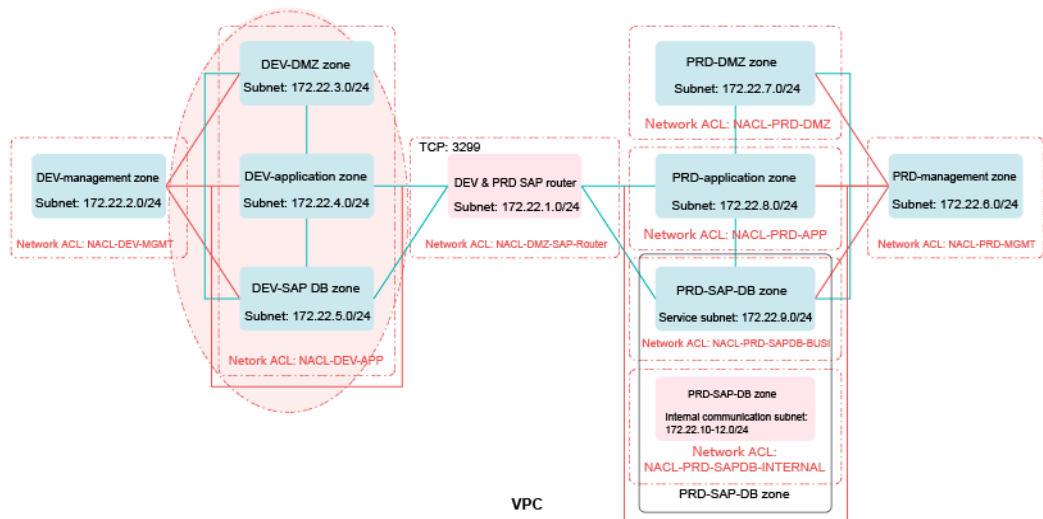
Security Policies

As shown in [Figure 2-6](#), network ACL **NACL-DEV-APP** is associated with the subnet for the DEV-application zone. Configure outbound rules of network ACL **NACL-DEV-APP** to strictly control access to the production environment according to the "minimum permission" principle, allowing access to only specified IP addresses and ports in the production environment. You can configure relatively loose inbound rules for access from the production environment.

NOTE

Stronger, securer, and complexer ACL rules mean higher deployment and configuration and O&M costs. You can use looser ACL rules based on your actual enterprise requirements.

Figure 2-6 Network ACL layout in the development and test environment



Access control policies for the border between the development and test environment and the production environment are mainly those for communication with the PRD-DMZ, PRD-application, and PRD-DB zones in the production environment. For details, see [Table 2-7](#) and [Table 2-8](#).

 **NOTE**

IP addresses and ports in this section are only used as examples. If there are other services, you can add ACL rules as required. This section describes only access control policies for the border between the development and test environment and the production environment.

Table 2-7 Outbound rules of network ACL **NACL-DEV-APP**

Rule	Destination IP Address	Protocol	Destination Port	Allow or Deny	Description
For the PRD-DMZ zone	172.22.7.0/24	TCP	1433	Allow	Allows VMs in the subnet in the development and test environment to access port 1433 of servers in the PRD-DMZ zone in the production environment for software and codes update pushing.
For the PRD-application zone	172.22.8.0/24	TCP	2433	Allow	Allows VMs in the subnet in the development and test environment to access port 2433 of servers in the PRD-application zone in the production environment for software and codes update pushing.
For the PRD-DB zone	172.22.9.0/24	TCP	3443	Allow	Allows VMs in the subnet in the development and test environment to access port 3443 of servers in the PRD-DB zone in the production environment for software and codes update pushing.
*	0.0.0.0/0	Any	Any	Deny	Denies all Outbound traffic that is not processed based on preset rules.

Table 2-8 Inbound rules of network ACL **NACL-DEV-APP**

Rule	Source IP Address	Protocol	Destination Port	Allow or Deny	Description
For the PRD-DMZ zone	172.22.7.0/24	TCP	Any	Allow	Allows VMs in the PRD-DMZ zone in the production environment to access any TCP port of servers in the DEV-DMZ, DEV-application, and DEV-SAP-DB zones.
For the PRD-application zone	172.22.8.0/24	TCP	Any	Allow	Allows VMs in the PRD-application zone in the production environment to access any TCP port of servers in the DEV-DMZ, DEV-application, and DEV-SAP-DB zones.
For the PRD-DB zone	172.22.9.0/24	TCP	Any	Allow	Allows VMs in the PRD-DB zone in the production environment to access any TCP port of servers in the DEV-DMZ, DEV-application, and DEV-SAP-DB zones.
*	0.0.0.0/0	Any	Any	Deny	Denies all outbound traffic that is not processed using preset fixed rules.

For security group rule configuration, see the related content in [Network Isolation and Access Control](#).

2.2.2 Service Border

The development and test environment needs to interconnect with enterprise intranets for service development and tests and communicate with the public network. Therefore, set up VPN channels between the development and test environment and enterprise intranets (IDCs). Configure access control policies between the cloud and the on-premises system and between the cloud and the Internet.

VPN

The development and test environment is used for service development and tests in an enterprise. Therefore, static connections are usually required in the development and test environment. When security and latency are taken into

consideration, the recommended priority is as follows: Direct Connect > IPsec VPN > SSL VPN.

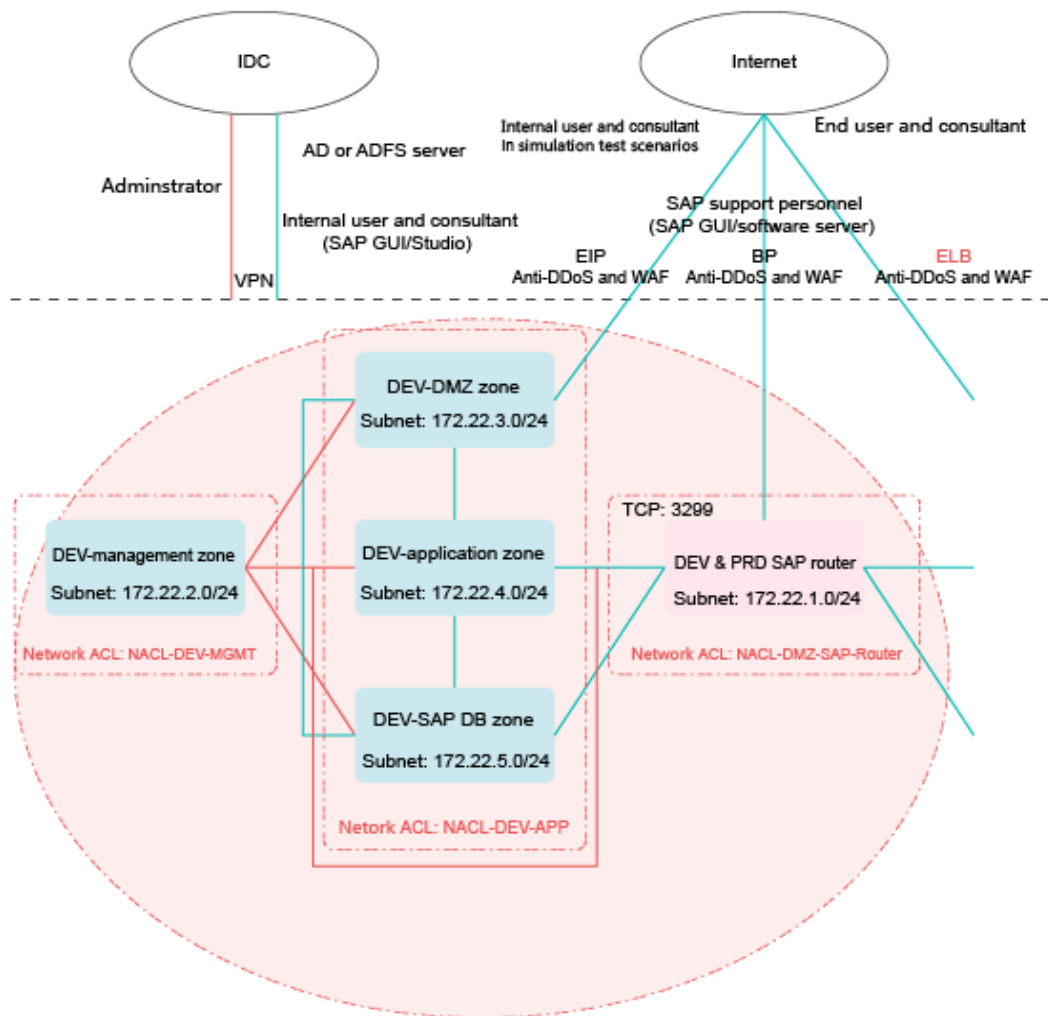
NOTE

Currently, the HUAWEI CLOUD VPN service supports only Direct Connect and IPsec VPN. If you need to use SSL VPN, you can deploy it using a third-party image.

Security Policies

The development and test environment needs to communicate with enterprise intranets and allow access from the Internet. Therefore, networks ACLs are used for access control.

Figure 2-7 Subnet for the development and test environment



As shown in [Figure 2-7](#), network ACL **NACL-DEV-APP** is associated with the subnets for the DEV-DMZ, DEV-application, and DEV-SAP DB zones. Configure outbound rules of network ACL **NACL-DEV-APP** to strictly control access to enterprise intranets (IDCs), allowing access to only specified IP addresses and ports in IDCs.

Configure inbound rules of network ACL **NACL-DEV-APP** based on your service requirements to control access from IDCs to the development and test environment. For a fixed scenario, such as an AD server, configure access control policies to allow the AD server to communicate with specified IP addresses and ports in the cloud. For end users, configure access control policies to allow them to access a specified IP address segment and port range and management ports, such as 22 and 3389.

Network ACL **NACL-DEV-APP** is associated with the subnets for the DEV-DMZ, DEV-application, and DEV-SAP DB zones. Network ACL **NACL-DMZ-SAP-Router** is associated with the subnet for the DEV&PRD SAP router. Configure their inbound rules to strictly control access from the Internet, allowing access from the Internet to only specified IP addresses and ports in the development and test environment.

 **NOTE**

IP addresses and ports in this section are only used as examples. If the public IP address is not fixed, you can create an ACL rule to allow access from a specified public source IP address to meet your service requirements (such as technical support) and then delete the rule when it is not required. If there are other services, you can add ACL rules as required.

Table 2-9 Outbound rules of network ACL **NACL-DMZ-SAP-Router**

Rule	Destination IP Address	Protocol	Destination Port	Allow or Deny	Description
*	0.0.0.0/0	Any	Any	Deny	Denies all outbound traffic that is not processed using preset fixed rules.

Table 2-10 Inbound rules of network ACL **NACL-DMZ-SAP-Router**

Rule	Source IP Address	Protocol	Destination Port	Allow or Deny	Description
For SAP technical support personnel (SAP GUI or software server)	123.123.123.0/24	TCP	3299	Allow	Allows Internet SAP technical support personnel (SAP GUI or software server) from specified source IP addresses to access the DEV&PRD SAP router and then access backend services.

Rule	Source IP Address	Protocol	Destination Port	Allow or Deny	Description
*	0.0.0.0/0	Any	Any	Deny	Denies all inbound traffic that is not processed based on preset rules.

Table 2-11 Outbound rules of network ACL **NACL-DEV-APP**

Rule	Destination IP Address	Protocol	Destination Port	Allow or Deny	Description
For AD or ADFS servers	IP address of an AD or ADFS network in the IDC	TCP	AD or ADF port	Allow	Allows access to AD or ADFS servers in IDCs.
*	0.0.0.0/0	Any	Any	Deny	Denies all outbound traffic that is not processed based on preset rules.

Table 2-12 Inbound rules of network ACL **NACL-DEV-APP**

Rule	Source IP Address	Protocol	Destination Port	Allow or Deny	Description
For Internet users and consultants	123.123.123.0/24	TCP	80	Allow	Allows Internet users and consultants from specified IP addresses to access web services in the development and test environment.
For Internal users and consultants	123.123.123.0/24	TCP	443	Allow	Allows Internet users and consultants from specified IP addresses to access web services in the development and test environment.

Rule	Source IP Address	Protocol	Destination Port	Allow or Deny	Description
For IDC users and consultants	A subnet (subnet b) in an IDC	TCP	80	Allow	Allows internal users and consultants in a subnet (subnet b) in an IDC to access web services in the development and test environment.
For IDC users and consultants	A subnet (subnet b) in an IDC	TCP	443	Allow	Allows internal users and consultants in a subnet (subnet b) in an IDC to access web services in the development and test environment.
*	0.0.0.0/0	Any	Any	Deny	Denies all inbound traffic that is not processed based on preset rules.

For security group rule configuration, see the related content in [Network Isolation and Access Control](#).

Security Services

- Anti-DDoS

The development and test environment needs to communicate with the public network. Therefore, it is recommended that you deploy Anti-DDoS on SAP router, SRM, and Hybrids servers. You can use HUAWEI CLOUD Anti-DDoS to protect elastic IP addresses (EIPs).

- WAF

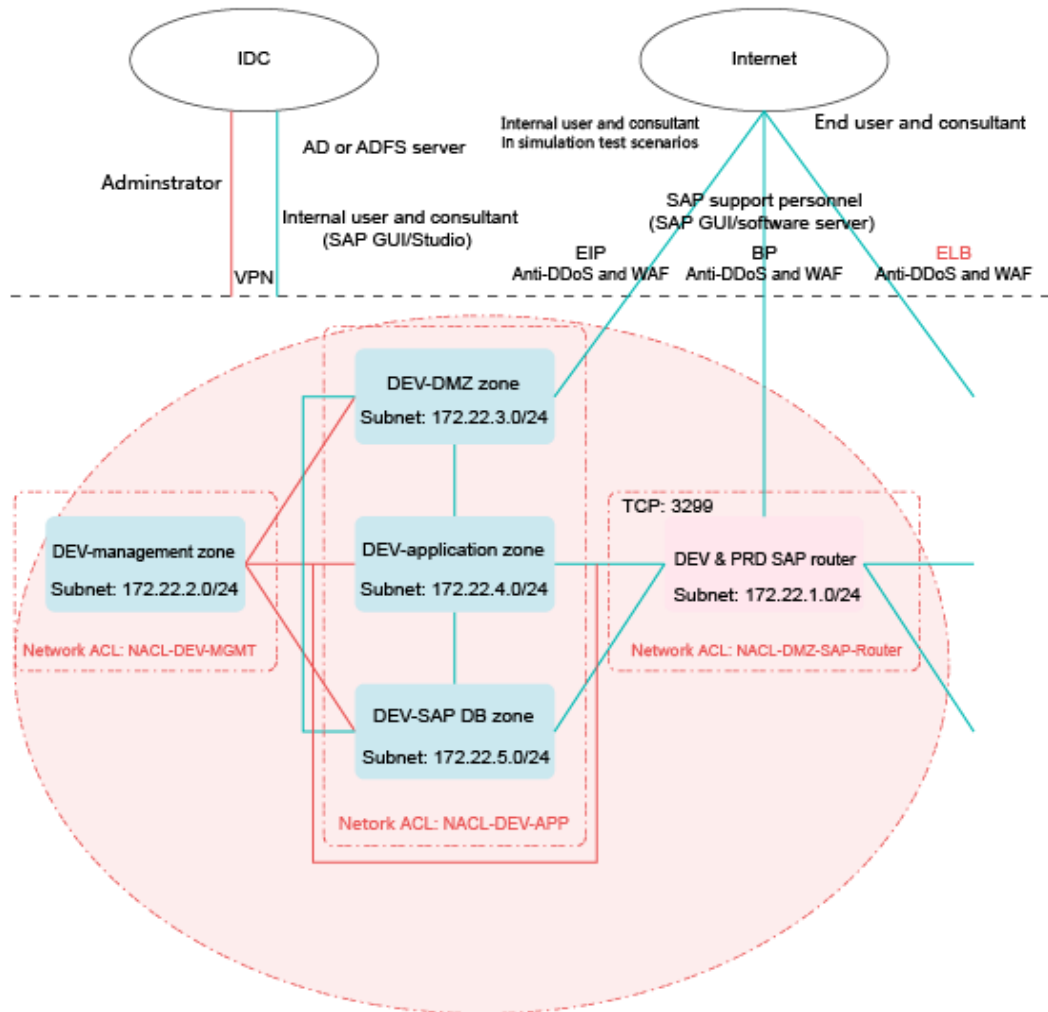
The development and test environment needs to provide web applications for the Internet. Therefore, it is recommended that you install WAF to defend against OWASP TOP10 and other web attacks. You can use the HUAWEI CLOUD WAF service to create WAF instances to protect EIPs.

2.2.3 O&M Border

The management zone does not need to communicate with the public network. Therefore, you only need to configure access control policies between the management zone and IDCs.

Security Policies

Figure 2-8 Subnet for the development and test environment



As shown in [Figure 2-8](#), network ACL **NACL-DEV-MGMT** is associated with the subnet for the management zone in the development and test environment. You can configure inbound rules of network ACL **NACL-DEV-MGMT** (for administrators) to allow access from IDCs to management ports (such as ports 22 and 3389) of hosts in the management zone.

NOTE

IP addresses and ports in this section are only used as examples. You can also configure access control policies associated with end users for the administrator so that the administrator can access service ports in the development and test environment.

Table 2-13 Inbound rules of network ACL **NACL-DEV-MGMT**

Rule	Source IP Address	Protocol	Destination Port	Allow or Deny	Description
For the administrator	A subnet (subnet a) in an IDC	TCP	22	Allow	Allows the administrator of a subnet (subnet a) in an IDC to access VMs in the management zone in the development and test environment.
For the administrator	A subnet (subnet a) in an IDC	TCP	3389	Allow	Allows the administrator of a subnet (subnet a) in an IDC to access VMs in the management zone in the development and test environment.
*	0.0.0.0/0	Any	Any	Deny	Denies all inbound traffic that is not processed based on preset rules.

Table 2-14 Outbound rules of network ACL **NACL-DEV-MGMT**

Rule	Destination IP Address	Protocol	Destination Port	Allow or Deny	Description
1	0.0.0.0/0	Any	Any	Allow	Allows all outbound traffic from the management zone.
*	0.0.0.0/0	Any	Any	Deny	Denies all outbound traffic that is not processed based on preset rules.

For security group rule configuration, see the related content in [Network Isolation and Access Control](#).

Security Services

With enterprise security practices considered, bastion hosts are used to free O&M and operations personnel from using system usernames and passwords (usernames and passwords for all system components are stored in the bastion host system). The rights of O&M operations performed through bastion hosts are controlled. The rights of high-risk operations are limited. The whole process of O&M operations is recorded and audited so that each event is monitorable and

traceable. Bastion hosts are deployed in the form of ECSs in the subnet for the management zone.

2.3 Security Management

Security Evaluation

It is recommended that you regularly perform security evaluation (provided by Huawei Security Assessment Service) on websites and key hosts in order to discover and mitigate security risks.

- Check items include:
 - For websites: structured query language (SQL) injection, cross-site scripting (XSS), file inclusion, any file upload, any file download, web weak password, and service weak password.
 - For hosts: remote vulnerability scanning, weak password scanning, high-risk port identification, high-risk service identification, and baseline check.
- The Huawei security expert team will review the security evaluation reports submitted by professional organizations and direct the professional organizations to improve service quality for better customer experience.
- Security evaluation identifies vulnerabilities accurately and provides information about how to fix them. Customized overall solutions are available for users to build a comprehensive security system.

Website Monitoring

- Unauthorized tampering detection (monitoring web page tampering, especially unauthorized tampering and hidden link tampering)
- Broken link detection (detecting links whose target pages were deleted or removed, invalid links whose associated websites were migrated, and unreachable article links that were static links)
- Vulnerability check (detecting SQL injection, XSS, file inclusion, sensitive information disclosure, and any file download)
- Availability check (monitoring network availability through nationwide availability and domain name service (DNS) monitoring sites)
- Unnecessary service check (regularly checking whether a website provides unnecessary services)
- Sensitive content audit (regularly checking whether a website provides sensitive content and generating alarms for pages with sensitive content)
- Collaborative prewarning (assisting the technical team to provide prewarning concerning newly-detected vulnerabilities and threats)

Key Management

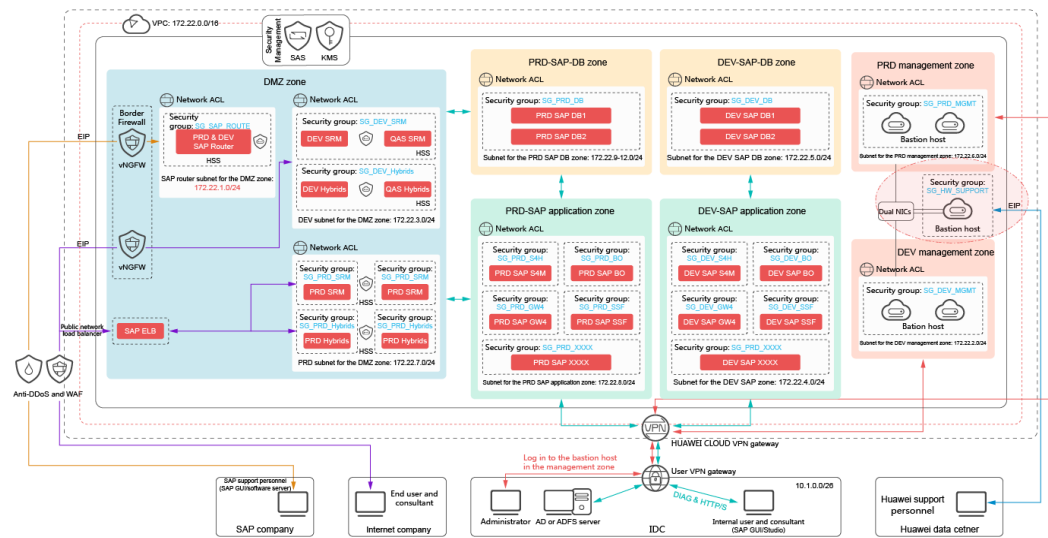
If a service in the system requires data encryption, it is recommended that you use HUAWEI CLOUD Key Management System (KMS) for key management on the service to meet security and compliance requirements.

2.4 Host Security

It is recommended that you perform security hardening on ECSs that communicate with the public network by referring to HUAWEI CLOUD **Brute Force Attack Prevention for Cloud Hosts**. Host security protection includes operating system (OS) security hardening and the use of host security products, such as host-based intrusion detection system (HIDS) and antivirus (AV).

3 Huawei Technical Support Channel Security Solution

Figure 3-1 Huawei technical support channel security solution



If you need Huawei technical support, install a Huawei dedicated bastion host to ensure O&M channel security. For details, see [Figure 3-1](#).

The Huawei dedicated bastion host differs from an enterprise intranet bastion host in the following aspects:

- The Huawei dedicated bastion host is configured with two network interface cards (NICs). The two NICs belong to the subnets for the PRD management zone and DEV management zone, respectively.
- You need to configure an EIP for the Huawei dedicated bastion host so that Huawei technical support can use the EIP for access.

The Huawei dedicated bastion host needs to allow access from the Internet. Therefore, you need to add inbound ACL rules to the subnet to which the NIC bound with the EIP belongs, allowing access from the Internet to the Huawei dedicated bastion host. You do not need to modify outbound ACL rules.

If the NIC bound with the EIP belongs to the subnet for the DEV-management zone, you need to add the following inbound ACL rules.

 **NOTE**

IP addresses and ports in this section are only used as examples. If necessary, add temporary ACL rules to allow access from other source IP addresses.

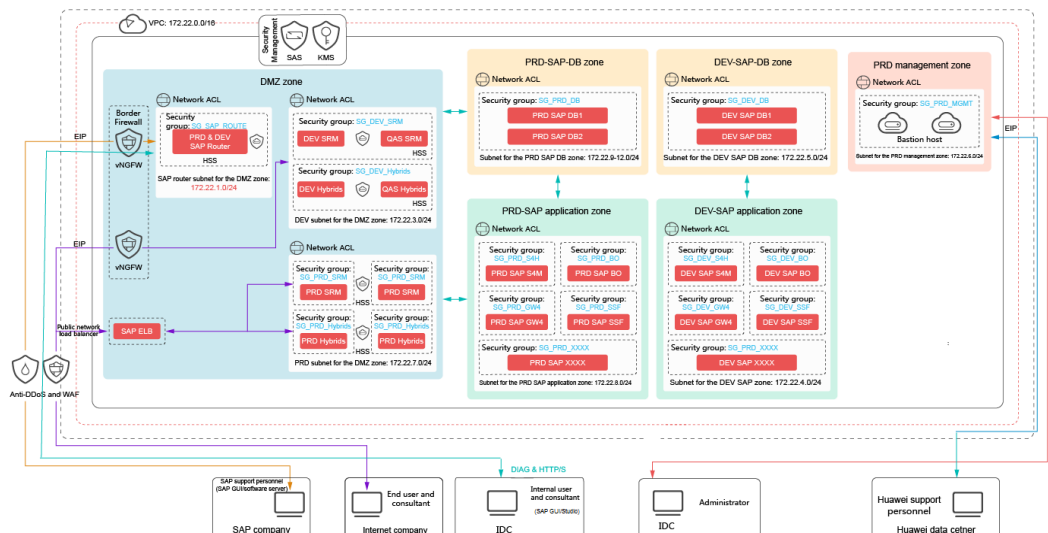
Table 3-1 Inbound rules of network ACL **NACL-DEV-MGMT**

Rule	Source IP Address	Protocol	Destination Port	Allow or Deny	Description
For Huawei technical support	2.2.2.0/24	TCP	8443	Allow	Allows the administrator in Huawei technical support (from fixed source IP addresses) to access the Huawei dedicated bastion host.

4 Other Security Solutions

If you want to save cost and your SAP system on the cloud is lightweight, you can use the public network to carry all your services and O&M channel instead of VPN or Direct Connect. For more information, see [Figure 4-1](#).

Figure 4-1 Special scenario security solution



This solution has the following characteristics:

- There is only one management zone instead of two management zones (PRD and DEV management zones). Only one bastion host is deployed.
- If it is unnecessary to open service ports and the O&M channel to the entire network, you need to tighten ACL rules on the service ports and O&M channel to strictly control access from source IP addresses.

5 Security Solution Mapping Table

 **NOTE**

HUAWEI CLOUD HSS has not supported Windows by Mar 5, 2018. Only Web Tamper Protection (WTP) supports Windows.

Table 5-1 Recommended HUAWEI CLOUD SAP security solution mapping

Requirement	Service or Product	Third-party?	Remarks	Recommended Default Configuration
Network isolation and access control	VPC-network ACL	No	Mandatory	N/A
	VPC-security group	No	Mandatory	N/A
Anti-DDoS	Anti-DDoS traffic cleaning	No	Mandatory. Anti-DDoS must be performed on all EIPs and public network load balancers.	N/A
vNGFW	Hillstone vNGFW	Yes	Strongly recommended. The number and specifications of vNGFW instances are based on your service bandwidth requirements.	Two of the flagship version, working in active/standby mode
Web protection	Web application firewall	No	Mandatory. WAF protection must be performed on all public network sites.	Professional edition for N years. N refers to contract validity duration.

Requirement	Service or Product	Third-party?	Remarks	Recommended Default Configuration
Direct Connect/VPN	Direct Connect	No	Mandatory. The recommended priority is Direct Connect > IPsec VPN and choose one from them.	N/A
	VPN	No	Mandatory. The recommended priority is Direct Connect > IPsec VPN and choose one from them.	N/A
Bastion host	Yunanbao-Yunxiazhi	Yes	Mandatory. The number and specifications of bastion hosts are based on your needs.	Two bastion hosts that support 50 assets (one for the production environment and one for the development and test environment)
Huawei dedicated bastion host	Yunanbao-Yunxiazhi	Yes	Optional. The number and specifications of Huawei dedicated bastion hosts are based on your needs.	One Huawei dedicated bastion host that supports 100 assets
Security Assessment Service (SAS)	SAS-Accurate Assessment (for sites and hosts)	No	Mandatory. You can buy SAS based on the number of your sites and core hosts.	Number: 10 (sites and hosts) x N years. N refers to contract validity duration.
	Website monitoring	No	Optional. You can buy the website monitoring service based on the number of your sites.	Number: 2 x N years. N refers to contract validity duration.
Host security (such as HIDS and AV)	Rising terminal security management software	Yes	Mandatory. Choose one from the four types of host security products.	Number: 10 agents

Requirement	Service or Product	Third-party?	Remarks	Recommended Default Configuration
	McAfee	Yes	Mandatory. Choose one from the four types of host security products.	Number: 10 agents
	Server security watchdog	Yes	Mandatory. Choose one from the four types of host security products.	Number: 10 agents
	HSS	No	Mandatory. Choose one from the four types of host security products.	Number: 10 agents (Linux enterprise edition) x N years. N refers to contract validity duration.
Key management	KMS	No	Optional	Based on your needs
Two-factor authentication	SecID	Yes	Optional. The specifications are based on your needs.	10 users and 10 hosts for a license

A Change History

Change History	Release Date
This is the first official release.	2018-03-12