ALIBABA CLOUD

Alibaba Cloud

Virtual Private Cloud

Network ACL

Document Version: 20220507

Alibaba Cloud

Legal disclaimer

Alibaba Cloud reminds you to carefully read and fully understand the terms and conditions of this legal disclaimer before you read or use this document. If you have read or used this document, it shall be deemed as your total acceptance of this legal disclaimer.

1. You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.

2. No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company or individual in any form or by any means without the prior written consent of Alibaba Cloud.

3. The content of this document may be changed because of product version upgrade, adjustment, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and an updated version of this document will be released through Alibaba Cloud-authorized channels from time to time. You should pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.

4. This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides this document based on the "status quo", "being defective", and "existing functions" of its products and services. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity, applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not take legal responsibility for any errors or lost profits incurred by any organization, company, or individual arising from download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, take responsibility for any indirect, consequential, punitive, contingent, special, or punitive damages, including lost profits arising from the use or trust in this document (even if Alibaba Cloud has been notified of the possibility of such a loss).

5. By law, all the contents in Alibaba Cloud documents, including but not limited to pictures, architecture design, page layout, and text description, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of this document shall be used, modified, reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates. The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates.

6. Please directly contact Alibaba Cloud for any errors of this document.

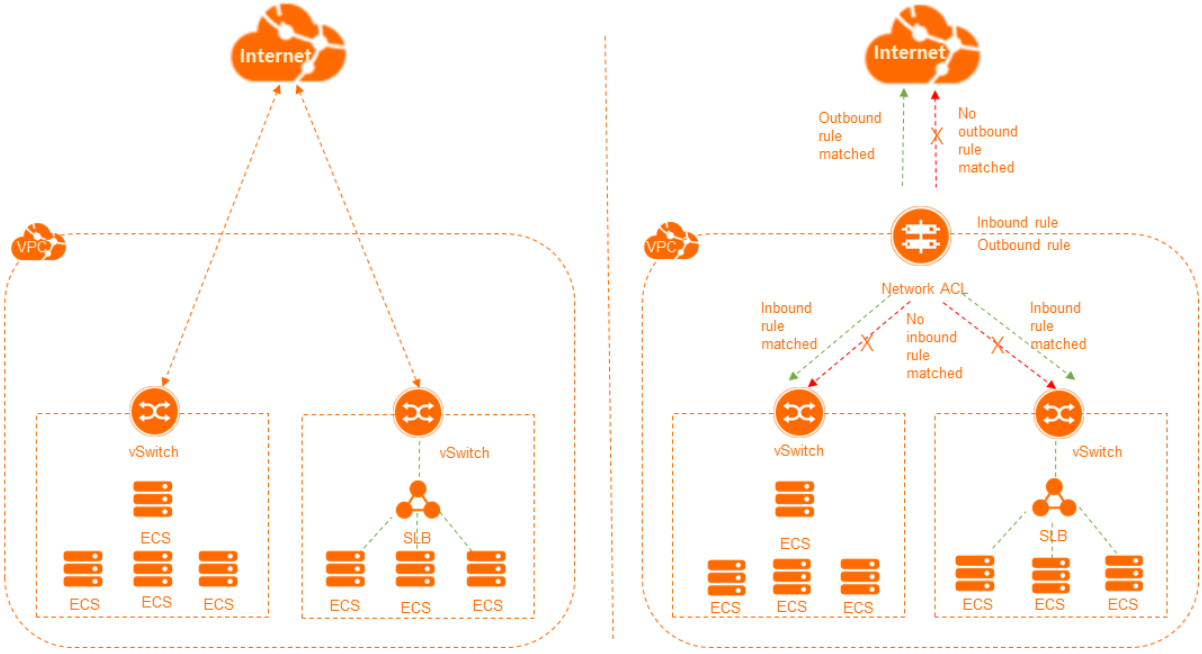
Document conventions

Style	Description	Example
Danger	A danger notice indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	**Danger:** Resetting will result in the loss of user configuration data.
Warning	A warning notice indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	**Warning:** Restarting will cause business interruption. About 10 minutes are required to restart an instance.
Notice	A caution notice indicates warning information, supplementary instructions, and other content that the user must understand.	**Notice:** If the weight is set to 0, the server no longer receives new requests.
Note	A note indicates supplemental instructions, best practices, tips, and other content.	**Note:** You can use Ctrl + A to select all files.
>	Closing angle brackets are used to indicate a multi-level menu cascade.	Click **Settings**> **Network**> **Set network type**.
Bold	Bold formatting is used for buttons , menus, page names, and other UI elements.	Click **OK**.
`Courier font`	Courier font is used for commands	Run the `cd /d C:/window` command to enter the Windows system folder.
Italic	Italic formatting is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	This format is used for an optional value, where only one item can be selected.	`ipconfig [-all|-t]`
{} or {a|b}	This format is used for a required value, where only one item can be selected.	`switch {active|stand}`

Table of Contents

1.Overview of network ACLs

Network access control lists (ACLs) allow you to implement access control for a virtual private cloud (VPC). You can create network ACL rules and associate a network ACL with a vSwitch. This allows you to control inbound and outbound traffic of Elastic Compute Service (ECS) instances that are attached to the vSwitch.



Feature release and supported regions

Area	Region
Asia Pacific	
Europe & Americas	
Middle East	

Features

- A network ACL is used to filter inbound and outbound network traffic of ECS instances that are attached to the vSwitch with which the network ACL is associated. The network traffic forwarded to ECS instances by a Server Load Balancer (SLB) instance is also filtered.

  > **Note** The network traffic of an ECS instance is not filtered by a network ACL in the following scenario: The ECS instance is associated with a secondary elastic network interface (ENI) and the secondary ENI is associated with an elastic IP address (EIP) in cut-through mode. For more information, see Associate an EIP with a secondary ENI in cut-through mode.

- Network ACLs are stateless. If you configure an inbound rule that allows traffic, you must also configure a corresponding outbound rule. Otherwise, the system may fail to respond to requests.
- If you create a network ACL that does not contain a rule, all inbound traffic and outbound traffic are

denied.

- If a network ACL is associated with a vSwitch, the network ACL does not filter the traffic forwarded between ECS instances that are attached to the vSwitch.

Descriptions

You can add rules to or delete rules from a network ACL. Changes to the rules are automatically synchronized to the associated vSwitch. By default, an inbound rule and an outbound rule are automatically added to a newly created network ACL. These rules allow all inbound and outbound network traffic transmitted through the associated vSwitch. You can delete the default rules. The following table describes the default inbound and outbound rules.

- Default inbound rule

Effective order	Protocol	Source IP Addresses	Destination Port Range	Action	Type
1	ALL	0.0.0.0/0	-1/-1	Accept	Custom

- Default outbound rule

Effective order	Protocol	Destination IP Address	Destination Port Range	Action	Type
1	ALL	0.0.0.0/0	-1/-1	Accept	Custom

A rule of a network ACL contains the following parameters:

- **Effective order**: the priority of the rule. A smaller value specifies a higher priority. The system matches requests against rules in descending order of priority. Rule 1 has the highest priority. If a request matches a rule, the system applies the rule to the request and ignores the other rules.

  For example, the following rules are added to a network ACL and requests destined for IP address 172.16.0.1 are sent from an ECS instance. In this case, the requests match Rules 2 and 3. Rule 2 has a higher priority than Rule 3. Therefore, the system applies Rule 2. Based on the action of Rule 2, the requests are denied.

Effective order	Protocol	Destination IP Address	Destination Port Range	Action	Type
1	ALL	10.0.0.0/8	-1/-1	Accept	Custom
2	ALL	172.16.0.0/12	-1/-1	Drop	Custom
3	ALL	172.16.0.0/12	-1/-1	Accept	Custom

- **Action**: the action to be performed on specific traffic. Valid values: Accept and Drop.
- **Protocol**: the protocol of traffic. Valid values:
  - **ALL**: all protocols. If you select ALL, you cannot specify a port range. The port range is set to **-1/-1**, which specifies all ports.
  - **ICMP**: Internet Control Message Protocol (ICMP). If you select ICMP, you cannot specify a port range. The port range is set to **-1/-1**, which specifies all ports.

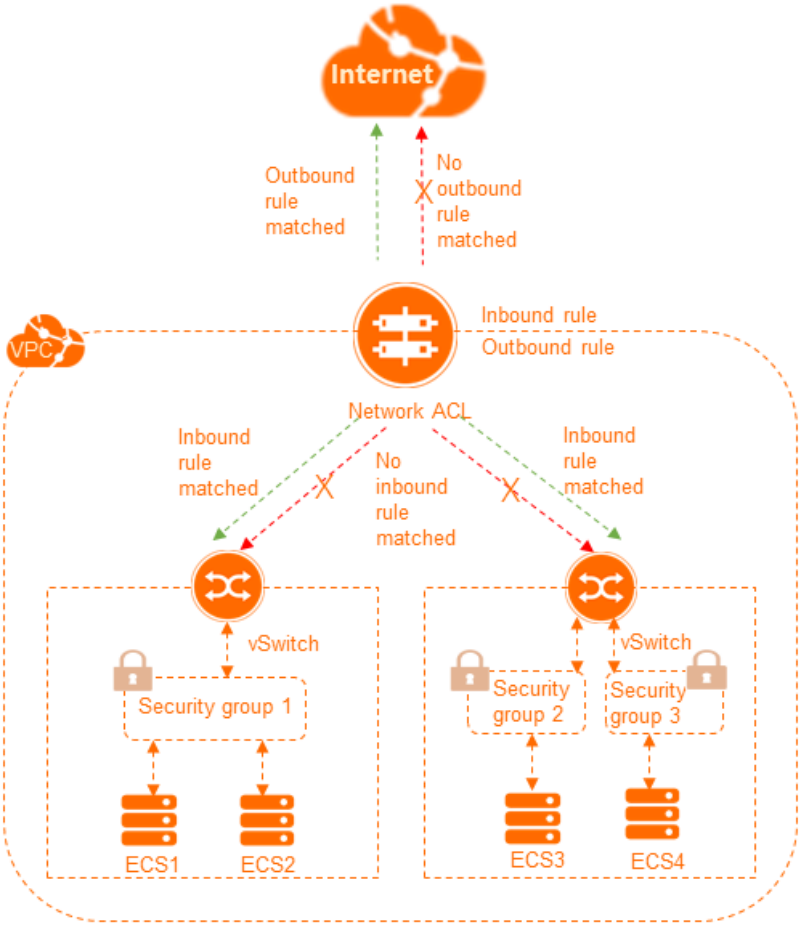
  - **GRE**: Generic Routing Encapsulation (GRE). If you select GRE, you cannot specify a port range. The port range is set to **-1/-1**, which specifies all ports.
  - **TCP**: Transmission Control Protocol (TCP). If you select TCP, you can specify a port range in *1/200* or *80/80* format. You cannot specify **-1/-1**. Valid values for a port: 1 to 65535.
  - **UDP**: User Datagram Protocol (UDP). If you select UDP, you can specify a port range in *1/200* or *80/80* format. You cannot specify **-1/-1**. Valid values for a port: 1 to 65535.
- **Source IP Addresses**: the source IP addresses from which inbound traffic is transmitted. This parameter is available only when you configure an inbound rule.
- **Destination IP Address**: the destination IP addresses to which outbound traffic is transmitted. This parameter is available only when you configure an outbound rule.
- **Destination Port Range**: the range of destination ports to which the inbound rule applies.
- **Destination Port Range**: the range of destination ports to which the outbound rule applies.

Comparison between network ACLs and security groups

Network ACLs control data transmitted through associated vSwitches while security groups control data transmitted through associated ECS instances. The following table describes the differences between network ACLs and security groups.

Feature	Network ACL	Security group
Application scope	vSwitches	ECS instances
Status of returned traffic	Stateless: Returned traffic must be allowed by inbound rules.	Stateful: Returned traffic is automatically allowed and not affected by rules.
Whether rules are evaluated	The system matches a request against rules in descending order of priority. Not all rules are matched.	The system matches a request against all rules before a rule is applied.
Association with ECS instances	The vSwitch to which an ECS instance belongs can be associated with only one network ACL.	Each ECS instance can be added to more than one security group.

The following figure shows how network ACLs and security groups are applied to ensure network security.

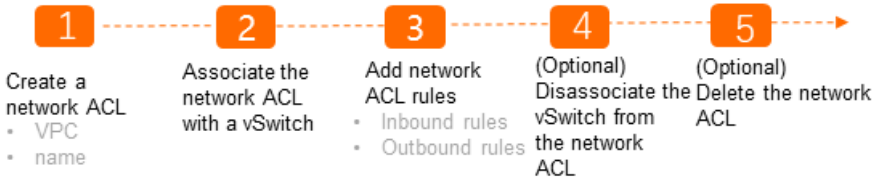


Limits

Item	Limit	Adjustable
Number of network ACLs that can be created in each VPC	200	N/A
Number of network ACLs that can be associated with a vSwitch	1	
Number of rules that can be added to a network ACL	• Inbound rules: 20 • Outbound rules: 20	You can navigate to the Quota Management page to request a quota increase. For more information, see Manage resource quotas.

Item	Limit	Adjustable
VPCs that do not support network ACLs	If the VPC contains an ECS instance of the following types, the VPC does not support network ACLs: For more information, see Advanced VPC features.	**Note** If the VPC contains one of the specified ECS instance types and the network ACL feature is enabled, you must upgrade or release the ECS instance for the network ACL to work as expected.

Procedure



For more information, see Work with network ACLs.

2.Scenarios

If you are familiar with the ports that are commonly used by ECS instances, you can specify them in access control list (ACL) rules to facilitate precise network traffic filtering. This topic describes the ports that are commonly used by ECS instances and the application scenarios of these ports.

Ports

The following table lists the ports and the services that use these ports.

Port	Service	Description
21	FTP	The FTP port. It is used to upload and download files.
22	SSH	The SSH port. It is used to log on to Linux instances in the command line method by using username and password pairs.
23	Telnet	The Telnet port. It is used to remotely log on to ECS instances.
25	SMTP	The SMTP port. It is used to send emails.
80	HTTP	The HTTP port. It is used to access services such as IIS, Apache, and NGINX.
110	POP3	The POP3 port. It is used to send and receive emails.
143	IMAP	The Internet Message Access Protocol (IMAP) port. It is used to receive emails.
443	HTTPS	The HTTPS port. It is used to access services. The HTTPS protocol can implement encrypted and secure data transmission.
1433	SQL Server	The TCP port of SQL Server. It is used for SQL Server to provide external services.
1434	SQL Server	The UDP port of SQL Server. It is used to return the TCP/IP port occupied by SQL Server.
1521	Oracle	The Oracle communication port. ECS instances that run Oracle SQL must have this port open.
3306	MySQL	The MySQL port. It is used for MySQL databases to provide external services.
3389	Windows Server Remote Desktop Services	The Windows Server Remote Desktop Services port. It is used to log on to a Windows instance.
8080	Proxy port	An alternative to port 80. It is commonly used for WWW proxy services.

Custom network ACLs

Inbound rules and Outbound rules describe a network ACL example for VPCs that support IPv4 addresses only.

- The inbound rules in effective order 1, 2, 3, and 4 respectively allow HTTP, HTTPS, SSH, and RDP traffic to the vSwitch. Outbound response rules are those in effective order 3.
- The outbound rules in effective order 1 and 2 respectively allow HTTP and HTTPS traffic from the vSwitch. Outbound response rules are those in effective order 5.
- The inbound rule in effective order 6 denies all inbound IPv4 traffic. This rule ensures that packets that do not match any other rules are denied.
- The outbound rule in effective order 4 denies all outbound IPv4 traffic. This rule ensures that packets that do not match any other rules are denied.

> **Note** An inbound or outbound rule must correspond to an inbound or outbound rule that allows response traffic.

Inbound rules

Effective order	Protocol	Source IP addresses	Destination port range	Action	Description
1	TCP	0.0.0.0/0	80/80	Accept	Allows inbound HTTP traffic from any IPv4 addresses.
2	TCP	0.0.0.0/0	443/443	Accept	Allows inbound HTTPS traffic from any IPv4 addresses.
3	TCP	0.0.0.0/0	22/22	Accept	Allows inbound SSH traffic from any IPv4 addresses.
4	TCP	0.0.0.0/0	3389/3389	Accept	Allows inbound RDP traffic from any IPv4 addresses.
5	TCP	0.0.0.0/0	32768/65535	Accept	Allows inbound IPv4 traffic from the Internet. This port range is for reference only. For more information on how to select appropriate ephemeral ports, see Ephemeral ports.
6	All	0.0.0.0/0	-1/-1	Drop	Denies all inbound IPv4 traffic.

Outbound rules

Effective order	Protocol	Destination IP addresses	Destination port range	Action	Description
1	TCP	0.0.0.0/0	80/80	Accept	Allows outbound IPv4 HTTP traffic from the vSwitch to the Internet.
2	TCP	0.0.0.0/0	443/443	Accept	Allows outbound IPv4 HTTPS traffic from the vSwitch to the Internet.
3	TCP	0.0.0.0/0	32768/65535	Accept	Allows outbound IPv4 traffic from the vSwitch to the Internet. This port range is for reference only. For more information on how to select appropriate ephemeral ports, see Ephemeral ports.
4	All	0.0.0.0/0	-1/-1	Drop	Denies all outbound IPv4 traffic.

Network ACLs for SLB

If the ECS instance in the vSwitch acts as the backend server of an SLB instance, you must add the following network ACL rules.

- Inbound rules

Effective order	Protocol	Source IP addresses	Destination port range	Action	Description
1	SLB listener protocol	Client IP addresses allowed to access the SLB instance	SLB listener port	Accept	Allows inbound traffic from specified client IP addresses.
2	Health check protocol	100.64.0.0/10	Health check port	Accept	Allows inbound traffic from health check IP addresses.

- Outbound rules

Effective order	Protocol	Destination IP addresses	Destination port range	Action	Description
1	All	Client IP addresses allowed to access the SLB instance	-1/-1	Accept	Allows all outbound traffic to specified client IP addresses.
2	All	100.64.0.0/10	-1/-1	Accept	Allows outbound traffic to health check IP addresses.

Ephemeral ports

Clients use different ports to initiate requests. You can select different port ranges for network ACL rules based on the client type. The following table lists ephemeral port ranges for common clients.

Client	Port range
Linux	32768/61000
Windows Server 2003	1025/5000
Windows Server 2008 and later	49152/65535
NAT gateway	1024/65535

3.Work with network ACLs

A network access control list (ACL) allows you to manage network access in a virtual private cloud (VPC). You can create a network ACL in a VPC and add inbound and outbound rules to the network ACL. After you create a network ACL, you can associate it with a vSwitch. This way, you can use the network ACL to control the traffic that flows through the Elastic Compute Service (ECS) instances that are connected to the vSwitch.

Operations

- Create a network ACL
- Add rules to the network ACL
- Change the priorities of network ACL rules
- Associate a network ACL with a vSwitch
- Disassociate a network ACL from a vSwitch
- Delete a network ACL

Create a network ACL

A VPC is created. For more information, see 创建和管理专有网络.

1.
2.
3. In the top navigation bar, select the region where you want to create the network ACL.

   For more information about the regions that support network ACLs, see Feature release and supported regions.
4. On the **Network ACL** page, click **Create Network ACL**.
5. In the **Create Network ACL** dialog box, set the following parameters and click **OK**.

Parameter	Description

Parameter	Description
VPC	Select the VPC for which you want to create the network ACL. **Note** The VPC and network ACL must be deployed in the same region. If the VPC contains an ECS instance that belongs to one of the following instance families, you cannot create a network ACL for the VPC. In this case, you must upgrade or release the ECS instances that do not support VPC advanced features. For more information about advanced VPC features, see Advanced VPC features. ○ For more information about how to upgrade an ECS instance, see Upgrade the instance types of subscription instances or Change the instance type of a pay-as-you-go instance. ○ For more information about how to release an ECS instance, see Release an instance. **Note** If the VPC contains one of the specified ECS instance types and the network ACL feature is enabled, you must upgrade or release the ECS instance for the network ACL to work as expected.
Name	Enter a name for the network ACL. The name must be 2 to 128 characters in length and can contain digits, underscores (_), and hyphens (-). The name must start with a letter.
Description	Enter a description for the network ACL. The description must be 2 to 256 characters in length. The description cannot start with `http://` or `https://`.

Add rules to the network ACL

After you create a network ACL, you can add inbound rules to the network ACL. You can use inbound rules to control whether ECS instances in a vSwitch can be accessed over the Internet or private networks. You can also add outbound rules to the network ACL. You can use outbound rules to control whether ECS instances in a vSwitch can access the Internet or private networks.

1.
2.
3.
4.
5. On the **Basic Information** page, you can create inbound and outbound rules.
   - Create an inbound rule
     a. Click the **Inbound Rule** tab, and then click **Manage Inbound Rule**.

b. Set the following parameters and click **OK**.

Parameter	Description
Priority	The priority of the inbound rule. A smaller value indicates a higher priority. You can create at most 20 rules. For more information, see Rule priorities.
Rule Name	Enter a name for the inbound rule. The name must be 2 to 128 characters in length, and can contain letters, digits, underscores (_), and hyphens (-). The name must start with a letter but cannot start with `http://` or `https://`.
Action	Select an action for the inbound rule. Valid values: ■ **Accept**: accepts network traffic that is destined for the ECS instances connected to the vSwitch. ■ **Drop**: drops network traffic that is destined for the ECS instances connected to the vSwitch.
Protocol	Select a transport layer protocol. Valid values: ■ **ALL**: all protocols ■ **ICMP**: Internet Control Message Protocol (ICMP) ■ **GRE**: Generic Routing Encapsulation (GRE) ■ **TCP**: Transmission Control Protocol (TCP) ■ **UDP**: User Datagram Protocol (UDP)
Source IP Addresses	The source CIDR block from which data is transmitted. Default value: *0.0.0.0/32*.
Destination Port Range	Enter the destination port range of the inbound rule. Valid values: 1 to 65535. Separate the first port and last port with a forward slash (/), for example, *1/200* or *80/80*. A value of *-1/-1* specifies all ports. Therefore, you cannot set the value only to -1/-1.

- Create an outbound rule

a. Click the **Outbound Rule** tab, and then click **Manage Outbound Rule**.

b. Set the following parameters and click **OK**.

Parameter	Description
Priority	The priority of the outbound rule. A smaller value indicates a higher priority. You can create at most 20 rules. For more information, see Rule priorities.
Rule Name	Enter a name for the outbound rule. The name must be 2 to 128 characters in length, and can contain letters, digits, underscores (_), and hyphens (-). The name must start with a letter. It cannot start with `http://` or `https://`.
Action	Select an action for the outbound rule. Valid values: ■ **Accept**: allows ECS instances connected to the vSwitch to access the Internet or other private networks. ■ **Drop**: forbids ECS instances connected to the vSwitch to access the Internet or other private networks.
Protocol	Select a transport layer protocol. Valid values: ■ **ALL**: all protocols ■ **ICMP**: ICMP ■ **GRE**: GRE ■ **TCP**: TCP ■ **UDP**: UDP
Destination IP Address	Specify the destination CIDR block of traffic. Default value: *0.0.0.0/32*.
Destination Port Range	Enter the destination port range of the outbound rule. Valid values: 1 to 65535. Separate the first port and last port with a forward slash (/), for example, *1/200* or *80/80*. A value of *-1/-1* specifies all ports. Therefore, you cannot set the value only to -1/-1.

Change the priorities of network ACL rules

Network ACL rules take effect in descending order of priority. A smaller value indicates a higher priority. You can prioritize network ACL rules based on your business requirements.

1.
2.
3.
4.
5. On the **Basic Information** page, you can change the priorities of inbound and outbound rules.
   - Change the priority of an inbound rule

a. Click the **Inbound Rule** tab, and then click **Manage Inbound Rule**.
b. Drag and drop an inbound rule upwards or downwards, and then click **OK**.

- Change the priority of an outbound rule
  a. Click the **Outbound Rule** tab, and then click **Manage Outbound Rule**.
  b. Drag and drop an inbound rule upwards or downwards, and then click **OK**.

Associate a network ACL with a vSwitch

Before you associate a network ACL with a vSwitch, make sure that the following requirements are met:

- A network ACL is created and network ACL rules are added to it.
- A vSwitch is created. The vSwitch and network ACL must belong to the same VPC. For more information, see Work with vSwitches.

1.
2.
3.
4.
5. On the **Resources** tab, click **Associate vSwitch**.
6. In the **Associate vSwitch** dialog box, select the vSwitch and click **OK**.

   The network ACL and vSwitch must belong to the same VPC. A vSwitch can be associated only with one network ACL.

Disassociate a network ACL from a vSwitch

You can disassociate a network ACL from a vSwitch. After the network ACL is disassociated from the vSwitch, the network ACL no longer controls traffic that flows through the ECS instances connected to the vSwitch.

1.
2.
3.
4.
5. On the **Resources** tab, find the vSwitch and click **Unbind** in the **Actions** column.
6. In the **Unbind Network ACL** message, click **OK**.

Delete a network ACL

Before you delete a network ACL, you must disassociate the network ACL from the vSwitch.

1.
2.
3.
4. On the **Network ACL** page, find the network ACL that you want to delete and click **Delete** in the **Actions** column.
5. In the **Delete Network ACL** message, click **OK**.

References

- CreateNetworkAcl: creates a network ACL.
- UpdateNetworkAclEntries: updates the rules of a network ACL.
- AccosicateNetworkAcl: associates a network ACL with a vSwitch.
- UnassociateNetworkAcl: disassociates a network ACL from a vSwitch.
- DeleteNetworkAcl: deletes a network ACL.

4.Best practices

4.1. Manage intercommunication among ECS instances connected to different vSwitches

This topic describes how to use network access control lists (ACLs) to manage intercommunication among Elastic Compute Service (ECS) instances that are connected to different vSwitches.

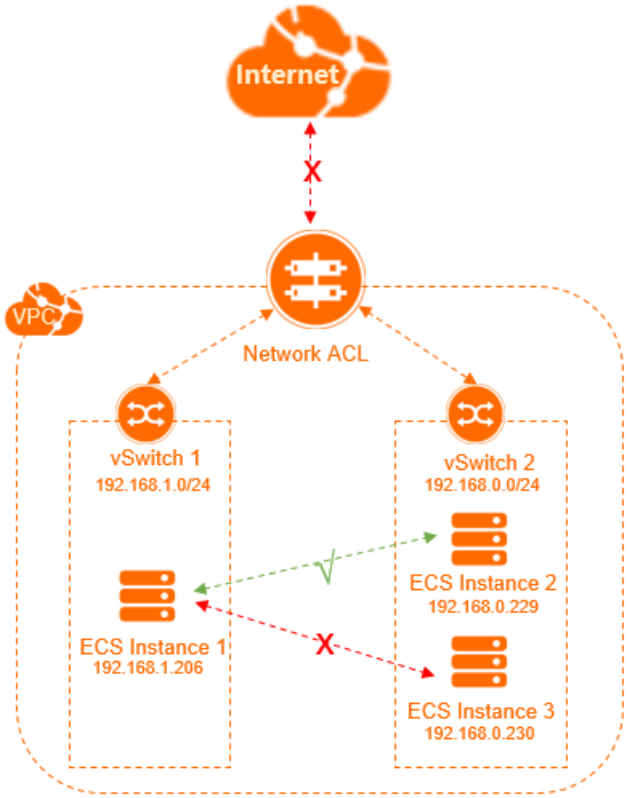
Prerequisites

- A VPC and a vSwitch are created. For more information, see 创建和管理专有网络 and Work with vSwitches.
- ECS instances are created in a vSwitch. For more information, see Create an instance by using the wizard.

Context

An enterprise creates a VPC in the cloud and two vSwitches in the VPC. ECS Instance 1 (192.168.1.206) is connected to vSwitch 1. ECS Instance 2 (192.168.0.229) and ECS Instance 3 (192.168.0.230) are connected to vSwitch 2. To meet business requirements, the enterprise must control intercommunication among the ECS instances, and between the ECS instances and the Internet.

- ECS 1, ECS 2, and ECS 3 are not allowed to communicate with the Internet.
- ECS 1 and ECS 3 are not allowed to communicate with each other.
- ECS 1 and ECS 2 are not allowed to communicate with each other.



You can customize network ACL rules and associate the network ACL with vSwitches, as shown in the preceding figure. This way, you can control network traffic transmitted among the ECS instances connected to the vSwitches.

The following flowchart shows the procedure.

Step 1: Create a network ACL

1.
2.
3.
4. On the **Network ACL** page, click **Create Network ACL**.
5. In the **Create Network ACL** dialog box, set the following parameters and click **OK**:
   - **VPC**: Select the VPC for which you want to create the network ACL.
   - **Name**: Enter a name for the network ACL.

     The name must be 2 to 128 characters in length and can contain digits, underscores (_), and hyphens (-). It must start with a letter.
   - **Description**: Enter a description for the network ACL.

The description must be 2 to 256 characters in length. It cannot start with `http://` or `https://`.

Step 2: Associate the network ACL with a vSwitch

Associate the network ACL with vSwitch 1 and vSwitch 2.

1.
2.
3.
4.
5. On the **Resources** tab, click **Associate vSwitch**.
6. In the **Associate vSwitch** dialog box, select vSwitch 1 and vSwitch 2, and click **Associate**.

Step 3: Add rules to the network ACL

Add inbound and outbound rules to the network ACL.

1.
2.
3.
4. On the **Network ACL** page, find the network ACL that you want to manage and click **Inbound Rule** in the **Actions** column.
5. On the **Inbound Rule** tab, click **Manage Inbound Rule**.
6. Set the following parameters and click **OK**.

Priority	Rule Name	Action	Protocol	Source IP Addresses	Destination Port Range
1	Allow-traffic-from-ECS-Instance 2	Accept	ALL	192.168.0.229/32	-1/-1
2	Allow-traffic-from-ECS-Instance-1	Accept	ALL	192.168.1.206/32	-1/-1
3	Block-traffic-from-all-IP-addresses	Drop	ALL	0.0.0.0/0	-1/-1

7. Click the **Outbound Rule** tab, and then click **Manage Outbound Rule**.
8. Set the following parameters and click **OK**.

Priority	Rule Name	Action	Protocol	Destination IP Address	Destination Port Range

Priority	Rule Name	Action	Protocol	Destination IP Address	Destination Port Range
1	Allow-traffic-destined-for-ECS-Instance-2	Accept	ALL	192.168.0.229/32	-1/-1
2	Allow-traffic-destined-for-ECS-Instance-1	Accept	ALL	192.168.1.206/32	-1/-1
3	Block-traffic-destined-for-all-IP-addresses	Drop	ALL	0.0.0.0/0	-1/-1

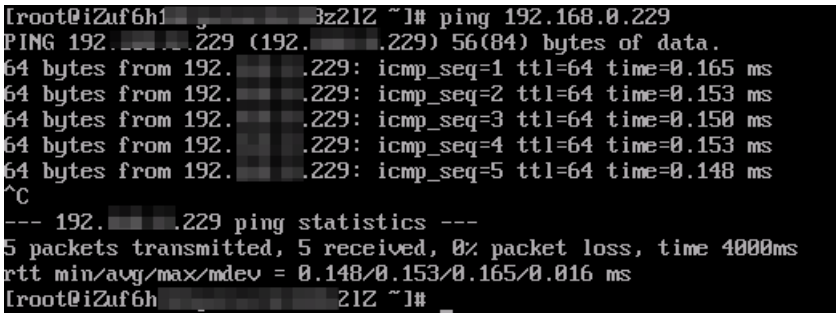
Step 4: Test the connectivity

Test the connectivity among the ECS instances, and between the ECS instances and the Internet.

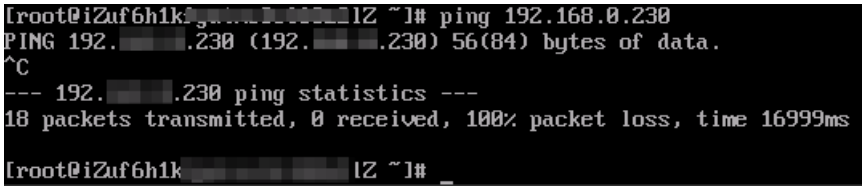
1. Log on to ECS Instance 1. For more information, see Connection methods.
2. Run the `ping` command to `ping` ECS Instance 2, ECS Instance 3, and a public IP address to test the connectivity.

   The result indicates that ECS Instance 1 can access ECS Instance 2, but cannot access ECS Instance 3 or the Internet.

   ECS Instance 1 can access ECS Instance 2



   ECS Instance 1 cannot access ECS Instance 3



   ECS Instance 1 cannot access the Internet

4.2. Manage communication between a data center and a VPC

This topic describes how to use network access control lists (ACLs) to manage communication between a data center and a virtual private cloud (VPC).

Prerequisites

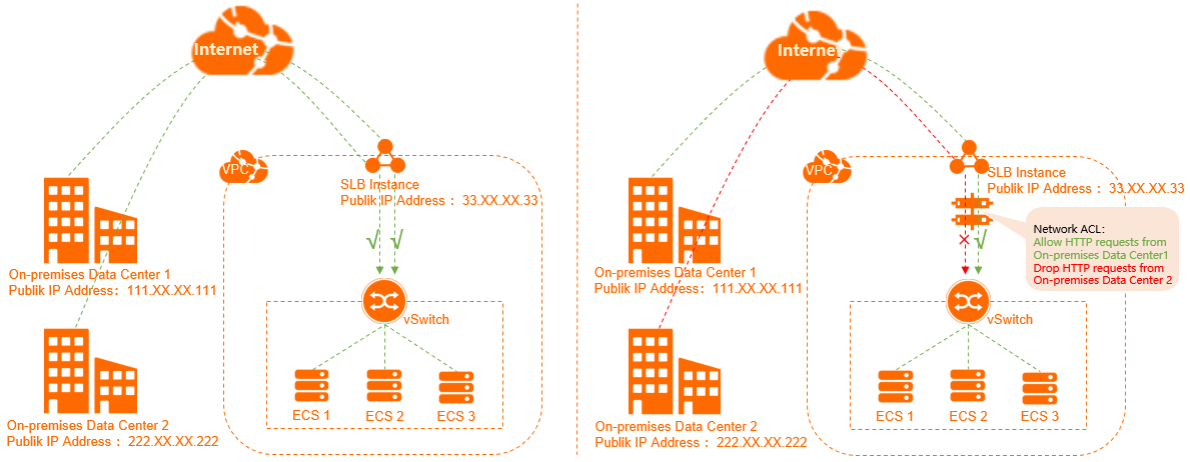
- A VPC and a vSwitch are created. For more information, see 创建和管理专有网络 and Work with vSwitches.
- Elastic Compute Service (ECS) instances are created in the vSwitch. For more information, see Create an instance by using the wizard.
- The ECS instances are added to a security group that allows the HTTP services on the ECS instances to be accessed over the Internet. For more information, see Security group rules for websites to provide web services.

Context

A company has created an Internet-facing Server Load Balancer (SLB) instance and ECS instances. Static pages are hosted on the ECS instances. A listener has been configured for the SLB instance, and the ECS instances are added as backend servers for the SLB instance. By default, Data Center 1 and Data Center 2 can access the static pages through the public IP address of the SLB instance. To meet business requirements, the company wants to allow Data Center 1 to access the static pages, and deny access from Data Center 2 to the static pages.

The following table lists the public IP addresses of the data centers and the SLB instance.

Network	Public IP address
Data Center 1	111.XX.XX.111
Data Center 2	222.XX.XX.222
SLB instance	33.XX.XX.33



You can associate a network ACL with the vSwitch to which the ECS instances belong. Then, you can configure network ACL rules to control inbound and outbound network traffic transmitted through the vSwitch.

The following flowchart shows the procedure.

Step 1: Create a network ACL

1.
2.
3.
4. On the **Network ACL** page, click **Create Network ACL**.
5. In the **Create Network ACL** dialog box, set the following parameters and click **OK**:
   - **VPC**: Select the VPC for which you want to create the network ACL.
   - **Name**: Enter a name for the network ACL.

     The name must be 2 to 128 characters in length and can contain digits, underscores (_), and hyphens (-). It must start with a letter.
   - **Description**: Enter a description for the network ACL.

     The description must be 2 to 256 characters in length. It cannot start with `http://` or `https://`.

Step 2: Associate the network ACL with a vSwitch

1.
2.
3.
4.
5. On the **Resources** tab, click **Associate vSwitch**.
6. In the **Associate vSwitch** dialog box, select the vSwitch and click **OK**.

Step 3: Add rules to the network ACL

Add inbound and outbound rules to the network ACL.

1.
2.
3.
4. On the **Network ACL** page, find the network ACL that you want to manage and click **Inbound Rule** in the **Actions** column.
5. On the **Inbound Rule** tab, click **Manage Inbound Rule**.

6. Set the following parameters and click **OK**.

Priority	Rule Name	Action	Protocol	Source IP Addresses	Destination Port Range
1	Allow-HTTP-requests-from-Data-Center-1	Accept	TCP	The public IP address of Data Center 1. *111.XX.XX.111* is used in this example.	*80/80*
3	Drop-HTTP-requests-from-Data-Center-2	Drop	TCP	The public IP address of Data Center 2. *222.XX.XX.222* is used in this example.	*80/80*

You must add the following inbound rule if the health check feature is enabled for the SLB instance.

Priority	Rule Name	Action	Protocol	Source IP Addresses	Destination Port Range
2	Allow-health-checks	Accept	ALL	The CIDR block used to perform health checks. Set the value to *100.64.0.0/10*.	*-1/-1*

7. Click the **Outbound Rule** tab, and then click **Manage Outbound Rule**.
8. Set the following parameters and click **OK**.

Priority	Rule Name	Action	Protocol	Destination IP Address	Destination Port Range
1	Allow-HTTP-traffic-destined-for-Data-Center-1	Accept	TCP	The public IP address of Data Center 1. *111.XX.XX.111* is used in this example.	*80/80*
3	Drop-HTTP-requests-destined-for Data-Center-2	Drop	TCP	The public IP address of Data Center 2. *222.XX.XX.222* is used in this example.	*80/80*

You must add the following outbound rule if you enable the health check feature for the SLB instance.

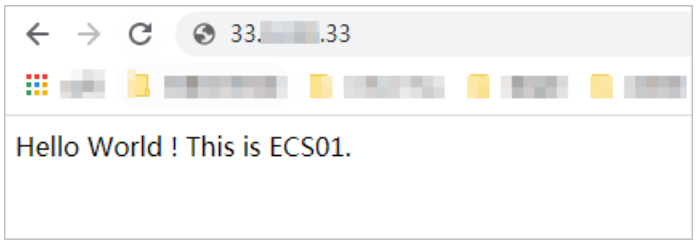
Priority	Rule Name	Action	Protocol	Destination IP Address	Destination Port Range
2	Allow-health-checks	Accept	ALL	The CIDR block used to perform health checks. Set the value to *100.64.0.0/10*.	*-1/-1*

Step 4: Test the connectivity

To test the connectivity between the data centers and the SLB instance, perform the following steps:

1. Open the browser on a computer in Data Center 1.
2. Enter `http://33.XX.XX.33` in the address bar of the browser to test the connectivity.

   The result shows that the device in Data Center 1 can access the static pages on the ECS instances.



3. Open the browser on a device in Data Center 2.
4. Enter `http://33.XX.XX.33` in the address bar of the browser to test the connectivity.

   The result shows that the device in Data Center 2 cannot access the static pages on the ECS instances.