ALIBABA CLOUD

Alibaba Cloud

Virtual Private Cloud

Network ACL

Document Version: 20201024

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

Network access control lists (ACLs) provided by Virtual Private Cloud (VPC) allow you to manage network access permissions. 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 associated with the VSwitch.

> **Note** The network ACL feature is available in the following regions:
>
> - Users in the following regions can use this feature without submitting a ticket: China (Hohhot), China (Chengdu), Indonesia (Jakarta), UK (London), India (Mumbai), and China (Heyuan).
> - Users in the following regions must submit a ticket to use this feature: China (Qingdao), China (Beijing), China (Hangzhou), China (Shanghai), China (Shenzhen), China (Hong Kong), US (Silicon Valley), Singapore (Singapore), and Germany (Frankfurt). To use this feature,submit a ticket.
>
> The network ACL feature is available only in the preceding regions.

Features

Network ACLs have the following features:

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

  > **Note** The inbound and outbound network traffic of an ECS instance are not filtered by network ACLs in the following scenario: The ECS instance is associated with a secondary elastic network interface (ENI) and the secondary ENI is assigned an elastic IP address (EIP) in cut-through mode.

- Network ACLs are stateless. You must set both inbound and outbound rules. Otherwise, the system may fail to respond to requests.
- If you create a network ACL that does not contain any rule, all inbound and outbound access are rejected.
- If a network ACL is associated with a VSwitch, the network ACL does not filter the traffic forwarded between ECS instances that are associated with the VSwitch.

Network ACL rules

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 and 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 lists the default inbound and outbound rules.

- Default inbound rule

Priority	Protocol	Source CIDR block	Destination port range	Policy	Type
1	all	0.0.0.0/0	-1/-1	Accept	Custom

- Default outbound rule

Priority	Protocol	Destination CIDR block	Destination port range	Policy	Type
1	all	0.0.0.0/0	-1/-1	Accept	Custom

A network ACL contains the following parameters:

- Priority: A smaller value indicates a higher priority. Network traffic is matched against rules in descending order of priorities starting from rule number 1. The system applies only one rule to each request and ignores the remaining rules.

  For example, the following rules are added and requests destined for IP address 172.16.0.1 are sent from an ECS instance. In the following table, 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.

Priority	Protocol	Destination CIDR block	Destination port range	Policy	Type
1	all	10.0.0.0/8	-1/-1	Accept	Custom
2	all	172.16.0.0/12	-1/-1	Deny	Custom
3	all	172.16.0.0/12	-1/-1	Accept	Custom

- Policy: indicates whether to allow or deny specific traffic.
- Protocol: the protocol type. Available options include All, ICMP, GRE, TCP, and UDP.
- Source CIDR block: the source CIDR block from which inbound traffic is transmitted.
- Destination CIDR block: the destination CIDR block to which outbound traffic is transmitted.
- 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 the inbound and outbound traffic transmitted through the associated VSwitches. Security groups control the traffic transmitted through ECS instances. The following table lists the differences between network ACLs and security groups.

Network ACL	Security group
Applied to VSwitches.	Applied to instances.
Stateless: Returned traffic must be allowed by inbound rules.	Stateful: Returned traffic is automatically allowed and not affected by any rule.

Network ACL	Security group
Rules are prioritized and matched against traffic in descending order. Only one rule applies to each request.	All rules are evaluated before a rule is applied.
Each VSwitch 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

Before you use network ACLs, note the following limits.

Item	Default limit	Quota increase
Number of network ACLs that can be created in each VPC	200	N/A
Number of network ACLs that can be associated with each VSwitch	1	
Number of rules that can be added to a network ACL	• Inbound rules: 20 • Outbound rules: 20	Go to the Quota Management page to increase the quota. For more information, see Manage service quotas.

Item	Default limit	Quota increase
VPCs that do not support network ACLs	VPCs that contain an instance that belongs to one of the following instance families: ecs.c1, ecs.c2, ecs.c4, ecs.ce4, ecs.cm4, ecs.d1, ecs.e3, ecs.e4, ecs.ga1, ecs.gn4, ecs.gn5, ecs.i1, ecs.m1, ecs.m2, ecs.mn4, ecs.n1, ecs.n2, ecs.n4, ecs.s1, ecs.s2, ecs.s3, ecs.se1, ecs.sn1, ecs.sn2, ecs.t1, and ecs.xn4. For more information, see Overview of VPC advanced features.	Upgrade or release an Elastic Compute Service (ECS) instance that does not support advanced network features. • For more information, see 包年包月实例升配规格 and Change the instance type of a pay-as-you-go instance. • For more information, see Release an instance. Note If the VPC contains one of the specified ECS instance families and the network ACL feature is enabled, you must upgrade or release the ECS instance for the network ACL to work as expected.

Procedure

The following flowchart shows how to configure a network ACL.

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.Create a network ACL

This topic describes how to create a network access control list (ACL) in a Virtual Private Cloud (VPC) network. ACL is a feature provided by VPC. It allows you to manage network access permissions.

Prerequisites

- The network ACL feature is available based on different regions as described in the following:
  - Users in the following regions can use this feature without submitting a ticket: China (Hohhot), China (Chengdu), Indonesia (Jakarta), UK (London), India (Mumbai), and China (Heyuan).
  - Users in the following regions must submit a ticket to use this feature: China (Qingdao), China (Beijing), China (Hangzhou), China (Shanghai), China (Shenzhen), China (Hong Kong), US (Silicon Valley), Singapore (Singapore), and Germany (Frankfurt). To use this feature,submit a ticket.

  The network ACL feature is available only in the preceding regions.
- A VPC network is created. For more information, see Create a VPC.

Procedure

1. Log on to the VPC console.
2. In the left-side navigation pane, click **Network ACL**.
3. In the top navigation bar, select the region where you want to create the network ACL.
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 network for which you want to create the network ACL. If a VPC network contains an Elastic Compute Service (ECS) instance that belongs to one of the following instance families, you cannot create a network ACL for the VPC network. ecs.c1, ecs.c2, ecs.c4, ecs.ce4, ecs.cm4, ecs.d1, ecs.e3, ecs.e4, ecs.ga1, ecs.gn4, ecs.gn5, ecs.i1, ecs.m1, ecs.m2, ecs.mn4, ecs.n1, ecs.n2, ecs.n4, ecs.s1, ecs.s2, ecs.s3, ecs.se1, ecs.sn1, ecs.sn2, ecs.t1, and ecs.xn4. In this case, you must upgrade or release the ECS instances that do not support advanced VPC features. ○ For more information about how to upgrade an ECS instance, see 包年包月实例升配规格 and 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 your VPC network contains ECS instances of the preceding instance families and you have created a network ACL, you must upgrade or release the ECS instances to ensure that the network ACL can work as expected. For more information, see Overview of VPC advanced features.
Name	The name of the network ACL. The name must be 2 to 128 characters in length, and can contain letters, Chinese characters, digits, underscores (_), and hyphens (-). It must start with a letter or a Chinese character.
Description	The description of the network ACL. The description must be 2 to 256 characters in length, and cannot start with `http://` or `https://`.

Related information

- CreateNetworkAcl

4.Associate a network ACL with a VSwitch

This topic describes how to associate a network access control list (ACL) with a VSwitch. By doing so, you can control the traffic moving in and out of ECS instances in the VSwitch.

Prerequisites

Before you associate a network ACL with a VSwitch, make sure the following conditions are met:

- A network ACL is created. For more information, see Create a network ACL.
- A VSwitch is created. For more information, see Create a VSwitch.

Context

You can only associate a network ACL with the VSwitches in the VPC to which the network ACL belongs. Each VSwitch can be associated with only one network ACL.

Procedure

1. Log on to the VPC console.
2. In the left-side navigation pane, click **Network ACL**.
3. In the top navigation bar, select the region of the network ACL.
4. On the **Network ACL** page, find the target network ACL, and then click **Manage** in the **Actions** column.
5. On the **Resources** tab, click **Bind Resource**.
6. In the **Bind Resource** dialog box, select the VSwitch with which the network ACL is to be associated, and then click **OK**.

Related information

- AssociateNetworkAcl

5.Add network ACL rules

5.1. Add an inbound rule

This topic describes how to add an inbound rule to a network access control list (ACL). You can associate a network ACL with a VSwitch and then use inbound rules to allow or deny network traffic sent from a public or internal network to the ECS instances connected to the VSwitch.

Prerequisites

You have created a network ACL. For more information, see Create a network ACL.

Procedure

1. Log on to the VPC console.
2. In the left-side navigation pane, click **Network ACL**.
3. In the top navigation bar, select the region of the network ACL.
4. On the **Network ACL** page, find the target network ACL, and then click **Inbound Rule** in the **Actions** column.
5. On the **Inbound Rule** tab, click **Create Inbound Rule**.
6. On the **Create Inbound Rule** page, configure the inbound rule according to the following information, and then click **OK**.

Parameter	Description
Name	Enter a name for the inbound rule to be created. The name must be 2 to 128 characters in length and can contain letters, numbers, underscores (_), and hyphens (-). The name must start with a letter or Chinese character and cannot start with `http://` or `https://`.
Effective order	The order in which the inbound rule is evaluated. Valid values: 1 to 20. A smaller number indicates a higher priority. For more information, see Rule evaluation order.
Action	Select an action for the inbound rule. Valid values: ○ Accept ○ Drop
Protocol	Select the transport layer protocol. Valid values: ○ all: All protocols are supported. ○ ICMP ○ GRE ○ TCP ○ UDP

Parameter	Description
Source IP Addresses	Enter the range of source IP addresses. Default value: 0.0.0.0/32.
Destination Port Range	Enter the destination port range. Valid values: 1 to 65535. Separate the first port and last port with a forward slash (/), for example, 1/200 or 80/80. You cannot set the port range to -1/-1, which indicates that all ports are allowed.

Related information

- UpdateNetworkAclEntries

5.2. Add an outbound rule

This topic describes how to add an outbound rule to a network access control list (ACL). After creating a network ACL, you can add outbound rules to it to allow or deny the ECS instances in a VSwitch to access the public or private network.

Prerequisites

A network ACL is created. For more information, see Create a network ACL.

Procedure

1. Log on to the VPC console.
2. In the left-side navigation pane, click **Network ACL**.
3. In the top navigation bar, select the region of the network ACL.
4. On the **Network ACL** page, find the target network ACL, and then click **Outbound Rule** in the **Actions** column.
5. On the **Outbound Rule** tab, click **Create Outbound Rule**.
6. In the **Create Outbound Rule** dialog box, configure the outbound rule according to the following information, and then click **OK**.

Configuration	Description
Name	Enter a name for the outbound rule to be created. The name must be 2 to 128 characters in length and can contain letters, numbers, underscores (_), and hyphens (-). The name must start with a letter and cannot start with `http://` or `https://`.
Effective order	The order in which the outbound rule is evaluated. Value range: [1~20]. A smaller number indicates a higher priority. For more information, see Rule evaluation order.

Configuration	Description
Action	Select an authorization policy for the outbound rule. Valid values: ○ Accept ○ Drop
Protocol	Select the transport layer protocol. Valid values: ○ ALL: All protocols are supported. ○ ICMP ○ GRE ○ TCP ○ UDP
Destination IP Addresses	Enter the destination IP address range. Default value: 0.0.0.0/32.
Destination Port Range	Enter the destination port range. Value range: [1~65535]. Separate the start port and the end port by using a forward slash (/), for example, 1/200 or 80/80. Note that you cannot set the port range to -1/-1, which indicates that all ports are allowed.

Related information

- UpdateNetworkAclEntries

5.3. Adjust the rule evaluation order

This topic describes how to adjust the rule evaluation order of a network access control list (ACL). The rules within a network ACL are evaluated in the effective order. A smaller order number indicates a higher priority. You can sort rules to specify the sequence in which rules are evaluated.

Adjust the inbound rule sequence

1. Log on to the VPC console.
2. In the left-side navigation pane, click **Network ACL**.
3. In the top navigation bar, select the region of the network ACL.
4. On the **Network ACL** page, find the target network ACL and click **Manage** in the **Actions** column.
5. Click the **Inbound Rule** tab, and then click **Sort**.
6. On the **Sort** page, adjust the evaluation sequence by dragging the inbound rules into the desired order, and then click **OK**.

Adjust the outbound rule sequence

1. Log on to the VPC console.

2. In the left-side navigation pane, click **Network ACL**.
3. In the top navigation bar, select the region of the network ACL.
4. On the **Network ACL** page, find the target network ACL and click **Manage** in the **Actions** column.
5. Click the **Outbound Rule** tab, and then click **Sort**.
6. On the **Sort** page, adjust the evaluation sequence by dragging the outbound rules into the desired order, and then click **OK**.

6.Disassociate a VSwitch from a network ACL

This topic describes how to disassociate a VSwitch from a network access control list (ACL). After the disassociation, the network ACL no longer filters the incoming or outgoing traffic of the ECS instances in the VSwitch.

Procedure

1. Log on to the VPC console.
2. In the left-side navigation pane, click **Network ACL**.
3. In the top navigation bar, select the region of the network ACL.
4. On the **Network ACL** page, find the target network ACL and click **Manage** in the **Actions** column.
5. On the **Resources** tab, find the target VSwitch and click **Unbind** in the **Actions** column.
6. In the **Unbind Network ACL** dialog box, click **OK**.

Related information

- UnassociateNetworkAcl

7.Delete a network ACL

This topic describes how to delete a network access control list (ACL) that is no longer in use.

Prerequisites

The network ACL to be deleted is not associated with any VSwitch. If the network ACL is associated with a VSwitch, disassociate the VSwitch first. For more information, see Disassociate a VSwitch from a network ACL.

Procedure

1. Log on to the VPC console.
2. In the left-side navigation pane, click **Network ACL**.
3. In the top navigation bar, select the region of the target network ACL.
4. On the **Network ACL** page, find the target network ACL and click **Delete** in the **Actions** column.
5. In the **Delete Network ACL** dialog box, click **OK**.

Related information

- DeleteNetworkAcl

8.Best practices

8.1. Manage intercommunication among ECS instances attached to different VSwitches

This topic describes how to use network access control list (ACL) to control intercommunication among Elastic Compute Service (ECS) instances attached to different VSwitches.

Prerequisites

Before you start, make sure that the following requirements are met:

- An Alibaba Cloud account is created. If you do not have an Alibaba Cloud account, click Create an Alibaba Cloud account.
- The network ACL feature is available based on different regions as described in the following:
  - Users in the following regions can use this feature without submitting a ticket: China (Hohhot), China (Chengdu), Indonesia (Jakarta), UK (London), India (Mumbai), and China (Heyuan).
  - Users in the following regions must submit a ticket to use this feature: China (Qingdao), China (Beijing), China (Hangzhou), China (Shanghai), China (Shenzhen), China (Hong Kong), US (Silicon Valley), Singapore (Singapore), and Germany (Frankfurt). To use this feature,submit a ticket.

  The network ACL feature is available only in the preceding regions.
- A VPC network and VSwitches are created. For more information, see Create a VPC.
- Elastic Compute Service (ECS) instances are created and attached to the VSwitches. For more information, see Create an instance by using the provided wizard.

Context

A company creates a VPC network and two VSwitches in the VPC network. ECS Instance 1 (192.168.1.206) is attached to VSwitch 1. ECS Instance 2 (192.168.0.229) and ECS Instance 3 (192.168.0.230) are attached to VSwitch 2. To meet business requirements, the company must control intercommunication among the ECS instances, and between the ECS instances and the Internet.

- Forbid the three ECS instances to access the Internet.
- Forbid ECS Instance 1 and ECS Instance 3 to communicate with each other.
- Allow ECS Instance 1 and ECS Instance 2 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 attached to the VSwitches.

The following flowchart shows the configuration procedure.

Step 1: Create a network ACL

To create a network ACL, perform the following steps:

1. Log on to the VPC console.
2. In the left-side navigation pane, click **Network ACL**.
3. In the top navigation bar, select the region where you want to create the network ACL.
4. On the **Network ACL** page, click **Create Network ACL**.
5. In the **Create Network ACL** dialog box that appears, set the following parameters, and click **OK**.
   - **VPC**: Select the VPC network 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 letters, Chinese characters, digits, underscores (_), and hyphens (-). It must start with a letter or a Chinese character.
   - **Description**: Enter a description for the network ACL.

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

Step 2: Associate the network ACL with VSwitches

To associate the network ACL with VSwitch 1 and VSwitch 2, perform the following steps:

1. Log on to the VPC console.
2. In the left-side navigation pane, click **Network ACL**.
3. In the top navigation bar, select the region where the network ACL is created.
4. On the **Network ACL** page, find the network ACL that you want to manage, and click **Manage** in the **Actions** column.
5. On the **Resources** tab, click **Bind Resource**.
6. In the **Bind Resource** dialog box, select VSwitch 1 and VSwitch 2, and click **OK**.

Step 3: Add network ACL rules

To add inbound and outbound rules to the network ACL, perform the following steps:

1. Log on to the VPC console.
2. In the left-side navigation pane, click **Network ACL**.
3. In the top navigation bar, select the region where the network ACL is created.
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 **Create Inbound Rule**.
6. In the **Create Inbound Rule** dialog box, set the following parameters, and click **OK**.

Name	Effective order	Action	Protocol	Source IP address	Destination port range
Allow traffic from ECS Instance 2	1	Allow	all	192.168.0.229/32	-1/-1
Allow traffic from ECS Instance 1	2	Allow	all	192.168.1.206/32	-1/-1
Block traffic from all IP addresses	3	Deny	all	0.0.0.0/0	-1/-1

7. Click the **Outbound Rule** tab, and click **Create Outbound Rule**.
8. In the **Create Outbound Rule** dialog box, set the following parameters, and click **OK**.

Name	Effective order	Action	Protocol	Destination IP address	Destination port range
Allow traffic destined for ECS Instance 2	1	Allow	all	192.168.0.229/32	-1/-1
Allow traffic destined for ECS Instance 1	2	Allow	all	192.168.1.206/32	-1/-1
Block traffic destined for all IP addresses	3	Deny	all	0.0.0.0/0	-1/-1

Step 4: Test the connectivity

To test the connectivity among the ECS instances, and between the ECS instances and the Internet, perform the following steps:

1. Log on to ECS Instance 1.
2. Run the `ping` command to `ping` ECS Instance 2, ECS Instance 3, and a public IP address to test the connectivity.The result shows 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

   

8.2. Manage intercommunication between an on-premises data center and a VPC network

This topic describes how to use network access control lists (ACLs) to manage intercommunication between an on-premises data center and a Virtual Private Cloud (VPC) network.

Prerequisites

Before you start, make sure that the following requirements are met:

- An Alibaba Cloud account is created. To create an Alibaba Cloud account, go to the Alibaba Cloud site. For more information, see Create an Alibaba Cloud account.
- The network ACL feature is available based on different regions as described in the following:
  - Users in the following regions can use this feature without submitting a ticket: China (Hohhot), China (Chengdu), Indonesia (Jakarta), UK (London), India (Mumbai), and China (Heyuan).
  - Users in the following regions must submit a ticket to use this feature: China (Qingdao), China (Beijing), China (Hangzhou), China (Shanghai), China (Shenzhen), China (Hong Kong), US (Silicon Valley), Singapore (Singapore), and Germany (Frankfurt). To use this feature,submit a ticket.

  The network ACL feature is available only in the preceding regions.
- A VPC network and a VSwitch are created. For more information, see Create a VPC.
- Elastic Compute Service (ECS) instances are created and attached to the VSwitch. For more information, see Create an instance by using the provided wizard.
- The ECS instances are added to a security group that allows Internet access to the ECS instances over HTTP. For more information, see Scenario 8 in Scenarios for security groups.

Context

A company has created a public-facing Server Load Balancer (SLB) instance and multiple ECS instances. Static pages are hosted on the ECS instances. A listener has been configured for the SLB instance, and the ECS instances are specified 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 forbid Data Center 2 to access the static pages.

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

Data center/SLB instance	Public IP address
On-premises Data Center 1	111.xx.xx.111
On-premises Data Center 2	222.xx.xx.222
SLB instance	33.xx.xx.33

The preceding figure shows that you can associate a network ACL with the VSwitch to which the ECS instances are attached. You can configure network ACL rules to manage inbound and outbound network traffic transmitted through the VSwitch.

The following flowchart shows the configuration procedure.

Step 1: Create a network ACL

To create a network ACL, perform the following steps:

1. Log on to the VPC console.
2. In the left-side navigation pane, click **Network ACL**.
3. In the top navigation bar, select the region where you want to create the network ACL.
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 network 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 letters, Chinese characters, digits, underscores (_), and hyphens (-). It must start with a letter or a Chinese character.
   - **Description**: Enter a description of the network ACL.

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

Step 2: Associate the network ACL with a VSwitch

To associate a VSwitch with the network ACL, perform the following steps:

1. Log on to the VPC console.
2. In the left-side navigation pane, click **Network ACL**.
3. In the top navigation bar, select the region where the network ACL is created.
4. On the **Network ACL** page, find the network ACL that you want to manage, and click **Manage** in the **Actions** column.
5. On the **Resources** tab, click **Bind Resource**.
6. In the **Bind Resource** dialog box, select a VSwitch, and click **OK**.

Step 3: Add network ACL rules

To add inbound and outbound rules to the network ACL, perform the following steps:

1. Log on to the VPC console.
2. In the left-side navigation pane, click **Network ACL**.
3. In the top status bar, select the region where the network ACL is created.
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 **Create Inbound Rule**.

6. In the **Create Inbound Rule** dialog box, set the following parameters, and click **OK**.

Name	Effective order	Action	Protocol	Source IP address	Destination port range
Accept HTTP requests from Data Center 1	1	Allow	TCP	The public IP address of Data Center 1. Enter 111.xx.xx.111 in this example.	80/80
Drop HTTP requests from Data Center 2	3	Deny	TCP	The public IP address of Data Center 2. Enter 222.xx.xx.222 in this example.	80/80

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

Name	Effective order	Action	Protocol	Source IP address	Destination port range
Allow health checks	2	Allow	all	The CIDR block that is used to perform health checks. Only 100.64.0.0/10 is allowed.	-1/-1

7. Click the **Outbound Rule** tab, and click **Create Outbound Rule**.
8. In the **Create Outbound Rule** dialog box, set the following parameters, and click **OK**.

Name	Effective order	Action	Protocol	Destination IP address	Destination port range
Accept HTTP traffic destined for Data Center 1	1	Allow	TCP	The public IP address of Data Center 1. Enter 111.xx.xx.111 in this example.	80/80
Block HTTP traffic destined for Data Center 2	3	Deny	TCP	The public IP address of Data Center 2. Enter 222.xx.xx.222 in this example.	80/80

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

Name	Effective order	Action	Protocol	Destination IP address	Destination port range
Allow health checks	2	Allow	all	The CIDR block that is used to perform health checks. Only 100.64.0.0/10 is allowed.	-1/-1

Step 4: Test the connectivity

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

1. Open the browser on the computer in Data Center 1.
2. Enter `http://33.xx.xx.33` into the address bar of the browser to test the connectivity.The result shows that the computer in Data Center 1 can access the static pages on the ECS instances.
3. Open the browser on the computer in Data Center 2.
4. Enter `http://33.xx.xx.33` into the address bar of the browser to test the connectivity.The result shows that the computer in Data Center 2 cannot access the static pages on the ECS instances.