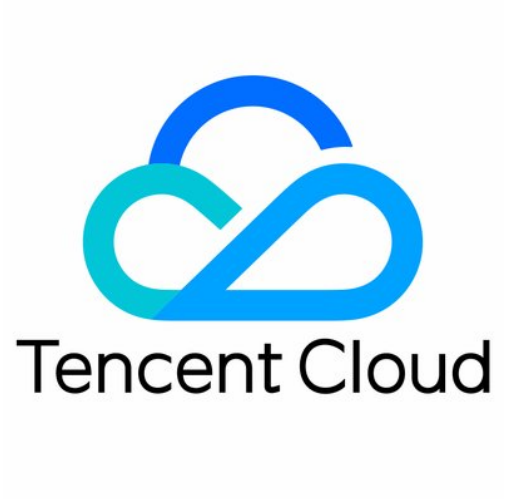
Virtual Private Cloud

Security

Product Documentation



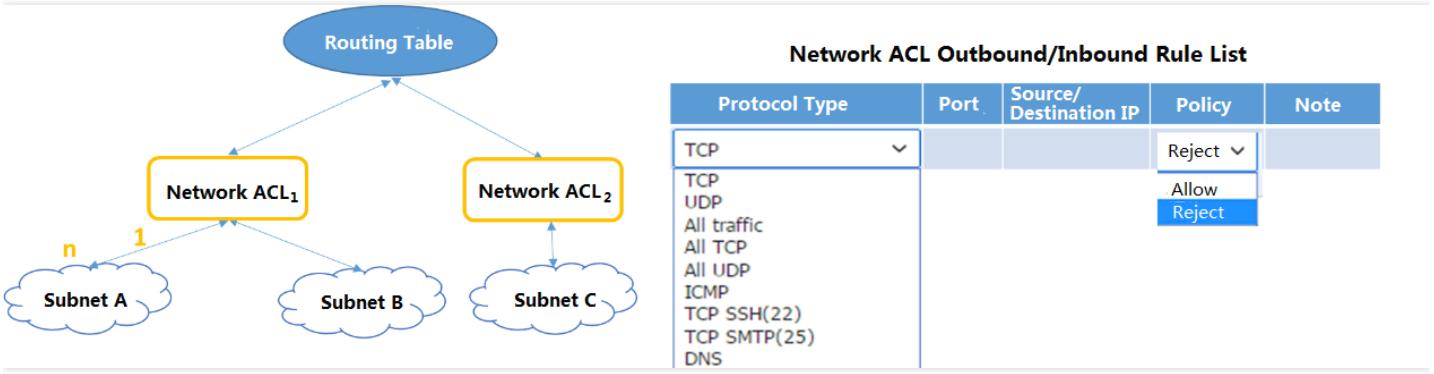
Contents

Security
Network ACL

Last updated：2018-10-18 15:51:25

Basics

The network Access Control List (ACL) is a stateless optional layer of security at the subnet level to control the traffic in and out of subnets (accuracy up to protocol and port granularity). The network ACL rules are similar to security group, as shown below: However, since the network ACL is stateless, even if certain access is set allowed in inbound rules, the access will still become unavailable due to lack of proper settings in outbound rules.



Usage Scenarios

The user can associate a network ACL with multiple subnets with the same network traffic control. By setting the outbound and inbound allowing rules, the traffic in and out of subnets can be precisely controlled. For example, when multiple layers of Web applications are hosted in Tencent Cloud private gateways, and Web layer, logic layer and data layer services are deployed for different subnets, you can control the access among the three subnets through network ACL: Web layer subnet and data layer subnet cannot access each other, and only the logic layer can access the Web layer and data layer subnet.

ACL Rules

ACL rules are the parts of network ACL. When you add or remove rules from a network ACL, the changes are automatically applied to the subnets it's associated with.

The network ACL rules consist of the following four components:

- Protocol types, such as TCP, UDP and HTTP.
- Destination port or port range.
- The IP or IP range of the source data (inbound) or destination data (outbound) (represented by CIDR).
- Policy: Allow or refuse.

Tencent Cloud will evaluate the data packet and determine whether to allow the packets to flow in and out of the subnets to which it is associated based on the ACL inbound/outbound rules associated with the subnet.

Priority of ACL Rules

The network ACL rules shall be sequentially applied from the first rule (the top of the list) to the last rule (the bottom of the list). In case of conflicts between rules, the rule that is ***higher in the list*** will be applied by default.
For example, if you need to allow all source IPs to access all ports on the CVM, and refuse only the HTTP access to port 80 of the host with the source IP of `192.168.200.11/24`, you can set it as follows:

Protocol Type	Port	Source IP	Policy
HTTP	80	192.168.200.11/24	Refuse
ALL	ALL	0.0.0.0/0	Allow

Ephemeral Port Range

Ephemeral ports need to be set when the client initiates a request. Please note this when setting the network ACL outbound rules. Since the network ACL is stateless, even if certain access is set allowed in inbound rules, the access will still become unavailable due to lack of proper settings in outbound rules.

For example, a client initiates a request to a CVM in a subnet in your VPC, and the subnet is associated with a network ACL. The ports configured by the client by default belong to the ephemeral port range. If the traffic allowed on the corresponding ephemeral ports is not set in the network ACL outbound rules, the client request cannot be returned. The range varies depending on the client's operating system.

- Many Linux kernels use ports 32768-61000.
- Windows Server 2003 uses ports 1025-5000.
- Windows Server 2008 uses ports 49152-65535.

Therefore, if a request comes into a Web server in a subnet in your VPC from a Windows XP client on the Internet, and the subnet is associated with a network ACL, your network ACL must have proper outbound rules to enable traffic destined for ports 1025-5000.

Comparison of Security Group and Network ACL

Security Group	Network ACL
Control traffic at the CVM instance level (the first layer of defense)	Control traffic at the subnet level (the second layer of defense)
Supports allowing rules and refusing rules	Supports allowing rules and refusing rules
Stateful: Returning traffic is automatically allowed, regardless of any rules	Stateless: Returning traffic must be explicitly allowed by rules
Applies to an instance only if you specify the security group when activating the CVM instance, or associates the security group with the instance later on	Automatically applies to all CVM instances in the associated subnets (backup layer of defense if the CVM instance is associated with security group)

Usage Constraints

The following are what you need to know about network ACL:

- You can associate a network ACL with multiple subnets; however, a subnet can be associated with only one network ACL at a time.
- A network ACL has separate inbound and outbound rules, each of which includes protocol type, port, source/destination IP, policy (refuse/allow), and note.
- By default, each new network ACL is set closed (refuse all traffic) until you add rules.
- Network ACLs are stateless; responses to allowed inbound traffic are subject to the rules for outbound traffic (and vice versa). In other words, you need to set rules for the traffic request and response respectively.
- Network ACLs do not affect the access between CVM instances in the associated subnets.

Resource	Limit
Number of network ACLs per VPC	50
Number of rules per network ACL	Inbound: 20, outbound: 20

Resource	Limit
Number of network ACLs associated per subnet	1
Number of subnets associated per network ACL	Unlimited

Billing Method

Network ACL services are free of charge. For more information about charges for other VPC services, please refer to Overview of VPC Service Billing

Operation Instruction

Creating a Network ACL

1) Log in to Tencent Cloud Console, click on the **Virtual Private Cloud** navigation bar to enter the Virtual Private Cloud Console, and then select **Security - Network ACL** tab on the left.
2) Click **New**, enter the name of the new network ACL and the VPC to which it belongs in the pop-up box, and then click **OK**.

Querying a Network ACL

1) Log in to Tencent Cloud Console, click on the **Virtual Private Cloud** navigation bar to enter the Virtual Private Cloud Console, and then select **Security - Network ACL** tab on the left.
2) Select the region and VPC on the top to check the network ACL of the VPC.

Adding Network ACL Rules

1) Log in to Tencent Cloud Console, click on the "Virtual Private Cloud" navigation bar to enter the Virtual Private Cloud Console, and then select **Security - Network ACL** tab on the left.
2) Click on the ID of the network ACL to be modified in the list to enter the details page of network ACL.
3) Click on the **Inbound Rule** or **Outbound Rule** tab, and **Edit** button next to the rule list, and then click on **New Line**.
4) The new rule will be added in the ***first line*** of the rule list by default. Select the protocol type and enter the port, source IP/destination IP and policy, and then click **Save**. The new rule will then be displayed in the ACL rule list.

Deleting Network ACL Rules

1) Log in to Tencent Cloud Console, click on the "Virtual Private Cloud" navigation bar to enter the Virtual Private Cloud Console, and then select **Security - Network ACL** tab on the left.

2) Click on the ID of the network ACL to be modified in the list to enter the details page of network ACL.
3) Click on the **Inbound Rule** or **Outbound Rule** tab, and **Edit** button next to the rule list, and then click **Delete** in the network ACL line to be deleted.
4) This ACL rule will then become gray. If this rule is deleted by mistake, you can undo it by clicking on **Recover the Deletion** button.
5) Click **Save** to save the above operations.

> Note: The deletion of ACL rules will take effect only after clicking on Save button.

Associating a Subnet with Network ACL

1) Log in to Tencent Cloud Console, click on the **Virtual Private Cloud** navigation bar to enter the Virtual Private Cloud Console, and then select **Security - Network ACL** tab on the left.
2) Click on the ID of the network ACL to be associated to enter the details page of network ACL.
3) Click on the **Basic Info** tab and then **Bind** button in the Associated Subnets.
4) In the pop-up box, select the subnet in the VPC that needs to be associated, and then click on **OK** to associate the network ACL with the subnet.

Dissociating a Subnet with Network ACL

1) Log in to Tencent Cloud Console, click on the **Virtual Private Cloud** navigation bar to enter the Virtual Private Cloud Console, and then select **Security - Network ACL** tab on the left.
2) Click on the ID of the network ACL to be dissociated to enter the details page of network ACL.
3) Click on the **Basic Info** tab; in the Associated Subnets list, click **Unbind** in the subnet line to be dissociated, or check all the subnets to be unbound, and click on **Unbind Selected** button to unbind the subnets to network ACL.

Deleting Network ACL

1) Log in to Tencent Cloud Console, click on the "Virtual Private Cloud" navigation bar to enter the Virtual Private Cloud Console, and then select **Security - Network ACL** tab on the left.
2) Click on **Delete** button in the network ACL line to be deleted, and then click on **OK** in the pop-up box to confirm deletion to delete the network ACL and its rules.
3) If the **Delete** button is gray, the network ACL is associated with a subnet. You need to unbind first before deleting it.

Related APIs

You can use API operations to set and manage network ACL APIs. For more information about VPC API functions, please refer to Overview of All VPC APIs.