9

Oracle Compute Cloud Service Network Settings

Objectives

After completing this lesson, you should be able to:

- Explain networking concepts
- Create security lists and security rules to enable access to your instance
- Disable access to your instance

How Do I Control Access to My Instance?

When you've created an instance, you can enable SSH access to your instance.

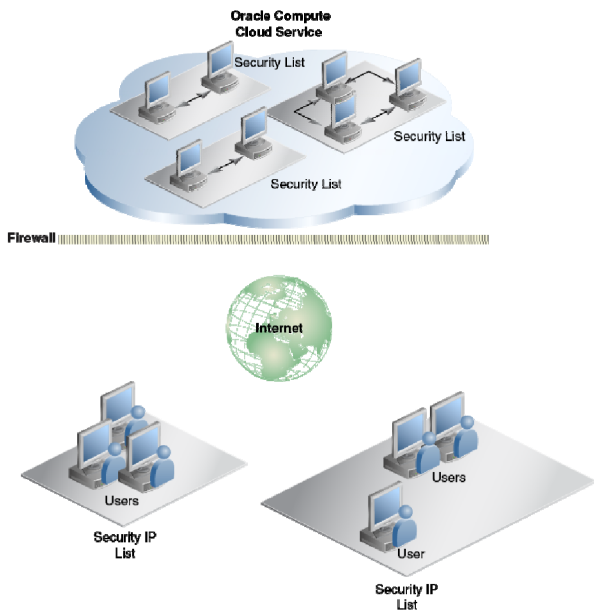
After creating an instance, you can enable or disable access to or from your instance by configuring network settings from the Oracle Compute Cloud Service web console.

You can implement fine-grained control over network access to your Oracle Compute Cloud Service instances, both from other instances as well as from external hosts over the public Internet.

When you've created an instance, you can enable SSH access to the instance. This SSH access is permitted only from hosts that have the SSH private key corresponding to the SSH public key stored on the instance. By default, your instance cannot be accessed from any other external host using any other protocol.

If you want to enable or disable access to your instance from other Oracle Compute Cloud Service instances or from other external hosts over the public Internet, you can use the web console to create security lists and configure network security rules.

How Do Security Lists Work?



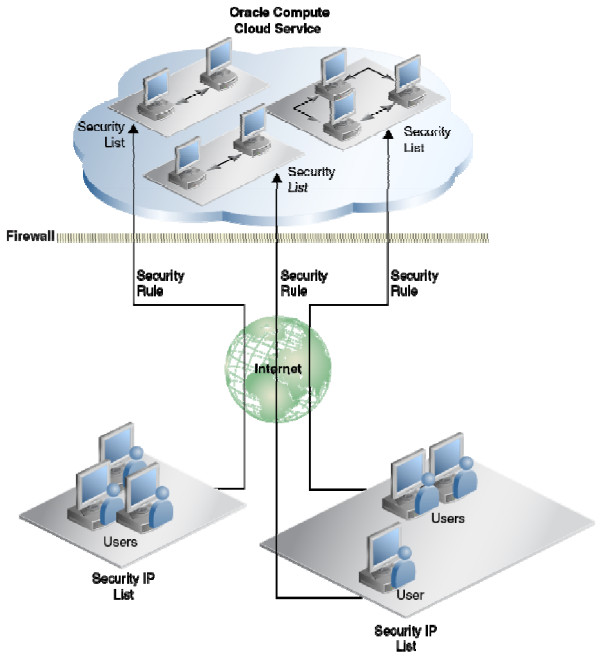
A security list is:

- A grouping of instances
- They can communicate with each other
- They cannot receive traffic from outside the security list

When you create an Oracle Compute Cloud Service instance, your instance is effectively protected by a firewall that controls the traffic to each instance.

If you want your instances to be able to communicate with each other, you can create a security list. A security list is a grouping of instances. When you add an instance to a security list, the instance can communicate with all the other instances in the same security list. However, instances in a security list by default cannot receive traffic from instances or external hosts outside their security list.

How Do Security Rules Work?



Security rules:

- Enable or disable access to instances in a security list
- From other security lists or from external hosts specified in security IP lists
- Over a specified protocol and port

Security rules allow you to enable or disable access to instances in a security list. Each security rule defines a specific source, a destination, and a protocol-port combination over which communication is allowed. If you want instances in two different security lists to be able to communicate with each other, you can create a security rule with one security list as the source and the other security list as the destination.

If you want your instance to be accessible to a specified set of external hosts, you can list the IP addresses of those hosts in a security IP list.

You can then create a security rule that specifies the security IP list as the source. This enables traffic from the specified set of external hosts to access the instances in your security list.

What Should I Know About Security Lists?

- Security lists define inbound and outbound policies.
  - The inbound policy controls the flow of traffic into the security list.
  - The outbound policy controls the flow of traffic out of the security list.
- By default, the inbound policy is deny and the outbound policy is permit.
- When you add an instance to a security list, the inbound and outbound policies of the security list are applicable to that instance.
- If no security rules are defined for a security list, then by default, instances in that security list cannot receive traffic from hosts outside the security list.
- When you remove an instance from a security list, the instance can no longer communicate with other instances in that security list, and it is no longer subject to the security rules defined for that security list.

Security lists define inbound and outbound policies to control the flow of traffic to and from instances.

The inbound policy

The inbound policy controls the flow of traffic into the security list. For example, if the inbound policy is set to permit, packets from all sources using any port or protocol are permitted to the instances in the security list. The default setting for this policy is deny. To control the flow of traffic to the instances in a security list, ensure that the inbound policy is set to deny, and then define security rules to allow only traffic from specified sources to access your instances using specified ports and protocols.

The outbound policy

The outbound policy controls the flow of traffic out of the security list. For example, if the outbound policy is set to deny, packets cannot flow out of the security list. The default setting for this policy is permit. To prevent instances in a security list from communicating with hosts outside the security list, set the outbound policy to deny.

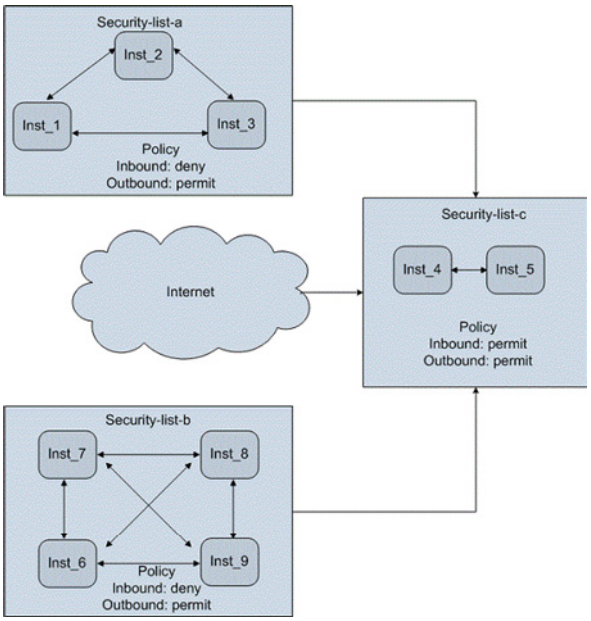
If you retain the default settings of a security list, the instances in that security list cannot receive inbound traffic from hosts outside the security list. You can override this default setting by creating security rules that use this security list as a destination.

A security list can be a source or destination in multiple security rules.

If no security rules are defined for a security list, then by default, instances in that security list cannot receive traffic from hosts outside the security list. However, instances in the security list can still access other instances in the same security list.

When you remove an instance from a security list, the instance can no longer communicate with other instances in that security list, and traffic to and from that instance is no longer controlled by the security rules defined for that security list.

Security Lists: An Example



- Security-list-a cannot receive inbound traffic
- Security-list-b cannot receive inbound traffic
- Security-list-c has inbound policy permit, so it can receive inbound traffic from Security-list-a and Security-list-b, as well as from the public Internet.

This illustration shows three security lists. Security-list-a and Security-list-b have the default inbound and outbound policies. Because the default inbound policy is deny, instances in these two security lists cannot be accessed from hosts outside their own security list. Security-list-c, however, has its inbound policy specified as permit. Instances in this security list can receive inbound traffic from Security-list-a and Security-list-b, as well as from the public Internet.

If an instance is added to multiple security lists that have different policies, then the most restrictive policy is applicable to the instance. For example, in this example, Inst_4 is in Security-list-c, which has the inbound policy permit. If you are to add Inst_4 to Security-list-b as well (inbound policy deny), then the effective inbound policy for Inst_4 would be deny. Inst_4 would still be able to communicate with Inst_5 in Security-list-c, as well as with Inst_6, Inst_7, Inst_8, and Inst_9 in Security-list-b. However, it would not be able to receive traffic from instances in Security-list-a or from external hosts.

What Should I Know About Security Rules?

Security rules consist of a source, a destination, and a security application.

- The source specifies the origin of inbound traffic. You can select either a security list or a security IP list as the source.
- The destination specifies the targeted end point of traffic. Usually, you specify a security list that you have already created as the destination in a security rule. However, if you have created a security list with the outbound policy deny, then you can specify that security list as the source and a security IP list as the destination in a security rule.
- A security application is a protocol-port mapping. When you specify a security application in a security rule, traffic is enabled over the specified protocol and port.

A security rule consists of a source, a destination, and a security application.

Source

The source in a security rule specifies the origin of inbound traffic. You can select either a security list that you have already created, or a predefined security IP list as the source. If you want your instances to receive traffic from any host over the public Internet, then select the predefined public-internet security IP list.

Destination

The destination in a security rule specifies the targeted end point of traffic. Usually, you specify a security list that you have already created as the destination in a security rule. However, if you have created a security list with the outbound policy deny, then you can specify that security list as the source and a security IP list as the destination in a security rule. This allows you to restrict traffic from your instances to a specific set of external hosts, identified by their IP addresses.

Security Application

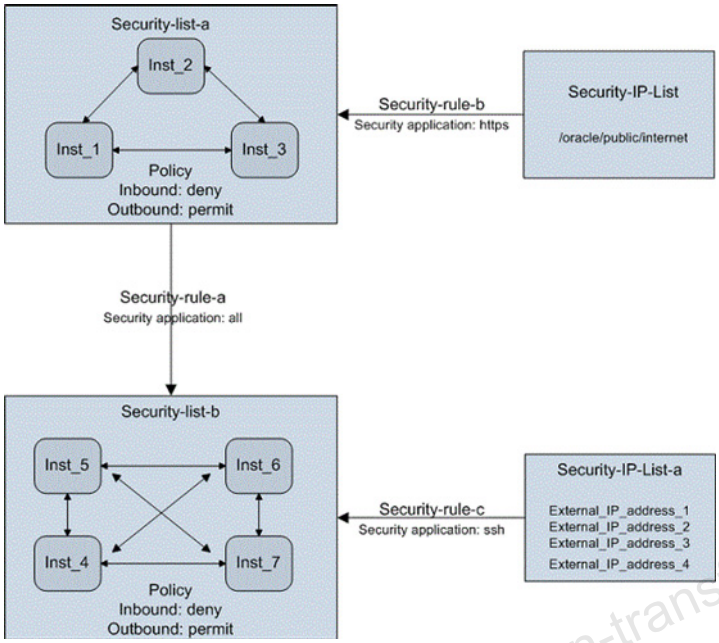
A security application is a protocol-port mapping. Several commonly-used protocols and their default ports are provided as predefined security applications. You can select one of these, or create a security application of your own.

When you specify a security application in a security rule, traffic is enabled over the specified protocol and port. If you want to enable traffic over all protocols and ports, select All.

A security rule acts only on a security list policy that is set to deny. If a security list has its inbound policy set to permit, then you do not need to define security rules to permit traffic to instances in that security list.

You can enable or disable a security rule at any time.

Security Rules: An Example



This illustration shows how you can use security lists and security rules to restrict traffic between your instances and control access to them.

This diagram shows the following communication paths:

- Instances in Security-list-a can send traffic to instances in Security-list-b over any protocol, as defined by Security-rule-a.
- Instances in Security-list-a can receive HTTPS traffic from any host on the public internet, as defined by Security-rule-b.
- Instances in Security-list-b can receive traffic over SSH from any of the IP addresses specified in Security-IP-list-a, as defined by Security-rule-c.

Is That How SSH Access to My Instance Works?

To enable SSH access to your instance:

- Associate a public IP address with your instance
- Add your instance to a security list
- Create a security rule to allow SSH access to the specified security list

To enable SSH access to your instance, add your instance to a security list and create a security rule which allows SSH access. You must also specify a public IP address for your instance.

Remember that instances in a security list can communicate with each other over all protocols and ports.

So, when you add your instance to a security list, if other instances also belong to the same security list, all those instances can communicate with each other.

Also, if you create a security rule with a security list as the source or destination, the security rule applies to all instances in that security list. So if you want to enable SSH access for one instance but not for other instances in the same security list, then create a separate security list for SSH access and add only instances that you want to access over SSH to the new security list.

So, Does My Instance Need a Public IP Address?

If you want to enable access to your instance over the public Internet, you must associate a public IP address with your instance.

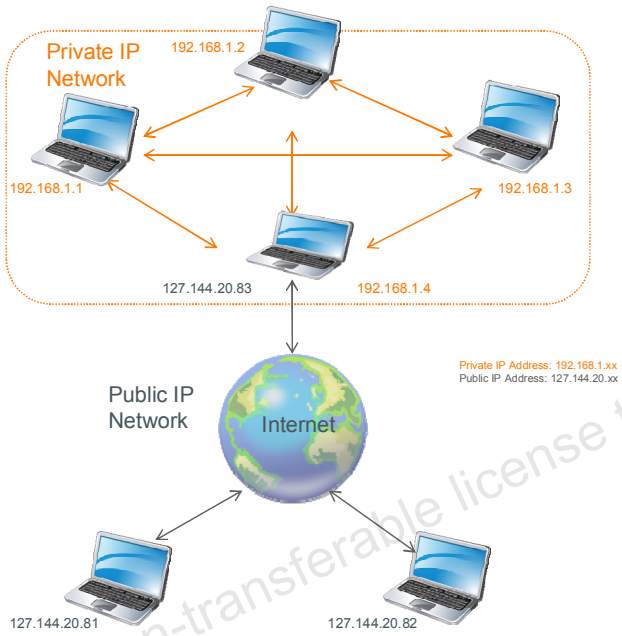
1. Go to the Oracle Compute Cloud Service console.
2. Click the Network tab.
3. Click Create IP Reservation.
4. Enter a name for the IP reservation.
5. In the **For Instance** field, select the instance that the IP address must be attached with.
6. Click Create.

An IP reservation is a public IP address that you can attach to an Oracle Compute Cloud Service instance that requires access to or from the Internet. You can create an IP reservation and associate it with an instance to enable access to the instance from the public Internet. You can do this either while creating an instance, or later on, when your instance is running.

- Go to the web console.
- Click the Network tab.
- Click the IP Reservations tab in the left pane.
- Click Create IP Reservation.
- Enter a name for the IP reservation.
- If your instance is running, then in the For Instance field, you can select the instance that the IP address must be attached with. Alternatively, you can create the IP reservation now without attaching it to any instance, and attach it later, while creating your instance.
- Click Create.

Does My Instance Need a Private IP Address?

- Each instance has a private IP address associated with it.
- When an instance is created, its private IP address is assigned dynamically from a range of private IP addresses.
- You can access an instance from another instance using its private IP address



- Each Oracle Compute Cloud Service instance has a private IP address automatically associated with it.
- When an instance is created, its private IP address is assigned from a range of private IP addresses.
- Private IP addresses aren't constant. When an instance is restarted, its private IP address might change.
- Private IP addresses can be repeated across several private networks, because they are not visible on the public networks.
- If, for reasons of data privacy, you don't want an instance to be accessible over the public Internet, you can opt not to associate a public IP address with that instance. You can then use the private IP address of the instance to access that instance from other instances in the same Oracle Compute Cloud Service account.
- Instances in the same security list also use private IP addresses to access each other. So instances in the same security list can communicate with each other even if they don't have public IP addresses.

I Get It. Can I Configure My Network Settings Now?

To configure your network settings:

1. Create a security list.
2. Add your instance to the security list.
3. Create a security IP list or use the predefined public-internet security IP list.
4. Create a security application or identify a predefined security application.
5. Create a security rule.

How Do I Create a Security List?

1. Go to the Oracle Compute Cloud Service console.
2. Click the Network tab.
3. Click the Security Lists tab in the left pane.
4. Click Create Security List.
5. Enter or select the required details:
   - Name
   - Description
   - Inbound policy
   - Outbound policy
6. Click Create.

To create a security list:

1. Go to the Oracle Compute Cloud Service console.
2. Click the Network tab.
3. Click the Security Lists tab in the left pane.
4. Click Create Security List.
5. Enter or select the required details:
   - **Name:** Enter a name that enables you to identify the purpose of this security rule
   - **Description:** Enter an appropriate description
   - **Inbound policy and Outbound policy:** Select the required inbound and outbound policies. Accept the defaults for now
6. Click Create.

How Do I Add My Instance to a Security List?

1. Go to the web console.
2. Click the Instances tab.
3. Go to your instance and from the menu icon, select View.
4. On the instance details page, click Add to Security List.
5. Select the required security list and click Attach.

To add your instance to a security list:

1. Go to the web console.
2. Click the Instances tab.
3. Go to your instance and, from the menu icon, select View.
4. On the instance details page, click Add to Security List.
5. Select the required security list and click Attach.

How Do I Create a Security IP List?

1. Go to the web console.
2. Click the Network tab.
3. Click the Security IP Lists tab in the left pane.
4. Click Create Security IP List.
5. Enter the following details:
   - Name
   - IP List
   - Description
6. Click Create.

To create a security IP list:

1. Go to the web console.
2. Click the Network tab.
3. Click the Security IP Lists tab in the left pane.
4. Click Create Security IP List.
5. Enter the following details:
   - **Name:** Enter a name for the security IP list.
   - **IP List:** Enter a comma-separated list of the subnets (in CIDR format) or IPv4 addresses for which you want to create the security IP list. For example, to create a security IP list containing the IP addresses 203.0.113.1 and 203.0.113.2, enter one of the following in the IP List field: **203.0.113.0/30 or 203.0.113.1, 203.0.113.2**
   - **Description:** Enter an appropriate description.
6. Click Create.

Which Security Application Do I Use?

Security list | Add instance | Security IP list | **Security application** | Security rule

Identify a Predefined Security Application:

1. Go to the web console.
2. Click the Network tab.
3. Click the Security Applications tab in the left pane.
4. Identify the security application that you want to use.

Create a Security Application:

1. Go to the web console.
2. Click the Network tab.
3. Click the Security Applications tab in the left pane.
4. Click Create Security Application.
5. Enter or select the following information:
   - Name
   - Port Type
   - Description
6. Click Create.

Several security applications are predefined for you. You can create a new security application, or use one of the predefined security applications in your security rules. To see the set of predefined security applications:

1. Go to the web console.
2. Click the Network tab.
3. Click the Security Applications tab in the left pane.

For now, identify the http security application and make a note of the name and port number of this security application. You can use this security application to create your security rule.

At any time, if you want to create a security application:

1. Go to the web console.
2. Click the Network tab.
3. Click the Security Applications tab in the left pane.
4. Click Create Security Application.
5. Enter or select the following information:
   - Name: Enter a name for the security application.
   - Port Type: Select the port type.
     - If you select the tcp or udp port type, then enter the port range.
     - If you select the icmp port type, then enter the ICMP type.
   - Description: Enter a meaningful description.
6. Click Create.

How Do I Create a Security Rule?

1. Go to the Oracle Compute Cloud Service console.
2. Click the Network tab.
3. Click Create Rule. The Create Security Rule dialog box is displayed.
4. Enter or select the following:
   - Name
   - Status
   - Security Application
   - Source
   - Destination
   - Description
5. Click Create.

To create a security rule:

1. Go to the web console.
2. Click the Network tab.
3. Click Create Rule. The Create Security Rule dialog box is displayed.
4. Enter or select the following:
   - **Name:** Enter a name for the security rule.
   - **Status:** By default, new security rules are enabled. Keep this default setting for now.
   - **Security Application:** Select the protocol that you want this security rule to use. Select the predefined http security application for now.
   - **Source:** Select the security list or security IP list from which traffic over the specified protocol should be allowed. Select public-internet for now.
   - **Destination:** Select the security or security IP list to which traffic should be allowed. Select the security list that you just created.
5. Click Create.

You can now access instances in your security list from any host over the public Internet using http.

But I Don't Want My Instance to be Accessible by Everybody. How Do I Disable Access to My Instance?

You can disable access to an instance in two ways:

- To prevent other hosts from accessing one specific instance, you can remove the instance from specific security lists that it is attached to.
- To prevent other hosts from accessing all the instances in a specific security list, you can disable specific security rules that use that security list.

To prevent other hosts from accessing an instance, you can restrict or disable access to the instance in either of the following ways:

To prevent other hosts from accessing one specific instance, remove the instance from specific security lists that it is attached to. When you remove an instance from a security list, the security rules that are defined for the security list are no longer applicable to the instance, and the instance cannot communicate with other instances in the security list. An instance that isn't associated with any security list is completely inaccessible. You can always use the web console to add such an instance to required security lists.

To prevent other hosts from accessing all the instances in a specific security list, you can disable specific security rules that use that security list. For example, consider a security list that is used as the destination in two security rules, one controlling traffic originating at external hosts listed in a specified security IP list, and the other controlling traffic originating at instances in another security list. You can disable either security rule, without affecting traffic controlled by the other security rule.

How Do I Remove an Instance from a Security List?

1. Go to the web console.
2. Click the Instances tab.
3. On the Instances page, identify the instance that you want to restrict access to. From the menu, select View.
4. On the instance details page, go to the security list that you want to remove your instance from. From the menu, select Remove from Security List.

How Do I Disable a Security Rule?

1. Go to the web console.
2. Click the Network tab.
3. Identify the security rule that you want to disable. From the menu, select Update.
4. In the Update Security Rule dialog box, set the Status to Disabled.
5. Click Update.

Quiz

Which steps are required to enable access to your instance?

a. Create the required security lists and security rules and add your instance to the appropriate security lists.
b. Ensure that you have associated a public IP address with your instance.
c. While creating an instance, select the option to configure the instance for SSH access.
d. Both a) and b)
e. Both b) and c)

Quiz

Which action should you take to prevent an instance from being accessed by an external host?

a. Remove the instance from security lists that it is attached to
b. Disable the security rules that apply to security lists that the instance is attached to

Quiz

An instance is a part of security list that has the inbound policy Deny. That security list used as a destination in a security rule that allows HTTP access from the public Internet. Can you access that instance from your computer using HTTP?

a. Yes
b. No

Summary

In this lesson, you should have learnt how to:

- Explain networking concepts
- Create security lists and security rules to enable access to your Instance
- Disable access to your Instance

Resource: Links

For more information regarding Oracle Compute Cloud Service, visit
http://docs.oracle.com/cloud/latest/stcomputecs/index.html