Setting up Network Restricted Access

Subtopics

Identity Domain Administrators and Service Administrators, by configuring a whitelist or a blacklist, can control whether Internet Protocol (IP) addresses belonging to a network can connect to a service instance. When used, a whitelist limits access to a service instance to the IP addresses that are associated with rules that allow such access. A blacklist, on the other hand, allows any IP address to connect to the service instance unless a rule that prohibits such access is enabled.

You use the Service Details screen of My Services to create whitelist or blacklist rules to regulate how users access a service instance. While creating rules, the Domain Administrator or Service Administrator identifies individual IP addresses, a range of IP address, subnets/masks, or Classless Inter-Domain Routing (CIDR) to identify the addresses that are allowed or denied access to the service instance.

See Managing Internet Protocol Whitelist and Blacklist Rules in *Getting Started with Oracle Cloud*.

Considerations

- Create a comprehensive plan that clearly identifies the IP addresses, address range, subnets, and CIDR that are allowed to access the service instance.
- Avoid conflicting rules (for example, rules that allow and deny access to an IP address or a range of addresses) by using a predefined list of addresses that should be allowed access to the service instance.
- To switch disposition (from using a whitelist to a blacklist or vice versa), you must first delete the rules of the disposition from which you are switching to the new disposition. For

example, if you switch from using a whitelist to using a blacklist, you must delete all existing whitelist rules.

- Only IPv4 addresses can be used to enable network restricted access.

Caution! Illustrations and examples in this discussion use private IP address (192.168.0.0) and its derivatives to demonstrate concepts. These are not intended to be examples to be emulated.

Creating a Whitelist

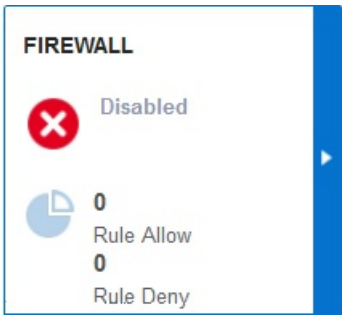
Generally, your whitelist includes rules that identify the outbound IP addresses that enable users of your network to access resources on the internet. If you want to further restrict access to a service instance, you can create allow rules for specific IP addresses or create rules that allow all IP addresses within an address range, subnet, or CIDR within your network to access the service instance.

Note: Allow rules that are defined for IP address range, CIDR, and subnet allows all IP addresses within the range, CIDR, or subnet to access the service instance. You can deny access to some IP addresses within the range, CIDR, or subnet by creating a rules that use the Deny rule type.

You must have at least one rule of allow rule type to enable the firewall using a whitelist.

➤ To create a whitelist to control access to a service instance:

1. Access My Services as an Identity Domain Administrator or as a Service Administrator.
2. Click the service instance for which you want to define restricted access.
3. In **Service Details**, click **FIREWALL**.

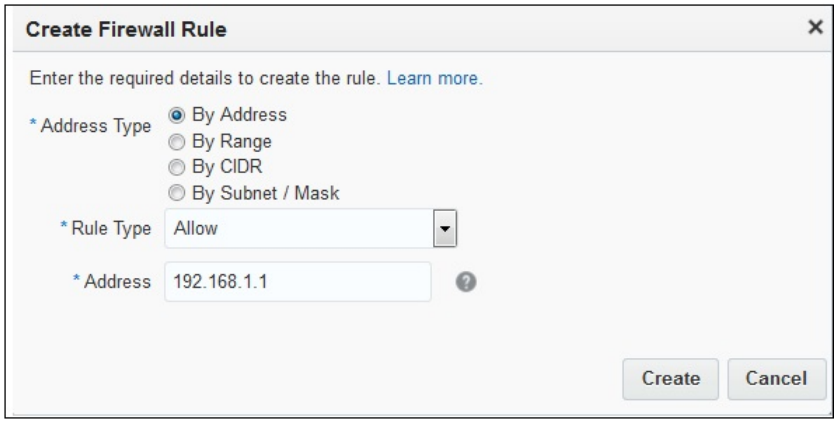


4. In **Disposition**, select **Whitelist**.

5 Click **Create Rule**.

6 In **Create Firewall Rule**, enter or select information:

- To create a rule that allows access to a specific IP address, select **By Address**, and then complete these steps:
  - In **Rule Type**, select **Allow** to permit this address to access the service instance.
  - In **Address**, enter an IP address.



- To create a rule for an IP addresses range, select **By Range** and then complete these steps:
  a. In **Rule Type**, select **Allow** to permit all the addresses within the range to access the service instance.
  b. In **Range**, enter the IP address range.
- To create a rule based on a CIDR, select **By CIDR**, and then complete these steps:
  a. In **Rule Type**, select **Allow** to permit all the addresses within the CIDR to access the service instance.
  b. In **Prefix**, enter a routing prefix (an IPv4 address)
  c. In **Size**, enter the CIDR prefix length which determines the part of the prefix used.
- To create a rule for addresses within a subnet, select **By Subnet / Mask**, and then complete these steps:
  a. In **Rule Type**, select **Allow** to permit all the addresses within the subnet to access the service instance.
  b. In **Subnet**, enter an IPv4 subnet address.
  c. In **Netmask**, enter the mask or number that determines the bits in use.

7 Click **Create**.

8 Click **Apply** to save your changes.

9 Click **Enable** to activate the firewall using the whitelist.

Enabling the whitelist takes a few moments.

Creating a Blacklist

Generally, your blacklist employs many deny rules to identify the IP addresses that should be prevented from accessing a service instance. You can create deny rules for specific IP addresses. You can also create deny rules that apply to an address range, subnet or CIDR to prevent all IP addresses within them from accessing the service instance.

Note: Deny rules that are defined for IP address range, CIDR, and subnet prevent all IP addresses within the range, CIDR, or subnet from accessing the service instance. You can allow access to some IP addresses within the range, CIDR, or subnet by creating a rule that uses the Allow rule type.

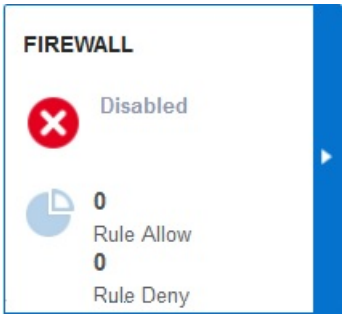
You can enable the firewall using a blacklist even if you have no blacklist rules.

➤ To create a blacklist to control access to a service instance:

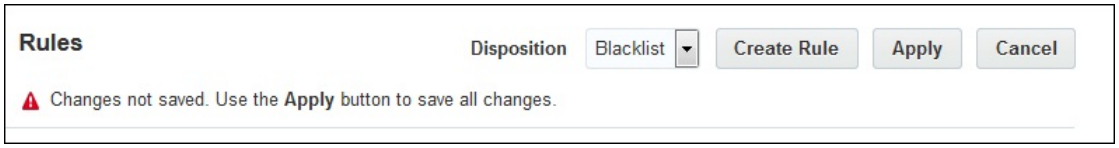
1 Access My Services as an Identity Domain Administrator or as a Service Administrator.

2 Click the service instance for which you want to define restricted access.

3 In **Service Details**, click **FIREWALL**.



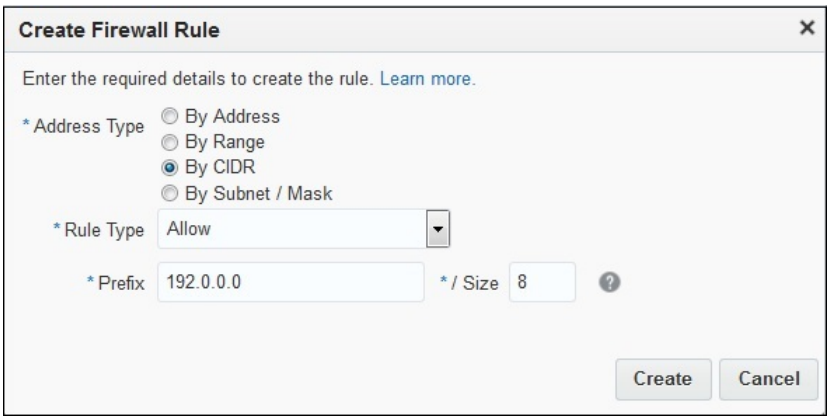
4 In **Disposition**, select **Blacklist**.



5 Click **Create Rule**.

6 In **Create Firewall Rule**, enter or select information:

- To create a rule for a specific IP address, select **By Address**, and then complete these steps:
  a. In **Rule Type**, select **Deny** to prevent this address from accessing the service instance.
  b. In **Address**, enter an IP address.
- To create a rule for an IP addresses range, select **By Range** and then complete these steps:
  a. In **Rule Type**, select **Deny** to prevent all the addresses within the range from accessing the service instance.
  b. In **Range**, enter the IP address range.
- To create a rule based on a CIDR, select **By CIDR**, and then complete these steps:
  a. In **Rule Type**, select **Deny** to prevent all the addresses within the CIDR from accessing service instance.
  b. In **Prefix**, enter a routing prefix (an IPv4 address)
  c. In **Size**, enter the CIDR prefix length which determines the part of the prefix used.



- To create a rule for addresses within a subnet, select **By Subnet / Mask**, and then complete these steps:
  a. In **Rule Type**, select **Deny** to prevent all the addresses within the subnet from accessing the service instance.
  b. In **Subnet**, enter an IPv4 subnet address.
  c. In **Netmask**, enter the mask or number that determines the bits in use.

7 Click **Create**.

8 Click **Apply** to save changes.

9 **Click Enable to activate the firewall using the blacklist.**

Enabling the blacklist takes a few moments.

Use-Cases

Subtopics

- Whitelist
- Blacklist

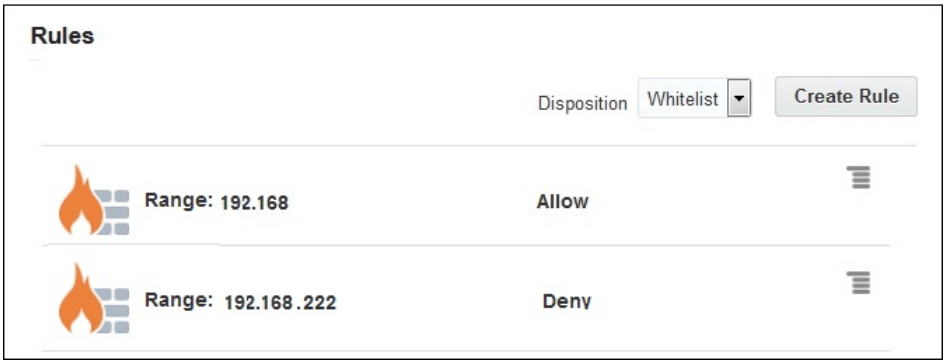
Illustrations and examples in this discussion use the private IP address (192.168.0.0) and its derivatives to demonstrate concepts. These are not intended to be examples to be emulated.

Whitelist

This graphic shows two allow rules, one that allows a specific IP address (192.168.45.21) and the other, which allows all IP addresses within a CIDR (192.168.1.0/24) to connect to the instance.

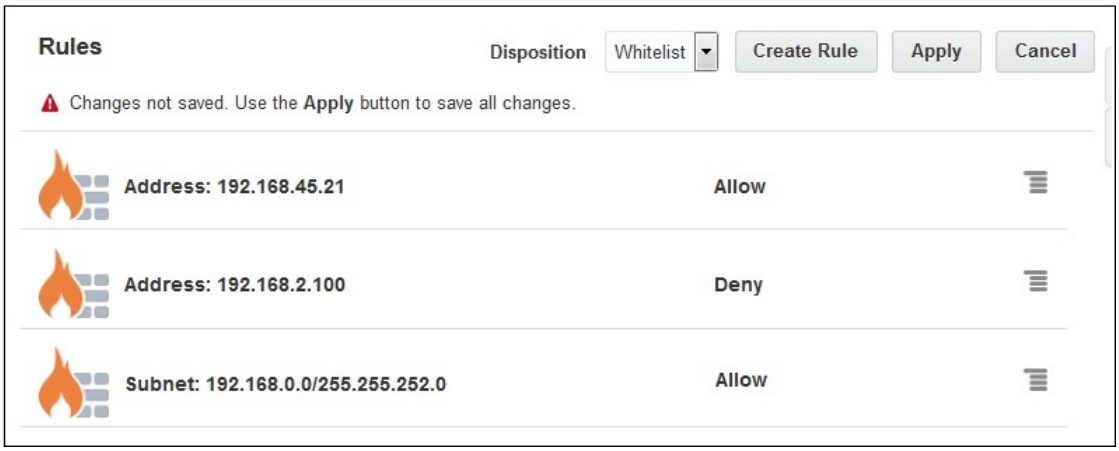
This graphic shows two allow rules, one that allows a specific IP address (192.168.45.21) and the other, which allows all IP addresses within a subnet (192.168.0.0/255.255.252.0) to connect to the instance.

This graphic shows a rule that allows an IP address from a range (192.168) to access the instance. A deny rule is used to prevent IP Addresses from a part of the range (192.168.222) from accessing the instance.



This graphic shows two allow rules, one that allows a connection from a specific IP address (192.168.44.21), and the other, which allows access from all IP addresses within a CIDR (192.168.1.0/24). A deny rule prevents access from an address (192.168.1.0/24) within the CIDR.

This graphic shows two allow rules, one that allows a connection from a specific IP address (192.168.45.21), and the other, which allows access from all IP addresses within a subnet (192.168.0.0/255.255.252.0). A deny rule prevents access from a specific IP address (192.168.2.100) within the subnet.



Blacklist

This graphic illustrates two deny blacklist rules that block access to the service by two specific IP addresses.

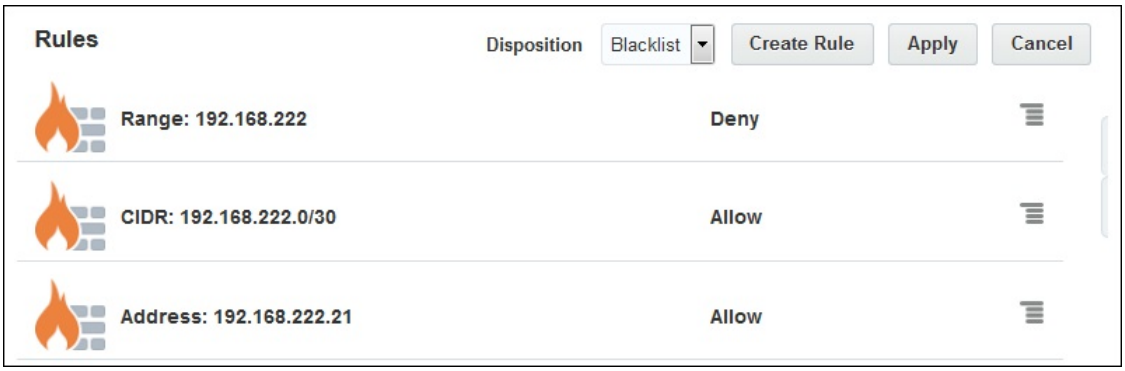
The following graphic depicts scenario in which a deny rule is used to block access to the service by all IP addresses of a range.

This graphic depicts a scenario in which deny rules are used to block access to the service by all IP addresses belonging to a specific range and CIDR.

This graphic depicts a deny rule that is used to block access for all IP addresses belonging to a subnet.

This graphic depicts two deny rules, one that blocks a range of IP addresses and the other that blocks all IP addresses of a CIDR. An allow rule is included in the blacklist to allow an address belonging to the range to access the service.

This graphic depicts a deny rule that blocks the IP addresses of a CIDR from accessing the service instance. Two allow rules, one providing access to a specific IP address and the other allowing access to addresses belonging to a subset of the CIDR, ensure access for authorized users.



COPYRIGHT NOTICE

Authors: EPM Information Development Team