Shared Objects

In an environment where you may have cloud-based managers such as AWS or GCP interacting with on-premises datacenters, it is crucial to be able to share objects within policies to protect your environment. Shared objects make it easy to maintain policies because you can modify an object in one place and that change affects all the other policies that use that object. Without shared objects, you would need to modify all the policies individually that require the same change.

Note that sharing objects is only supported when you deploy an access control policy that allows traffic from your cloud-based datacenter. Ensure that your policy includes, or excludes, instances or attributes from your third-party datacenter.

Multicloud Defense has the capability to communicate with either a datacenter or a cloud platform, ensuring your policies for security can be managed anywhere.

Static Objects

Static objects are shared between Multicloud Defense and CDO through a secure VPN tunnel. This allows you to create and share objects that maintain the same IP address or FQDN within a hybrid environment.

When looking at a shared object, Multicloud Defense shows you the contents of the object in the object table. Shared objects have exactly the same contents. Multicloud Defense shows you a combined or "flattened" view of the elements of the object in the details pane. Notice that in the details pane, the network elements are flattened into a simple list and not directly associated with a named object.

If you opt to delete an object that is shared, the deletion only occurs in Multicloud Defense. The object continues to exist within CDO.

Dynamic Objects

A dynamic object is an object that specifies one or many IP addresses that are shared between Multicloud Defense and CDO Unlike most other objects, dynamic objects do not have to be deployed to managed devices to take effect; any changes made to the original object, whether it originates from Multicloud Defense or not, is updated in real time and changes are immediately pushed with the next official deployment.

You must create a connector in CDO and attach the connector to an applicable policy to enable this feature and then import objects to see them in the Multicloud Defense Controller. See About the Multicloud Defense Connector, on page 2 for more information.

About the Multicloud Defense Connector

You can optionally send address objects from Cisco Multicloud Defense to the configured Cloud-delivered Firewall Management Center using a connector included with the Cisco Secure Dynamic Attributes Connector. A connector is responsible for gathering dynamic data (such as IP addresses) and streaming them to the Cloud-delivered Firewall Management Center so they can be used in access control policies.

For more information about Multicloud Defense objects, see the Address Objects chapter and address object API documentation.

For more information about the Multicloud Defense Connector, see the *Managing Firewall Threat Defense with Cloud-delivered Firewall Management Center in Cisco Defense Orchestrator*.

Import Objects From Cisco Defense Orchestrator

Note You do not have to enable dynamic sharing in the CDO dashboard to import objects to Multicloud Defense.

Use the following procedure to manually import Cisco Defense Orchestrator objects into Multicloud Defense using the Multicloud Defense Controller dashboard:

Step 1 Log into Cisco Defense Orchestrator and in the navigation pane located to the left, click Multicloud Defense.

Step 2 Click **Multicloud Defense Controller** located in the upper right to cross-launch into the controller dashboard.

Step 3 Navigate to **Manage** > **Security Policies** > **Addresses**

Step 4 Click **Import Objects**.

Step 5 From the pop-up window of Cisco Defense Orchestrator objects, scroll or use the search bar to locate an individual object.

NOTE: Objects with names that contain "**.**" are not supported by Multicloud Defense at this time. Attempting to share or import objects with periods in their name results in an error message.

Step 6 Select the object so it is highlighted and click **Import**. At any point click **Cancel** to back out of the action.

What to do next

Allow a few minutes for Multicloud Defense to communicate with Cisco Defense Orchestrator and synchronize the object you imported. From the Cisco Defense Orchestrator dashboard you will be able to see an updated shared object count in the "Multicloud Defense Shared Object" widget.