Address Objects

Address Objects

An **Address Object** represents a set of one or more IPs, CIDRs or FQDNs for use as a **Source** or **Destination** in a **Security Policy Rule Set Rule**, or as a **Target Backend Address** in a **Reverse Proxy Service Object**, depending on how it is defined. The Address Object can be configured statically using traditional constructs or dynamically using cloud constructs.

An address object represents a set of one or more IPs, CIDRs or FQDNs within a **Source**, **Destination**, or **Reverse Proxy Target** field within a security policy rule or rule set. It can also be defined as a target backend address within a reverse proxy service object. This section focuses on source and destination objects.

As of Version 24.04 and later, you can now configure an address object to **exclude** specific IP addresses or an IP address range.

Src/Dest

These objects are used to define match criteria that maps explicitly to IP addresses or CIDRs. The objects are referenced inside a policy rule and are evaluated against traffic entering a gateway instance when a policy rule is processed.

Source and destination address objects are useful when IP Addresses and CIDRs are explicitly needed to match application traffic entering a gateway instance. These objects are referenced inside the source anddestination fields of a policy rule definition. The type of address object used to populate each of these fields depends on the traffic flow, application type, and use-case.

Source or Destination Address Objects

A source or destination address object specifies a source or destination for a rule inside a security policy rule set. It is used by the rule to match traffic based on its source or destination IP address. The different types of address objects are defined as follows:

IP/CIDR/FQDN (Static) Address Objects

An IP/CIDR/FQDN address object is configured as a set of IP addresses, CIDR blocks or FQDNs. Examples of IP/CIDR address objects include:

- Destination IPs for DNS servers.
- Destination IPs for SMTP Relay Servers.
- Destination IPs for NTP servers.
- Source IPs or subnets for application workloads.

FQDN address objects define an explicit set of FQDNs for allowing or blocking IPs based on DNS resolution. When an FQDN is defined inside an FQDN address object and then referenced inside a policy rule, the gateway instance does a DNS resolution to retrieve the corresponding IP address(es) to match incoming traffic against. By default, caching is not enabled. In this case, the DNS resolution is done every 60 seconds, and the gateway instance uses the retrieved resolution for 60 seconds. If the FQDNs specified inside the FQDN address object are resolving to a large set of IP addresses (i.e. more than 400 each), then caching can be enabled. In this case, the DNS resolution interval can be specified, along with the cache size and cache TTL.

FQDN address objects are useful to match on application traffic that is either UDP based (ex. NTP) or TCP traffic for which host information does not exist in the request packet (ex. SMTP). In either case, it is recommended to use an FQDN address object to match on this kind of application traffic instead of manually defining a list of IP addresses for all appropriate NTP servers or SMTP servers, for example, your internal workloads are required to connect to.

Dynamic Cloud Constructs

Cloud-Native address objects are dynamic cloud resources discovered by the Multicloud Defense Controller through either periodic inventory collection (API-Based) or real-time event tracking (GCP Pub/Sub integration). These resources can be individual resources such as VPCs/VNETs, Instance IDs, security groups, Subnet IDs or a set of resources referenced through user-defined Tags. The multicloud defense controller uses a combination of real-time event tracking and targeted API calls to dynamically populate the IP addresses associated with the cloud resource. Therefore, any subsequent changes made to a cloud-native resource with be automatically reflected inside the address object referencing this resource.

Note Using cloud-native constructs to define source or destination address objects allows you to create a truly dynamic cloud policy across both single and multi-cloud environments. As cloud resources are added, deleted, or changed within a cloud environment, the address objects are dynamically updated to reflect these changes, making sure your security posture is automatically updated across all applications and functions in your environment.

User-Defined Tags in VNet and VPC Environments

Tags map the IP addresses or CIDR for a cloud resource defined with a set of tags to an address object. In GCP, labels are key-value pairs that are often used to categorize resources dedicated to different environments (i.e., development, staging, production, etc.). Inside a source or destination address object, user-defined tags can be used to reference resources including instances, VPCs/VNETs, subnets, and security groups. Most commonly, organizations use tags to categorize instances.

Tag based policy rules are a very powerful component of dynamic cloud policies. Granular policy rules can be defined for groups of instances with specific tags. With these policy rules in place, anytime a new instance is deployed with the appropriate tags, it automatically inherits the desired security policy defined for the category of instances it belongs to. This is because the Multicloud Defense Controller does not only discover a new instance has been deployed, but also the tags that have been assigned to that instance. It will then dynamically update the source or destination address object referencing this instance-based tags with the new instance's IP address. If an instance is deployed with the incorrect tags or no tags, it will not be allowed to communicate to any other resources because the appropriate policy rule is not matched against.

In VNets and VPCs, tags map the CIDR associated with the VPC to an address object CIDR. Provides a contextual way of creating a rule that matches any instance deployed within a VPC or VNET. Can use the name of a discovered VPC or VNET to define match criteria instead of having to manually figure out what CIDR is associated with a particular VPC or VNET. Any changes to the VPC or VNET will be dynamically updated in the policy rule with no intervention. If a VPC or VNET is removed and a new VPC/VNET is created in its place, the rule will no longer apply even if reusing the CIDR.

Instance ID

Instance IDs map the IP addresses associated with an instance to a list of IP addresses inside an address object. This provides a contextual way of creating a policy rule for a specific instance without manually figuring out how the instance is configured. The policy rule reflects any changes to the instance or its removal. Note that the policy rule cannot apply to any other instance, even if the instance is deleted and replaced with a new instance with the same configuration.

Security Group

Security Groups map the IP addresses of network interfaces associated with a security group to a list of IP addresses inside an address object. Any interface related changes, such as fields that are added or removed)to the security group, are dynamically reflected in the list of IP addresses inside the address object. This provides an organization with the ability to align existing security groups with the advanced security capabilities of the gateway data path pipeline.

Subnet IDs

Subnet IDs map the CIDR associated with a subnet to an address object CIDR. This provides a contextual way of creating a policy rule for all resources associated with a specific subnet ID without manually figuring out how the subnet is configured. A VPC or VNET is typically divided into multiple subnets and resources deployed within these subnets may serve different purposes. For example, instances in one subnet may require a specific set of advanced security profiles or may have a different traffic flow requirement. To simplify the process of creating different security rules for each subnet, Multicloud Defense gives you the capability to define a policy rule using the subnet's name as match criteria. Therefore, each subnet can have a unique policy rule, with unique security profiles. Any changes to the subnet and any instance deployed within the subnet is dynamically reflected in the policy rule.

Geo IP

A Geo IP address object is configured as a set of Geo IP country names. These objcts are used to allow or block traffic that is coming from or going to IP addresses based on their geographic location (country). Multicloud Defense integrates with the MaxMind GeoIP2 Database for maintaining a list of updated GeoIPs.

To review a full list of country names and codes, or IP address to GeoIP country codes, go to the GeoNames website.

Group

A group address object is configured as a set of sour or destination address objects. A group provides flexibility by defining individual address objects and then grouping them together, simplifying the number of rules necessary to match traffic based on the members of the group. The group inherits the set of IPs, CIDRs or FQDNs from the members of the group, whether the members are static, dynamic or a combination of the two.

Source or Destination Address Object Parameters

Type	Mode: Dynamic or Static	Parameter	Required or Optional	Notes
IP/CIDR/FQDN	Static	Value	Required	The total number of FQDNs per Address Object is limited to 200 where each FQDN can resolve to at most 400 IPs. The Multicloud Defense Gateway will perform DNS resolution every 60 seconds, regardless of the DNS record TTL.
VPC/VNet ID	Dynamic	CSP Account	Required	
		Region	Required	
		Resource Group	Optional	Azure Only
		VPC/VNet ID	Required	
Security Group	Dynamic	CSP Account	Required	
		Region	Required	
		VPC/VNet ID	Required	
		Resource Group	Optional	Azure Only
		Security Group ID	Required	

Type	Mode: Dynamic or Static	Parameter	Required or Optional	Notes
Application Security Group	Dynamic	CSP Account	Required	Azure Only
		Region	Required	
		Resource Group	Required	
		Application Security Group	Required	
Instance ID	Dynamic	CSP Account	Required	
		Region	Required	
		VPC/VNet ID	Required	
		Resource Group	Optional	Optional
		Instance ID	Required	
Subnet ID	Dynamic	CSP Account	Required	
		Region	Required	
		VPC/VNet ID	Required	
		Resource Group	Optional	Azure Only
		Subnet ID	Required	
User Defined Tag	Dynamic	CSP Account	Optional	
		Region	Optional	
		VPC/VNet ID	Optional	
		Resource Group	Optional	Azure Only
		Resource/Tag/Value	Required	List of Resources and Tag Key-Value Pairs.Resources can be Instance, VPC/VNet, Subnet, Load Balancer, Security Group, Security Group (Azure).
Geo IP		Value	Required	
Group		Address	Required	

Reverse Proxy Target Address Object

A reverse proxy target address object is specified as a backend target address in a reverse proxy service object. It is used by the service object to establish a backend connection to an application. The application can be the address of one or more application load balancers or instances in the form of IPs or FQDNs. The different types of reverse proxy target address objects are defined as follows:

Static IP/FQDN Address Object

An IP/FQDN address object is configured as a set of IP addresses or FQDNs. When more than one IP or FQDN is configured, the gateway handles the addresses without priority amongst the configured fields when setting up a backend connection. When an FQDN is configured, the gateway resolves the FQDN with DNS to determine the IP address to use when setting up a backend connection.

Dynamic Applications Address Object

An applications address object is configured as an individual application load balancer cloud resource determined by its applications tag. The configuration dynamically populates a set of IPs or FQDNs represented by the cloud resources, obtained from the cloud account using the Multicloud Defense real-time inventory discovery. Any changes to the cloud resources will be automatically reflected in the address object. When the configuration results in more than one IP or FQDN, the gateway handles the fields with no priority amongst the set when setting up a backend connection. When the configuration result is an FQDN, the gateway will resolve the FQDN with the DNS to determine the IP address to use when setting up a backend connection.

Reverse Proxy Target Address Object Parameters

Type	Mode: Dynamic or Static	Parameter	Required or Optional	Notes
IP/FQDN	Static	Value	Required	
Applications	Dynamic	CSP Account	Required	
		Region	Required	
		VPC/VNet ID	Required	
		Resource Group	Optional	Azure Only
		Tag/Value	Required	Single Tag Key-Value pair

System Objects

Multicloud Defense provides a list of pre-defined address objects to simplify policy creation. All system objects cannot be deleted or modified. Users can choose to clone system objects if modification is needed.

Name	Description
Any	This represents the entire IPv4 address space.

Name	Description
any-private-rfc- 1918	This represents all IPv4 private address as defined in RFC-1918.
Internet	This represents the entire IPv4 public address space, minus the private IPv4 addresses (RFC1918).

Create a Source/Destination Address Object

For information on what this object is, see Source or Destination Address Object Parameters, on page 4.
Use the following procedure to create a src/dst address object in Multicloud Defense:

Procedure

Step 1 Navigate to **Manage** > **Security Policies** > **Addresses**.

Step 2 Click **Create**.

Step 3 Select **Src/Dest**.

Step 4 Enter a unique **Name** to identify the address object.

Step 5 (Optional) Enter a description for the object. This may provide context to help differentiate the object from other objects.

Step 6 Select the **Object Type**. For information on object types and what they are, see Address Objects, on page 1. Select one of the following types:

- IP/CIDR/FQDN
- VPC/VNet ID
- Security Group
- Application ID (Azure only)
- Instance ID
- Subnet ID
- User-Defined Tag
- Geo IP
- Service End Point (Cloud Service IP)
- Group

Note If you select **Group**, you can include a specific IP address or a range of IP addresses to either include or exclude.

Step 7 Depending on which type you selected in step 6, enter the following paramters:

- **Value** - Enter a valid IP, CIDR, or FQDN IP address.

- **CSP Account** - Use the drop-down menu to select a cloud service provider account that has already connected to the controller.
- **Region** - Select the region your cloud service provider is located in.
- **VPC** - Use the drop-down menu to select the VPC or VNet. Note that options available may change depending on the cloud service provider account your choose.
- **Subnet** - Use the drop-down menu to select the subnet that applies to your VPC or VNet.
- (Azure only) **Resource Group** - Use the drop-down menu to select the resource group that is compatible with your selections.
  - **Resource Level** - Use the drop-down menu to select a value.
  - **Resource Tag** - Use the drop-down menu to select a keyword as the resource tag.
  - **Value** - Enter a valid value for the resource group. Note that this is different from the Value entry expected for IP/CIDR/FQDN objects.
- **Geo IP** - Use the drop-down menu to select a specific IP that is associated with the gelocation of your choice.
- **X-Forwarded-For Match Enabled** - Check this box to allow the gateway to match against XFF HTTP header fields.
- **Address** - Select an existing object. This selection determines the group of addresses that
- **Include Addresses** - This option is only applicable if you select "Group" as the type in step 6. Enter a specific IP address or a range of IP addresses to include. You can also use `any` to include all valid addresses.
- **Exclude Addresses** - This option is only applicable if you select "Group" as the type in step 6. Enter a specific IP address or a range of IP addresses to exclude. You can also use `any` to include all valid addresses. Note that there is no validation from the Multicloud Defense Controller for address exclusion.

Step 8 (Optional) Include a **Matching Expression**. This represent the set of conditions which must be matched for the object to execute.

Step 9 Click **Save** when complete.

Create a Reverse Proxy Target Address Object

For more information on what this object is, see Reverse Proxy Target Address Object Parameters, on page 6. Use the following procedure to create a reverse proxy target address object in Multicloud Defense:

Procedure

Step 1 Navigate to **Manage** > **Security Policies** > **Addresses**.

Step 2 Click **Create**.

Step 3 Select **Reverse Proxy Target**.

Step 4 Enter a unique **Name** to identify the address object.

Step 5 (Optional) Enter a description for the object. This may provide context to help differentiate the object from other objects.

Step 6 Select the **Object Type**. For information on object types and what they are, see Address Objects, on page 1. Select one of the following types:

- IP/CIDR/FQDN
- Applications

Step 7 Depending on which type you selected in step 6, enter the following paramters:

- **Value** - Enter a valid IP, CIDR, or FQDN IP address.
- **CSP Account** - Use the drop-down menu to select a cloud service provider account that has already connected to the controller.
- **Region** - Select the region your cloud service provider is located in.
- **VPC** - Use the drop-down menu to select the VPC or VNet. Note that options available may change depending on the cloud service provider account your choose.
- **Subnet** - Use the drop-down menu to select the subnet that applies to your VPC or VNet.
- (Azure only) **Resource Group** - Use the drop-down menu to select the resource group that is compatible with your selections.

Step 8 Use the drop-down menus to select both an existing **Applications Tag** and its **Value** for this object.

Step 9 Click **Save** when complete.

Edit Address Objects

If you need to modify a parameter that cannot be modified, you will need to Clone Address Objects the address object and then change the parameters as desired.

Use the following steps to edit an address object. Note that not all parameters can be edited.

Procedure

Step 1 Navigate to **Manage** > **Security Policies** > **Addresses**.

Step 2 Check the box next to the address object you would like to **Edit**.

Step 3 Click **Edit**.

Step 4 Modify the parameters as desired.

Step 5 Click **Save** when complete.

Clone Address Objects

If the desire is to use the clone in place of the original, you will need to replace all associations of the original with the clone. The associations will be in a set of one or more security policy rule set rules or reverse proxy service objects. The associations can be seen by viewing the View Details.

Use the following steps to clone an existing address object:

Procedure

Step 1 Navigate to **Manage** > **Security Policies** > **Addresses**.
Step 2 Check the box next to the address object you would like to **Clone**.
Step 3 Click **Clone**.
Step 4 Specify and modify the parameters as desired.
Step 5 Click **Save** when complete.

Delete Address Object

If an address object is actively used in a policy rule set or a reverse proxy service object, it will have one more associations and you will be unable to delete the address object. In order to delete an address object, you must first remove all associations, then the address object can be deleted. The associations can be seen by viewing the View Details.

Procedure

Step 1 Navigate to **Manage** > **Security Policies** > **Addresses**.
Step 2 Check the box next to the address object you would like to **Delete**.
Step 3 Click **Delete**.
Step 4 Click **Save** to confirm the delete.

View Details

You can view the address object **Details** by clicking the **Name** of an object from the **Manage** > **Security Policies** > **Addresses** page. The **Details** will display the IPs, CDIRs and FQDNs populated based on its type and configuration. It will also display the associations with policy rule sets and any object services.