Cisco Multicloud Defense User Guide

First Published: 2023-05-19

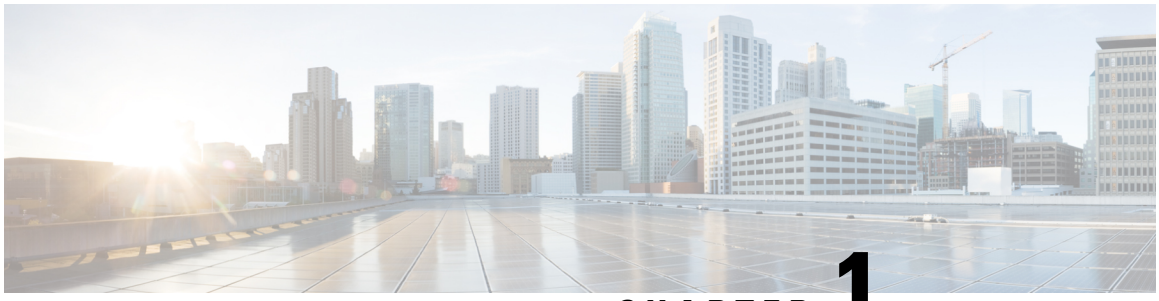
Last Modified: 2024-04-30

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

PART I

Multicloud Defense User Guide



CHAPTER 1

About Multicloud Defense

About Multicloud Defense

Multicloud Defense (MCD) is a comprehensive security solution consisting of two primary components: the Multicloud Defense Controller and Multicloud Defense Gateway. These components collaborate to establish a secure multicloud environment

Multicloud Defense currently supports Amazon Web Services (AWS), Azure, Google Cloud Platform (GCP), and Oracle OCI cloud accounts. The range of support for these platforms vary.

In essence, Multicloud Defense offers a sophisticated and streamlined security framework, harmonizing controller orchestration, gateway communication, and optimized datapath processing for a robust and efficient multicloud protection mechanism.

This documentation has been prepared for practitioners who have a basic understanding of public cloud networking and security concepts, and participate in various functional teams, including:

- Development Operations (DevOps and DevSecOps)
- Security Operation Centers (SOCs)
- Security Architects Info
- Sec Architects Cloud Architects

For more information on the components of this product, continue reading.

Additional Information

You can find additional information about Multicloud Defense in the following documents:

- Multicloud Defense Release Notes

Recommended Versions of Multicloud Defense Components

We recommend keeping your components up to date with the latest upgrades and updates for enhancements and new features, as well as bug fixes. For more information on what updates and upgrades are available, and what each package addresses, see the Cisco Multicloud Defense Release Notes.

Third Party Product Support and Versioning

Multicloud Defense utlilizes additional products and functions. For optimal operations, consider using the appropriate versions listed.

Internet Browsers

We support and recommend the following internet browsers for Multicloud Defense components:

Table 1: Internet Browser Support

Browser	Supported
Chrome	Yes. We **strongly** recommend this browser.
Firefox	Yes.
Edge	Yes.
Safari	Yes.
Inernet Explorer	Yes.

Instance Metadata Service For AWS

The Instance Metadata Service (IMDS) is used to access instance metadata from an Amazon EC2 instance. The Multicloud Defense Controller version 23.10 sets up IMDSv2 to be **Required** or **Optional** depending on the corresponding Multicloud Defense Gatewayversion.

We **strongly** recommend upgrading to a Multicloud Defense Gateway version that specifically supports IMDSv2 in the **Required** mode for optimal security with Amazon EC2 instances.

Note The Multicloud Defense Controller version 23.10 forces Multicloud Defense Gateway versions 23.04 and later to default to IMDSv2 for EC2 instances.

Use the table below to determine which IMDS version will be setup inside the EC2 instance for your environment:

Multicloud Defense Gateway Version	Required IMDS Version
23.08	IMDSv2 (required)
23.06	IMDSv2 (required)

Multicloud Defense Gateway Version	Required IMDS Version
23.04	IMDSv2 (required)
23.02	IMDSv1 IMDSv2 (optional)
22.12	IMDSv1 IMDSv2 (optional)

For more information on IMDS versions and how to migrate to the version of your choice, see AWS documentation.

Supported Disk Size

Consider the following disk size support for the appropriate gateway versions:

Table 2: Disk Size per Gateway Version

Gateway Version	Supported Disk Size
23.12 and later	128GB
up to 23.10	256GB

Multicloud Defense Components

Multicloud Defense uses a common principle in public clouds and software defined networking (SDN) which decouples the control and data plane, translating to two solution components - the Multicloud Defense Controller and the Multicloud Defense Gateway.

Multicloud Defense Controller

The Multicloud Defense Controller is a highly reliable and scalable centralized controller that provides the management and control plane. This runs as software-as-a-service (SaaS) and is fully managed and maintained by Multicloud Defense. Customers access a web portal to utilize the Multicloud Defense Controller, or they may choose to use the Multicloud Defense provider for terraform to instantiate security into the DevOps/DevSecOps processes.

Multicloud Defense Gateway

The Multicloud Defense Gateway is an auto-scaling fleet of Multicloud Defense software deployed as patform-as-a-service (PaaS) into the customers public cloud account/s by the Multicloud Defense Controller. This provides advanced, inline security protections to defend against external attacks, prevent egress data exfiltration and prevent the lateral movement of attacks. Multicloud Defense Gateways include functionality for TLS decryption, intrusion detection and prevention (IDS/IPS), web application firewall (WAF), antivirus filtering, data loss prevention (DLP) and FQDN/URL filtering capabilities.

Multicloud Defense SaaS Controller

The Multicloud Defense SaaS Controller manages the gateway stack. The controller, equipped with various microservices, includes an API Server facilitating orchestration of CSP LBs and gateway instances. This enables dynamic scaling through instance additions and removals from the load balancer's "target pool," monitored by the load balancer itself.

Communications

Multicloud Defense Gateways engage in continuous communication, approximately every 3 seconds, with the Multicloud Defense Controller, transmitting health status and policy updates. This enables proactive health reporting, gateway replacement, and scalability adjustments as needed.

Optimized Gateway Instances

Multicloud Defense Gateway instances operate on highly optimized software, incorporating a single pass datapath pipeline for efficient traffic processing and advanced security enforcement. Each gateway instance comprises three core processes: a "worker" process responsible for policy enforcement, a "distributor" process for traffic distribution and session management, and an "agent" process communicating with the controller. Gateway instances can seamlessly transition "in service" for a "datapath restart," enabling smooth updates without disrupting traffic flow.

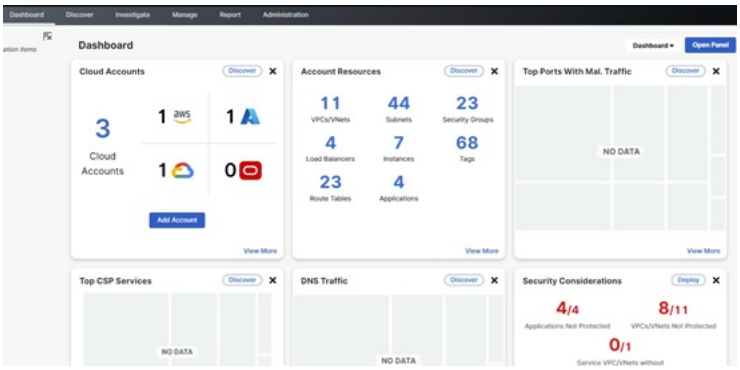
Advanced Security Profiles

Multicloud Defense Gateways implement granular security profiles within the single pass datapath pipeline, catering to evolving traffic needs. Customers have the flexibility to enable or disable **Advanced Security Profiles** as required. The pipeline's single pass architecture negates the need for traffic offloading to third-party engines. For instance, full TLS decryption is selectively triggered within the pipeline, ensuring efficient handling without unnecessary data transfers.

In essence, Multicloud Defense offers a sophisticated and streamlined security framework, harmonizing controller orchestration, gateway communication, and optimized datapath processing for a robust and efficient multicloud protection mechanism.

Multicloud Defense Controller Dashboard

The dashboard of the Multicloud Defense Controller has a multitude of widgets to give you a quick snapshot of the current state of your accounts, account resources, and top-hitting policies or profiles.



For your ease, you can drag/drop any of the following widgets to customize and organize the dashboard to whatever fits your needs. You can also click "x" on any of the widgets to remove it from your dashboard view, or "View More" to go directly to the page affiliated with the widget in question. At the top of each widget is an indication as to what function of Multicloud Defense the widget serves: discovery, detection, deployment, or defending.

The following widgets are generated by default:

Cloud Accounts

This is a high-level view to how many cloud accounts you have connected to the Multicloud Defense Controller, and how many of what cloud service provider.

You can easily click "Add Account" from this widget and launch into the connecting wizard to assist onboarding a new cloud service provider.

Account Resources

This is a general list of allocated resources across all of your connected cloud accounts. It displays how many of the following resources are currently used:

- VPC/VNets.
- Subnets.
- Security Groups.
- Load Balancers.
- Instances.
- Tags.
- Route Tables.
- Applications.

Top CSP Services

This top-down display of cloud service provider services generalizes DNS traffic of the cloud service providers you already have connected to the Multicloud Defense Controller.

DNS Traffic

Similar to "Top CSP Services", this DNS Traffic widget offers a limited view of current DNS traffic for the cloud service providers that are actively processing traffic. We recommend expanding the widget to the full discovery scope for more insight.

VPCs/VNets with Malicious Traffic

This widget displays any recent VPC or VNet that has encountered mlaicious traffic. For a comprehensive list of events and attacks, expand the widget and view the traffic.

Top Ports with Malicious Traffic

This small snapshot displays whi ports amongst your cloud accounts have the most hits against malicious traffic.

Security Considerations

The Security Considerations widget is a suggestive widget, summarizing which applications, VPCs or VNets, and associated gateways are not protected by the means provided in Multicloud Defense.

System Logs

The System Logs window supplies a recent history of logs that catalogue the accounts affects, the gateway associated, the severity of events or attacks and more. We strongly recommend utilizing this widget, if not the whole System Log page as a valuable resource.

Top Applications

This window accounts for the top-most applications across all cloud service providers that are used.

Threats

View a graph depicting the last seven days of traffic and how much of the incoming traffic was categorized as threats.

Top Countries by Threat

This horizontal bar chart depicts a snapshot of the top 10 countries that during the entirety of the timespan produced the most events, then displayed breaking that volume across the time increments for which the events occurred during the timespan.

Exfiltration Attempts

View a general display of egress data exfiltration that have occurred on the cloud service providers currently connected to Multicloud Defense.

My Profile Information

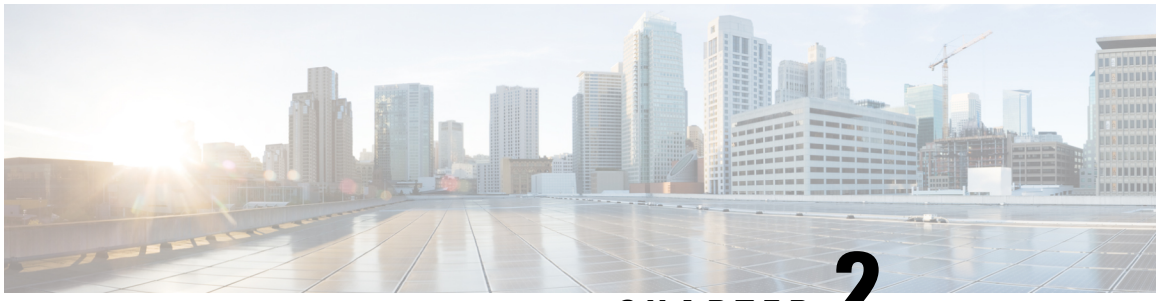
The User Profile page is the page that details your user information. Access this page by dropping down the **Admin** arrow in the upper right corner of the Multicloud Defense dashboard. Click your username to see the following information:

- Your name.
- The email address associated with your Multicloud Defense account.
- The user role you currently have.
- The name of the tenant you are currently logged into.
- Any and all assigned accounts.

This page can be useful for general knowledge, or in the case you reach out for assistance with the Cisco Support team.

PART II

Setup with the Multicloud Defense Wizard



CHAPTER 2

Setup with the Multicloud Defense Wizard

The Multicloud Defense Controller provides a SaaS-delivered centralized control plane to deploy and manage Multicloud Defense and its security policy.

The **Setup** helps guide users through the process of setting up Multicloud Defense security using a series of these simple steps:

- **Connect your Account** - This process onboards your cloud service provider account to Multicloud Defense and simultaneously discovers regions and additional inventory and assets affiliated with your account.
- **Enable Traffic Visibility** - Utilizing the easy setup method enables the collection of logs to understand the flow of traffic.
- **Secure Your Account** - This procedure facilitates setting up a VNET or VPC, depending on the cloud account you have, and a Multicloud Defense Gateway to secure your experience.

- Connect Cloud Account, on page 9
- Enable Traffic Visibility, on page 15
- Secure Your Account, on page 16

Connect Cloud Account

The first step is to onboard a set of one or more coud accounts. This allows the Multicloud Defense Controller to interact with each account by discovering inventory, enabling traffic and logs, orchestrating security deployment, and creating and managing policy.

Use the following procedures to connect you cloud service provider account to Multicloud Defense Controller.

Connect AWS Account

Use the following procedure to connect to an AWS subscription through Multicloud Defense's easy setup wizard.

Before you begin

- You must have an active Amazon Web Services (AWS) account.
- You must have an Admin or Super Admin user role in your CDO tenant.

- You must have Multicloud Defense enabled for your CDO tenant.

Note Multicloud Defense Controller version 23.10 defaults to IMDSv2 in the AWS EC2 instance when using Multicloud Defense Gateway version 23.04 or newer. For more information about the difference beween IMDSv1 and IMDSv2, see AWS documentation.

Step 1 In the CDO dashboard, click the **Multicloud Defense** tab located in the left naviation pane.

Step 2 Click **Multicloud Defense Controller** located in the upper right window.

Step 3 From the Multicloud Defense Controller dashboard, click **Setup** located to the left of the window.

Step 4 Select **Connect Account**.

Step 5 Select the AWS icon.

Step 6 Enter the following information in the modal:

a) Click **Launch Stack** to download and deploy our CloudFormation template. This should open up another tab to deploy the template. Login to AWS is required.

b) Copy and paste the controller IAM role ARN from the CloudFormation stack output in the CloudFormation template.

c) In the Multicloud Defense Controller easy setup modal, enter the **AWS Account Number**. This number can be found in the output value **Current Account** of the CloudFormation Template.

d) Enter an **Account Name** that will be assigned to your account in the Multicloud Defense Controller.

e) (Optional) Enter an account **Description**.

f) Enter the **External ID**. This is a random string for IAM role's trust policy. This value will be used in the controller IAM role created. You can edit or regenerate the External ID.

g) Enter the **Controller IAM Role**. This is the IAM role created for the Multicloud Defense Controller during CloudFormation Template (CFT) deployment. Look for the output value MCDControllerRoleArn in CFT stack. It should be something similar to this: `arn:aws:iam::<Acc Number>:role/ciscomcdcontrollerrole`.

h) Enter the **Inventory Monitor Role**. This is the IAM role created for Multicould Defense Inventory during CFT deployment. Look for the output value MCDInventoryRoleArn in CFT stack. Should be something similar to this: `arn:aws:iam::<Acc Number>:role/ciscomcdinventoryrole`.

Step 7 Click **Next**. The account is onboarded to the Multicloud Defense Controller.

What to do next

Once you've connected the account, Multicloud Defense Controller automatically starts to discover assets and inventory associated with the cloud service provider account. Note that this is different from discovering traffic. Because Multicloud Defense Controller discovers account assets and inventory by default, the next step in this wizard is to Enable Traffic Visibility.

Connect Azure Account

Use the following procedure to connect to an Azure subscription through Multicloud Defense Controller's easy setup wizard:

Before you begin

- You must have an active Azure subscription.
- You must have an Admin or Super Admin user role in your CDO tenant.
- You must have Multicloud Defense enabled for your CDO tenant.

Step 1 In the CDO dashboard, click the **Multicloud Defense** tab located in the left naviation pane.

Step 2 Click **Multicloud Defense Controller** located in the upper right window.

Step 3 From the Multicloud Defense Controller dashboard, click **Setup** located to the left of the window.

Step 4 Select **Connect Account**.

Step 5 Select the Azure icon.

Step 6 Enter the following information in the modal:

a) Click the link to open an Azure Cloud Shell in bash mode.
b) In the Azure account modal, click **Copy** to copy the onboading script and execute it in the bash shell that was opened in step 1.
c) In the Azure account modal, provide a name for this Azure account. You can choose to name this the same as your Azure subscription name. This name is visible on the Multicloud Defense Controller accounts page only.
d) (Optional) Provide a description for the subscription.
e) Enter the **Directory ID**, also referred as the Tenant ID.
f) Enter the **Subscription ID** for the subscription being onboarded.
g) Enter the **Application ID**, also referred to as the Client ID, created by the onboarding script.
h) Enter the **Client Secret**, also referred to as the Secret ID.

Step 7 Click **Next**.

What to do next

Once you've connected the account, Multicloud Defense Controller automatically starts to discover assets and inventory associated with the cloud service provider account. Note that this is different from discovering traffic. Because Multicloud Defense Controller discovers account assets and inventory by default, the next step in this wizard is to Enable Traffic Visibility.

Connect Google Cloud Platform Account

Use the following procedure to use the Multicloud Defense Controller's easy setup wizard to onboard a GCP project as an account:

Before you begin

- You must have an active Google Cloud Platform (GCP) project.
- You must have the necessary permissions to create VPCs, subnets, and a service account withint your GCP project. See GCP doucmentation for more information.
- You must have an Admin or Super Admin user role in your CDO tenant.
- You must have Multicloud Defense enabled for your CDO tenant.

Step 1 In the CDO dashboard, click the **Multicloud Defense** tab located in the left naviation pane.

Step 2 Click **Multicloud Defense Controller** located in the upper right window.

Step 3 From the Multicloud Defense Controller dashboard, click **Setup** located to the left of the window.

Step 4 Select **Connect Account**.

Step 5 Select the GCP icon.

Step 6 Enter the following information in the modal:

a) Click the **Cloud Platform Cloud Shell** to launch the Cloud Shell.

b) Copy the command generated in the Multicloud Defense Controller easy setup modal and paste the command into the Cloud Shell. Execute it to initiate the onboarding process. This script automatically creates user accounts for the Multicloud Defense Controller to communicate directly with your GCP project.

c) In the Multicloud Defense Controller easy setup modal enter a name for the account. You can choose to name this the same as your GCP project name. This name is visible on the Multicloud Defense Controller only.

d) (Optional) Enter a **Description**.

e) Enter the **Project ID** for the GCP project.

f) Enter the **Client Email** for the service account created for Multicloud Defense Controller.

g) Enter the **Private key** of the service account.

Step 7 Click **Next**.

What to do next

Once you've connected the account, Multicloud Defense Controller automatically starts to discover assets and inventory associated with the cloud service provider account. Note that this is different from discovering traffic. Because Multicloud Defense Controller discovers account assets and inventory by default, the next step in this wizard is to Enable Traffic Visibility.

Connect OCI

You must execute the following prerequisites prior to onboarding an Oracle Cloud (OCI) account.

Login to OCI

1. Login to your OCI tenant.

Create Group

Step 1 Navigate to **Identity & Security** > **Groups**.

Step 2 Click **Create Group**.

Step 3 Specify the following:

- **Name:** Multicloud Defense-controller-group
- **Description:** Multicloud Defense Group

Step 4 Click **Create**.

Create Policy

When creating an OCI account with Multicloud Defense you need to create and apply a firewall policy. Use the following procedure and recommendations to create a policy:

Step 1 Navigate to **Identity & Security** > **Policies**.

Step 2 Select the **Compartment** *root* .

Step 3 Click **Create Policy**.

Step 4 Specify the following:

- **Name:** Multicloud Defense-controller-policy.
- **Description:** Multicloud Defense Policy.
- **Compartment:** [Must be the "root" Compartment].

Step 5 Under **Policy Builder** enable **Show manual editor**.

Step 6 Modify and paste the following policy:

```
Allow group <group_name> to inspect instance-images in compartment <compartment_name>
Allow group <group_name> to read app-catalog-listing in compartment <compartment_name>
Allow group <group_name> to use volume-family in compartment <compartment_name>
Allow group <group_name> to use virtual-network-family in compartment <compartment_name>
Allow group <group_name> to manage volume-attachments in compartment <compartment_name>
Allow group <group_name> to manage instances in compartment <compartment_name>
Allow group <group_name> to {INSTANCE_IMAGE_READ} in compartment <compartment_name>
Allow group <group_name> to manage load-balancers in compartment <compartment_name>
Allow group <group_name> to read marketplace-listings in tenancy
Allow group <group_name> to read marketplace-community-listings in tenancy
Allow group <group_name> to inspect compartments in tenancy
Allow group <group_name> to manage app-catalog-listing in compartment <compartment_name>
```

- **group_name:** Multicloud Defense-controller-group.
- **compartment_name:**[Compartment where Multicloud Defense will be deployed].

Note When replacing the **<compartment_name>** with the name of the compartment where the policy will apply, if the compartment is a sub-compartment, the name format is **compartment:sub-compartment** (e.g., Prod:App1).

If the **<compartment_name>** is specified as the root compartment (e.g., multicloud (root)), OCI will not accept the policy and will produce an error: *Invalid parameter*. The policy will need to be defined for an specific compartment and that compartment cannot be the root compartment.

Step 7 Click **Create**.

Create User

Step 1 Navigate to **Identity & Security** > **Users**.

Step 2 Click **Create User**.

Step 3 Specify the following:

- **Name:** *Multicloud Defense-controller-user*
- **Description:** *Multicloud Defense User*

Step 4 Click **Create**.

Create API Key

Step 1 From the **User Details** view for the User, select **API Keys**.

Step 2 Click **Add API Key**.

Step 3 Select **Download Private Key** and retain the Private Key for future use.

Step 4 Select **Download Public Key** and retain the Public Key for future use.

Step 5 Click **Add**.

Accept Terms and Conditions

Use the following procedure to acceot the Terms and Conditions for an OCI account:

Step 1 Select **Compute** > **Instance**.

Step 2 Choose the desired **Compartment**.

Step 3 Click **Create instance**.

Step 4 Under **Image and shape**, select **Change image**.

Step 5 Under **Image source**, select **Community images**.

Step 6 Search for **Multicloud Defense**.

Step 7 **Check the box** for Multicloud Defense.

Step 8 **Check the box** for *I have reviewed and accept the Publishers terms of use, Oracle Terms of Use, and the Oracle General Privacy Policy*.

Step 9 Click **Select image**.

Step 10 Exit out (do not deploy the image).

Repeat the steps for each Compartment you plan to deploy a Multicloud Defense Gateway.

Connect Oracle Account

Use the following procedure to connect to an OCI account through Multicloud Defense Controller's easy setup wizard:

Before you begin

- You must have an existing Oracle Cloud (OCI) account.
- You must have the prerequisites for you OCI account completed prior to onboarding. See Connect OCI, on page 12 for more information.
- You must have a CDO tenant.
- You must have an Admin or Super Admin user role in your CDO tenant.
- You must have Multicloud Defense enabled for your CDO tenant.

Step 1 In the CDO dashboard, click the Multicloud Defense tab located in the left naviation pane.

Step 2 Click Multicloud Defense Controller located in the upper right window.

Step 3 From the Multicloud Defense Controller dashboard, click **Setup** located to the left of the window.

Step 4 Select **Connect Account**.

Step 5 Select the OCI icon.

Step 6 Enter the following information in the modal:

a) Enter an **OCI Account Name**. This name is used only within the Multicloud Defense Controller and used for idenfitication purposes.
b) (Optional) Enter a **Description** of your account.
c) Enter you **Tenancy OCID** . This is your Tenancy Oracle Cloud Identifier obtained from the OCI User.
d) Enter the **Private Key** that is assigned to the OCI User.

Step 7 Click **Next**.

What to do next

Once you've connected the account, Multicloud Defense Controller automatically starts to discover assets and inventory associated with the cloud service provider account. Note that this is different from discovering traffic. Because Multicloud Defense Controller discovers account assets and inventory by default, the next step in this wizard is to Enable Traffic Visibility.

Enable Traffic Visibility

Enabling traffic visibility provides awareness into the traffic flows within the Cloud Accounts by collecting the following logs:

- NSG Flow Logs
- (**AWS only**) VPC Flow Logs
- DNS Logs

- Route53 Query Logging

The flow and DNS query logs are used by Multicloud Defense to understand traffic flow, correlate with threat intelligence feeds, and provide insight into existing threats that can be protected using Multicloud Defense.

Enabling traffic visibility is a different process for every cloud account type, but typically you will need to identiy account characteristics such as your cloud account's region, VPC/VNet you want to monitor, network security groups, and a cloud storage account for logs.

Use the following procedure to enable traffic visibility from the Setup wizard:

Before you begin

You must have already connected at least one cloud service provider account to the Multicloud Defense Controller.

Step 1 In the Multicloud Defense Controller portal click **Setup** in the left navigation bar.

Step 2 In the setup wizard, click **Enable Traffic Visibility**.

Step 3 **CSP Account** - Use the drop-down menu to select the cloud service provider account to which Multicloud Defense Controller deploys the Service VPC/VNet.

Step 4 **Region** - Use the drop-down menu to select the region where the cloud service provider you selected is located.

Step 5 Scroll through the table of available available VPCs that are applicable to the type of cloud service provider you selected and check the appropriate VPC. Note that if you do not immediately see the VPC, click the **Refresh** icon to refresh the current list.

Step 6 (Optional) Use the drop-down menu to select the S3 bucket in your account where DNS queries and VPC flow logs are stored. The S3 bucket selected is created by Multicloud Defense as part of the process when enabling traffic.

Step 7 Click **Next**.

What to do next

Secure your account.

Secure Your Account

Secure your account with a gateway deployed in either a centralized or a distributed model.

In a **Centralized** model, Multicloud Defense orchestrates and deploys a VPC or VNet to contain the gateway. This means that the VPC or VNet and all the additional components required are orchestrated as well as the deployment of the gateway within this construct.

In a **Distributed** model, Multicloud Defense builds and deploys a gateway within the existing infrastructure that your network already has available.

Continue with either of the procedures below to secure your account.

Centralized Model: Add a VPC or VNet

Use the following procedure to create and add a VPC or VNet to house your gateway and secure your account:

Before you begin

You must have at least one cloud service provider connected to the Multicloud Defense Controller before you begin this wizard. Note that this procedure changes for some providers based on their required parameters.

Step 1 In the Multicloud Defense Controller portal click **Setup** in the left navigation bar.

Step 2 In the setup wizard, click **Secure Account**.

Step 3 Select **Centralized** so it is highlighted.

Step 4 Click **Next**.

Step 5 Add a Service VPC/VNet:

a) **Name** - Enter a name for the service VPC/VNet. Once created, this name is displayed in the **Manage** > **Gateways** > **Service VPC/VNETS** page.

b) **CSP Account** - Use the drop-down menu to select a cloud service provider account that is already connected to the Multicloud Defense Controller. The Service VPC/VNet is deployed to the selected account.

c) **Region** - Use the drop-down menu to select the region where the selected cloud service provider is located.

d) **CIDR Block** - Enter the unique value for the Transit Gateway that the Service VPC/VNet is attaching to.

e) **Availablity Zones** - Of the generated list, select at least one availability zone. We **strongly** recommend selected two zones for best results.

f) (Azure accounts only) **Resource Group** - Use the drop-down menu to select a resource group to associate the gateway to. If there are none currently listed, you can **Create Resource Group** from this screen.

g) (AWS accounts only) **Transit Gateway** - Use the drop-down menu to select an available transit gateway for the VPC to assocaite with. If you do not have one available, click **create_new** to create a transit gateway from this window.

h) (AWS account only) **Use NAT Gateway** - check this option if you want all egress traffic to be directed through the NAT gateway. Multicloud Defense automatically creates a NAT gateway for each availability zone that is selected.

Step 6 Click **Next**.

What to do next

Add a Gateway.

Distributed Model

For a distributed gateway model, use the following procedures according to which cloud service provider you are using.

Azure Distributed Model: Create a Gateway

Use the following procedure to create a gateway for an Azure account with the distributed model:

Step 1 In the Multicloud Defense Controller portal click **Setup** in the left navigation bar.

Step 2 In the setup wizard, click **Secure Account**.

Step 3 Select **Distributed** so it is highlighted.

Step 4 Click **Next**.

Step 5 Enter the following Gateway Information:

a) **Account** - Use the drop-down menu to select an Azure account you want to deploy the gateway to.
b) **Name** - Enter a name for the gateway. This name is displayed in the **Manage** > **Gateways** page.
c) (Optional) **Description** - Enter a description for the gateway that might help identify it from other gateways.
d) **Instance Type** - Use the drop-down menu to select the instance type that deploys the Gateway.
e) **Minimum Instances** - Select the minimum number of instances deployed in auto scaling group per availability zone.
f) **Maximum Instance** - Select the maximum number of instances deployed in auto scaling group per availability zone.
g) **HealthCheck Port** - Enter the healthcheck port number. Multicloud Defense Controller uses `65534` as the default value.
h) **User Name** - Enter the user name used to access the gateway once created.
i) **Packet Capture Profile** - Use the drop-down menu to select where packets are stored in the cloud storage bucket. If there are no option listed, click **Create Packet Capture Profile** to create one from this window.
j) **Log Profile** - Use the drop-down menu to select which cloud service provider is used to forward logging to.
k) **Metrics Profile** - Use the drop-down menu to select an entity to forward metrics to. If there are no option listed, click **Create Metrics Forward Profile** to create one from this window.
l) **NTP Profile** - Use the drop-down menu to select the NTP profile associated with the gateway. If there are no options listed, click **Create** to create one from this window.
m) **Security** - Select the type of traffic flow your gateway is expected to handle. Ingress security targets traffic that flows from the public internet to a private network; east-west & egress security targets traffic that is outbound from your private network and traffic that moves between your data centers.
n) **Gateway Image** - Use the drop-down menu to select the gateway image to be deployed to the gateway.
o) **Policy Ruleset** - Use the drop-down menu to select a policy rulset to be deployed and start processing traffic. If there is not ruleset listed, click **Create new** to create a policy rulset from this window.
p) **Region** - Use the drop-down menu to select the region your gateway is deployed to.
q) **VPC/VNet ID** - Use the drop-down menu to select the VPC where the gateway is deployed to.
r) **Key Selection** - Select either an SSH Public key or an SSH Key Pair. Enter the value that is applied to the gateway in the next text field.
s) **Resource Group** - Use the drop-down menu to select an existing resource group that is applied to the gateway.
t) **User Assigned Identity ID** - Enter a valid value.
u) **Mgmt. Security Group** - Use the drop-down menu to select a security group used for the gateway management interface. Note that if you select a Multicloud Defense-created service VPC, a security group is created specifically for management.
v) **Datapath Security Group** - Use the drop-down menu to select a security group used for the gateway datapath interface. If selecting Multicloud Defense-created service VPC, a security group is created specifically for the datapath.
w) **Disk Encryption** - Enable disk encryption with either the Azure managed encryption or a customer-managed encryption key. Note that if you opt for a customer-managed encryption key, you need to create and deploy an IAM policy for successful deployment.
x) **Availability Zone** - Use the drop-down menu to select an availablilty zone.
y) **Mgmt. Subnet** - Use the drop-down menu to select a management subnet for the management interface.
z) **Datapth Subnet** - Use the drop-down menu to select a datapath subnet for the datapth interface.

To add more instance types, click the "+" icon. Subseuqntly, you can remove additional instance types with the "-" icon.

Step 6 Click **Next**.

Step 7 Enter the following Advanced Settings:

a)

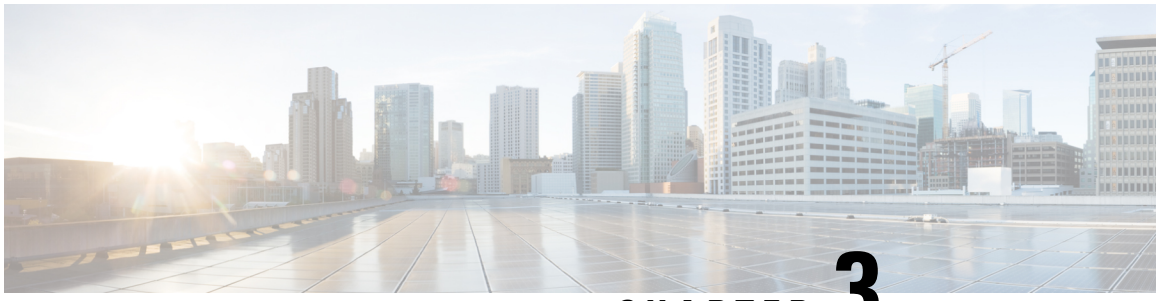
Step 8 Click **Next**.

Step 9 Review

What to do next

PART III

Account Onboarding



CHAPTER 3

AWS

AWS Overview

Multicloud Defense has created a CloudFormation template that you use when connecting an AWS account to the Multicloud Defense Controller.

To prepare cloud account for integration with Multicloud Defense Controller, there are certain steps that need to be performed in the cloud account. Below are the prerequisite steps you need to perform before connecting your AWS cloud account to Multicloud Defense Controller. This is intended to provide an overview of the operation and not intended to be performed manually. In CloudFormation section, there are details of deployments and parameters information.

Overview of steps

1. Create a cross account IAM role that's used by the Multicloud Defense Controller to manage your cloud account.
2. Create an IAM role that is assigned to the Multicloud Defense Gateway EC2 instances that run in your account.
3. Create a CloudWatch event rule that transfers the management events to the Multicloud Defense Controller.
4. Create an IAM role that is used by the above CloudWatch event rule that gives it the permissions to do the transfer of the management events.
5. Optionally create a S3 bucket in your account to store CloudTrail Events, Route53 DNS query logs and VPC Flow Logs.
6. Enable Route53 DNS Query Logging with the destination as the S3 Bucket created above and select the VPCs for which query logging must be enabled.
7. Enable CloudTrail to log all the management events to the S3 Bucket created above.
8. Enable VPC Flow Logs with destination as the S3 Bucket created above.

Connect AWS Account to Multicloud Defense Controller from The Multicloud Defense Dashboard

Multicloud Defense has created a CloudFormation template that makes it easy to connect an AWS account to the Multicloud Defense Controller.

Before you begin

You must have requested a Multicloud Defense Controller for your CDO tenant before you begin.

Note Multicloud Defense Controller version 23.10 defaults to IMDSv2 in the AWS EC2 instance when using Multicloud Defense Gateway version 23.04 or newer. For more information about the difference beween IMDSv1 and IMDSv2, see AWS documentation.

Step 1 In the CDO menu bar, click Multicloud Defense.

Step 2 Click Multicloud Defense Controller.

Step 3 In the Cloud Accounts pane, click **Add Account**.

Step 4 On the **General Information** page, select AWS from the **Account Type** list box.

Step 5 Click **Launch Stack** to download and deploy our CloudFormation template. This should open up another tab to deploy the template. Login to AWS is required.

Step 6 Acknowledge that the AWS CloudFormation might create IAM resources with custom names.

Step 7 Fill in these values:

- **AWS Account Number**: Enter the AWS account number of the account you wish to secure. This number can be found in the output value CurrentAccount of the CloudFormation Template.
- **Account Name**: Enter the name you want to give your account once it has been onboarded.
- **Description:**(Optional) Enter an account description.
- **External ID**: A random string for IAM role's trust policy. This value will be used in the controller IAM role created. You can edit or regenerate the External ID.
- **Controller IAM Role**: This is the IAM role created for theMulticloud Defense Controller during CloudFormation Template (CFT) deployment. Look for the output value MCDControllerRoleArn in CFT stack. It should be something similar to this: `arn:aws:iam::<Acc Number>:role/ciscomcdcontrollerrole`.
- **Inventory Monitor Role**: This is the IAM role created for Multicould Defense Inventory during CFT deployment. Look for the output value MCDInventoryRoleArn in CFT stack. Should be something similar to this: `arn:aws:iam::<Acc Number>:role/ciscomcdinventoryrole`.

Step 8 Click **Save and Continue**.
You are returned to the Multicloud Defense dashboard where you will see that the you have a new AWS cloud account recorded.

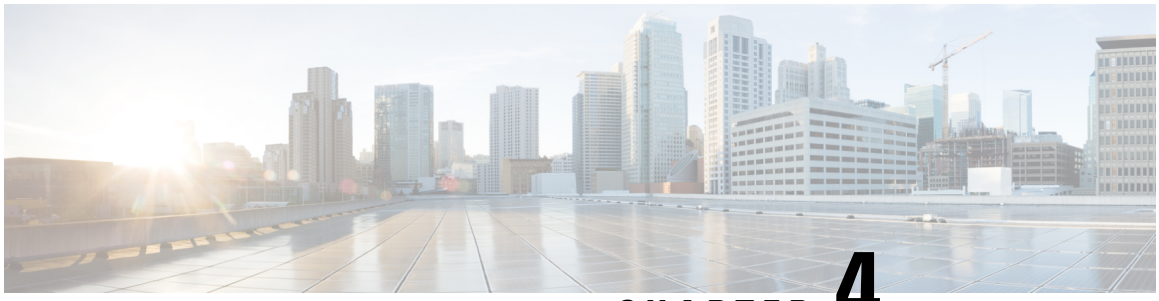
What to do next

Enable traffic visibility.

CloudFormation Outputs

From the **Outputs** tab, copy and paste the following informationin to a text editor:

- CurrentAccount (This is your AWS Account ID where applications run and Multicloud Defense Gateways will be deployed)
    - MCDControllerRoleArn
    - MCDGatewayRoleName
    - MCDInventoryRoleArn
    - MCDS3BucketArn
    - MCDBucketName



CHAPTER 4

Azure

Azure Overview

Prepare and connect your Azure environment to Multicloud Defense Controller with the following steps:

- Acquire an Azure subscription. Ensure the subscription is assocaited to an Azure Active Directory.
- Connect an Azure Subscription to the Multicloud Defense Controller from the Multicloud Defense Dashboard, on page 27

If you find that you cannot use the automated script, see the alternative procedure to manually onboard your account Manually Onboard an Azure Subscription.

Connect an Azure Subscription to the Multicloud Defense Controller from the Multicloud Defense Dashboard

Once you prepared the Azure account and subscription as described in the previous sections, you can link it to the Multicloud Defense Controller.

Step 1 In the CDO menu bar, click Multicloud Defense.

Step 2 Click the Multicloud Defense Controller button.

Step 3 In the Cloud Accounts pane, click **Add Account**.

Step 4 On the General Information page, select Azure from the **Account Type** list box.

Step 5 In step 1, click the link to open an Azure Cloud Shell in bash mode.

Step 6 In step 2, click the **Copy** button.

Step 7 Run the onboarding script in the bash shell.

Note

- If there is another Azure subscription already connected to Multicloud Defense, this script may fail when creating an IAM role with the same existing name. There cannot be more than one IAM role. As a workaround, run the Bash script with the `-p` prefix.
- To support spoke VNet protection across subscriptions, onboard subscriptions using Active Directory app registrations.

Step 8 Provide a name for this Azure account. You can choose to name this the same as your Azure subscription name. This name is visible on the Multicloud Defense Controller accounts page only.

Step 9 (Optional) Provide a description for the subscription.

Step 10 Enter the **Directory ID**, also referred as the Tenant ID.

Step 11 Enter the **Subscription ID** for the subscription being onboarded.

Step 12 Enter the **Application ID**, also referred to as the Client ID, created by the onboarding script.

Step 13 Enter the **Client Secret**, also referred to as the Secret ID.

Step 14 Click **Save & Continue**.

The Azure subscription is onboarded and you are returned to the dashboard to see that the new device has been added.

What to do next

- Post-Onboarding Procedures, on page 28.
- Enable traffic visiblilty.

Post-Onboarding Procedures

Subnets

When configuring your gateway deployment, the Multicloud Defense Controller will prompt you for the **management** and **datapath** subnet information.

The **management** subnet is a public subnet that must be associated with the route table that has a default route to the Internet. The Multicloud Defense Gateway instance has an interface attached to this subnet that it uses to communicate with the Multicloud Defense Controller. This interface is used for policy pushes and other management and telemetry activities between the Multicloud Defense Controller and the Multicloud Defense Gateway instances. Customer application traffic **does not** flow through this interface and subnet. The interface is associated with the**management** security group, which is described in the Security Groups section below.

The **datapath** subnet is a public subnet that must be associated with the route table that has a default route to the Internet. The Multicloud Defense Controller creates a network load balancer (NLB) in this subnet. In addition, a Multicloud Defense Gateway instance has an interface attached to this subnet. The customer applications traffic **flows** through this interface. A security policy is applied to the trafficingressing through this interface. The interface is associated with the **datapath** security group, which is described in the Security Groups section.

Azure VNet Setup

This document describes the requirements and resources (subnets, security-groups) to be created in your VNet so that you can create Multicloud Defense Gateways in the VNet.

Security Groups

The management and datapath security groups are associated with the respective interfaces on the Multicloud Defense Gateway instance, as described in the subnets section above.

The **management** security group must allow outbound traffic that allows the gateway instance to communicate with the controller. Optionally, for inbound rules, enable port 22 (SSH) to allow SSH access to the gateway instance. SSH is not mandatory for the Multicloud Defense Gateway to function properly.

The **datapath** security group is attached to the datapath interface and allows traffic from the Internet to the Multicloud Defense Gateway. Currently the Multicloud Defense Controller does not manage this security group. An outbound rule must exist, allowing the traffic to egress this interface. Inbound ports must be opened for each port that is configured in the Multicloud Defense Controller security policy and used by the Multicloud Defense Gateway.

For example, if an application is running on port 3000 and is proxied by the Multicloud Defense Gateway on port 443, port 443 must be opened on the datapath security group. This example also implies that port 3000 is open on the security group attached to your application.

Launch ARM Template

Use the to create all of the resources described on this page.

This template creates a new VNet. This is very useful to get started on Multicloud Defense without touching your existing production environment.

The template creates the following resources:

- VNet.
- Management subnet.
- Datapath subnet.
- Management security group with outbound rules.
- Datapath security group with outbound rules and Inbound rules for port 443.

You can create additional subnets to run apps and create app-specific security groups, as needed.

Use the following steps to launch an ARM template:

Step 1 Log into your Azure account and Deploy a custom template.

Step 2 Click **Build your own template in the editor**.

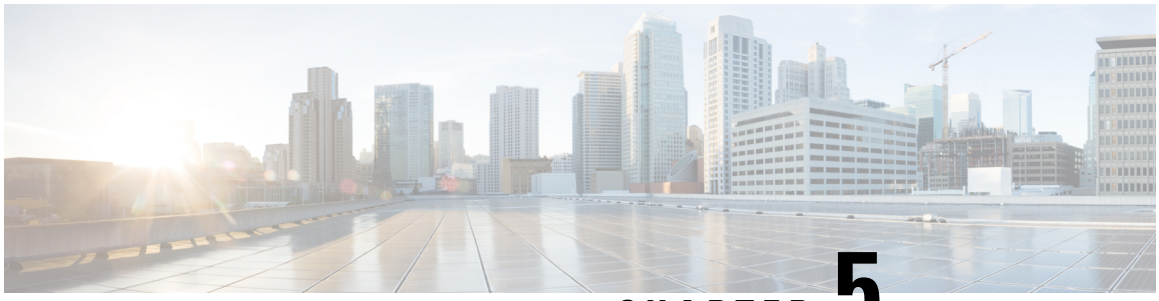
Step 3 Copy the content from the ARM template and paste into the editor.

Step 4 Click **Save**.

Step 5 Select the *Subscription*, *Resource group*and the *Region*.

Step 6 Click **Review+ create**.

Step 7 Wait for a few minutes for all the resources to be created.



CHAPTER 5

GCP

GCP Overview

GCP Project and GCP Folders

Multicloud Defense currently supports both GCP projects and GCP folders although these components are supported separately. Note the following limitations and exceptions for both of these options.

A GCP project has to potential to contain GCP resources like virtual machines, storage buckets, databases, and more. It can be used to create, enable, and use all Google Cloud services.

- Projects can be onbarded with terraform, manual onboarding, and scripted onboarding.
- Projects are ideal for environments that require orchestration, including discovery and investigation.
- You can interact with each project indvidually through the Multicloud Defense dashboard.

As of Version 23.10 you can connect a GCP folder with terraform. A GCP folder contains projects, other folders, or a combination of both. Organization resources can use folders to group projects under the organization resource node in a hierarchy.

- Folders that do not have the `roles/compute.admin` permission enabled are considered empty and are not used.
- Projects associated with onboarded folders are used for asset and traffic discovery only.
- Projects associated with onboarded folders do not accommodate orchestrating service VPC or gateway creation.
- Permissions made to folders from the GCP console must be made at the folder level. As such, Multicloud Defense actions are also made at the folder level.

If you want to onboard a GCP folder, see Terraform Repository.

Overview Proecdure

The following is an overview of how to connect your GCP project. An shell **script** is provided by Multicloud Defense and facilitates an easy connective process as part of a wizard. The script automates the following steps so you don't have to:

1. Create two service accounts.
2. Enable the following APIs (Compute Engine, Secret Manager).
3. Create the two following VPCs (management, datapath).
4. Create firewall rules to allow traffic to the Multicloud Defense Gateway (app traffic) in the datapath VPC.
5. Create firewall rules to allow management traffic from Multicloud Defense Gateway to the Multicloud Defense Controller in the management VPC.

If you find that the script does not work, or if you need to manually change your settings, these actions can be executed using the GCP cloud console web UI, or using the gcloud CLI. See the alternative method of connecting your project Manually Onboard a GCP Project.

Connect a GCP Project to the Multicloud Defense Controller from the Multicloud Defense Dashboard

Once you prepared the GCP project as described in the previous sections, you can link it to the Multicloud Defense Controller.

Before you begin

You must already have a Google Cloud Platform (GCP) project created and have permissions to create VPCs, subnets, and a service account.

Step 1 In the CDO menu bar, click Multicloud Defense.

Step 2 Click the Multicloud Defense Controller button.

Step 3 In the **Cloud Accounts** pane, click **Add Account**.

Step 4 On the **General Information** page, select **GCP** from the Account Type list box.

Step 5 Login to the Multicloud Defense Dashboard.

Step 6 Click **Manage** and then **Accounts**.

Step 7 Click **Add Account**.

Step 8 In step 1, click the link to open an Google Cloud Platform Cloud Shell.

Step 9 In step 2, click the **Copy** button.

Step 10 Run the bash script in the Google Cloud Platform Cloud Shell.

Step 11 Type a name for this GCP account. You can choose to name this the same as your GCP project name. This name is visible on the Multicloud Defense Controller only.

Step 12 (Optional) Enter a description.

Step 13 Enter the **Project ID** for the GCP project.

Step 14 Enter the **Client Email** for the service account created for Multicloud Defense Controller.

Step 15 Enter the **Private key** of the service account.

Step 16 Click **Save & Continue**.

What to do next

Enable traffic visibility.

Roles Created by Multicloud Defense

When you onboard a cloud service account to Multicloud Defense Controller with the provided script, user roles are created within the parameters of the cloud service provider to ensure that communication between the services are protected. Depending on the cloud service provider, different roles and permissions are created.

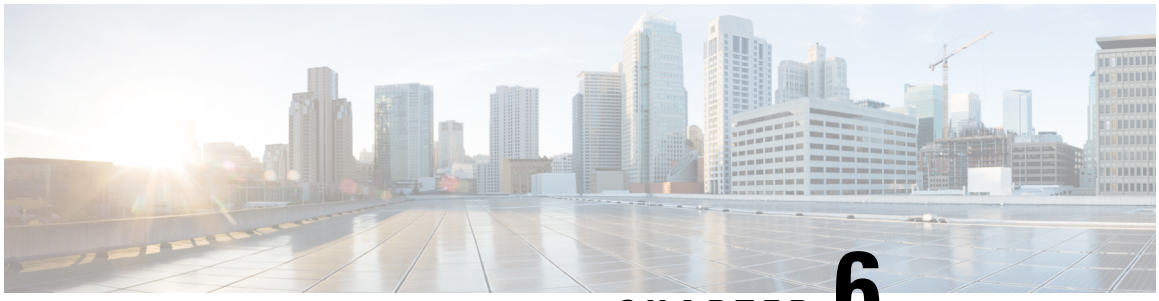
The following roles are created when you onboard an account.

GCP IAM Roles

This document explains the details of the service accountes created by the CloudFormation template used in the previous section.

The CloudFormation template creates the following accounts:

- **ciscomcd-controller service account** - This account is used by the Multicloud Defense Controller to access your GCP project to create resources (Multicloud Defense Gateway), load balancers for gateways, and read information about the VPCs, subnets, security grroup tags, and more.
- **ciscomcd-firewall service account** - This account is assigned to the Multicloud Defense Gateway (compute VM instances). The account provides access to the secret manager (private keys for TLS decryption) and storage. Also, the gateways many need permissions to send logs from Multicloud Defense Gatewayto the GCP logging instance (if configured by the user).



CHAPTER 6

OCI

Connect Oracle OCI Tenant to Multicloud Defense Controller Overview

In order to onboard an OCI tenant into the Multicloud Defense Controller, the OCI tenant needs to be properly setup. The following are the general steps required to prepare the tenant.

For more information on how to set up your OCI tenant, see OCI documentation. Once your tenant is completely set up, then you can Connect the Oracle OCI Tenant to the Multicloud Defense Controller from the the Multicloud Defense Dashboard, on page 36.

Note Multicloud Defense supports both Ingress and Egress/East-West protection for OCI. Inventory and traffic discovery are not supported.

In order to onboard the OCI tenant, it is required to subscribe to the US West (San Jose) region. If this region is not subscribed, then the onboarding of the OCI tenant will result in an error.

In order to deploy a Multicloud Defense Gateway into OCI, the Terms and Conditions for the Multicloud Defense compute image **must** be accepted in each OCI compartment. Otherwise the deployment will error out with an unauthorized error.

Overview of Steps

Tenant Setup in OCI

1. Create a Group.
2. Create a Policy. Note that the policy must have the `root` Compartment selected.
3. Create a User.
4. Add the User to the Group.

5. Create an API Key for the User.
6. Record the *user* and *tenancy* OCIDs.
7. Accept the Terms and Conditions.

What to do next:

Onboard the OCI tenant using Connect the Oracle OCI Tenant to the Multicloud Defense Controller from the the Multicloud Defense Dashboard, on page 36.

Connect the Oracle OCI Tenant to the Multicloud Defense Controller from the the Multicloud Defense Dashboard

Before you begin

Review the requirements in Connect Oracle OCI Tenant to Multicloud Defense Controller Overview, on page 35.

Step 1 From the CDO dashboard, click Multicloud Defense in the CDO menu bar.

Step 2 Click the Multicloud Defense Controller button.

Step 3 In the Cloud Accounts pane, click **Add Account.**.

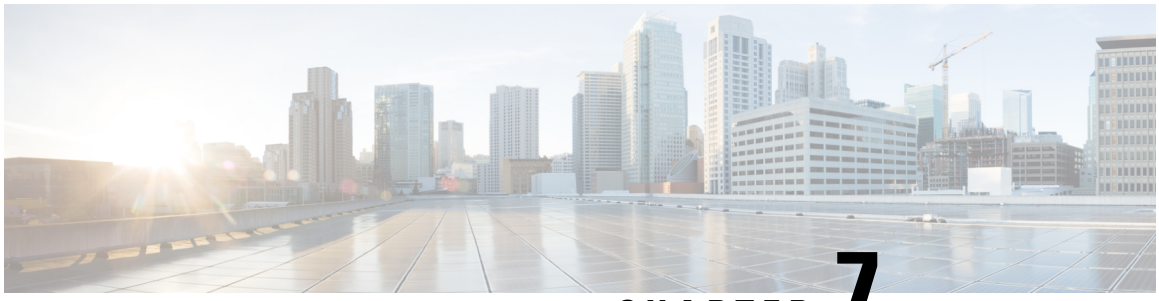
Step 4 In the General Information page, select **OCI** in the Account Type list box.

Step 5 Fill in the following fields:

- **OCI Account Name**- Used to identify this OCI Tenant within the Multicloud Defense Controller.
- **Tenancy OCID** - Tenancy Oracle Cloud Identifier obtained from the OCI User.
- **User OCID** - User OCID obtained from the OCI User.
- **Private Key** - API private key that was assigned to the OCI User.

What to do next

Enable traffic visibility.



CHAPTER 7

Roles Create by Multicloud Defense

Roles Created by Multicloud Defense

When you onboard a cloud service account to Multicloud Defense Controller with the provided script, user roles are created within the parameters of the cloud service provider to ensure that communication between the services are protected. Depending on the cloud service provider, different roles and permissions are created.

The following roles are created when you onboard an account.

AWS IAM Roles

This document explains the details of the IAM roles created by the CloudFormation template used in the previous section.

The CloudFormation template creates the following three IAM roles and one CloudWatch Event rule:

- **Multicloud DefenseControllerRole** - Used by the Multicloud Defense to connect to your AWS cloud account.
- **Multicloud DefenseFirewallRole** - Used by the Multicloud Defense instances running in your cloud account to access S3, SecretsManager, KMS.
- **Multicloud DefenseCloudWatchEventRole** - Used by the CloudWatch Event Rule to transfer inventory changes to the Multicloud Defense.
- **Multicloud DefenseCloudWatchEventRule** - A rule created on CloudWatch Events to transfer inventory changes to the Multicloud Defense. The rule assumes the Multicloud DefenseCloudWatchEventRole defined above provides permissions to transfer CloudWatch Events.

MCDControllerRole

Cross-account IAM role that allows Multicloud Defense to access your cloud account and take necessary actions, for example, Create EC2 instances, create load balancers, and change Route53 entries. The service principal is the Multicloud Defense-controller-account with an external id applied. Here is the IAM policy applied to the role (e.g controller role name used in this example is ***Multicloud Defense-controller-role***):

```
{
```

```
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "aacm:ListCertificates",
        "apigateway:Get",
        "ec2:*",
        "elasticloadbalancing:*",
        "events:DeleteRule",
        "events:ListTargetsByRule",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets",
        "globalaccelerator:*",
        "iam:ListPolicies",
        "iam:ListRoles",
        "iam:ListRoleTags",
        "logs:*",
        "route53resolver:*",
        "servicequotas:GetServiceQuota",
        "s3:ListAllMyBuckets",
        "s3:ListBucket"
        "wafv2:Get*"
        "wafv2:List*"
      ],
      "Effect": "Allow",
      "Resource": "*"
    },
    {
      "Action": [
        "iam:GetRole",
        "iam:ListRolePolicies",
        "iam:GetRolePolicy"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:iam::<ciscomcd-account>:role/ciscomcd-controller-role"
      ]
    },
    {
      "Effect": "Allow",
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::<S3Bucket>/*"
    },
    {
      "Action": [
        "iam:GetRole",
        "iam:ListRolePolicies",
        "iam:GetRolePolicy",
        "iam:PassRole"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:iam::<customer- account>:role/ciscomcd_firewall_role"
    },
    {
      "Action": "iam:CreateServiceLinkedRole",
      "Effect": "Allow",
      "Resource": "arn:aws:iam::*:role/aws-service-role/*"
    }
  ]
}
```

Service Principal:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::<ciscomcd-account>:root"
        ]
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "sts:ExternalId": "ciscomcd-external-id"
        }
      }
    }
  ]
}
```

MCDGatewayRole

Role that is assigned to the Multicloud Defense Gateway (Firewall) EC2 instances. The role gives the Gateway instance capabilities to access secretsmanager where the private keys for the application are stored, ability to decrypt keys using AWS KMS if the keys are stored in KMS, and save objects like PCAPs and technical support data onto a S3 bucket. The service principal of this role is ec2.amazonaws.com. Here is the IAM policy applied to the role:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "s3:PutObject",
        "s3:ListBucket"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::*/*"
    },
    {
      "Action": [
        "kms:Decrypt"
      ],
      "Effect": "Allow",
      "Resource": "*"
    },
    {
      "Action": [
        "secretsmanager:GetSecretValue"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

Tip You can download and edit the CloudFormation template to make the policy more restrictive e.g. restricting decrypt to use a specific key, or PutObject to a defined/specific S3 bucket.

MCDInventoryRole

This is the role used for dynamic inventory purposes and provides the capability for the CloudTrail events to be transferred to the Controller's AWS account. It does the following:

- Put events on the event bus in the AWS account where the Multicloud Defense Controller exists.
- Send events matching the rule to the Multicloud Defense Controller's webhook server directly from the customer's AWS account.

The Service Principal for this role is **events.amazonaws.com**. Here is the policy applied to the role:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": "events:PutEvents",
      "Effect": "Allow",
      "Resource": [
        "arn:aws:events:*:<ciscomcd-account>:event-bus/default"
      ]
    }
  ]
}
```

InventoryMonitorRule

Rule that is added to the MCDInventoryRole to put all CloudTrail inventory changes to EC2 and API gateways to be copied to the event bus on the AWS account where the Multicloud Defense Controller runs. The rule is required to match on specific event patterns that occur in the customer's AWS account. Once a match occurs, the rule states that the matched event should be sent to the webhook server (API based destination) of the controller. This rule is executed using the Multicloud DefenseMCDInventoryRole created in the previous section.

Custom Event Pattern:

```
{
  "detail-type": [
    "AWS API Call via CloudTrail",
    "EC2 Instance State-change Notification"
  ],
  "source": [
    "aws.ec2",
    "aws.elasticloadbalancing",
    "aws.apigateway"
  ]
}
```

Target:

```
Event Bus in another AWS Account (mcd-account) using the MCDInventoryRole
```

Azure IAM Roles

This document explains the details of the IAM roles created by the CloudFormation template used in the previous section.

The CloudFormation template creates the following role:

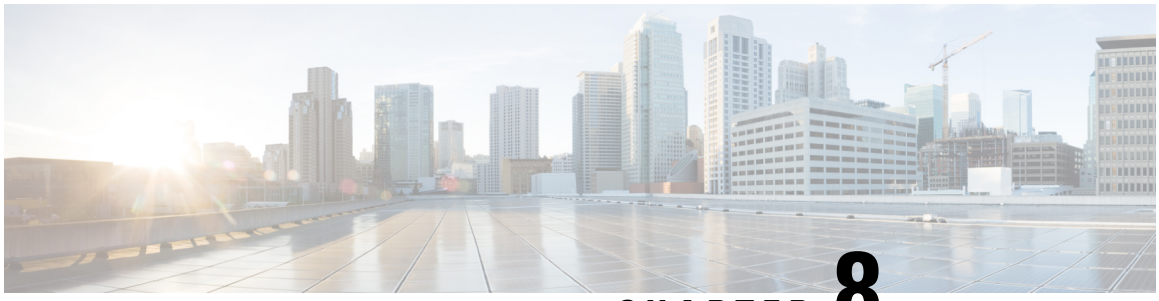
- **Custom Role** - The custom role gives the application permissions to read inventory information and create resources (e.g., VMs, load balancers, etc.) The custom role can be created in multiple ways.

GCP IAM Roles

This document explains the details of the service accountes created by the CloudFormation template used in the previous section.

The CloudFormation template creates the following accounts:

- **ciscomcd-controller service account** - This account is used by the Multicloud Defense Controller to access your GCP project to create resources (Multicloud Defense Gateway), load balancers for gateways, and read information about the VPCs, subnets, security grroup tags, and more.
- **ciscomcd-firewall service account** - This account is assigned to the Multicloud Defense Gateway (compute VM instances). The account provides access to the secret manager (private keys for TLS decryption) and storage. Also, the gateways many need permissions to send logs from Multicloud Defense Gatewayto the GCP logging instance (if configured by the user).



CHAPTER 8

Remove a Cloud Service Provider From Multicloud Defense

Use the following procedures to terminate comunications and permissions between Multicloud Defense and your cloud service provider. This action includes removing any gateways or Vnets that have been created within the Multicloud Defense Controller as well as any roles or perissions you have set up within you cloud service provider. You must perform **all** of the steps for a complete cleanup of every Multicloud Defense instance.

Note that some of these procedures do not occur in the Multicloud Defense Controller and that you may need access to the cloud service provider's dashboard to execute these procedures.

Delete a GCP Project From Multicloud Defense

Use the following procedure to delete a GCP account from the Multicloud Defense Controller and remove all instances of Multicloud Defense from your GCP project. You must delete any subnets, VNets, or gateways created in the Multicloud Defense Controller prior to deleting Multicloud Defense from your account.

Note This procedure requires you to remove orchestration preparation from both the Multicloud Defense UI and the GCP dashboard.

Step 1 Delete any curent gateways or VNets from Multicloud Defense:

a) In the Multicloud Defense Controller, navigate to **Manage** > **Gateways** > **Gateways**.
b) Select the gateway associated with the account so its checkbox is checked.
c) Expand the **Actions** drop-down menu and select **Delete.**
d) Confirm the deletion.
e) In the Multicloud Defense Controller, navigate to **Manage** > **Gateways** > **Service VPCs/VNets**.
f) Select the VPCs associated with the account so the checkbox is checked.

g) Expand the **Actions** drop-down menu and select **Delete.**
h) Confirm the deletion.

Note You do not have to delete any affiliated subnets after you delete the VPC and gateway.

Step 2 Delete the GCP project from Multicloud Defense Controller.
a) In the Multicloud Defense Controller, navigate to **Manage** > **Cloud Accounts** > **Accounts**.
b) Select the Azure account so the checkbox is checked.
c) Expand the **Actions** drop-down menu and select **Delete.**
d) Confirm the deletion.

Step 3 Delete the Multicloud Defense Controller service account from GCP.
a) Log into the GCP dashboard.
b) Open IAM in your GCP project.
c) In the navigation pane to the left, click **Service Accounts**.
d) Select the project associated with the Multicloud Defense.
e) Under the **View by Principals** tab, search for the `ciscomcd-controller`.
f) Click the row's checkbox is checked and then click **Delete**.

Step 4 Delete the Multicloud Defense firewall service account from GCP.
a) Log into the GCP dashboard.
b) Open IAM in your GCP project.
c) In the navigation pane to the left, click **Service Accounts**.
d) Select the project associated with the Multicloud Defense.
e) Under the **View by Principals** tab, search for the `ciscomcd-gateway`.
f) Click the row's checkbox is checked and then click **Delete**.

Delete an AWS Account From Multicloud Defense

Use the following procedure to completely remove an AWS account from your Multicloud Defense.

After you delete the AWS account, it may take up to 24 hours for the cloud service provider to clean up all objects within the S3 bucket that is associated with your account.

Step 1 Log into CDO and launch the Multicloud Defense Controller.
Step 2 Navigate the top menu bar to **Manage** > **Gateways**.
Step 3 Locate the gateway associated with your account and select the checkbox, then click the **Actions** drop-down menu.
Step 4 Select **Disable**. This action automatically removes all virutal machines associated with the account.
Step 5 Make sure the gateway's checkbox is still selected and click the **Actions** drop-down menu again.
Step 6 Select **Delete**. This action removes the load balancers associated with the AWS account.
Step 7 Navigate to **Manage** > **Cloud Accounts** > **Accounts**.
Step 8 Locate the AWS account in the list and select it so the checkbox is check.
Step 9 Click the **Actions** drop-down menu and select **Delete**.

Step 10 Confirm you want to delete the account.

Delete an Azure Account From Multicloud Defense

Use the following procedure to remove any and all instances of the Azure account from Multicloud Defense:

Before you begin

You must delete any subnets and VNets created in the Multicloud Defense Controller prior to deleting Multicloud Defense from your Azure account.

Note This procedure requires you to remove orchestration preparation from both the Multicloud Defense UI and the GCP dashboard.

Step 1 Log into CDO and launch the Multicloud Defense Controller.

Step 2 If you did not create a user-assigned Managed Identity for the key vault, continue to step 4. If you **did** create a key for the Azure account, do the following:

a) Navigate to **Manage** > **Security Policies** > **Certificates**.
b) Select the certificate associated with the account and then open the **Actions** drop-down menu.
c) Select **Delete** and confirm the deletion of the certificate for the key vault.

Step 3 In the Multicloud Defense Controller, delete any gateways or VNets associated with the account.

a) Navigate to **Manage** > **Gateways** > **Gateways** to delete any gateways previously created.
b) Select the gateway associated with the account so its checkbox is checked.
c) Expand the **Actions** drop-down menu and select **Delete.**
d) Confirm the deletion.
e) In the Multicloud Defense Controller, navigate to **Manage** > **Gateways** > **Service VPCs/VNets** to delete any VNets previously created.
f) Select the VNet associated with the account so the checkbox is checked.
g) Expand the **Actions** drop-down menu and select **Delete.**
h) Confirm the deletion.
i) In the Multicloud Defense Controller, navigate to **Manage** > **Cloud Accounts** > **Accounts**.
j) Select the Azure account so the checkbox is checked.
k) Expand the **Actions** drop-down menu and select **Delete**.
l) Confirm the deletion.

Step 4 Delete the Multicloud Defense Controller role in Azure.

a) Log into the Azure portal.
b) Navigate to **App Registrations**.
c) Select the **Owned Appications** tab.
d) Select the **ciscomcd-controller-app** application.
e) Once selected, click **Delete** at the top of the window.
f) Confirm the deletion.

g) Navigate to, or search for, **Subscriptions** and click **Access Control (IAM)**.
h) Select the **Roles** tab at the top of the window.
i) Search for **ciscomcd-controller-role-rw** and select it so the chekcbox is checked.
j) Click **Remove** at the top of the window.

Delete an OCI Account From Multicloud Defense

Use the following procedure to remove an OCI cloud environment from Multicloud Defense:

Step 1 Log into the OCI console.

Step 2 Delete the API key. See the "**Deleting API Signing Keys from a Roving Edge Infrastructure Device**" chapter in the Oracle Cloud Infastructure Documentation for more information.

Step 3 Delete Multicloud Defense Users. See the "**Deleting a User**" chapter in the Oracle Cloud Infastructure Documentation for more information.

Note that when you remove the user from the OCI account, this does not delete the audit data of the user from when it was valid.

Step 4 Delete the Multicloud Defense Group. See the "**Deleting Groups**" chapter in the Oracle Cloud Infastructure Documentation for more information.

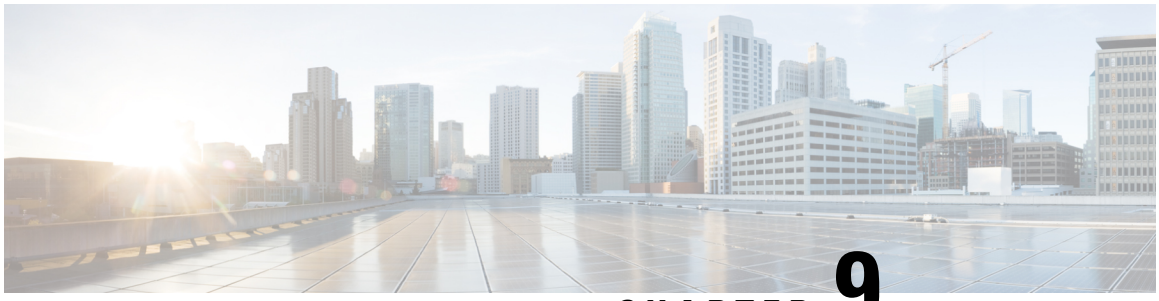
Step 5 Delete any and all Multicloud Defense access policies. See the "**Deleting an Access Policy**" chapter in the Oracle Cloud Infastructure Documentation for more information.

Step 6 Delete the OCI account from Multicloud Defense Controller. .

a) In the Multicloud Defense Controller, navigate to **Manage** > **Cloud Accounts** > **Accounts**.
b) Select the OCI account so the checkbox is checked.
c) Expand the **Actions** drop-down menu and select **Delete.**
d) Confirm the deletion.

PART IV

Discovery



CHAPTER 9

Asset and Inventory Discovery

Discovery is an important component of Multicloud Defense's approach of **"Discover, Deploy and Defend"**.

Discovery provides real-time visibility into the current resources deployed in any onboarded cloud accounts. In addition, it provides an interface into VPC flow logs and DNS logs to give a complete picture of your cloud deployment. The Multicloud Defense Controller, through the permissions granted to the IAM role (AWS), AD app registration (Azure) or the service account (GCP), periodically crawls your cloud resources, and also keeps tab on the changes, to maintain an "evergreen" inventory model of the resources.

Using the **Discovery** tab, you have the ability to see the attributes of your resources and how they are interconnected. Multicloud Defense collates this information into a succinct view of the security posture of all your resources with respect to the configuration and with context to the traffic flows.

Discovery Summary

The Dicsovery Summary page is a collection of widgets that summarize the available traffic and inventory. You can use the **Filter** at the top of the page to change the history of the widgets.

Traffic Summary Widgets

Currently, Multicloud Defense presents a condensed block of the traffic in two widgets: one for DNS traffic and one for VPC and VNet flow logs. These windows into traffic differentiate between malicious traffic and DNS or VPC/VNet traffic, respectively. Click inside either of these widgets to zoom into a specific time frame.

You can enable or disable logs on either of these widgets from this summary page by simply clicking the **Logs** toggle. For more information on either of these types of logs and the traffic that is compiled, see Types of Traffic, on page 115

Discovery Summary

The Discovery summary is a series of windows of inventory recovered by Multicloud Defense as part of the discovery process when connecting your cloud service provider. These statistics are condensed here for a quick preview. To see these in more detail, see Inventory, on page 50

Inventory

Through permissions granted to the IAM role (AWS), AD app registration (Azure) or the service account (GCP), Multicloud Defense continuously maintains an "evergreen" inventory model of the cloud resources as well as real-time discovery that exists in your cloud service provider accounts, subscriptions and projects that are relevant to apply advanced network security. Once discovered, the resources are available in workflows that enable administrators to quickly deploy security rules to mitigate risks of exposed applications. Any activity is immediately reported through the Multicloud Defense Controller.

When inventory is enabled, Multicloud Defense Controller will perform a full inventory discovery periodically. The default is 60 minutes, but is tunable). Real-time inventory discovery is enabled on regions where the CloudFormation template was deployed.

Part of the discovery process highlights the logs of each cloud service provide. Note the following types of logs per service provider:

- **AWS** - VPC flow logs, Mount53 flow logs, and DNS logs.
- **Azure** - NSG flow logs.
- **GCP** - VPC flow logs.

Note that Multicloud Defense does note provide the same level of support for all cloud service providers.

Applications

Application shows all load balancers and API gateways for the cloud accounts. Under the Applications section of **Inventory**, there are three filter buttons: **Known Tags**, **Tags**, and **Applications**. Within **Applications**, users can invoke a workflow to create and apply protection for the specific application.

Application Tags

Create a list of **Application Tags** used to identify applications. During the inventory discovery stage, all discovered load balancers that have the specified tags are treated as applications.

As an example, you can assign the **Application Tags** to all load balancers that act as applications. The value of this tag is shown as the **Application Tags** in the discovered inventory. See the table below as a visual example:

Load Balancer	Tag	Value
Load Balancer 1	ApplicationName	Billing
Load Balancer 2	ApplicationName	UserManagement

The discovered inventory will show the **Billing** and **UserManagement** applications in the discovered application assets.

To create a list of **application tags**, click **Create**.

Parameter	Description
Name	Pre-populated.

Parameter	Description
Description	User-specified description.
Value	The tag value that will be used assign to the load balancers.

For more information on application tags, see Application Tags, on page 228.

Known Tags

Known Tags show applications identified by application Load Balancers in your cloud account that the administrator has identified by a known tag. These known tags are listed in **Settings** > **Management** > **Account** > **Application Tags**.

Tags

Tags shows all applications identified by application load balancers with fields showing the tag keys and tag values and whether these applications are secured by Multicloud Defense Gateways.

Discovered Assets

When you enable inventory discovery in regions for your cloud account, the Multicloud Defense Controller continuously discovers cloud assets. To view the discovered assets, navigate to **Discover** or **Manage** > **Inventory**. The default views show the discovered assets for all cloud accounts. To filter to a specific cloud account, use the **Select Account** to specify a particular cloud account and view discovered assets.

The discovered asset categories and what they refer to are as follows:

- Security Groups - AWS Security Groups (SGs) and Azure Network Security Groups (NSGs).
- Network ACL - AWS Network Access Control Lists (NACLs).
- Subnets.
- Route Tables.
- Network Interfaces.
- VPCs/VNets - AWS VPCs, Azure VNets and GCP VPCs.
- Applications - Applications are identified by AWS Application Load Balancers (ALBs).
- Load Balancers.
- Instances - AWS Instances, Azure Virtual Machines and GCP Compute Instances.
- Tags - AWS Tags, Azure Tags and GCP Labels.
- Certificates - AWS Certificates Manager (ACM) certificates.

Enable Asset Discovery and Inventory

To enable discovery of assets in your cloud account:

Step 1 Navigate to **Manage** > **Accounts**.

Step 2 Select the checkbox next to the cloud account and click **Manage Inventory**.

Step 3 Select the **Regions** where you have cloud assets that you would wish Multicloud Defense to discover. The refresh interval is the time in minutes after which the inventory is refreshed (recommended default of 60 min). Multicloud Defense also performs continuous discovery using the cloud service provider's APIs and events instead of a regular poll. The refresh time interval specified here is for a full re-crawl; this reconciles all assets for any missed events during real time discovery.

Note that different refresh intervals can be defined for different regions by adding a new row and selecting the desired regions. A region can belong to a single refresh interval only.

Step 4 Click **Finish** to save.

Note The Multicloud Defense Controller will request the asset inventory for the newly added region immediately after saving.

What to do next

To review the discovered assets, navigate to **Manage** > **Inventory**.

Security Insights

Insights are a rules-based evaluations of assets discovered in AWS, Azure and GCP that are presented asfindings. Insights can be used without deploying Multicloud Defense Gateways since they operate on the periodic and real-time inventory monitoring accommodated by the Multicloud Defense Controller.

Step 1 In the Multicloud Defense Controller interface, click **Add Account**. As an alternative, we strongly recommend using the Setup with the Multicloud Defense Wizard wizard to connect to an account. Go through the steps to connect the account.

Step 2 Once the account is connected and onboarded, Enable Asset Discovery and Inventory.

Step 3 Navigate to **Discover** > **Discovery Summary**. This page displays a summary view of all discovered assets and the **Insight Findings**.

Types of Security Insights

Read through the following types of security insights to understand what the dashboard can do.

Security Groups

Customers often struggle with the proliferation of **Security Groups**. Security groups are often shared amongst resources that could present risk. Changes made to a security group intended for a specific resource could impact a larger group of resources.

Security groups provides a list of all security group, their details and the set of resources utilizing the security group. The **Is Inbound Public** and **Is Outbound Public** fields indicate security groups configured with 0.0.0.0/0.

In the search window, define the search criteria based on fields and their values with the option to create a rule based on the search criteria.

Rules

Rules provide a view of security groups based on their configured Inbound and outbound rules.

Ports

Ports provide a view of security groups based on their configured inbound and outbound ports.

Application Security Groups

Application Security Groups are an Azure construct similar to the AWS security group. Azure application security groups have a member of the security group that contains that system and it's interfaces. It has both membership and security controls. As a result, Multicloud Defense uses this membership construct to build dynamic policies. Create and use an application secuirty group within an Azure environment, Multicloud Defense recognizes the change and adapts the policy to incorporate it.

For more information about Azure's application security groups and how they operate, see the Microsoft Azure documentation.

Network ACL

Network access control list (ACL) provides a list of all network ACLs and their details. The **Is Inbound Public** and **Is Outbound Public** fields indicate network ACLs configured with 0.0.0.0/0.

Rules

Rules provide a view of network ACLs based on their configured inbound and outbound rules.

Subnets

Subnets provides a list of all subnets and their details. The **Is Public** field indicate subnets that are publicly accessible based on whether auto-assign public IP is enabled.

Route Tables

Route Tables provides a list of all route tables and their details. The **Is Inbound Public** and **Is Outbound Public** fields indicate route tables that are configured to provide default access the internet.

Network Interfaces

Network Interfaces provides a list of all network interfaces and their details. The **Is Inbound Public** and **Is Outbound Public** fields indicate network interfaces that are configured with a security group that is open (0.0.0.0/0), or route tables that allows default access to the internet.

VPCs\VNets

VPCs/VNets provides a list of all VPCs/VNets and their details.

Applications

Applications provides a list of all deployed application load balancers and their details. The **Secured** field identifies whether a Multicloud Defense Gateway and security policy is applied to secure the application and offers an ability to invoke a workflow to protect the application.

Load Balancers

Load Balancers provides a list of all deployed application, network and gateway load balancers and their details. The **Public** field shows whether resource is an internet-facing load balancer. The **CSP WAF Enabled** shows whether a CSP WAF has been enabled for the application load balancer.

Instances

Instances provides a list of all instances along with summary information on the number of security groups and interfaces that are assigned and configured for the resource. The **Is Inbound Public** and**Is Outbound Public** fields indicate instances that have network interfaces that are configured with a security group that is open (0.0.0.0/0), or route tables that allows default access to the internet.

Tags

Tags provides a list of all VPCs/VNets, subnets, security groups, instances and load balancers that are configured with tags.

Certificates

Certificates provides a list of all certificates available in AWS certificates manager along with summary information on issuer, domain name and expiry date.

Topology

this tab shows a high-level map view by region of cloud assets in cloud accounts. You can finetune the visuals with the **Filter** bar at the top of the screen. From here you can determine what cloud service provider accounts you want to pull data drom, which region of the world, specific VNet or VPCs, instances, and a period of time in history.

The **Global View** of the world map allows you to scroll in for a closer look at specific regions that are dictated by the Filter bar mentioned above. Immediately to the left of the map you can dictate which types of traffic and inventory you want to view. Check and uncheck the boxes appropriately for what you want to see .

Insights

Insights are a rules-based evaluations of assets discovered in AWS, Azure and GCP that are presented as findings.

Rules

Rules are a set of evaluations to identify findings in discovered assets. Multicloud Defense provides a set of default rules. New rules can be created by selecting an inventory category (e.g., security groups, applications, load balancers, tags, etc.), defining a search criteria, selecting **Add Rule** and specifying additional required information. Navigate to **Insights** > **Rules** to view the new rule. From there you can operate against existing and newly discovered assets.

Findings

Findings is a list of discovered assets that match the defined set of rules.

Rules and Findings

Rules can be configured to place checks and guardrails on your cloud resources.

Rules and Findings

Rules can be configured to place checks and guardrails on your cloud resources.

Pre-Defined Rules

Multicloud Defense Controller has some basic pre-defined rules:

- Application load balancers with no cloud service provider WAF enabled.
- Security groups with few instances (< 5) that have ingress open. Lots of low utilization security groups can create gaps that are hard to see and may make it easy to exploit.
- Instances with two or more network interfaces.
- Security groups with open outbound (0.0.0.0/0) access.
- Public subnets - all AWS subnets with **Auto-Assign Public IP** enabled.
- Security groups with with too many egress ports (25 or more) open to the internet.
- Security ports with too many ingress ports (5 or more) open to the internet.
- Security groups with 65,535 ports open for ingress with public access enabled.
- Certificates expiring in 30 days - AWS Certificate Manager only.

The cloud resources that match the rules, will be flagged as findings with a matching severity.

For information on custom rules, see Pre-Defined Rules, on page 55.

Custom Rules

The user can configure additional rules for a resource.

1. Navigate to **Discovery** > **Inventory** and select a resource e.g. load balancers.
2. Create a rule criteria in the text area and select **Add Rule**.
3. Enter content for the following entries and the number of finding meeting the rule criteria.
    - Name
    - Description
    - Severity

- Default Action
- Type
- Account

4. Click **Save**.

The default action of the rule can be either **info** or **alert**. If a rule is configured with a default action of alert, then any new findings for the rule results in an alert notification from the Multicloud Defense Controller. The following configurations are required if you want a default action of alert.

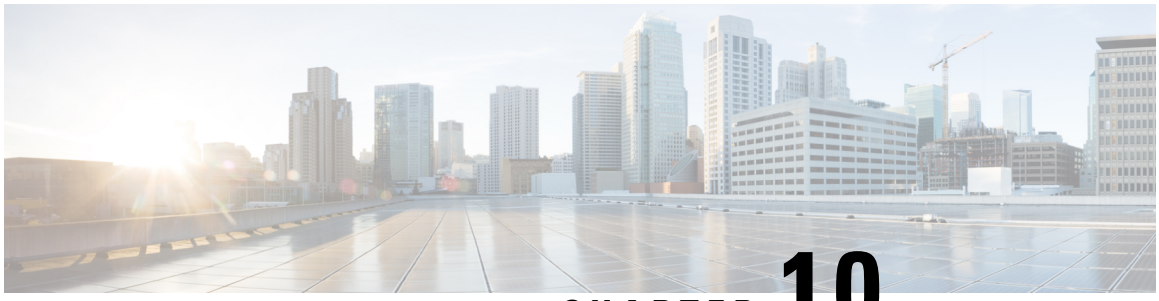
- Configure **Alert Profile** to indicate if the user wants ServiceNow, PagerDuty, or Webhook notifications.
- Configure **Alert Rule of type Discovery** and sub-type **Insights Rule** with the level of severity specified.

Findings

Based on the pre-defined and custom rules, you can view the findings for the resources. For easy access, the **Findings Summary** is located in the dashboard, and also in the Summary view in the Inventory tab.

PART V

Multicloud Defense Gateway



CHAPTER 10

Manage Multicloud Defense Gateways

Overview

Multicloud Defense Gateway is a network-based security platform comprised of a network load balancer with a cluster of Multicloud Defense Gateway instances. It is an auto-scaling and self-healing cluster that scales out and in depending on the traffic load. Multicloud Defense Controller and gateway instances exchange constant and continuous information about the state, health and telemetry. The Multicloud Defense Controller makes the decision to scale out/in by measuring the telemetry data received from the gateway instances. The gateways can be configured to run in multiple availability zones for a highly available, resilient architecture. This ensures that a single availability zones failure from a cloud service provider does not compromise the security posture for running applications.

Once you have configured a gateway and any corresponding VPCs or VNets, you can use the **Gateway Details** page in the Multicloud Defense Controller to view and manage the state of them.

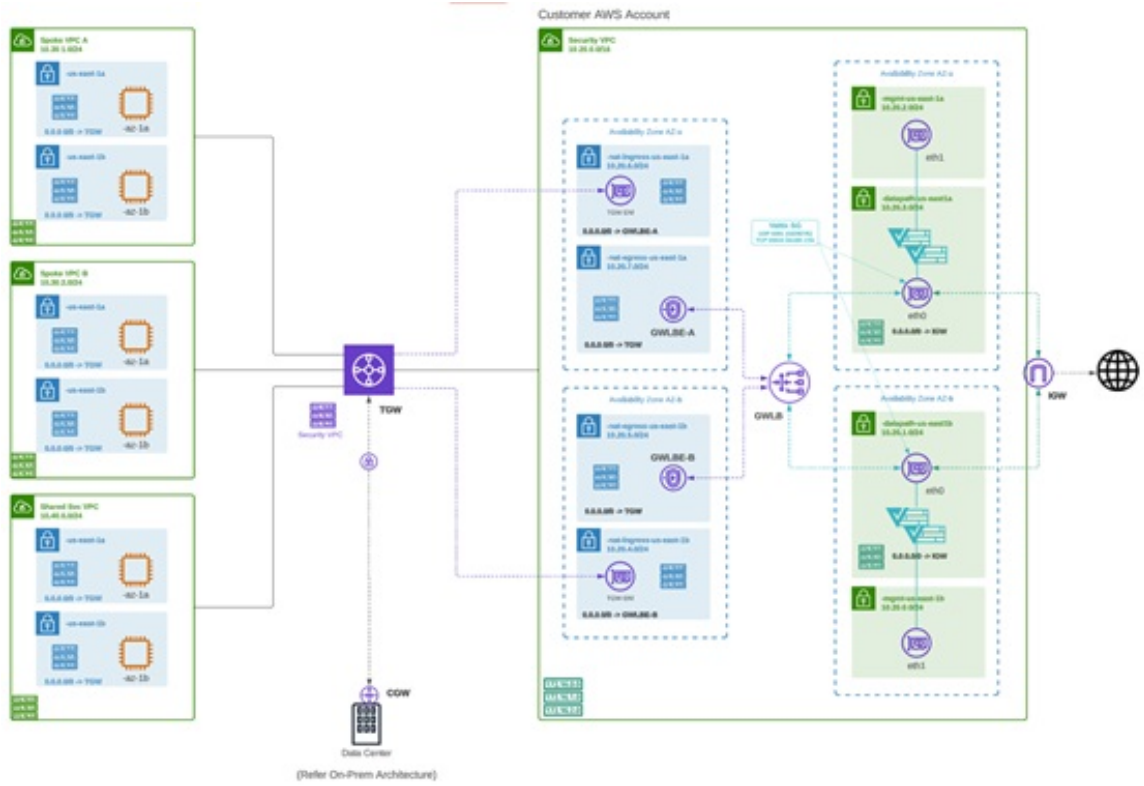
Multicloud Defense Gateways can be deployed in two ways; **Hub** mode and **Edge** mode.

Supported Gateway Use Cases

Egress

Deploying an Egress/East-West gateway to protect traffic leaving their public cloud networks. The egress gateway functions as a transparent forward proxy, performing full decryption and embedding advanced security features like intrusion prevention, antimalware, data loss prevention, and full-path URL filtering. Optionally, it can also operate in a forwarding mode, where it doesn't proxy or decrypt traffic but still applies security functionalities like malicious IP blocking and FQDN filtering.

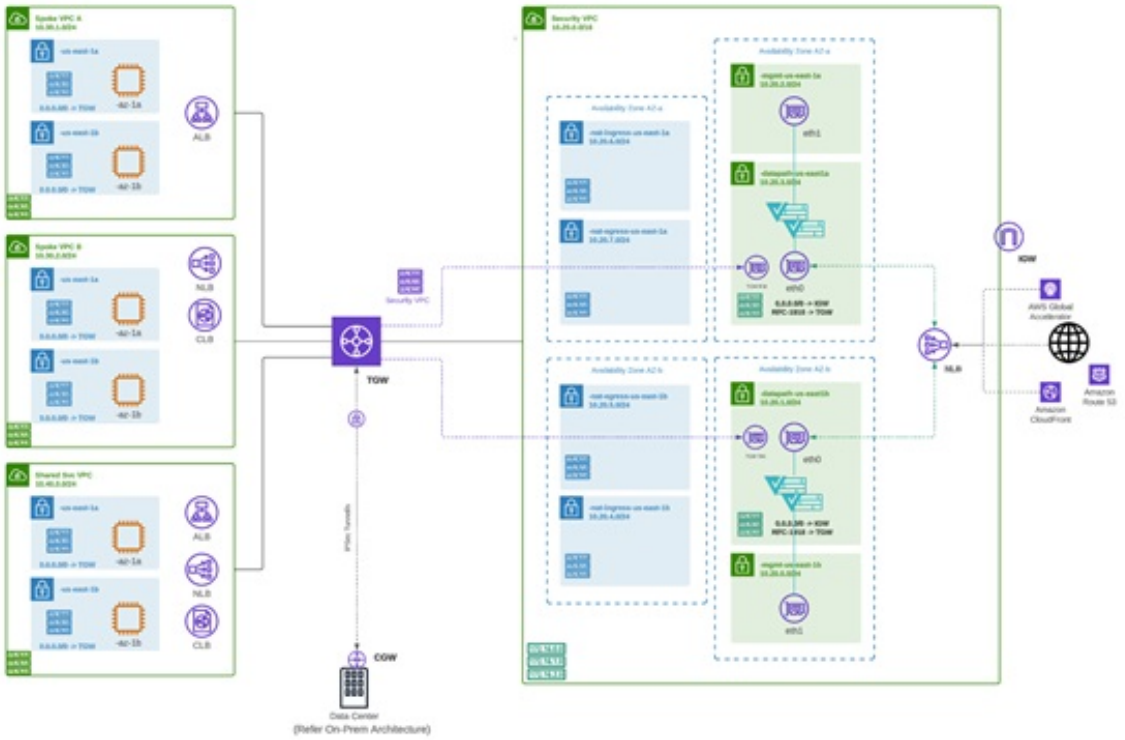
The following diagram is an example of an AWS account with an egress gateway in a centralized mode:



Ingress

Deploying an Ingress gateway protects our public-facing applications. The Ingress gateway acts as a reverse proxy that carries out full decryption and applies advanced security functionalities such as intrusion prevention, antimalware, web application firewall (WAF), and full-path URL filtering.

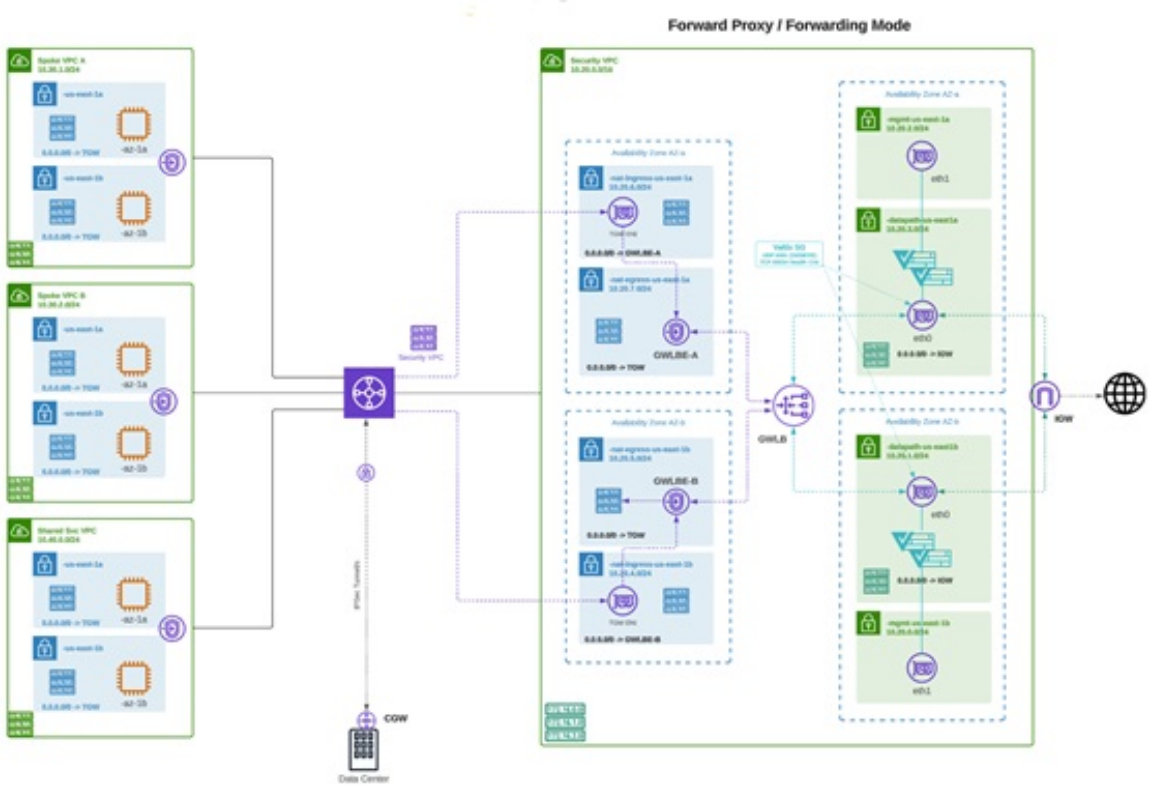
The following diagram is an example of an AWS account with an ingress gateway in a centralized mode:



East-West

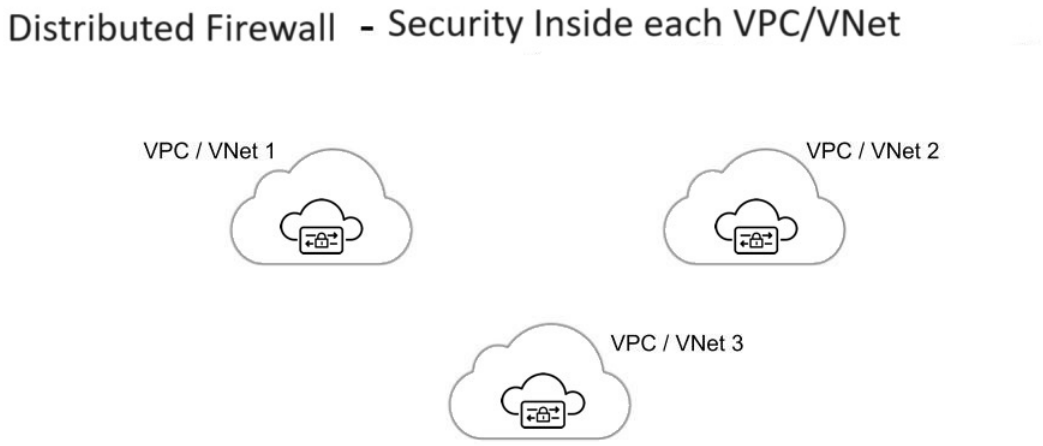
An Egress/East-West gateway deployment implements East-West L4 segmentation between subnets or VPCs/Vnets within their public cloud environments. The gateway functions in a forwarding mode with L4 firewall rules, allowing or denying traffic based on set parameters, with optional logging enabled.

The following diagram is an example of an AWS account with an east-west gateway in a centralized mode:



Distributed

You have applications running in multiple VPC/VNets. Deploy a Multicloud Defense Gateway in each of the VPCs/VNets.



Centralized / Hub

You have applications running in multiple VPCs/VNet. You would like to secure all the applications through a centralized security services VPC/VNet. This model deploys the Multicloud Defense Gateway in a service VPC. You attach all the application VPCs (Spoke VPCs) and the Services VPC to the AWS Transit Gateway or VNet/VPC peering in Azure and GCP. Multicloud Defense provides an option to orchestrate the AWS Transit Gateway, Services VPC and the Spoke VPC Attachments. This is the recommended solution for ease of deployment, removing the complexity of multiple route tables and Transit Gateway attachments.

Figure 1: AWS - Using AWS Transit Gateway

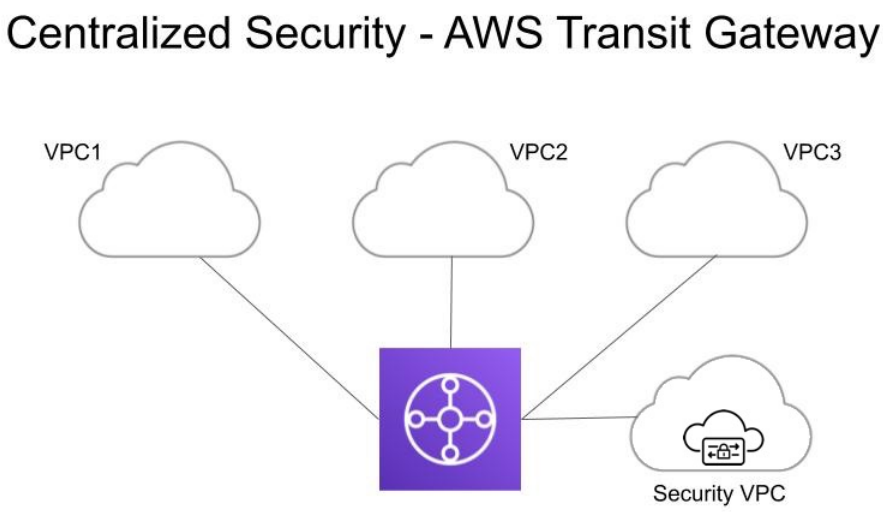


Figure 2: Azure - VNet Peering

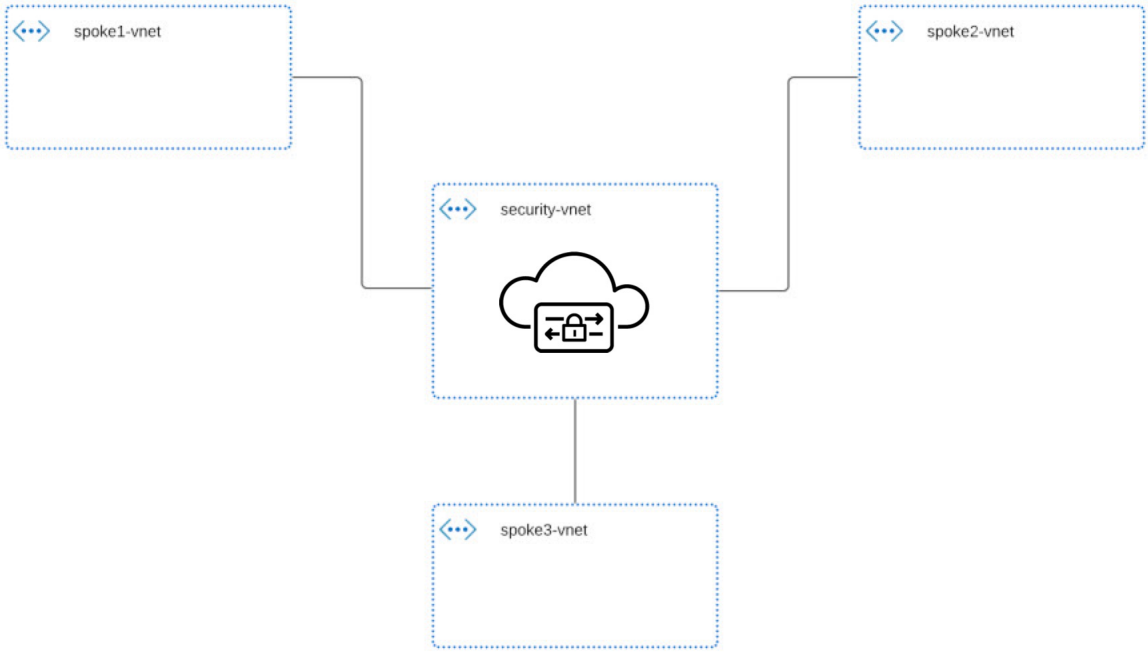
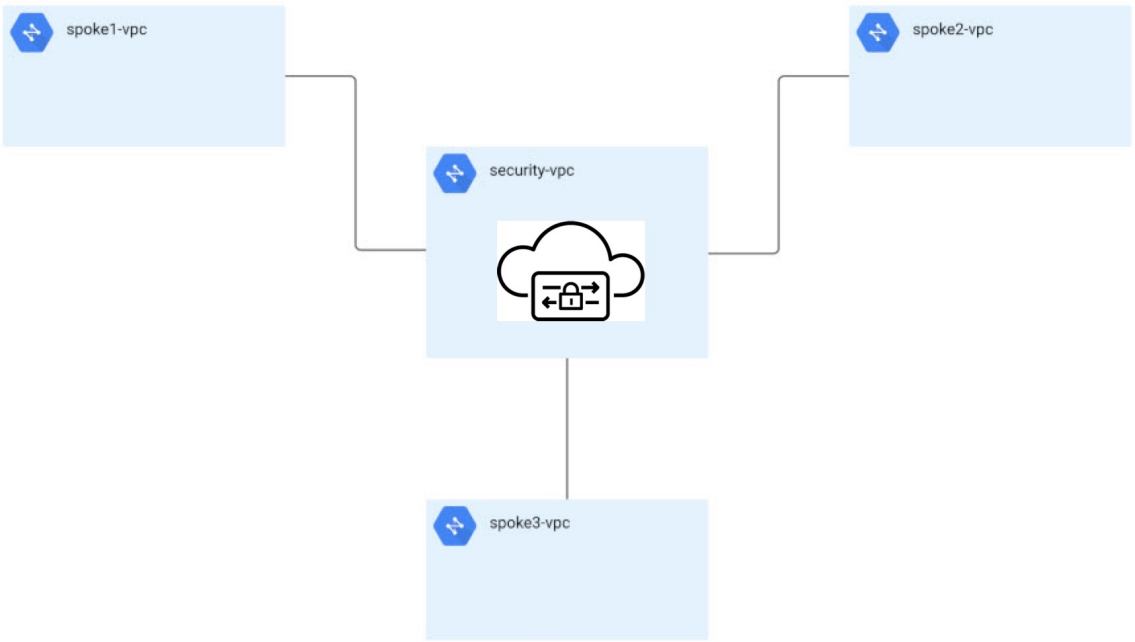


Figure 3: GCP - VPC Peering



Advanced Use Cases

There may be additional prerequisites or post-prrcedure steps for some gateways. Consider the following environments:

AWS: Accelerator to the Ingress Gateway

Multicloud Defense can integrate with a set of one or more AWS global accelerators to use as an ingress point to load balance traffic across the Multicloud Defense Gateway instances. This is similar to the AWS network load balancer that is created and managed by Multicloud Defense when an ingress gateway is deployed, but offers an alternative ingress point for the ingress gateway to protect applications and workloads.

Accelerator, it will manage the global accelerators' listener endpoint group to ensure the endpoint group has the active set of gateway onstances. Client IP addresses will be preserved as they pass through the global accelerator to the Multicloud Defense ingress gateway.

In order to integrate Multicloud Defense with a global accelerator, the user must have first created the global accelerator within AWS, defined a desired listener and created an empty endpoint group (or an endpoint group that contains the existing Multicloud Defense ingress gateway instances). Once the AWS resources exist, then the Multicloud Defense ingress gateway can be configured to integrate with the global accelerator.

Gateways Details

To view the **Gateway Details** page for already established gateways are available in **Manage** > **Gateways**. You can add and manage all gateways from this page. Managing a gateway allows you to edit, upgrade, enable, disable, export, or delete the instance. You must click the checkbox of the gateway you want to modify prior to making any changes.

Note You **must** be an Admin or SuperAdmin for these actions.

To filter and search the list of gateways, use the following criteria can be any of the following items:

- **Name** - The name of the gateway.
- **CSP Account** - The cloud service provider account that is associated with the gateway.
- **CSP Type** - The type of cloud service provider account.
- **Region** - The region of the cloud service provider that is associated with the gateway you are searching for.
- **State** - The current state of the gateway. Gateways can be active or inactive, or pending active or pending inactive.
- **Instance Type** - Each cloud service provider supports a number of instance types.
- **Mode** - Multicloud Defense Gateway instances can be depoyed in hub or edge mode.

Click **Switch to Advanced Search** to construct your own search. Use the drop-down option within the search bar to utilize some of the auto-generated search criteria if needed. For searches that have to repeated, you can **copy** or even **save** searches for future use.

Configure Multicloud Defense Gateway and VPC/VNets

Before You Begin

The supported cloud service providers are separate entities that use their own vocabulary and gateway environment. Not every option available in the Multicloud Defense Controller is compatible with your cloud service provider. For example, AWS uses its own Transit Gateway and you can add VPCs to it while Azure utilizes a load- balancer to manage web traffic and applications and you can add VNets to it. Keep this in mind when proceeding.

Note For AWS environments, when securing spoke VPCs in centralized mode, Multicloud Defense attaches VPCs to the Transit Gateway that is associated to the service VPC. By default, Multicloud Defense will randomly select a subnet in each availability zone for Transit Gateway attachment. You can change this option when you add a VPC or you can modify a VPC that is already assigned to the gateway.

You can also orchestrate a transit gateway through the Multicloud Defense Gateway or attach an existing Transit Gateway.

Resources Created by Multicloud Defense

The following resources are created by Multicloud Defense when you create a gateway, VPC, or VNet. These are created as part of the process and do not require any additional actions from the user. Note that difference resources are created per each cloud service provider requirements.

GCP Resources

Multicloud Defense creates two service VPCs and four firewalls. See the following for the exact resource allocation:

Service VPC

- Management
- Datapath

Firewall Rules

- Management (ingress)
- MAnagement (egress)
- Datapath (egress)
- Datapath (egress)

Note The Service VPC CIDR **cannot** overlap with the Spoke VPC.

AWS Resources

Multicloud Defense creates three service VPCs to address the supported use cases (ingress, egress/ east-west). Created and affiliated with each of these VPCs is the following:

- Four subnets in each availability zone.
- One route table for each of the subnets.
- Two security-groups: management and datapath.
- One Transit Gateway.

Note This Transit Gateway is created and attached to the gateway during the creation of the service VPC. This gateway can be reused with other service VPCs.

- A Transit Gateway route table.

Note The route table is attache to the Service VPC as part of the creation process.

Note The AWS Gateway Load Balancer (GWLB) does not support add/remove of availability zones after initial deployment of a GWLB. You will need to redeploy the service VPC if you need to change availability zones. See AWS documentation for more information.

Azure Resources

Multicloud Defense created one Service VNet with the following resources:

- One VNet.
- Two network security groups.

The Service VNet CIDR value must not overlap with spoke VNet.

Create a Service VPC or VNet

Use the following procedure to create a Service VPC or Service VNet, depending on the gateway you are creating this for. Note the options that are specific to your cloud service provider.

Step 1 From the Multicloud Defense Controller, navigate to **Manage** > **Service VPCs/VNets**.

Step 2 Click **Create Service VPC/VNet**.

Step 3 Input parameter values:

- **Name** - Assign a name to the Service VPC/VNet.
- **CSP Account** - Select the CSP account to create the Service VPC/VNet.

- **Region** - Select the region the Service VPC will be deployed to.
- (Azure only) **CIDR Block** – The CIDR Block for Service VNet. This must not overlap with your Spoke(application) VNets.
- (AWS/GCP only) **Datapath CIDR Block** - The CIDR Block for the Multicloud Defense Gateway datapath Service VPC. This CIDR block must not overlap with address ranges in your Spoke (application) VPCs.
- (AWS/GCP only) **Management CIDR Block** - The CIDR Block for the Multicloud Defense Gateway management Service VPC. This CIDR block must not overlap with address ranges in your Spoke (application) VPCs.
- **Availability Zones** - If you are creating a VPC, you **must** configure **one** availabilitliy zone only. For a VNet, Multicloud Defense recommends to select at least two availability zones for resiliency.
- (Azure only) **Resource Group** - The Resource Group to deploy Service VNet.
- (AWS only)**Transit Gateway** - The Transit Gateway connects virtual private cloud and on-premises networks through a central hub. Use the drop-down menu to select an existing gateway for this VPC. If there is no pre-existing gateway for you to select, choose **Create_new**. This option allows Multicloud Defense to create one as part of the VPC creation process.
- (AWS only) **Transit Gateway Name** - If you opted to create a new Transit Gateway, enter a name for the gateway in this field.
- (AWS only) **Auto accept shared attachments** - If you opted ot create a new Transit Gateway and intend to use this VPC for a multi-account hub gateway deployment, check this option.
- **Use NAT Gateway** - Enable this option if you want all egress traffic will go through NAT Gateway.

Caution Do **not** enable this NAT Gateway option if you intend to deploy this Service VPC to deploy a Multicloud Defense VPN gateway in AWS.

What to do next

Add a Multicloud Defense Gateway.

Add a Multicloud Defense Gateway

Use the following procedure to add a Multicloud Defense Gateway for your cloud service provider:

Step 1 Navigate to **Manage** > **Gateways**.

Step 2 Click **Add Gateway**.

Step 3 Select the cloud service provider you want to add the gateway to.

Step 4 Click **Next**.

Step 5 Enter the following information:

- **Instance Type** - Choose the type of cloud service provider. Note that there may be multiple variations of instances depending on which cloud service provider you are using.
- **Gateway Tpe** - Select either Ingress or Egress.

Note Select **Egress** if you have an east-west network flow.

- **Minimum Instances** - Select the minimum number of instances that you plan to deploy.
- **Maximum Instances** - Select the maximum number instances that you plan to deploy. This is the maximum number that is used for auto-scaling in each availability zone.
- **HealthCheck Port** - Default is 65534. The port number used by Multicloud Defense load balancer to check the health of the instances. Datapath security groups assigned to the instance(s) must allow traffic on this port.
- (Optional) **Packet Capture Profile** - Packet Capture Profile for threat and flow PCAPs.
- (Optional) **Diagnostics Profile** - Diagnostics Profile used to store Technical Support information.
- (Optional) **Log Profile** - Log Forwarding Profile used to forward Events/Logs to a SIEM.
- (Optional) **NTP Profile** - Network Time Protocol (NTP) for time synchonization.

Step 6 Click **Next**.

Step 7 Provide the following parameters:

- **Security** - Select either Egress or Ingress.

  Note Select **Egress** if you have an east-west network flow.

- **Gateway Image** - Image to be deployed.
- **Policy Ruleset** - Select the policy ruleset to associate with this gateway.
- **Region** - Select the region this gateway will be deployed into.
- **Resource Groups** - Select the resource group to associate the gateway with.
- **SSHPublic Key** - Paste the SSH public key. This public key is used by the controller to access the CLI of the deployed gateway instances for debug and monitoring.
- **VNet ID** - Select the VNet to associate with the gateway.
- **User Assigned Identity ID** - Enter the cloud service provider identity to associate with this gateway.
- **Mgmt. Security Group** - Select the security group to associate with the management interface.
- **Datapath Security Group** - Select the security group to associate with the datapath interface.
- **Disk Encryption** - Select the appropriate option from the drop-down menu. For customer managed encryption key, the user will need to input the resource ID of the encryption key.

Step 8 Select the **Availability Zone**, the **Mgmt Subnet** and the **Datapath Subnet**. The available subnets will be based on the VPC or VNet selected above. For high availabilty purposes the gateway instances can be deployed in multiple availability zones. Click the plus button to add a new availability zone and select the parameters for the selected zones.

Note Some cloud service provider regions do not support multiple availability zones. In such regions the gateway instances are deployed in only a single zone.

Step 9 (Azure only, optional) If you are deploying in distributed model with Multicloud Defense Gateway in the same VNet as application, ensure you complete the following:

- Add a route table in the Azure portal and associate the route table with all the subnets.

- Add a default route for 0.0.0.0/0 with **next-hop** as the IP address of the Gateway Network Load Balancer.

Step 10 Click **Next** to view the Advanced Settings.

Step 11 By default, the Multicloud Defense Gateway enables the use of the public IP of the router available. If you do not want this enabled, check the **Disable Public IP** box.

Step 12 Click **Save**. Multicloud Defense deploys the gateway.

What to do next

You **must** attach at least one ruleset to the gateway before you secure a spoke VPC/VNet. See Rule Sets and Rule Set Groups, on page 80 for more information.

Secure Spoke VPC/VNet from Service Menu

Use the following procedure to add a spoke VPC or spoke VNet from the service menu to a gateway:

Before you begin

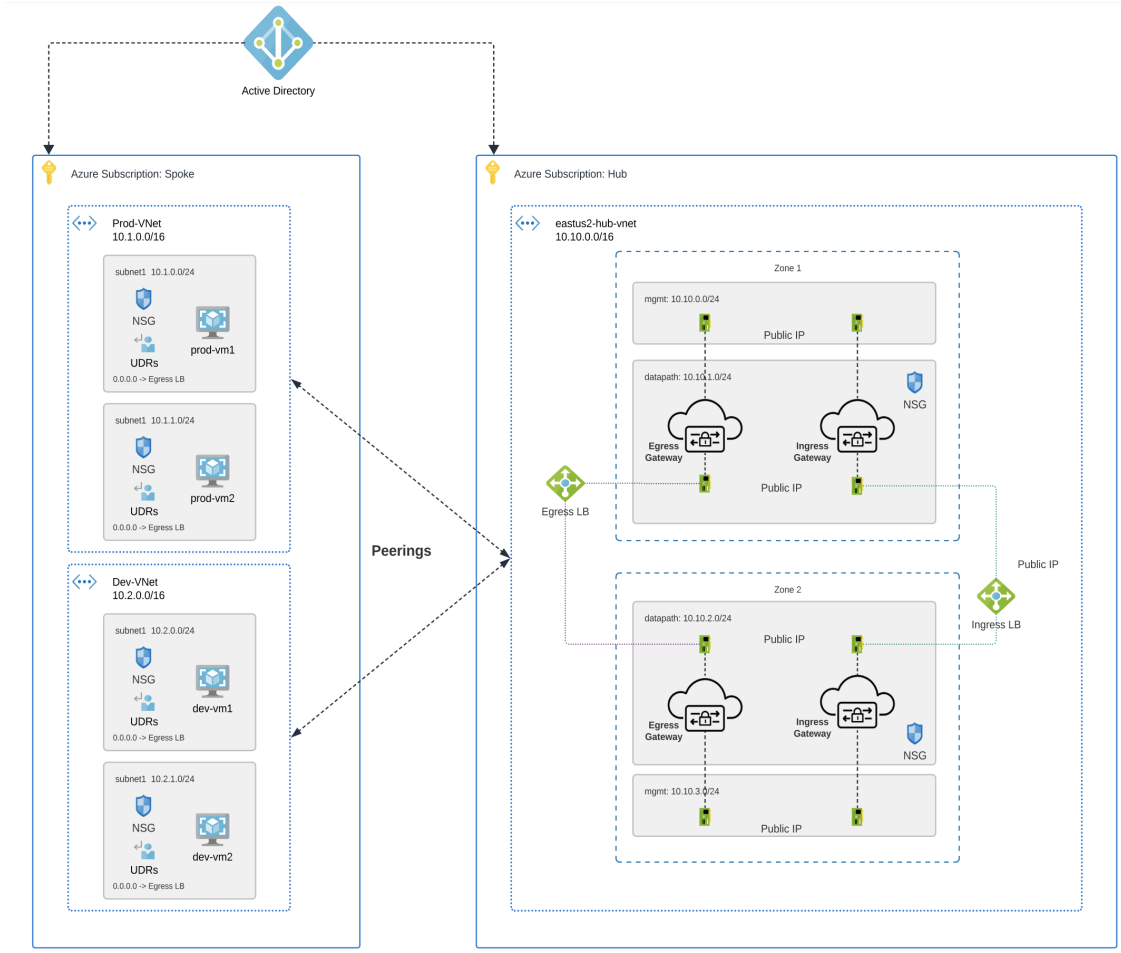
The following must be done prior to creating and assigning a spoke VPC or VNet:

- In AWS and GCP accounts, you must secure remote accounts before you add a gateway.
- Azure environments require a route table attached **prior** to securing spoke VPC/VNet. See the "Associate a route table to a subnet" chapter in the Azure user guide for more.

Note that when you protect an AWS spoke with VPCs in centralized model, Multicloud Defense attach VPCs to the Transit Gateway that is associated to the Service VPC. When attaching VPCs to the Transit Gateway, users can choose which subnet in each availability zone to place the ENIs. By default, Multicloud Defense will randomly select a subnet in each availability zone for Transit Gateway attachment.

VNet pairing is supported across accounts within the same CSP type. You can add spoke VPC/VNets within an account and across accounts. In Azure, for spoke VPCs peering across subscriptions, the CSP accounts should be onboarded using the same app registrations, and subscriptions should be within the same Active Directory.

Figure 4: Azure Combined Hub - Multisubscriptions



Step 1 From the Multicloud Defense Controller dashboard, navigate to **Manage** > **Service VPCs/VNets**.

Step 2 Select Service VPC or Service VNet and navigate to **Actions** > **Manage Spoke VPC/VNet**.

Step 3 Add all spoke VPC or VNets to protect the spoke table.

You can select spoke VPC or VNets from **Spoke VNets for Current Account**. If you want to add spoke VPC or VNets from another account, select from **Spoke VNets for Other Accounts**.

Step 4 Click the **View/Edit** link under the Route Tables column.

Step 5 Check the **Send Traffic via Multicloud Defense Gateway** box to update default route to point to Multicloud Defense Gateway for inspection.

Step 6 Click **Update routes**.

Step 7 Click **Save**.

Manage Your Gateway

View your Multicloud Defense Gateways and statistic in **Manager** > **Gateways**. From this page you can search and filter your gateways, view the cloud service providers assocaited with each gateway, current instance count and type, and more.

For more information on the supported use cases for specific gateway environments, see Supported Gateway Use Cases, on page 59.

Edit a Multicloud Defense Gateway

You can edit a gateway in any state, whether it is enabled or disabled. Use the following procedure to edit an existing Multicloud Defense Gateway:

Step 1 Navigate to **Manage** > **Gateways**.

Step 2 Select the Multicloud Defense Gateway you want to edit in the table so it is highlighted.

Step 3 Expand the **Actions** drop-down menu and click **Edit**.

Step 4 Modify the gateway configuration as needed.

Step 5 Click **Save** to confirm the changes. Alternatively, click **Cancel** to exit the changes.

Upgrade the Multicloud Defense Gateway

Multicloud Defense Gateways serve as an autoscaling self-healing Platform-as-a-Service (Paas), functioning as inline network-based security enforcement nodes. Unlike traditional firewalls, Multicloud Defense eliminates the need for customers to construct virtual firewalls, configure high-availability setups, or manage software installations.

Multicloud Defense Gateway instances operate on highly optimized software, incorporating a single pass datapath pipeline for efficient traffic processing and advanced security enforcement. Each gateway instance comprises three core processes: a "worker" process responsible for policy enforcement, a "distributor" process for traffic distribution and session management, and an "agent" process communicating with the controller. Gateway instances can seamlessly transition "in service" for a "datapath restart," enabling smooth upgrades without disrupting traffic flow.

New instances are spun up with new image. Once the instances are fully up, they are placed in the loadbalancer's (layer 4 sprayer of flows to gateway instances) target pool. The old instances are put in flow draining mode or flow timeout mode for the existing flows going through them. New flows will hit the new instances. Once the timeout (Azure) or the flows are drained (AWS), the old instances are reaped by the controller.

Use the following procedure to

Step 1 Navigate to **Manage** > **Gateways**.

Step 2 Select the checkbox for the gateway you want to upgrade. You can make only one selection at this time.

Step 3 Select **Actions** > **Upgrade**.

Step 4 From the **Gateway Image** list, select the desired image.

Step 5 Click **Save**.

Step 6 Confirm the cloud service provider resource allocation necessary for the upgrade.

Step 7 Click **Yes** if the resource allocation is sufficient. Click **No** if the resource allocation is insufficient, increase the resource allocation in the cloud service provider, and return to continue the upgrade.

Note You can view the upgrade progress and new gateway instances being created from theinstances info for the gateway. Select the gateway and view the **Instances** in the Details pane.

Abort a Multicloud Defense Gateway

You can only abort a Multicloud Defense Gateway that is currently going through an in-progress gateway update.

Use the following procedure to abort an existing Multicloud Defense Gateway:

Step 1 Navigate to **Manage** > **Gateways**.

Step 2 Select the Multicloud Defense Gateway you want to abort in the table so it is highlighted.

Step 3 Expand the **Actions** drop-down menu and click **Abort**.

Step 4 Confirm you want to abort the gateway and click **Yes**. To back out of the action, click **No**.

Enable a Multicloud Defense Gateway

You can only enable gateways that have been disabled. Use the following procedure to enable a

Step 1 Navigate to **Manage** > **Gateways**.

Step 2 Select the Multicloud Defense Gateway you want to enable in the table so it is highlighted.

Step 3 Expand the **Actions** drop-down menu and click **Enable**.

Step 4 Multicloud Defense validates the gateway configuration. If the validation is successful, a table of current and required resources for an upgrade generate for review. If you approve of the gateway resource allocation, click **Yes** to confirm the action.

What to do next

Wait a few minutes for the Multicloud Defense Gateway to successfully enable.

If you've disabled a Multicloud Defense Gateway and deleted the site-to-site VPN tunnels affiliated with it, you **must** create a new site-to-site VPN tunnel connection, or recreate the previous VPN tunnel connection and then add it to the gateway. When a gateway is disabled, Multicloud Defense forgets the public IP address associated with the VPN tunnel. You must create a new tunnel connection to establish a new IP for the gateway instance.

Disable a Multicloud Defense Gateway

You can only disable a Multicloud Defense Gateway if it is currently enabled. You cannot disable gateways that are already disabled.

Use the following procedure to disable a Multicloud Defense Gateway:

Step 1 Navigate to **Manage** > **Gateways**.
Step 2 Select the Multicloud Defense Gateway you want to disable in the table so it is highlighted.
Step 3 Expand the **Actions** drop-down menu and click **Disable**.
Step 4 Confirm you want to disable the gateway and click **Yes**. To cancel this action, click **No**.

What to do next

Wait a few minutes for the gateway to succesfully disable.

To completely disable the gateway, you **must** delete any site-to-site VPN tunnels affiliated with the gateway.

Export a Multicloud Defense Gateway

Use the following procedure to export the configuration of a Multicloud Defense Gateway:

Step 1 Navigate to **Manage** > **Gateways**.
Step 2 Select the Multicloud Defense Gateway you want to export in the table so it is highlighted.
Step 3 Expand the **Actions** drop-down menu and click **Export**.
Step 4 Multicloud Defense generates an export wizard.
Step 5 Either click **Download** to download the terraform locally or scroll down and click **Copy Code** to copy the JSON resource.
Step 6 Manually paste into the terraform script.
Step 7 Within the terraform prompt, execute the command provided in the lower half of the window: `terraform import "ciscomcd_gateway"."object-name" <object name>`.
Step 8 Follow the prompts within the terraform prompt to complete the task. **Close** the export window in Multicloud Defense. There are no more steps in the dashboard.

Delete a Multicloud Defense Gateway

Use the following procedure to delete a Multicloud Defense Gateway. Note that this action is different from disabling the gateway.

Step 1 Navigate to **Manage** > **Gateways**.
Step 2 Select the Multicloud Defense Gateway you want to delete in the table so it is highlighted.
Step 3 Expand the **Actions** drop-down menu and click **Delete**.

Step 4 Confirm the action and click **Yes**. To cancel the deletion action, click **Cancel**.

What to do next

We strongly recommend deleting any site-to-site VPN tunnel connections associated with this gateway after it is successfully deleted from the gateway table.

PART VI

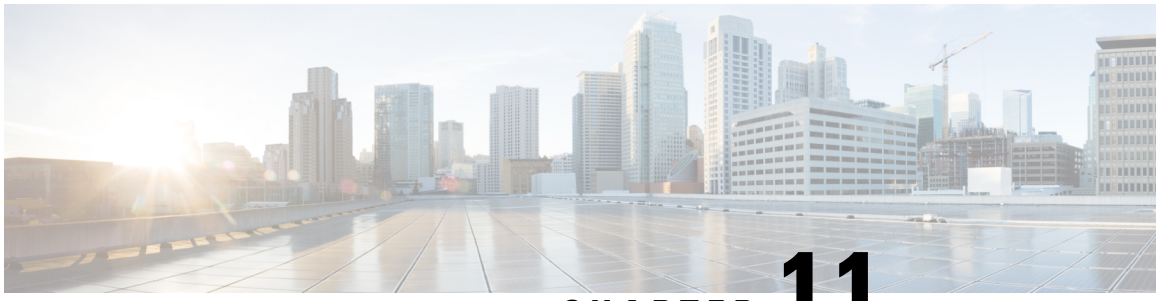
Security Policies

Advanced Policy Settings

Some policies support additional features or functionality.

XFF Header in Ingress Policy

Note that ingress policies support X-Forwarded-For (XFF) headers in the HTTP packet. XFF is a standard header for identifying the originating IP address of a client connecting to a web server through a proxy server.



CHAPTER 11

Rules and Rule Sets

Rules

In general, rules specify the rights of a user, group, role, or organization to access objects of a specified type and state within a domain. Multicloud Defense supports a variety of cloud service providers and each of these environments have their own requirements or methods for their rules. Rules created in your cloud account might be handled differently than rules that are created in the Multicloud Defense Controller. Some rules are applied to gateways and instances by default so the environments have a basic level of protection as you continue to add and modify the rules and policies for optimal performance and coverage.

Rule **types** are important when considering the type of gateway environment you are catering to. Not all rules or rule types are completely compatible with every gateway environment. Gateway types supported in Multicloud Defense Controller are ingress, egress, and east-west.

For information about rules and rule sets, or how to create or modify rules and rule sets for policies and groups, read the rest of this chapter.

Policy Management

Policies are created in the Multicloud Defense dashboard or through orchestration using the Multicloud Defense Terraform provider. The policies are stored and retained as part of the Multicloud Defense Controller database. The gateway retrieves the policy or any policy changes through a periodic heartbeat where the gateway provides the controller health and telemetry information, while also requesting if there are any policy changes that need to be applied. The gateway to controller communication is fully encrypted and established through a mutual TLS session. The heartbeats occur every 5 seconds to ensure that policies on the gateway are synchronized with the policies created or modified by the user.

Policy Rule Set Gateway and Management

Policy Rule Management

A policy rule set assigned to a gateway can be changed dynamically to a different policy rule set. If there is a requirement to swap in a different policy rule set to an active gateway, this operation can be initiated in a non-impactful way. The assignment of the new policy rule set operates similarly to a gateway update/upgrade process. New gateway instances are instantiated with the new policy rule set. New traffic sessions are redirected to the new fateway instances once they are active and healthy. Old traffic sessions are flushed from the old fateway instances. The old fateway instances are deleted. The operation completes in a matter of minutes. This change is initiated as part of the gateway configuration settings. Navigate to **Manage** > **Gateways** > **Gateways**. The change can be initiated using the Multicloud Defense portal or the Multicloud Defense Terraform Provider.

Policy Rule Set Gateway Status

The status of the connection between the policy rule and the gateway it is associated with can be one of the two options:

- **Updated** - The policy is active on the gateway and is synchronized with the controller.
- **Updating** - The gateway is actively processing a policy change. The policy change is known to the gateway, but is not yet active. The gateway is still process traffic using the current policy.

Rule Sets and Rule Set Groups

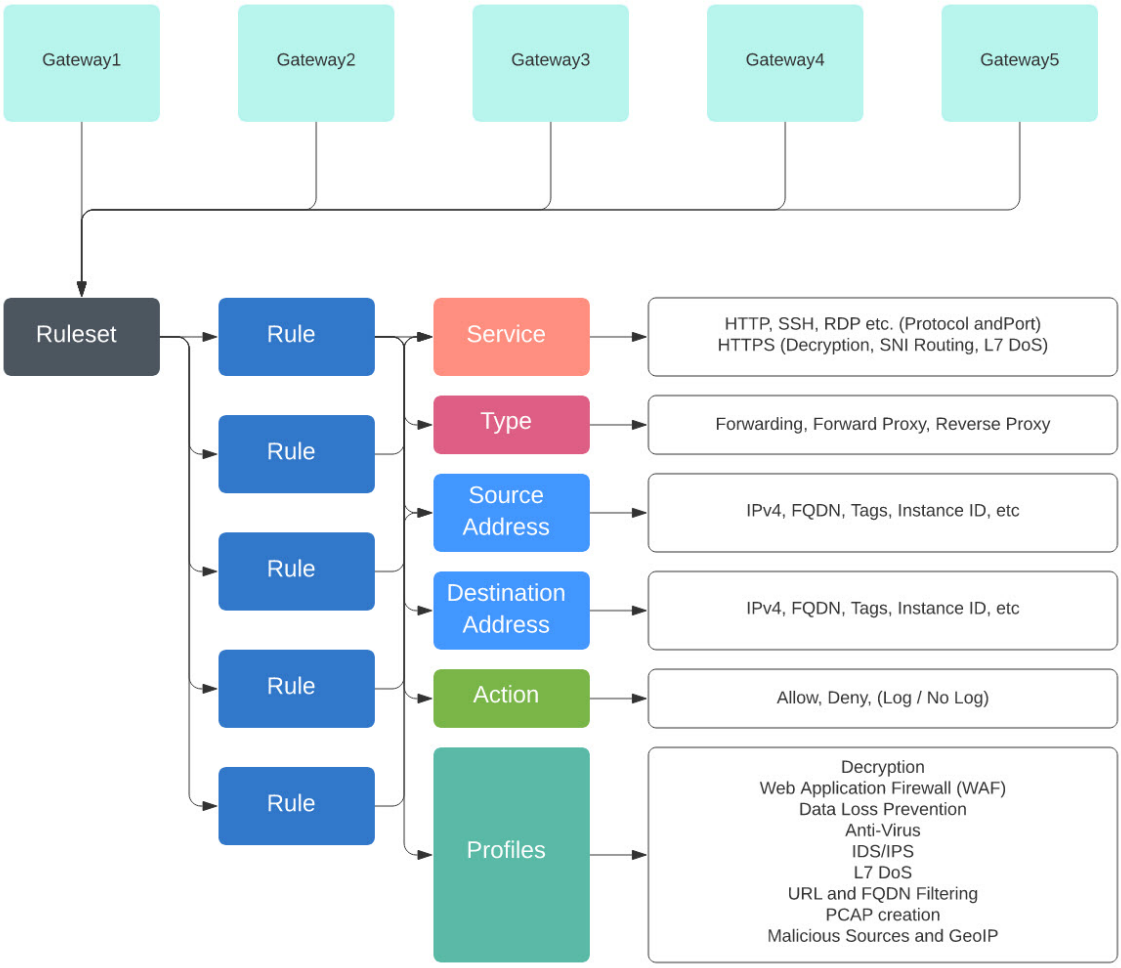
Rule Sets

Rule sets consist of a set of rules that define a segmentation and advanced security policy that are applied to a set of one or more gateways to accommodate application and workload protection. The rules are organized as a priority list where traffic is processed by an matched rule, a general action is taken to allow or deny, and further inspection is accommodated through advanced security.

Rule sets must be associated with at least one Multicloud Defense Gateway. The following limitations apply to all rule sets:

- Rule sets are cloud agnostic and can be applied to one or more gateways operation across multiple cloud environment.
- A gateway can only be associated with a single rule set, although more than one rule set can be applied using a rule set group.
- Rules within a rule set can use discovered cloud asset information to form a dynamic policy, or a policy that adapts in real time to changes.
- A rule set can include rules that only apply to specific cloud accounts and/or cloud regions, although the rule set is applied to gateways that cross cloud environments. Here is an example:
    - A dynamic tag-based address object used in a rule within a rule set that is applied to two gateways across two clouds can resolve to a set of IP addresses that are associated with a gateway in one cloud, while resolving to a different set of IP addresses that are associated with a gateway in another cloud.

- Rule sets can be created from the **Manage** > **Security Policies** > **Rule Sets** page or from within the gateway creation workflow. The following diagram is of a a single rule set applied to multiple gateways:



Another supported use case is of multiple rule sets associated with multiple gateways.

Policy Rule Set Groups

A policy rule set group is a collection of standalone rule sets. Users can combine multiple standalone rule sets into a policy rule set group and associate the group to one or more Multicloud Defense Gateways. Policy rule set groups allow organizations to separate policies in an organized fashion and combine them to an overarching policy.

Note

- A policy rule set group can only consist of rule set members.
- Ensure all rule sets associated with a policy rule set group do not have conflicting rules.
- A policy rule set group can have a maximum of 100 rule set members.

Create Policy Rule Set

To create a policy rule set:

Step 1 Navigate to **Manage** > **Security Policies** > **Rule Sets**.
Step 2 Click **Create**.
Step 3 Add a name and description for the policy rule set.
Step 4 Click **Save.**

What to do next

Once the policy rule set is created, Add or Edit a Forward Proxy Rule in a Rule Set to the rule set.

Create a Rule in a Rule Set

-

Add or Edit a Forwarding Rule in a Rule Set

Use the following procedure to add existing rules to a policy rule set or to edit rules that are already included in a policy rule set:

Before you begin

You can create a new rule within the Multicloud Defense Gateway. Note the following limitations before you add or edit rules to your rule set:

- A single policy rule set can have a maximum of 2047 rules.
- A policy rule set group can have a maximum combined set of 2047 rules.

Step 1 Navigate to **Manage** > **Security Policies** > **Rule Sets**.
Step 2 Click the policy rule set name to view the policy rule set.
Step 3 Click **Add Rule** to create a new rule or add an existing rule. This generates a prompt.
Step 4 Enter the following properties:

- **Name** - a unique name used to reference the rule.
- (optional) **Description** - A brief description of the rule.
- **Type** - Select **Forwarding**.

Step 5 Enter the following Object information:

- **Service** - The service object used to determine the protocols and ports for which the rule will apply.
- **Source** - The address object used to determine the resources for which the rule will apply.

- **Destination** - The address object used to determine the destination resources for which the rule will apply. For a **ReverseProxy** rule type, the destination is always the Multicloud Defense Gateway. For **ForwardProxy** rule types, the destination is always any.
- **FQDN** - Use the drop-down menu to select a set of FQDNs used for SNI match. Note this applies only to **Forwarding** rule types.

Step 6 Enter the Details:

- **Action** - The action defines whether the traffic should be allowed or denied, and whether the traffic should be logged or not logged in events. Traffic is always logged in traffic summary, no matter whether the action is set to **Log** or **No Log**. For traffic that is allowed by the rule, the advanced security profiles are evaluated. Note that each advanced security profile has its own action that will either use or override this action.
- **Reset On Deny** - If enabled, the Multicloud Defense Gateway will send a TCP Reset packet for the sessions that matches this policy and is dropped by the gateway. Note this only applies to **Forwarding** rule types.

Step 7 Enter the following Profiles information:

- (Optional) **Network Intrusion** - The Network Intrusion (IPS) profile to be used for advanced security.
- (Optional) **Anti-malware** - The Anti-malware profile to be used for advanced security. If you do not already have an Anti-malwre profile created, click **+ Create Anti Malware** here.
- (Optional) **Data Loss Prevention** - The Data Loss Prevention (DLP) profile to be used for advanced security. Note that this applies only to **ForwardProxy** rule types.
- (Optional) **FQDN Filtering** - The FQDN Filtering (FQDN) profile to be used for advanced security.
- (Optional) **Malicious IPs** - The Malicious IPs (MIP) profile to be used for advanced security.
- (Optional) **PCAP** - Check this box to enable. Whether packet capture is enabled or disabled for the rule. Whenever traffic matches a rule with PCAP enabled, a packet capture of the session traffic will occur and the PCAP will be stored in the location specified by the PCAP profile. The PCAP profile is configured on the Multicloud Defense Gateway.

Step 8 After specifying the configuration for the rule, click **Save**.

Step 9 Continue adding more rules. Once all desired rules have been added, click **Save Changes**. You will be presented with a before and after view of all changes made to the rule set. If satisfied with your changes, click **Save**. If you need to make further changes, click **Cancel** to return to editing your rule set.

Add or Edit a Reverse Proxy Rule in a Rule Set

Use the following procedure to add existing rules to a policy rule set or to edit rules that are already included in a policy rule set:

Before you begin

You can create a new rule within the Multicloud Defense Gateway. Note the following limitations before you add or edit rules to your rule set:

- A single policy rule set can have a maximum of 2047 rules.
- A policy rule set group can have a maximum combined set of 2047 rules.

Step 1 Navigate to **Manage** > **Security Policies** > **Rule Sets**.

Step 2 Click the policy rule set name to view the policy rule set.

Step 3 Click **Add Rule** to create a new rule or add an existing rule. This generates a prompt.

Step 4 Enter the following properties:

- **Name** - a unique name used to reference the rule.
- (optional) **Description** - A brief description of the rule.
- **Type** - Select **ReverseProxy**.

Step 5 Enter the following Object information:

- **Service** - The service object used to determine the protocols and ports for which the rule will apply.
- **Source** - The address object used to determine the resources for which the rule will apply.
- **Destination** - The address object used to determine the destination resources for which the rule will apply. For a **ReverseProxy** rule type, the destination is always the Multicloud Defense Gateway.
- **Target** - The address object used to specify the destination for which the Multicloud Defense Gateway will establish a gateway to server connection.

Step 6 Select the preffered rule **Action**. This defines whether the traffic should be allowed or denied, and whether the traffic should be logged or not logged in events. Traffic is always logged in traffic summary, no matter whether the action is set to **Log** or **No Log**. For traffic that is allowed by the rule, the advanced security profiles are evaluated. Note that each advanced security profile has its own action that will either use or override this action.

Step 7 Enter the following Profiles information:

- (Optional) **Network Intrusion** - The Network Intrusion (IPS) profile to be used for advanced security.
- (Optional) **Anti-malware** - The Anti-malware profile to be used for advanced security. If you do not already have an Anti-malwre profile created, click **+ Create Anti Malware** here.
- (Optional) **Web Protection** - The Web Protection (WAF) profile to be used for advanced security. Note that this applies only to **ReverseProxy** rule types.
- (Optional) **URL Filtering** - The URL Filtering (URL) profile to be used for advanced security. Note that this applies only to **ForwardProxy** and **ReverseProxy** rule types.
- (Optional) **Malicious IPs** - The Malicious IPs (MIP) profile to be used for advanced security.
- (Optional) **PCAP** - Check this box to enable. Whether packet capture is enabled or disabled for the rule. Whenever traffic matches a rule with PCAP enabled, a packet capture of the session traffic will occur and the PCAP will be stored in the location specified by the PCAP profile. The PCAP profile is configured on the Multicloud Defense Gateway.

Step 8 After specifying the configuration for the rule, click **Save**.

Step 9 Continue adding more rules. Once all desired rules have been added, click **Save Changes**. You will be presented with a before and after view of all changes made to the rule set. If satisfied with your changes, click **Save**. If you need to make further changes, click **Cancel** to return to editing your rule set.

Add or Edit a Forward Proxy Rule in a Rule Set

Use the following procedure to add existing rules to a policy rule set or to edit rules that are already included in a policy rule set:

Before you begin

You can create a new rule within the Multicloud Defense Gateway. Note the following limitations before you add or edit rules to your rule set:

- A single policy rule set can have a maximum of 2047 rules.
- A policy rule set group can have a maximum combined set of 2047 rules.

Step 1 Navigate to **Manage** > **Security Policies** > **Rule Sets**.

Step 2 Click the policy rule set name to view the policy rule set.

Step 3 Click **Add Rule** to create a new rule or add an existing rule. This generates a prompt.

Step 4 Enter the following properties:

- **Name** - a unique name used to reference the rule.
- (optional) **Description** - A brief description of the rule.
- **Type** - Select **ForwardProxy**.

Step 5 Enter the following Object information:

- **Service** - The service object used to determine the protocols and ports for which the rule will apply.
- **Source** - The address object used to determine the resources for which the rule will apply.
- **Destination** - The address object used to determine the destination resources for which the rule will apply. For **ForwardProxy** rule types, the destination is always any.
- **FQDN** - Use the drop-down menu to select a set of FQDNs used for SNI match. Note this applies only to **Forwarding** rule types.

Step 6 Enter the preffered rule **Action**. This defines whether the traffic should be allowed or denied, and whether the traffic should be logged or not logged in events. Traffic is always logged in traffic summary, no matter whether the action is set to **Log** or **No Log**. For traffic that is allowed by the rule, the advanced security profiles are evaluated. Note that each advanced security profile has its own action that will either use or override this action.:

Step 7 Enter the following Profiles information:

- (Optional) **Network Intrusion** - The Network Intrusion (IPS) profile to be used for advanced security.
- (Optional) **Anti-malware** - The Anti-malware profile to be used for advanced security. If you do not already have an Anti-malwre profile created, click **+ Create Anti Malware** here.
- (Optional) **Data Loss Prevention** - The Data Loss Prevention (DLP) profile to be used for advanced security. Note that this applies only to **ForwardProxy** rule types.
- (Optional) **URL Filtering** - The URL Filtering (URL) profile to be used for advanced security. Note that this applies only to **ForwardProxy** and **ReverseProxy** rule types.

- (Optional) **FQDN Filtering** - The FQDN Filtering (FQDN) profile to be used for advanced security.
- (Optional) **Malicious IPs** - The Malicious IPs (MIP) profile to be used for advanced security.
- (Optional) **PCAP** - Check this box to enable. Whether packet capture is enabled or disabled for the rule. Whenever traffic matches a rule with PCAP enabled, a packet capture of the session traffic will occur and the PCAP will be stored in the location specified by the PCAP profile. The PCAP profile is configured on the Multicloud Defense Gateway.

Step 8 After specifying the configuration for the rule, click **Save**.

Step 9 Continue adding more rules. Once all desired rules have been added, click **Save Changes**. You will be presented with a before and after view of all changes made to the rule set. If satisfied with your changes, click **Save**. If you need to make further changes, click **Cancel** to return to editing your rule set.

Disable, Edit, Clone, or Delete Rules in a Rule Set

Use the following procedure to edit or clone an existing rule that is configured for a rule set. You can also disable a rule if you do not need it active for your currenty policies or rule set. You can delete a rule if you do not need it now or for any future deployment.

Note that you can only edit or clone one rule at a time. You can disable or delete multiple rules simulatneously.

Step 1 Navigate to **Manage** > **Security Policies** > **Rule Sets**.

Step 2 Locate the rule set that contains the rule you want to disable, edit, clone, or delete and click the rule set name.

Step 3 Check the checkbox of the standalone rule.

Step 4 Expand the **Actions** button.

Step 5 Select your actionable item:

- **Disable** - This option keeps the rule in the rule set but disables the rule and the configured rule action from affecting traffic.
- **Edit** - This option launches the Properties window and allows you to edit the configuration of the rule. Click **Save** to keep the changes you made.
- **Clone** - This option creates a duplicate of the rule and opens the Properties window for you to name the cloned rule, or make any additional changes to the rule's configuration. Click **Save** to confirm the configuration. Saving a cloned rule automatically adds it to the rule set you are viewing.
- **Delete** - This option permanently removes the rule from the rule set. Note that this also removed the rule from the gateway.

Step 6 Click **Save Changes** to confirm the changes you made to the rule and, indirectly, do the rule set. If you do not want to save the changes, click **Cancel**. Confirm that losing any changes made to the gateway is OK.

Create a Policy Rule Set Group

To create a policy rule set group:

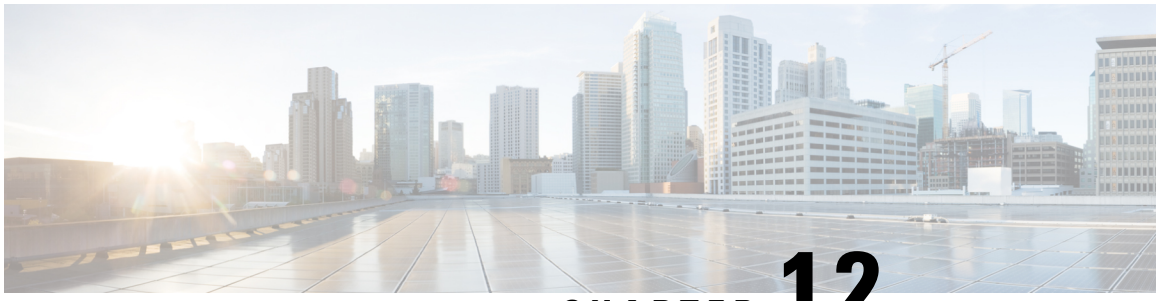
Step 1 Navigate to **Manage** > **Security Policies** > **Rules**.

Step 2 Click **Create**.

Step 3 Add a name and description for the policy rule set group.

Step 4 Select **Type** as the group.

Step 5 Expand the drop-down menu to add rule sets in the **Rule Set List** section. If you want to add more rule sets, click **Add Rule Sets** to add another row.



CHAPTER 12

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 92. Use the following procedure to create a src/dst address object in Multicloud Defense:

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 89. 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 94. Use the following procedure to create a reverse proxy target address object in Multicloud Defense:

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 89. 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.

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:

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.

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

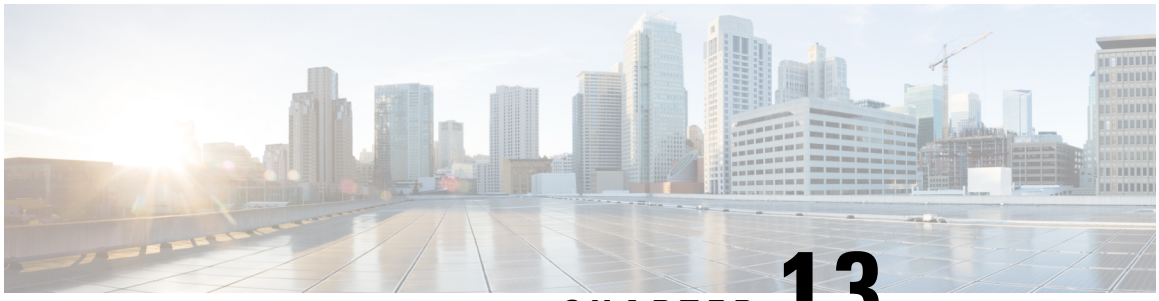
Step 2 Check the box next to the address object you would like to **Delete**.

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.



CHAPTER 13

FQDN Objects

FQDN Match Object

An FQDN (Fully Qualified Domain Name) Match Object evaluates the SNI (Server Name Indication) associated with TLS-encrypted traffic and uses the results of the evaluation for rule matching. If traffic matches all match objects (Address, FQDN, Service) associated with a rule, then the rule will be used for processing the traffic. In order to evaluate the FQDN, traffic must be TLS encrypted and contain an SNI in a TLS hello header. The FQDN can be evaluated for traffic that is processed by either a **Forwarding** or**Forward Proxy** rule. The set of FQDNs in the profile can be specified as strings representing the full domain or as strings represented by a Perl Compatible Regular Expression (PCRE).

Note The FQDN match object is organized as a table containing user-specified rows (FQDNs).

The limits for each FQDN match object are as follows:

- Maximum user-specified rows: 254 (Standalone or Group of Standalones)
- Maximum FQDNs per row: 60
- Maximum FQDN character length: 255

When specifying a multi-level domain (e.g., `www.example.com`), it's important to escape the `.` character (for example,`www\.example\.com`) otherwise it will be treated as a wildcard for any single character.

Standalone vs. Group

A FQDN Match Object can be specified as Type Standalone or Group.

A FQDN Match Standalone Object contains FQDNs. The Object will be applied directly to a set of one or more Policy Ruleset Rules or associated with a FQDN Match Group Object.

A FQDN Match Group Object contains an ordered list of Standalone FQDN Objects that can be defined for different purposes and combined together into a Group Object. The Group Object can be applied directly to a set of one or more Policy Ruleset Rules. Each team can create and manage specific Standalone Profiles. These Standalone Profiles can be combined together into a Group Profile to create hierarchies or different

combinations based on use case. An example combination could be a global FQDN list that would apply to everything, a CSP-specific list that would apply to each different CSP, and an application-specific list that would apply to each different application.

Create Standalone FQDN Match Object

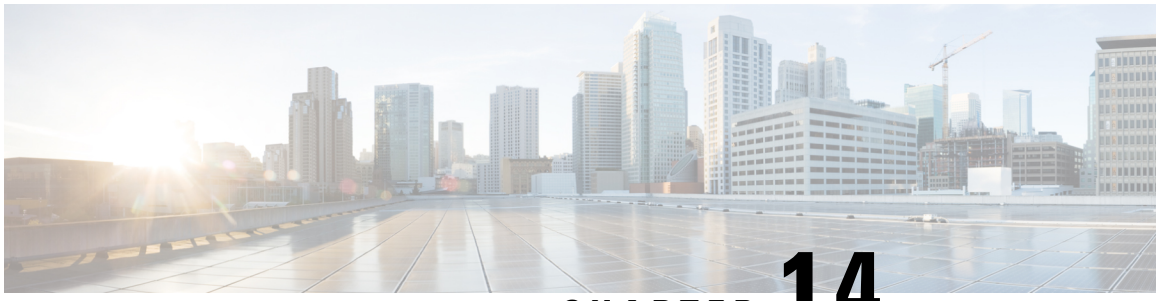
Step 1 Navigate to **Manage** > **Security Policies** > **FQDNs**.
Step 2 Click **Create**.
Step 3 Provide a Profile Name and Description.
Step 4 Specify the Type as Standalone.
Step 5 Click **Add** to create a new row.
Step 6 Specify individual FQDNs (e.g., www.twitter.com,.*.google.com)
a) Each FQDN is specified as a PCRE (Perl Compatible Regular Expression).
b) Consider escaping the . character else it will be treated as a single character wildcard.
Step 7 (Optional) Specify Decryption Exception for any FQDNs where decryption is not desired or possible. Possible reasons for considering Decryption Exception include:
Step 8 Desire to not inspect encrypted traffic (financial services, defense, health care, etc.).
Step 9 SSO authentication traffic where decryption is not possible.
Step 10 NTLM traffic that cannot be proxied.
Step 11 Click **Save** when completed.

Create Group FQDN Match Object

Step 1 Navigate to **Manage** > **Security Policies** > **FQDNs**.
Step 2 Click **Create**.
Step 3 Provide a Profile Name and Description.
Step 4 Specify the Type as Group.
Step 5 Select an initial Standalone Profile (at least one Standalone Profile is required).
Step 6 Specify additional Standalone Profiles.
Step 7 Click **Add FQDN Profile** to create a new row.
Step 8 Select a Standalone Profile.
Step 9 Click **Save** when completed.

Associate the Object

Check Rules to create/edit Policy Rules.



CHAPTER 14

Service Objects

Reverse Proxy Service Object (Ingress)

Ingress service objects are used in the ngress/Reverse proxy rules. The object defines a listener port that the Multicloud Defense gateway listens for the traffic it receives and forwards to the target/backend address. Listener port can be configured with a decryption profile that has a TLS certificate configured. When the traffic hits the listener port, Multicloud Defense Gateway returns the TLS certificate configured. consider the following confiugrable options:

- An SNI can be configured on this port. This enables a single listener port (e.g 443) to be proxied to multiple backend targets based on the SNI.
- L7 DoS (L7 Denial of Service) can be configured on the service to set rate limits for an URI and/or HTTP method.
- Target defines the backend address object and port to forward the traffic. The proxied traffic can be forwarded as HTTP, HTTPS, TCP or TLS.

Use the following procedure to create and add a reverse proxy service object:

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

Step 2 Click **Create**.

Step 3 Click **Reverse Proxy**.

Step 4 Provide a **Name** and **Description**.

Step 5 Configure proxy parameters as defined below:

Option	Description
Decryption Profile	Assign a decryption profile, which also includes the server certificate, to be used for the proxy service.

Option	Description
Dst Port	Assign a destination port. For most web-based services, the destination port will be 443. This is the port Multicloud Defense Gateway listens on for the incoming traffic.
Protocol	TCP is the default.
SNI	Enter the list of SNIs.
L7 DoS	Enter the Layer 7 DoS profile to assign to this proxy service.
Target Backend Port	Enter the Target/Backend application port number.
Protocol	Select the backend protocol.
Address	Select a backend IP address. The IP address in most cases will be the frontend IP of an internal load balancer.

Note If the proxy service is required to run on multiple ports, you can add more entries. However all the ports serve the same certificate and are proxied to the same backend destination address object.

Forward Proxy Service Object (Egress / East-West)

Forward Proxy services are specifically used for HTTP based traffic. The object defines a listener port that the Multicloud Defense Gateway listens for the traffic it receives and forwards to the address/host that's available in the TLS SNI extension header or HTTP Host Header.

Note We recommend using this for egress/east-west traffic.

Use the following procedure to create and add a forward proxy service.

Step 1 Navigate to **Manage** > **Security Policies** > **Services**.
Step 2 Click **Create**.
Step 3 Click **Forward Proxy**.
Step 4 Provide a name and description.
Step 5 Optionally select the Application IDs to match.
Step 6 Configure proxy parameters as defined below.

Option	description
Decryption Profile	Assign a decryption profile, which also includes the certificate. Multicloud Defense impersonates the external certificate by signing it with the certificate provided in this profile. The root certificate is assumed to be installed on all the client application instances.
Dst Port	Assign a destination port. For most web-based services, the destination port will be 443.
Protocol	HTTP or HTTPS.

Note

- Multicloud Defense listens on the **Dst Port** and waits for the HTTP Host header or TLS SNI Header packet. Once Multicloud Defense receives this packet it connects to the host using the protocol. If the protocol is HTTPS, the received certificate data from the external host is signed by the certificate in the decryption profile and sent to the client. The root certificate **must** be installed on the client app instances to avoid a certificate error.
- For a given destination port, there can be only one decryption profile (root CA certificate) association in a policy rule set across all service objects.
- During a forward proxy session, Multicloud Defense Gateway performs a DNS lookup on the destination with DNS request timeout of 30 seconds and cache age-out of TTL seconds.

Forwarding Service Object (Egress / East-West)

Forwarding service objects are used in the forwarding rules. The traffic that matches this type of rule/service is not proxied, and is forwarded as-is. This means there is no deep packet inspection and no Application ID on *encrypted* traffic.

Note We **strongly** recommend using this for East-West traffic.

Use the following procedure to create and add a forwarding service object:

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

Step 2 Click **Create**.

Step 3 Click **Forwarding**.

Step 4 Provide a name and description.

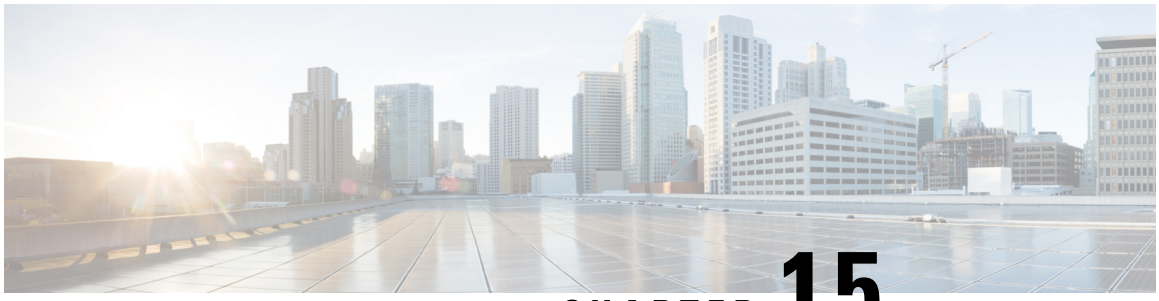
Step 5 Multicloud Defense supports source NAT on a per service level. For traffic that requires source IP preservation(e.g. East-West traffic), disable SNAT.

For Egress traffic, SNAT **must** always be enabled.

Step 6 Configure port parameters as defined below.

Option	description
Dst Port	Assign a destination port or a range of destination ports as `start-end`.
Protocol	TCP, UDP, ICMP

Note In a forwarding policy, deep packet inspection operations **only** occur on non-encrypted traffic.



CHAPTER 15

Certificates and Keys

Certificates and Keys

TLS certificates and keys are used by the Multicloud Defense Gateway in proxy scenarios. For ingress (reverse proxy) users access the application via Multicloud Defense Gateway and it presents the certificate configured for the service. For egress (forward proxy) cases, the external host's certificate is impersonated and signed by the certificate defined.

Certificate body is imported to the Multicloud Defense Controller. The private key can be provided in the following ways:

- Import the private key contents.
- Store in AWS secrets manager and provide the secret name.
- Store in AWS KMS and provide the cipher text contents.
- Store in GCP secrets manager and provide the secret name.
- Store in Azure keyvault and secret and provide the keyvault and secret name.

For testing purposes you can also generate a self-signed certificate on the Multicloud Defense Controller. This is similar to importing the private key contents from your local file system.

Note Certificates are **NOT** editable once created. If you need to replace the existing certificate, you will need to create a new certificate, edit the decryption profile to reference the new certificate, and then delete the old certificate.

When importing the certificate and private key, the Multicloud Defense Controller / UI can detect if there is a mismatch. However, when using any other import method where the private key is stored within the cloud service provider, the Multicloud Defense Controller / UI will not be able to detect if there is a mismatch. This is by design to ensure the private key remains private and within your cloud service provider. When the private key is needed by the Multicloud Defense Gateway, it is accessed and used, and if there is a mismatch, an error is generated.

Import Certificate

Step 1 Navigate to **Mange** > **Security Policies** > **Certificates**.
Step 2 Click **Create**.
Step 3 When prompted with the **Method**, choose **Import your Certificate and Private Key**.
Step 4 Copy the contents of the certificate file in the **Certificate Body**. This can include the certificate and the chain.
Step 5 Copy the contents of the private key in **Certificate Private Key**.
Step 6 (Optional) Import the chain into the **Certificate Chain** if your certificate and the chain are in different files.
Step 7 Click **Save**.

AWS - KMS

Step 1 Navigate to **Mange** > **Security Policies** > **Certificates**.
Step 2 Click **Create**.
Step 3 In the Method choose *Import AWS - KMS*.
Step 4 Select the Cloud Account and the region.
Step 5 Copy the contents of the Certificate file in the *Certificate Body*. This can include the certificate and the chain.
Step 6 Copy the AWK KMS encrypted cipher text in the *Private Key Cipher Text*. .
Step 7 Click **Save**.

AWS - Secrets Manager

Step 1 Navigate to **Mange** > **Security Policies** > **Certificates**.
Step 2 Click **Create**.
Step 3 In the Method choose *Import AWS - Secret*.
Step 4 Select the Cloud Account and the region.
Step 5 Copy the contents of the Certificate file in the *Certificate Body*. This can include the certificate and the chain.
Step 6 Provide the Secret Name where the private key is stored. The private key contents must be stored as *Other type of Secrets* > *Plain Text* in the AWS Secrets Manager.
Step 7 Click **Save**.

Azure Key Vault

Step 1 Navigate to **Mange** > **Security Policies** > **Certificates**.

Step 2 Click **Create**.
Step 3 In the Method choose *Import Azure - Key Vault Secret*.
Step 4 Select the Cloud Account and the region.
Step 5 Copy the contents of the Certificate file in the *Certificate Body*. This can include the certificate and the chain.
Step 6 Provide the Key Vault Name and the Secret Name where the private key is stored.
Step 7 Click **Save**.

GCP - Secret Manager

Step 1 Navigate to **Mange** > **Security Policies** > **Certificates**
Step 2 Click **Create**
Step 3 In the Method choose *Import GCP - Secret*
Step 4 Select the Cloud Account
Step 5 Provide the Secret Name (full path) and the Secret Version
Step 6 Copy the contents of the Certificate file in the *Certificate Body*. This can include the certificate and the chain
Step 7 Click **Save**.

Server Certificate Validation

When the gateway acts as a forward proxy, server certificate validation is automatically included in traffic processing. A designated server certificate validation **action** is not required in order to process traffic but it can improve the general security. By default, server certificate validation is not enabled and traffic going to servers that may have an invalid server certificate passes. Enable a server certificate validation action to prioritize rules for traffic that should not be allowed, or for specific traffic that should be trusted even regardless of its server certificate validations state.

Note This validation process is **only** applicable for forward proxy environments and when **decryption** is enabled.

We recommend enable server certificate validation actions primarily in the TLS decrpytion profile for general rule actions. FQDN service objects can be modified to enable validation actions if you need to override the TLS decryption selection. You can include and enable a server certificate validation in two methods:

- Server Certificate Validation in the TLS Decryption Profile
- Server Certificate Validation in the FQDN Service Object

Server Certificate Validation in the TLS Decryption Profile

When you select an action for server certificate validation within a TLS decryption profile, this action is used in all the rule sets that use this decryption profile. By default the validation action is configured to allow all

traffic regardless of whether the server certificate is valid or not, and Multicloud Defense does not generate an alert within the HTTPs logs.

Note If you enable the validation check to **Log**, locate the logs in **Investigate** > **Flow Analytics** > **HTTPS Logs**.

Use the following procedure to enable the server certificate validation in the TLS decrpytion profile:

Step 1 From the Multicloud Defense Controller, navigate to **Manage** > **Profiles** > **Decryption**.

Step 2 Select the TLS decryption profile you want add the server certificate validation to. If you do not have a profile ready, create one here. See Decryption Profile, on page 123 for more information.

Step 3 **Edit** the decryption profile.

Step 4 Under the **Profile Properties** section, expand the **Invalid Server Certificate Action** drop-down.

Step 5 Select one of the following options:

- **Deny Log** - This option automatically drops connections that do not provide a validated server certificate and logs the incident.
- **Deny No Log** - This option automatically drops connections that do not provide a validated server certificate and **does not** log the incident.
- **Allow Log** - This option allows connections that do not provide a validated server certificate to pass and logs the incident.
- **Allow No Log** - This option allows connections that do not provide a validated server certificate to pass and **does not** log the incident. This is the default action selection.

Step 6 Click **Save**.

What to do next

Ensure the TLS decryption profile is correctly associated with a forward proxy service object. See Forward Proxy Service Object (Egress / East-West), on page 102 for more information.

Once the TLS decrpytion profile is included in a service object, confirm that the rule order within the policy is ordered in a way that supports how you want traffic processed.

Server Certificate Validation in the FQDN Service Object

Invalid server certificate validation within the FQDN service object is optional. If specified it will override the behavior designated in the TLS decryption profile. If you do not specify a selection here, no additional action or override action is taken. You can use the invalid server certificate validation within the FQDN service object to block or allow traffic for a specific server that may otherwise be blocked or allowed by the TLS decryption profile.

Note that when you enable the validation check to **Log**, these logs are located in **Investigate** > **Flow Analytics** > **HTTPS Logs**.

Use the following procedure to include a server certificate validation action in a FQDN service object:

Step 1 From the Multicloud Defense Controller, navigate to **Manage** > **Security Profile** > **FQDNs**.

Step 2 Select the FQDN service object you want to modify.

Step 3 **Edit** the selected FQDN service object.

Step 4 In the list of FQDN service objects included in the ruleset, expand the **Invalid Server Certificate Action** drop-down menu and select one of the following options:

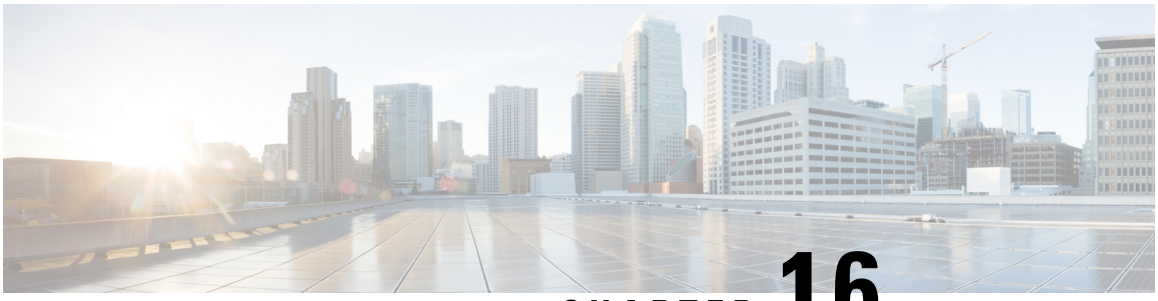
- **Deny Log** - Automatically drop connections that do not provide a validated server certificate and logs the incident.
- **Deny No Log** - Automatically drop connections that do not provide a validated server certificate and **does not** log the incident.
- **Allow Log** - Allow connections that do not provide a validated server certificate to pass and logs the incident.
- **Allow No Log** - Allow connections that do not provide a validated server certificate to pass and **does not** log the incident.

Step 5 Click **Save**.

What to do next

Ensure the FQDN service object is correctly associated with a rule or rule set. See Rule Sets and Rule Set Groups, on page 80 for more information.

Once the FQDN service object is successfully assocaited with a rule or rule set in your policy, confirm that the rule order within the policy is ordered in a way that supports how you want traffic processed.



CHAPTER 16

Certificate and Keys Tech Notes

Generate a Self-Signed Root CA

Generate a self-signed root certificate authority (CA).

```
openssl genrsa -out myca.key 2048
# password protect key: openssl genrsa -out myca.key -des3 2048
openssl req -x509 -new -key myca.key -sha384 -days 1825 -out myca.crt \
  -subj "/C=US/ST=CA/L=Santa
Clara/O=MyOrg/OU=SecurityOU/CN=rootca.myorg.com/emailAddress=rootca@myorg.com"
```

This root CA must be installed as a trusted root CA on the users (client) machines

Note Generating a self-signed certificate using **MacOS** will not generate a proper certificate that can be used for forward and reverse proxy scenarios. The certificate must have the *Is CA* option set to *True* and the certificate generated using MacOS does not. It is recommended that the self-signed certificate be generated from within the Multicloud Defense UI (Certificates > Create > Generate) or using **Linux**.

Generate a Certificate Signed by your Self-Signed Root CA

Generate a certificate signed by the above root certificate authority (CA). This certificate can be used in the applications.

```
openssl genrsa -out app1.key 2048
# password protect key: openssl genrsa -out -des3 app1.key 2048
openssl req -new -key app1.key -out app1.csr \
  -subj "/C=US/ST=CA/L=Santa
Clara/O=MyOrg/OU=AppOU/CN=app1.myorg.com/emailAddress=app1@myorg.com"
openssl x509 -req -in app1.csr -CA myca.crt -CAkey myca.key -out app1.crt -sha384\
```

```
  -days 365 -CAcreateserial -extensions SAN \
  -extfile <(printf "
[SAN]\nbasicConstraints=CA:false\nsubjectAltName=DNS:app1.myorg.com,DNS:app1-
1.myorg.com,IP:192.168.10.21,IP:192.168.10.22")
```

Generate an Intermediate CA Signed by Your Root CA

If you don't want to use the root certificate authority (CA) to sign app certs, then create an intermediate CA signed by the root CA, then sign the app certs using the intermediate CA. Append the intermediate cert to the app cert. At this point the app crt has 2 certs (as a chain).

```
openssl genrsa -out interca.key 2048
# password protect key: openssl genrsa -out -des3 interca.key 2048
openssl req -new -key interca.key -out interca.csr \
  -subj "/C=US/ST=CA/L=Santa
Clara/O=MyOrg/OU=InterSecurityOU/CN=interca1.myorg.com/emailAddress=interca1@myorg.com"
openssl x509 -req -in interca.csr -CA myca.crt -CAkey myca.key -out interca.crt - sha384 \
  -days 365 -CAcreateserial -extensions SAN \
  -extfile <(printf "[SAN]\nbasicConstraints=CA:true")
```

App Certificate signed using the Intermediate CA

```
openssl genrsa -out app1.key 2048
# password protect key: openssl genrsa -out -des3 app1.key 2048
openssl req -new -key app1.key -out app1.csr \
  -subj "/C=US/ST=CA/L=Santa
Clara/O=MyOrg/OU=AppOU/CN=app1.myorg.com/emailAddress=app1@myorg.com"
openssl x509 -req -in app1.csr -CA interca.crt -CAkey interca.key -out app1.crt - sha384 \
  -days 365 -CAcreateserial -extensions SAN \
  -extfile <(printf "
[SAN]\nbasicConstraints=CA:false\nsubjectAltName=DNS:app1.myorg.com,DNS:app1-
1.myorg.com,IP:192.168.10.21,IP:192.168.10.22")
```

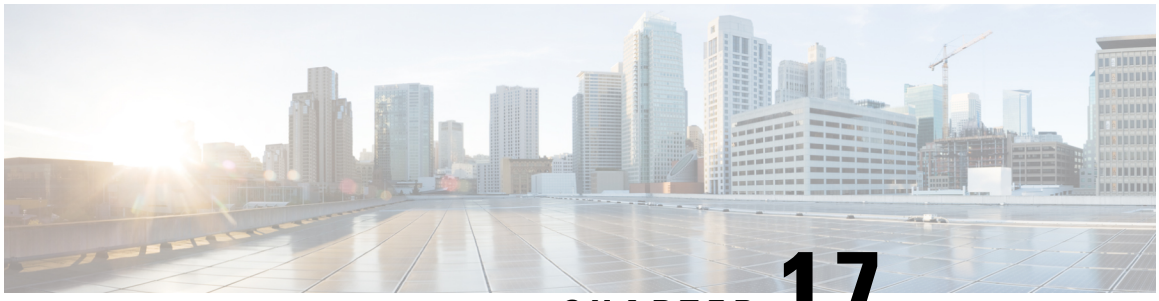
Append files app1.crt and interca.crt to make a combined certificate and use the combined certificate in your application. The root CA must be installed as a trusted root CA on your client machines.

Install Root CA as Trusted CA on the Hosts

OS	Command
Ubuntu	Copy crt file to `/usr/local/share/ca-certificates`, Run command `sudo update-ca- certificates`.
CentOS	Copy crt file to `/etc/pki/ca-trust/source/anchors`, Run command `sudo update-ca- trust extract`.
Windows	Double click the file and add the cert to Trusted Root, or Run command `certutil -addstore "Root" <crt-file>`.

PART VII

Traffic Discovery and Visiblilty



CHAPTER 17

Types of Traffic

When enabled, traffic logs are generated whenever traffic hits a rule. These log interactions record information about incoming and outgoing traffic, including the source and destination IP addresses, port numbers, and protocols used. Logs can be incredibly useful to audit the network: monitor activity, investigate potential security breaches, or simply keep an eye on what is happening with your firewall. Traffic visibility can be enabled at any time but we strongly recommend enabling traffic immediately after onboarding a cloud service provider account and assigning a gateway policy.

Enabling traffic visibility is a different process for every cloud account type, but typically you will need to identify account characteristics such as your cloud account's region, VPC/VNet you want to monitor, network security groups, and a cloud storage account for logs.

If you did not onboard an account with the Easy Setup wizard or if you did not enable traffic visibliilty from the Enable Traffic Visibility we strongly recommend enabling the following logs:

- NSG Flow Logs
- VPC Flow Logs
- DNS Logs
- Route53 Query Logging

- Enable DNS Logs, on page 115
- Enable VPC Flow Logs, on page 117

Enable DNS Logs

AWS: Enable DNS Logs

If you provided a S3 bucket during the stack creation from the CloudFormation template in the previous section, a S3 bucket is created by the template that acts as the destination for the route53 Query Logs. The VPCs that are monitored for the DNS query logs must be added manually.

Step 1 In AWS Console go to the Route53Query Logging .

Step 2 Select the **Query Logger** created by the template. Locate the logger with the prefix name provided in the template.

Step 3 Select and all the VPCs for which you want to get the traffic insights and clikc **Add**.

a. Under the " VPCs that queries are logged for" section, click **Log queries for VPCs** or **Add VPC**.

b. Select all the VPCs and click **Choose**.

GCP: Enable DNS Logs

To enable GCP DNS query logs, follow the below steps.

Step 1 Navigate to VPC network in GCP console.

Step 2 Open Google cloud shell and execute this command:

```
gcloud dns policies create POLICY_NAME --networks=NETWORK --enable-logging
```

Step 3 Navigate to **Cloud Storage** section and create a storage bucket. You can leave everything as default when creating storage bucket.

Note *Both DNS and VPC logs can share the same cloud storage bucket.*

Step 4 Navigate to **Logs Route** section.

Step 5 Click on **Create Sink**.

Step 6 Provide a sink name.

Step 7 Select "Cloud Storage bucket" for sink service.

Step 8 Select the cloud storage bucket that was created above.

Step 9 In "Choose logs to include in sink" section, put in this string: `resource.type="dns_query"`.

Below steps are the same as mentioned in VPC flow log for GCP. If you are sharing cloud storage bucket, you only need to perform below steps once.

Step 10 Click **Create Sink**.

Step 11 Navigate to **IAM** > **Roles**.

Step 12 Create a custom role with this permission: **storage.buckets.list**.

Step 13 Create another custom role with following permission:

storage.buckets.get storage.objects.get storage.objects.list.

Step 14 Add both custom role to the service account created for Multicloud Defense Controller. When adding the second custom role, put this condition:

```
(resource.type == "storage.googleapis.com/Bucket" || resource.type ==
 "storage.googleapis.com/Object") &&
resource.name.startsWith('projects/_/buckets/<cloud storage name>')
```

Step 15 Navigate to **Pub/Subs**.

Step 16 Click on **Create Topic**.

Step 17 Provide a Topic name and click **create**.

Step 18 Click on **Subscriptions**. You will find that there is a subscription created for the topic that was just created.

Step 19 Edit the subscription.

Step 20 Change Delivery type as **Push**.

Step 21 Once **Push** is selected, enter in the endpoint URL: `https://prod1-webhook.vtxsecurityservices.com:8093/webhook/<tenant name>/gcp/cloudstorage`. Tenant name is assigned by Multicloud Defense. To view tenant name, navigate to Multicloud Defense Controller and click on your username.

Step 22 Click **Update**.

Step 23 Create a cloud storage notification by opening a Google cloud shell and execute this command: `gsutil notification create -t <TOPIC_NAME\> -f json gs://<BUCKET_NAME>`.

Azure: DNS Logs

Azure currently does not expose DNS log queries. Multicloud Defense Controller cannot enable logs for this cloud service provider.

Enable VPC Flow Logs

AWS: Enable VPC Flow Logs

If you provided a S3 bucket during the stack creation from the CloudFormation template in the previous section, a S3 bucket is created by the template that acts as the destination for the VPC flow logs. Flow logs must be enabled for each of the VPCs.

To enable AWS VPC flow logs, follow the below steps:

Step 1 In the AWS Console, go to the VPCs section.

Step 2 Select the VPC and select the **Flow Logs** tab for that VPC.

Step 3 Select **All** as the filter.

Step 4 Select **Send to an Amazon S3 bucket** as the destination.

Step 5 Provide the S3 bucket ARN copied from the tutputs of the CloudFormation template stack.

Step 6 Choose **Custom Format** as the log record format.

Step 7 Select all the fields from the log format dropdown.

Step 8 Click **Create Flow Log**.

GCP: Enable VPC Flow Logs

To enable GCP VPC flow logs, follow the below steps.

Step 1 In the GCP console, navigate to **VPC network**

Step 2 to enable the VPC flow log, select the **subnet**.

Step 3 Ensure that flow logs is turned **On**. If it is off, click the **Edit**option and turn flow logs on.

Step 4 Turn on flow log on all subnets where you want to enable flow log.

Step 5 Navigate to **Cloud Storage** section and create a storage bucket. You can leave everything as default when creating storage bucket.

Note Both DNS and VPC logs can share the same cloud storage bucket.

Step 6 Navigate to the **Logs Route** section.

Step 7 Click **Create Sink**.

Step 8 Enter a name for the sink.

Step 9 Select **Cloud Storage bucket** for sink service.

Step 10 Select the cloud storage bucket that was created above.

Step 11 In the **Choose logs to include in sink** section, enter this string: `logName:(projects/<project-id>/logs/compute.googleapis.com%2Fvpc_flows)`

If you are sharing cloud storage bucket, you only need to perform the remaning steps of this procedure once.

Step 12 Click **Create Sink**.

Step 13 Navigate to **IAM** > **Roles**.

Step 14 Create one custom role with this permission: `storage.buckets.list`.

Step 15 Create one custom role with following permission: `storage.buckets.get storage.objects.get storage.objects.list`.

Step 16 Add both custom roles to the service account created for Multicloud Defense Controller. When adding the second custom role, enter the following condition:

```
(resource.type == "storage.googleapis.com/Bucket" || resource.type ==
"storage.googleapis.com/Object") && resource.name.startsWith('projects/_/buckets/<cloud
storage name>')
```

Step 17 Navigate to **Pub/Subs**.

Step 18 Click **Create Topic**.

Step 19 Provide a **Topic** name and click **Create**.

Step 20 Click **Subscriptions**. A subscription is created for the topic created in step 18.

Step 21 **Edit** the subscription.

Step 22 Change the **Delivery** type to **Push**.

Step 23 Enter this as the endpoint URL:`https://prod1- webhook.vtxsecurityservices.com:8093/webhook/<tenant name>/gcp/cloudstorage`.

Multicloud Defense autmoatically assigns the tenant name. To see tenant name, navigate to Multicloud Defense Controller and click on your username.

Step 24 Click **Update**.

Step 25 Open a Google cloud shell and execute the following command: `gsutil notification create -t <TOPIC_NAME> -f json gs://<BUCKET_NAME>`.

Azure: Enable NSG Flow Logs

To enable Azure VPC flow logs, follow the below steps.

Step 1 Go to the **Resource Groups** section in Azure portal.

Step 2 Click the **Create** button.

Step 3 Select the subscription and provide a name for this new resource group.

Step 4 Select a **Region**. (example: (US) East US).

Step 5 Click the **Review + create** button.

Step 6 Go to the **storage accounts** section and click the **Create** button.

Step 7 Select the **Subscription** and **Resource** group that was just created.

Step 8 Select the same **region** as the resource group.

Step 9 Provide a name for the storage account.

Note that **Redundancy cannot** be locally-redundant storage(LRS)

Step 10 Click the **Review + create** button. This creates a storage account where NSG flow logs are stored.

Step 11 Go to the **Subscription** section and find the subscription that was recently created.

Step 12 Navigate to **Resource Providers**.

Step 13 Ensure that the `microsoft.insights` and `Microsoft.EventGrid` providers are registered. If they are not registered, click the **Register** button.

Step 14 Go to the **Network Watcher** section.

Step 15 Click **Add** and add the regions that you want NSG flow logs to be enabled for.

Step 16 Go to **Network Watcher** > **NSG flow logs**.

Step 17 Create flow logs for the NSG where you want to enable NSG flow log. Provide the storage account created above. Set the **Retention days** as 30.

Step 18 Navigate to the storage account created and click on **Events**.

Step 19 Click **Event Subscription**.

Step 20 Provide a name for this event subscription.

Step 21 Select the resource group that was created above.

Step 22 Provide a **System Topic Name**.

Step 23 For **Filter to Event Types**, the default value is **Blob Created** and **Blob Deleted**.

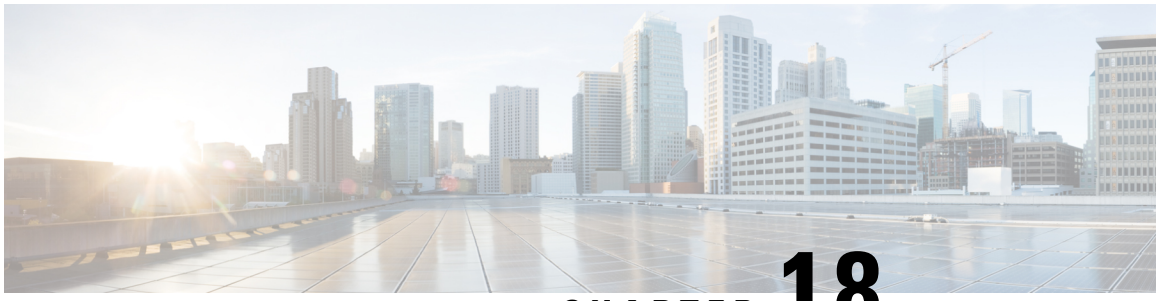
Step 24 For **Endpoint Type**, select **Web Hook**.

Step 25 Click the **Select an endpoint** link.

The Subscriber Endpoint is `https://prod1-webhook.vtxsecurityservices.com:8093/webhook/<tenant_name>/azure`. Tenant name is assigned by Multicloud Defense. You can find tenant name by clicking on the username in Multicloud Defense Controller.

PART VIII

Security Profiles



CHAPTER 18

Security Profiles

Decryption Profile

A decryption profile is used by the Multicloud Defense Gateway in a reverse proxy **or** forward proxy scenario. When a connection is proxied, the front-end session is terminated on the gateway and a new back-end session is established to the server. The intention of this termination is to decrypt and inspect the traffic to protect against malicious activity. In order to decrypt encrypted traffic, a decryption profile is necessary.

Create a Decryption Profile

Use the following procedure to create a decryption profile.

Step 1 Navigate to **Manage** > **Profiles** > **Decryption**.

Step 2 Click **Create**.

Step 3 Specify a **Profile Name** and a **Description**.

Step 4 For **Certificate Method** choose **Select Existing**.

Step 5 For **Certificate** choose the desired certificate.

Step 6 For **Min TLS Version** choose the lowest TLS version that is accepted by the decryption profile. The default is TLS 1.0.

Step 7 If using non-default (non-PFS) cipher suites, select the set of desired cipher suites from the Diffie- Hellman or PKCS (RSA) menus.

Step 8 Click **Save**.

What to do next

- View a Profile Details, on page 145
- Add a Gateway Association to a Profile, on page 146

TLS Versions in your Decryption Profile

The Multicloud Defense Gateway supports all TLS versions (TLS 1.3, TLS 1.2, TLS 1.1, TLS 1.0). Users can specify a minimum TLS version to use and Multicloud Defense Gateway will negotiate a TLS version that is equal to or higher than the specified minimum TLS version. The Multicloud Defense Gateway will always use the highest TLS version possible during the TLS negotiation. In the case where the Multicloud Defense Gateway cannot negotiate a version that meets the minimum TLS version specified, the Multicloud Defense Gateway will drop the session and logging a `TLS_ERROR` event.

Note Only a single minimum TLS version can be applied to a gateway. A consistent minimum TLS version must be used across all decryption profiles referenced by all service objects that are used within a policy ruleset or policy ruleset group. If different minimum TLS versions are specified, the minimum TLS version that will be applied cannot be predetermined.

Cipher Suites

The Multicloud Defense Gateway supports a set of default and user-selectable cipher suites. The default set are PFS cipher suites that are always selected. The user-selectable set are Diffie-Hellman and PKCS (RSA) cipher suites that can be selected by the user. The combined set of cipher suites (default and user-selected) are used by the gateway for establishing a secure front-end encrypted session. The client will send an ordered list of preferred cipher suites. The gateway will respond with a cipher suite chosen from the ordered set submitted by the client and the set available by the gateway. If the client allows the server to define the order, then the cpher suite chosen is from the ordered set available by the gateway and the set submitted by the client.

The following is an ordered list of cipher suites supported by the gateway and available in a decryption profile:

Category	Cipher Suite	Key Exchange	Cipher	Hash	Default
PFS	ECDHE-RSA-AES256-GCM-SHA384	ECDHE-RSA	AES256-GCM	SHA384	☐
PFS	ECDHE-RSA-AES256-CBC-SHA384	ECDHE-RSA	AES256-CBC	SHA384	☐
Diffie-Hellman	DH-RSA-AES256-GCM-SHA384	DH-RSA	AES256-GCM	SHA384	
PFS	DHE-RSA-AES256-GCM-SHA384	DHE-RSA	AES256-GCM	SHA384	☐
PFS	DHE-RSA-AES256-CBC-SHA256	DHE-RSA	AES256-CBC	SHA384	☐
PFS	DHE-RSA-AES256-CBC-SHA	DHE-RSA	AES256-CBC	SHA	☐

Category	Cipher Suite	Key Exchange	Cipher	Hash	Default
Diffie-Hellman	DH-RSA-AES256-SHA256	DH-RSA	AES256-CBC	SHA256	
Diffie-Hellman	DH-RSA-AES256-SHA	DH-RSA	AES256-CBC	SHA160	
PKCS (RSA)	AES256-GCM-SHA384	PKCS-RSA	AES256-GCM	SHA384	
PKCS (RSA)	AES256-SHA256	PKCS-RSA	AES256-CBC	SHA256	
PKCS (RSA)	AES256-SHA	PKCS-RSA	AES256-CBC	SHA160	
PFS	ECDHE-RSA-AES128-GCM-SHA256	ECDHE-RSA	AES128-GCM	SHA256	□
PFS	ECDHE-RSA-AES128-CBC-SHA256	ECDHE-RSA	AES128-CBC	SHA256	□
Diffie-Hellman	DH-RSA-AES128-GCM-SHA256	DH-RSA	AES128-GCM	SHA256	
PFS	DHE-RSA-AES128-GCM-SHA256	DHE-RSA	AES128-GCM	SHA256	□
PFS	DHE-RSA-AES128-CBC-SHA256	DHE-RSA	AES128-CBC	SHA256	□
Diffie-Hellman	DH-RSA-AES128-SHA256	DH-RSA	AES128-CBC	SHA256	
Diffie-Hellman	DH-RSA-AES128-SHA	DH-RSA	AES128-CBC	SHA160	
PKCS (RSA)	AES128-GCM-SHA256	PKCS-RSA	AES128-GCM	SHA256	
PKCS (RSA)	AES128-SHA256	PKCS-RSA	AES128-CBC	SHA256	
PKCS (RSA)	AES128-SHA	PKCS-RSA	AES128-CBC	SHA160	
PFS	ECDHE-RSA-DES-CBC3-SHA	ECDHE-RSA	DES-CBC3	SHA	□
PFS	ECDHE-RSA-RC4-SHA	ECDHE-RSA	RC4	SHA	□
PKCS (RSA)	RC4-SHA	PKCS-RSA	RC4	SHA160	
PKCS (RSA)	RC4-MD5	PKCS-RSA	RC4	SHA160	

Network Intrusion (IDS/IPS) Profile

Network intrusion profiles are a collect of Intrusion Detection and Protection (IDS/IPS) rules that can be used to evaluate transactions to ensure the traffic is not malicious.

Multicloud Defense supports the following IDS/IPS rule sets:

Table 3: Multicloud Defense supports the following IDS/IPS Rule Sets

Rule Sets	Description
Talos Rules	The Talos rules are a premium set of rules from Cisco based on intelligence gathered from real-world investigations, penetration tests and research that provide an advanced level of protection for applications and frameworks.

Rule Sets	Description
Custom Rules	Custom rules are a particular set of rules written by customers that provide a specialized level of protection for custom applications.

Create an IPS/IDS Profile

Use the following procedure to create and add an IPS/IDS profile to a ruleset:

Step 1 Navigate to **Manage** > **Profiles** > **IPS/IDS**.

Step 2 Click **Create Intrusion Profile**.

Step 3 Enter a unique **Profile Name**.

Step 4 (Optional) Enter a **Description**. This may help differntiate between other profiles with a similar name.

Step 5 Specify the **Action** with one of the following options:

- **Rule Default** - Allow or Deny the requests based on the action specified in each triggered Rule and log an Event.
- **Allow Log** - Allow the requests and log an event.
- **Allow No Log** - Allow the requests and do not log an event.
- **Deny Log** - Deny the requests and log an event.
- **Deny No Log** - Deny the requests and do not log an event.

Step 6 Check for whether to generate a Threat PCAP file if the IDS/IPS Profile detects malicious activity.

Step 7 Specify the **Rule Set**. Note that at least one ruleset from a rules library (Talos, Custom) is required to be specified in the IDS/IPS profile. If Talos rules and custom rulesets are used, at least one of the two must be enabled. If the desire is to disable the entire IDS/IPS Profile, remove the IDS/IPS Profile from any policy ruleset so the IDS/IPS profile will not be evaluated.

epcify one of the following **Talos Rules** desginations:

- **Disabled** - Specify whether to disable the use of Talos rules.
- **Manual** - Specify the Talos rule's version.
- **Automatic** - Specify the number of days from publish date to delay automatic update to the latest Talos rule's version.

Step 8 Add specific **Custom Rulesets** to the IPS/IDS Profile.

Step 9 Specify the **Rules Suppression** for rules that can be suppressed for a specific IP or a list of CIDRs and click **Add**.

Step 10 Locate and select the **Advanced Settings** tab and under "Rule Suppression", click **Add**.

a) For **Rule ID List**, provide a comma-separated list of rule IDs. For **Source IP/CIDR List**, provide a comma-separated list of IPs or CIDRs.

b) For **Action**, provide a selection, but this selection does not apply since a rule being suppressed will not be evaluated.

Step 11 Select the **Event Filtering Type**; this reduces the number of security events that are generated when the IPS/IDS profile is triggered, and the event filtering can be configured to one of the following options:

- **Rate** - the generated events are rate limited based on the specified **Number of Events** triggered over a Timeevaluation interval (in seconds).
- **Type** - the generated events are sampled based on the specified **Number of Events**.

Step 12 Under **Rule Event Filtering**, click **Add**.

Step 13 For **Rule ID List**, specify a comma-separated list of rule IDs.

Step 14 Specify the rule event filtering **Type** with one of the following options:

- **Rate** - Specify the **Number of Events** and the **Time** evaluation interval (in seconds).
- **Sample** - Specify the **Number of Event**s.

What to do next

- View a Profile Details, on page 145
- Add a Gateway Association to a Profile, on page 146

Data Loss Prevention (DLP) Profile

The DLP (Data Loss Prevention) profile provides Multicloud Defense customers with the ability to specify policy rules to detect and take action upon finding exfiltration patterns in the data when the Multicloud Defense solution is deployed in the forward proxy (egress) mode.

Multicloud Defense allows customers to specify common pre-packaged data patterns such as Social Security Numbers (SSN), AWS secrets, credit card numbers etc., in addition to custom PCRE based regular expression patterns. This makes it easy to enforce protections for PCI, PII, and PHI data to meet compliance requirements. This feature is integrated with the existing Multicloud Defense feature set requiring no separate DLP services.

Create a Data Loss Prevention Profile

Step 1 Navigate to **Manage** > **Profiles** > **Network Threats**.

Step 2 Click **Create Intrusion Profile**.

Step 3 Select **Data Loss Prevention**.

Step 4 Provide a unique **Name** and enter a description for the profile.

Step 5 Enter the **DLP FIlter List** in the table.

Step 6 Click **Add** to insert more rows as needed.

Step 7 Provide a **Description** for the filter.

Step 8 Choose a predefined static pattern (e.g CVE Number) from the dropdown list or provide a custom Regular expression.

Step 9 Provide a **count** to define the number of times the pattern must be seen in the traffic.

Step 10 Select an **Action** to take if the pattern matches the count number of times.

Note There are cases where the pre-defined pattern for AWS Access Key and AWS Secret Key doesn't match in DLP inspection due to pattern being more restrictive. Use the following relaxed custom pattern in DLP profile to detect AWS Access Key and AWS Secret Key. Be aware that this could generate false positives log events.

```
AWS Access Key: (?<![A-Z0-9])[A-Z0-9]{20}(?![A-Z0-9])

AWS Secret Key: (?<![AZa-z0-9/+=])[A-Za-z0-9/+=]{40}(?![A-Za-z0-9/+=])
```

What to do next

- View a Profile Details, on page 145
- Add a Gateway Association to a Profile, on page 146

Anti-Malware Profile

An anti-malware profile enables anti-malware protection using the Talos ClamAV virus detection engine. ClamAV® is an antivirus engine for detecting trojans, viruses, malware and other malicious threats.

The following steps will guide you creating an anti-malware profile and associate it with a policy rule.

Create an Anti-Malware Profile

Step 1 Navigate to **Manage** > **Profiles** > **Network Threats**.

Step 2 Select **Anti-malware**.

Step 3 Provide a unique **Name** and enter a description.

Step 4 Select one of the following modes for Talos ruleset:

- **Manual Mode** - select the Talos Ruleset Version from dropdown. The selected ruleset version is used by the Multicloud Defense datapath engine on all Gateways which use this profile and is not automatically updated to newer ruleset versions.
- Automatic Mode - select how many days to delay the deployment by, after the ruleset version is published by Multicloud Defense. New rulesets are published daily by Multicloud Defense and the gateways using this profile are automatically updated to the latest ruleset version which is **N** days or older, where **N** is the "delay by days" argument selected from the dropdown. For example, if you select to delay the deployment by 5 days on Jan 10, 2024, the Multicloud Defense Controller will select a ruleset version which was published on Jan 5th or before. Note that Multicloud Defense may not publish on some days if our internal testing with that ruleset version fails for some reason.

Step 5 Select the desired **Action** to take when a match for a virus signature is found.

What to do next

- View a Profile Details, on page 145
- Add a Gateway Association to a Profile, on page 146

Web Application Firewall (WAF) Profile

Web protection profiles are a collection of Web Application Firewall (WAF) rules that can be used to evaluate web-based transactions to ensure the traffic is not malicious.

Multicloud Defense supports the following WAF rulesets:

Table 4: Multicloud Defense supports the following WAF Rulesets

Rulesets	Description
Core Rules	The Core rules are a standard set of rules from ModSecurity CRS (Core Rule Set) that provide a base level of protection for any web application.
Trustwave Rules	The Trustwave rules are a premium set of rules from ModSecurity based on intelligence gathered from real-world investigations, penetration tests and research that provide an advanced level of protection for specific web applications and frameworks.
Custom Rules	The Custom rules are a particular set of rules written by customers that provide a specialized level of protection for custom web applications.

Create WAF Profile

Use the following procedure to create a WAF profile.

Note If core Rulesets are specified, the core rules cannot be disabled. In order to disable the core rules, remove all core rulesets from the WAF profile so they will not be evaluated.

Step 1 Navigate to **Manage** > **Profiles** > **WAF**.

Step 2 Click **Create**.

Step 3 Specify the following general settings:

a) Enter a unique **Profile Name**.

b) (Optional) Enter a **Description**. This may help differentiate between profiles with a similar name.

c) Specify the action:

- **Rule Default** - Allow or deny the requests based on the action specified in each triggered rule and log an event.
- **Allow Log** - Allow the requests and log an event.

- **Deny Log** - Deny the requests and log an event.

d) Specify whether to generate a Threat HAR file if the WAF profile detects malicious activity. The gateway should have a Pcap profile attached, for this to work.
e) Specify whether to generate a HTTP Request HAR file if the WAF profile detects malicious activity.
f) In the **RULE SETS**section, in the vertical tab located to the left, click **Core Rules**. You must specify at least one ruleset from a rules library (Core, Trustwave, Custom):
   - Specify the following:
     - **Manual** - Specify the core rules version to use.
     - **Automatic** - Specify the numbers of days from publish date to delay automatic update to the latest core rules version.
   - Identify the rules you want to add to the profile and click **Add to Profile**. The selections appear in the table located to the right.
g) In the vertical tab located to the left, click **Trustwave Rules**.
   - Specify the following:
     - **Disabled** - Specify whether to disable the use of Trustwave rules.
     - **Manual** - Specify the Trustwave rules version to use.
     - **Automatic** - Specify the number of days from publish date to delay automatic update to the latest Trustwave rules version.
   - Identify the rules you want to add to the profile and click **Add to Profile**. The selections appear in the **Profile Selections** table located to the right.
h) In the vertical tab located to the left, click **Custom Rules**.
   - Specify one of the following options:
     - **Disabled** - Specify whether to disable the use of custom rules.
     - **Manual** - Specify the custom rules version to use.
     - **Automatic** - Specify the number of days from publish date to delay automatic update to the latest custom rules version.
   - Identify the rules you want to add to the profile and click **Add to Profile**. The selections appear in the **Profile Selections**table located to the right.

Step 4 Scroll to the top of the window and click the **Advanced Settings** tab:
a) Under "Rule Suppression", click **Add** to add one or more rows for rules. Rules can be suppressed for a specific IP or a list of CIDRs:
   - For **Source IP/CIDR List**, provide a comma-separated list of IPs or CIDRs.
   - For **Rule ID List**, provide a comma-separated list of rule IDs.
b) Under "Event Filtering" provide the following information:

- **Type - Rate** or **Sample**
- **Number of Events**
- **Time (Seconds)**

c) Under "Rule Event Filtering" click **Add** to add one or more rows for rules. For every new row you create, enter a valid **Rule ID List**, **Number of Events**, **Time (Sec)**, and choose either Type or Sample as the **Type**.
d) Under "Core Rule Set", select a value for both the **Request Anomaly** and **Response Anomaly**. Note that using a value less than 3 for the "Request Anomaly" results in a huge volume of alerts.
e) Select the **Paranoia Level**. Your options range from 1–4.

Step 5 Click **Save**.

What to do next

- View a Profile Details, on page 145
- Add a Gateway Association to a Profile, on page 146

Event Filtering

To reduce the number of security events that are generated when the WAF Profile is triggered, the Event Filtering under **Advanced Settings** can be configured to rate limit or sample the events. The configuration does not alter the detection or protection behavior.

When specifying Type as **Rate**, the generated events are rate limited based on the specified *Number of Events* triggered over a *Time* evaluation interval (in seconds). For example, if *Number of Events* is specified as 50 and *Time* is specified as 5 seconds, only 10 events per second will be generated.

When specifying Type as **Sample**, the generated events are sampled based on the specified *Number of Events*. For example, if *Number of Events* is specified as 10, only 1 event will be generated for every 10 events triggered.

Profile Event Filtering

Profile Event Filtering applies to all rules that are configured in the WAF Profile:

- Specify the Type as **Rate** or **Sample**:
  - **Rate**- Specify the *Number of Events* and the *Time* evaluation interval (in seconds).
  - **Sample**- Specify the *Number of Events*.

Rule Event Filtering

To reduce the number of security events that are generated when the WAF profile is triggered, event filtering can be configured to rate limit or sample the events. The configuration does not alter the detection or protection behavior.

Rule event filtering applies to specific rules that are configured in the WAF profile.

Step 1 Click **Add** under Rule Event Filtering.
Step 2 For **Rule ID List**, specify a comma-separated list of **Rule IDs**.

Step 3 Specify Type as **Rate** or **Sample**.

- **Rate**- Specify the **Number of Events** and the **Time** evaluation interval (in seconds).
- **Sample**- Specify the **Number of Events**.

What to do next

Add or Edit a Forward Proxy Rule in a Rule Set

Create L7 DoS Profile

Multicloud Defense Gateways provide the ability to monitor, detect, and remediate application layer attacks by continuously monitoring the client requests to a backend web server. Layer 7 DoS attacks are targeted at depleting web server resources, affecting service availability by sending many HTTP requests. This feature is enabled when the gateways are enabled to proxy inbound connections to a backend web service to maintain availability of web based applications. Enabling this feature also allows the gateways to provide additional security for cases where a frontend load balancer may not support, or, may not be optimized to detect and remediate against application DoS attacks.

This feature can also be used to provide DoS protection against backend web servers hosting API services.

Step 1 Navigate to **Manage** > **Profiles**.

Step 2 Select **Layer 7 DOS**.

Step 3 Provide a unique **Profile Name**.

Step 4 (Optional) Enter a **Description**. This may help differentiate between other profiles that may have similar names.

Step 5 Add **Request Rate Limits**.

Limiting excessive requests to a resource is based on the following parameters. The values for these parameters should be based on measuring and understanding the traffic patterns for your web services to be protected by the Layer 7 DoS option.

Table 5: Parameters

Parameter	Description
URI	A relative URI used to indicate the path to limit requests for a resource. For example, if you intend to monitor and protect your service resource at https://www.example.com/login.html, you would enter /login.html as the URI parameter in the **Request Rate Limits** table.

Parameter	Description
HTTP Methods	HTTP methods can be specified per-resource URI to control which HTTP methods in the client requests are rate limited and which ones are not. You can select multiple methods from the drop down for each row in the table. An empty HTTP method list means that method is ignored and the rate applies to all calls to the resource. **Note** The rate is applied for each resource; therefore, multiple methods share the rate limit specified in the Request Rate in that row. For example, if the rate is 3 requests for every second, and GET, POST and PUT are specified in the HTTP Methods, and 2 GETs and 1 POST happen to that URI from a single client IP in the same second, a PUT will NOT be allowed in that same second.
Request Rate	The number of requests for every second. It determines the rate at which a single client can send requests to the URI resource mentioned in the URI part of the rule.
Burst Size	Specifies the maximum number of simultaneous requests that a client can send to the URI resource mentioned in the URI part of the rule. Any requests beyond this threshold, arriving at the proxy at the same time, will not be sent to the backend server.

Step 6 Click **Save** when completed. The order of the rules is important based on the URI as the rules are checked from the top down and applied on first match. If the URI added higher in the list includes a resource path that includes resources in the rules below it, the first rule matched will be applied.

What to do next

- View a Profile Details, on page 145
- Add the L7 DoS profile to a **service object**. Then, Add a Gateway Association to a Profile, on page 146. Note that if you update a rule set, changes may not be deployed immediately.

URL (Uniform Resource Locator) Filter Profile

A URL filtering profile evaluates the URL of an HTTP request and applies an action to either allow or deny the traffic. In order to evaluate the URL, the traffic must be processed by a **Forward Proxy** rule. The set of URLs in the profile can be specified as strings representing the full path or as strings representing a Perl Compatible Regular Expression (PCRE). If only domain filtering is required, it is best to use an FQDN filtering profile. An FQDN filtering profile can also be used in conjunction with URL filtering, where the domain is evaluated using the FQDN filtering profile and the URL is evaluated using the URL filtering profile.

The URL filtering profile can use a set of pre-defined categories. To view more information on categories, please see FQDN / URL Filtering Categories, on page 149.

Note The URL filtering is organized as a table containing user-specified rows (URLs and Categories) along with two default rows (**Uncategorized** and **ANY**). Categories and URLs can be combined within each row if desired.

The limits for each URL filtering profile are as follows:

- Maximum user-specified rows: 254 (Standalone or a group of standalones)
- Maximum Categories and URLs per row: 60
- Maximum URL character length: 2048

When specifying a multi-level domain (e.g., `www.example.com`), it's important to escape the `.` character (e.g., `www\.example\.com`) otherwise it will be treated as a wildcard for any single character

Uncategorized

- The penultimate row in a URL filtering profile, which is represented as **Uncategorized**.
- Specifies the policy action to take for URLs that do not match the user-specified URLS or do not have a category.
- If a standalone profile is used in a group profile and the group profile is applied to a policy ruleset, the **Uncategorized** row will be taken from the group profile. The **Uncategorized** row of a standalone profile is only applicable if the standalone profile is directly applied to a policy ruleset.

Default (ANY)

- The final row in a URL filtering profile, which is represented as **ANY**.
- Specifies the policy action to take for URLs that do not match the user-specified URLs or categories, or are not uncategorized.
- If a standalone profile is used in a group profile and the group profile is applied to a policy ruleset, the **ANY** row will be taken from the group profile. The **ANY** row of a standalone profile is only applicable if the standalone profile is directly applied to a policy ruleset.

Create the URL Filtering Profile

Use the following procedure to create a standalone URL filtering profile:

Step 1 Navigate to **Manage** > **Profiles** > **URL Filtering**.

Step 2 Click **Create**.

Step 3 Provide a unique **Name**.

Step 4 (Optional) Enter a **Description**. This may help differenatiate between other profiles with similar names.

Step 5 Click **Add** to create a new row.

Step 6 Specify individual URLs (e.g., https://www.google.com):

- Each URL is specified as a PCRE (Perl Compatible Regular Expression).

- Each URL must be specified as a full path.
- Consider escaping the decimal "." character else it will be treated as a single character wildcard.

Step 7 Specify **Categories** (e.g., Gambling, Sports, Social Networking).

Step 8 Specify the HTTP methods to which the policy is applied.

Step 9 Select on of the following as a subset of methods:

- Delete
- Get
- Head
- Options
- Patch
- Post
- Put

Step 10 Specify **All** for all methods.

Step 11 Specify the policy **Action** for the user-specified URLs/Categories, Uncategorized and ANY rows:

- **Allow Log** - Allow the requests and log an event.
- **Allow No Log** - Allow the requests and do not log an event.
- **Deny Log** - Deny the requests and log an event.
- **Deny No Log** - Deny the requests and do not log an event.

Step 12 Specify the **Return Status Code**.

Step 13 Specify an integer value **greater than or equal to 100 and less than 600**. The value represents the HTTP status that will be returned to the client making the request. A common return code is **503**.

Step 14 Click **Save**.

What to do next

- View a Profile Details, on page 145
- Add a Gateway Association to a Profile, on page 146

Fully Qualified Domain Name Filter Profile

A Fully Qualified Domain Name (FQDN) filter profile evaluates the FQDN associated with traffic and applies an action to either allow or deny the traffic. In order to evaluate the FQDN, traffic must be TLS encrypted and contain an FQDN in the SNI field of a TLS hello header. The FQDN can be evaluated for traffic that is processed by either a **Forwarding** or **Forward Proxy** rule. The set of FQDNs in the profile can be specified as strings representing the full domain or as strings represented by a Perl Compatible Regular Expression

(PCRE). If only domain allowlisting is required, it is best to use an FQDN filtering profile. An FQDN filtering profile can also be used in conjunction with a URL filtering profile, where the domain is evaluated using the FQDN filtering profile and the URL is evaluated using the URL filtering profile.

The FQDN filtering profile can also use a set of pre-defined categories. To view more information on categories, see FQDN / URL Filtering Categories, on page 149.

Note The FQDN filtering profile is organized as a table containing user-specified rows (FQDNs and categories) along with two default rows (Uncategorized and ANY). Categories and FQDNs can be combined within each row if desired.

The limits for each FQDN filter profile are as follows:

- Maximum user-specified rows: 254 (standalone or group of standalones)
- Maximum categories and FQDNs per row: 60
- Maximum FQDN character length: 255

When specifying a multi-level domain (e.g., 'www.example.com'), it's important to escape the `.` character (e.g.,`www\.example\.com`) otherwise it will be treated as a wildcard for any single character.

Standalone vs. Group

A FQDN filter profile can be specified as standalone or group.

A standalone FQDN filter profile contains FQDNs and categories. The profile will be applied directly to a set of one or more policy rulesets or associated with a FQDN group profile.

A FQDN filter group profile contains an ordered list of standalone profiles that can be defined for different purposes and combined together into a group profile. The group profile can be applied directly to a set of one or more policy rulesets. Each team can create and manage specific standalone profiles. These standalone profiles can be combined together into a group profile to create hierarchies or different combinations based on the use case. An example combination could be a global FQDN list that would apply to everything, a CSP-specific list that would apply to each different CSP, and an application-specific list that would apply to each different application.

Uncategorized

- The second-to-last row in an FQDN filter profile which is represented as **Uncategorized**.
- Specifies the policy action to take for FQDNs that do not match the user-specified FQDNs or do not have a category.
- If a standalone profile is used in a group profile and the group profile is applied to a policy ruleset, the **Uncategorized** row will be taken from the group profile. The **Uncategorized** row of a standalone profile is only applicable if the standalone profile is directly applied to a policy ruleset.

Default (ANY)

- The final row in an FQDN filter profile, which is represented as **ANY**.
- Specifies the policy action to take for FQDNs that do not match the user-specified FQDNs or categories, or are not **Uncategorized**.

- If a standalone profile is used in a group profile and the group profile is applied to a policy ruleset, the **ANY** row will be taken from the group profile. The **ANY** row of a standalone profile is only applicable if the standalone profile is directly applied to a policy ruleset.

Create a Standalone FQDN Filter Profile

Use the following procedure to create a standalone FQDN filter profile:

Step 1 Navigate to **Manage** > **Profiles** > **FQDN Filtering**.

Step 2 Click **Create**.

Step 3 Provide a unique **Name**.

Step 4 (Optional) Enter a **Description**. This may help differentiate between profiles with a similar name.

Step 5 Specify the Type as **Standalone**.

Step 6 Click **Add** to create a new row.

Step 7 Specify individual FQDNs (for example, google.com).

a) Each FQDN is specified as a PCRE (Perl Compatible Regular Expression).

b) Consider escaping the "**.**" character else it will be treated as a single character wildcard.

Step 8 Specify a **Category** (for example, Gambling, Sports, Social Networking).

Step 9 Specify the policy **Action** for the user-specified FQDNs/Categories, Uncategorized and ANY rows.

- **Allow Log** - Allow the requests and log an event.
- **Allow No Log** - Allow the requests and do not log an event.
- **Deny Log** - Deny the requests and log an event.
- **Deny No Log** - Deny the requests and do not log an event.

Step 10 (Optional) Specify **Decryption Exception** for any FQDNs where decryption is not desired or possible. Possible reasons for considering decryption exception include:

- Desire to not inspect encrypted traffic (for example, financial services, defense, health care, etc.).
- SSO authentication traffic where decryption is not possible.
- NTLM traffic that cannot be proxied.

Step 11 Click **Save** when completed.

What to do next

- View a Profile Details, on page 145
- Add a Gateway Association to a Profile, on page 146

Create a Group FQDN Filter Profile

Use the following procedure to create a group FQDN filter profile with at least two standalone profiles:

Step 1 Navigate to **Manage** > **Profiles** > **FQDN Filtering**.

Step 2 Click **Create**.

Step 3 Provide a unique **Name**.

Step 4 (Optional) Enter a **Description**. This may help differentiate between profiles that may have a similar name.

Step 5 Specify the Type as **Group**.

Step 6 Select an initial standalone profile (at least one standalone profile is required).

Step 7 Click **Add FQDN Profile** to create a new row for additional profiles.

Step 8 Select a standalone profile.

Step 9 Specify the policy **Action** for uncategorized FQDNs.

Step 10 Specify the policy **Action** for **ANY** FQDNs (default).

Step 11 (Optional) Specify the **Decryption Exception** for uncategorized or ANY if decryption is not desired or possible. Possible reasons for considering decryption exception include:

- Desire to not inspect encrypted traffic (financial services, defense, health care, etc.).
- SSO authentication traffic where decryption is not possible.
- NTLM traffic that cannot be proxied.

Step 12 Click **Save**.

What to do next

- View a Profile Details, on page 145
- Add a Gateway Association to a Profile, on page 146

Malicious IP Profile

Additional security protections can be enabled to prevent communication from and to known malicious IPs. These malicious IPs are defined by Trustwave and integrated into Multicloud Defense as a security profile ruleset. The ruleset is updated frequently as updates are made available by Trustwave. The updates can be either dynamically or manually applied to a policy ruleset using the automatic update configuration or manual update configuration. For more information, see Create a Malicious IP Profile, on page 139.

Note Malicious IP are identified by Trustwave based on various learned behavior:

- Malicious attackers identified from web honeypots
- Botnet C&C hosts
- TOR exit nodes
- Other learned behavior

Create a Malicious IP Profile

Use the following procedure to create a malicious IP profile:

Step 1 Navigate to **Manage** > **Profiles** > **Malicious IPs**.

Step 2 Click **Create**.

Step 3 Provide a unique **Profile Name**.

Step 4 (Optional) Enter a **Description**. This can help differentiate between other profiles with similar names.

Step 5 Check the box to enable **IP Reputation**.

Step 6 Choose one of the two options for the **Trustwave Ruleset Version** drop-down menu:

- **Manual** - The selected ruleset version is used by the Multicloud Defense datapath engine on all gateways which use this profile. The profile will not be automatically updated to newer ruleset versions.
- **Automatic** - Select the number of days to delay the update, after the ruleset version is published by Multicloud Defense. New rulesets are published frequently by Multicloud Defense. The gateways using this profile are automatically updated to the latest ruleset version which is **N** days or older, where **N** is the "delay by days" argument selected from the dropdown. For example, if you select to delay the deployment by 5 days on Jan 10, 2021, the Multicloud Defense controller will select a ruleset version which was published on Jan 5th or before. Note that Multicloud Defense may not publish on some days if our internal testing with that ruleset version fails for some reason.

Step 7 Click **Save**.

What to do next

- View a Profile Details, on page 145
- Add a Gateway Association to a Profile, on page 146

IP Reputation

The IP reputation checkbox is used as a means to **enable** or **disable** the profile. When checked and the profile is attached to a policy ruleset, malicious IP protection will be enforced. When unchecked and the profile is attached to policy rules, malicious IP protection will not be enforced. Our recommendation is to always check

the IP reputation checkbox. If you want to disable the malicious IP profile, then remove its association from the policy rules rather than uncheck the checkbox.

Packet Capture Profiles

Packet capture profiles are configured and associated with a Multicloud Defense Gateway and enabled in policy rules, network threat profiles, and web protection profiles. A packet capture can capture traffic flows (PCAP files), and application and network threats (HAR files).

Packet Capture Formats

Consider the following format rules:

`Policy Rule Capture` - `<bucketname>/<cspaccountname>/<gatewayname>/flow-packet-captures/<year>/<month>/<day>/<instanceid>_<timestamp>_<policyname>.pcap.gz`

`IPS Threat Capture` - `<bucketname>/<cspaccountname>/<gatewayname>/network-threats-captures/<year>/<month>/<day>/<instanceid>_<timestamp>_<sessionid>.pcap.gz`

`WAF Threat Capture` - `<bucketname>/<cspaccountname>/<gatewayname>/web-protection-captures/<year>/<month>/<day>/<instanceid>_<timestamp>_<sessionid>.har.gz`

`API Logging` - `<bucketname>/<cspaccountname>/<gatewayname>/api-logging-captures/<year>/<month>/<day>/<instanceid>_<timestamp>_<sessionid>.har.gz`

Create a Packet Capture Profile

Use the following procedure to create a pack capture profile:

Step 1 Navigate to **Manage** > **Profiles** > **Packet Capture**.

Step 2 Click **Create**.

Step 3 Specify a unique **Name**.

Step 4 (Optional) Enter a **Description**. This may help differentiate between other profiles with a similar name.

Step 5 Specify a **CSP Account**.

Step 6 The type of cloud service provider may determine the parameters for the storage bucket. Be aware of the following requirments per cloud service provider:

- **AWS** - S3 Bucket.
- **Azure** - Storage Account Name, Blog Container , and Storage Access Key.
- **GCP** - Storage Bucket.

Step 7 Click **Save**.

What to do next

- View a Profile Details, on page 145
- Add a Gateway Association to a Profile, on page 146

Log Forwarding Profile

A log forwarding profile allows you to send a collection of gateway, VPC, and VNet logs to a third party. The comunication between Multicloud Defense and the third party of your choice contains the log type that needs to be forwarded and the destination server profiles the logs will be sent to. You can have a single profile, or a profile group that sends logs to multiple endpoints simultaneously.

Note that this profile does not include metrics. See Gateway Metrics Forwarding Profile, on page 142 for more information about forwarding log metrics.

Create a Standalone Log Forwarding Profile

Use the following procedure to create a standalone profile to forward logs with:

Step 1 Navigate to **Manager** > **Profiles** > **Log Forwarding**.
Step 2 Click **Create**.
Step 3 Enter a unique **Profile Name**.
Step 4 (Optional) Enter a **Description**. This may help differentiate from other profiles with a similar name.
Step 5 Expand the **Type** drop-down menu and select **Standalone**.
Step 6 Expand the **Destination** drop-down menu and select the third-party application to send logs to.
Step 7 Based on the type of destination you select in step 6, enter the appropriate information when prompted to secure the final endpoint where the logs are forwarded to. Note that not all options are available based on the type of destination.
Step 8 Click **Save**.

What to do next

- View a Profile Details, on page 145
- Add a Gateway Association to a Profile, on page 146

Create a Log Forwarding Group

Use the following procedure to create a profile group to forward logs with:

Before you begin

- You must have at least one third party application to forward the metric to prior to creating this profile.
- You must have at least two standalone metrics forwarding profiles already created. See Create a Standalone Log Forwarding Profile, on page 141 for more information.

Step 1 Navigate to **Manager** > **Profiles** > **Log Forwarding**.
Step 2 Click **Create**.

Step 3 Enter a unique **Profile Name**.

Step 4 (Optional) Enter a **Description**. This may help differentiate from other profiles with a similar name.

Step 5 Expand the **Type** drop-down menu and select **Group**.

Step 6 Under **Group Details**, click **Add** for every new row you need to add to the profile.

Step 7 Expand the drop-down menus for each row to select a profile to add to the group. If you want to remove a profile at any point prior to saving, select the profile's checkbox so it is highlighted and select **Remove**.

Step 8 Click **Save**.

What to do next

- View a Profile Details, on page 145
- Add a Gateway Association to a Profile, on page 146

Gateway Metrics Forwarding Profile

This profile is intended to forward gateway metrics generated by the Multicloud Defense Gateway for data monitoring and analysis.While the metrics are generated by the gateway, it is the Multicloud Defense Controller that forwards the metrics to the third party analysis application. With this forwarding profile you are able to monitor, analyze, and organize your gateway metrics without logging into Multicloud Defense. Use this information to gauge the performance and behavior of your gateway environment; you can also utilize this information for environmental troubleshooting.

Note As of Multicloud Defense Controller version 23.09, only Datadog is supported as a third party analytics application.

For the majority of analytics applications available, for example, Datadog, you must already be an authorized user to access the tool's APIs and rendered data.

Create a Standalone Metrics Forwarding Profile

Use the following procedure to create a standalone profile and forward metrics to be processed by a third party:

Before you begin

You must have at least one third party application to forward the metric to prior to creating this profile.

Step 1 Navigate to **Manager** > **Profiles** > **Metrics Forwarding**.

Step 2 Click **Create**.

Step 3 Enter a unique profile **Name**.

Step 4 (Optional) Enter a **Description**. This may help differentiate from other profiles with a similar name.

Step 5 Expand the **Type** drop-down menu and select **Standalone**.

Step 6 Expand the **Destination** drop-down menu and select the third-party application to process and analyze the metrics.

Step 7 Enter the **Endpoint** to be used as the endpoint location for the metrics.

Step 8 Click **Save**.

If you select Datadog as your analyitics application, the **Endpoint** is filled in by default with an HTTPs webhook. This entry, if defaulted, can be modified prior to saving the profile.

What to do next

- View a Profile Details, on page 145
- Add a Gateway Association to a Profile, on page 146

Create a Group Metrics Forwarding Profile

In this process, you create a profile and then assign it to a specific gateway. A group profile combines up to five standalone metrics forwarding profile that can then be assigned to a single gateway. Use the following procedure to create a grouped metrics forward profile:

Before you begin

- You must have at least one third party application to forward the metric to prior to creating this profile.
- You must have at least two standalone metrics forwarding profiles already created. See Create a Standalone Metrics Forwarding Profile, on page 142 for more information.

Step 1 In the Multicloud Defense Controller interface navigate to **Manager** > **Profiles** > **Metrics Forwarding**.

Step 2 Click **Create**.

Step 3 Enter a unique **Profile Name**

Step 4 (Optional) Enter a **Description**. This may help differentiate between profiles with a similar name.

Step 5 Expand the **Type** drop-down menu and select **Group**.

Step 6 Under **Group Details**, click **Add** for every new row you need to add to the profile.

Step 7 Expand the drop-down menus for each row to select a profile to add to the group. If you want to remove a profile at any point prior to saving, select the profile's checkbox so it is highlighted and select **Remove**.

Step 8 Click **Save**.

What to do next

- View a Profile Details, on page 145
- Add a Gateway Association to a Profile, on page 146

NTP

The Multicloud Defense Gateway uses NTP to ensure its time in sychronized. NTP operates through the Management interface and is configured as part of the Linux shell used for management purposes. The NTP default configuration is slightly different for each CSP as follows:

- **AWS:** `2.centos.pool.ntp.org`, `169.254.169.123`
- **Azure:** `0.centos.pool.ntp.org`, `1.centos.pool.ntp.org`, `2.centos.pool.ntp.org`, `3.centos.pool.ntp.org`
- **GCP:** `metadata.google.internal`
- **OCI:** `0.centos.pool.ntp.org`, `1.centos.pool.ntp.org`, `2.centos.pool.ntp.org`, `3.centos.pool.ntp.org`, `169.254.169.254`

In order to override the default configuration, the NTP profile can be created and applied to each gateway. Once the NTP profile is applied to the gateway, the new configuration will be used. This operation applies immediately.

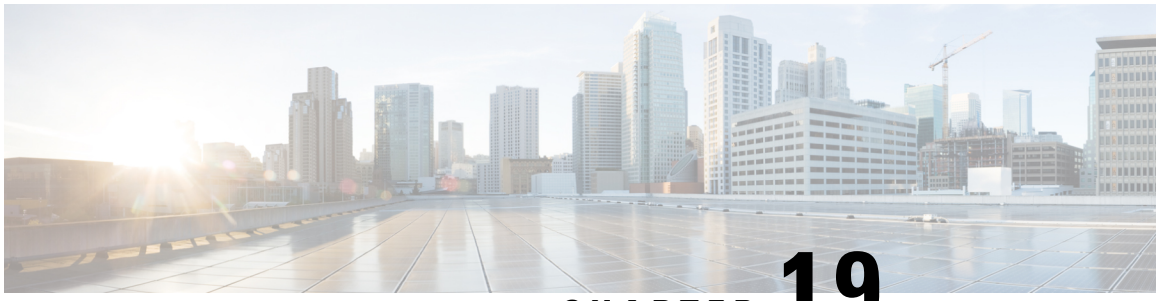
Create a Profile

Use the following procedure to create an NTP profile:

Step 1 Navigate to **Manage** > **Profiles** > **NTP**.
Step 2 Click **Create**.
Step 3 Specify a unique **Name**.
Step 4 (Optional) Enter a **Description**. This may help differentiate between other profiles with a similar name.
Step 5 Specify the **List** of NTP servers.
Step 6 Click **Save**.

What to do next

- View a Profile Details, on page 145
- Add a Gateway Association to a Profile, on page 146



CHAPTER 19

Profile Actions

View a Profile Details

Use the following procedure to view the details of a Packet Capture profile.

Step 1 Navigate to **Manage** > **Profiles** and select the appropriate profile **Type**.
Step 2 Select the profile you want to view the details of.
Step 3 View the profile's details.

Edit a Standalone Metrics Forwarding Profile

Use the following procedure to edit a standalone profile that has already been created.

Step 1 Navigate to **Manage** > **Profiles** and select the appropriate profile **Type**.
Step 2 Check the box next to the profile you want to edit.
Step 3 Click **Edit**.
Step 4 Modify the parameters as desired.
Step 5 Click **Save**.

Edit a Group Profile

Use the following procedure to edit a set of grouped profiles that has already been created:

Step 1 Navigate to **Manage** > **Profiles** and select the appropriate profile **Type**.
Step 2 Check the box next to the profile you want to *Edit*.
Step 3 Click **Edit**.
Step 4 Modify, add or remove group profiles.
Step 5 Click **Save**.

Add a Gateway Association to a Profile

Use the following procedure to add a gateway assocaition to the desired packet capture profile:

Step 1 Navigate to **Manage** > **Gateways** > **Gateways**.
Step 2 Check the box next the gateway you want to associate the profile to.
Step 3 Click **Edit**.
Step 4 Expand the profile's drop-down menu and select the desired **Profile** from the menu.
Step 5 Click **Save**.

Remove a Gateway Association

Use the following procedure to remove an existing gateway that is assocaited with a packet capture profile. Note that this procress only removes the gateway association from the profile. This does not delete the gateway or the profile from Multicloud Defense.

Step 1 Navigate to **Manage** > **Gateways** > **Gateways**.
Step 2 Check the box next the gateway you want to dissassociate from a packet capture profile.
Step 3 Click **Edit**.
Step 4 Scroll towards the bottom of the page and click the '**X**' within the appropriate profile drop-down menu to remove the association.
Step 5 Click **Save**.

Delete a Profile

Use the following procedure to delete a packet capture profile. This process includes removing any and all existing gateway associations as well as deleting the profile.

Step 1 Navigate to **Manage** > **Profiles** and select the appropriate profile **Type**.

Step 2 View the profile details and examine the associated gateways.

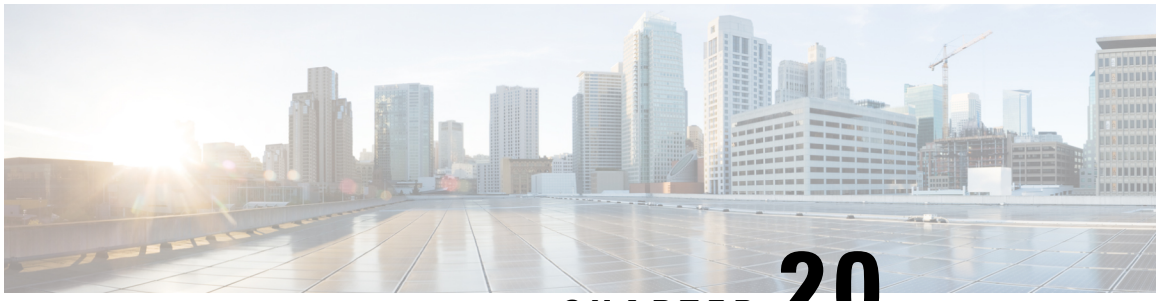
Step 3 Remove all gateway associations. See Remove a Gateway Association for more information.

Step 4 Navigate to **Manage** > **Profiles** and select the same prilfue type that you selected in step 1.

Step 5 Check the box next to the profile you want to delete.

Step 6 Click **Delete**.

Step 7 Click **Yes** or **No** to either confirm or cancel the delete action.



CHAPTER 20

FQDN and URL Filtering Categories

FQDN / URL Filtering Categories

Multicloud Defense uses threat intelligence from WebRootTM BrightCloud (www.brightcloud.com) to categorize web sites based on their risk score. This includes fully qualified domain names (FQDNs), sometimes referred to as domain names, and URLs. This provides sites across 84 categories when traffic from your public cloud environment makes outbound connections (egress) to these sites:

- FQDNs (domains) - 1+ billion categorized FQDNs (domains)
- URLs - 45+ billion categorized URLs

To improve efficiency in recognizing and processing traffic, The gateway will pre-load a cache of the top 1 million FQDNs/URLs and their categories. The gateway will also utilize a runtime cache of 10k FQDNs/URLs and their Categories that are not part of the top 1 million. If traffic contains any of the cached FQDNs/URLs, then the categories will be known immediately. If the FQDN/URL is not found in the cache, the gateway will query the Controller to resolve the category via BrightCloud. This operation is expected to complete in no more than 200ms. If it completes within the expected time, then the traffic will be processed based on the learned category and the profile will operate on the traffic based on the policy defined for the category. If the operation does not complete within the expected time, then the traffic will be processed as Uncategorized and the profile will operate on the traffic based on the policy defined for Uncategorized. Once the resolution returns, the learned category will be added to the cache for subsequent resolutions, even if the resolution occurs for the available the expected time and the traffic has already been processed. If the run-time cache is exhausted, the gateway will purge the oldest accessed FQDNs/URLs and their categories in batches of 10 entries to ensure space is available for more recently accessed FQDNs/URLs and their categories.

Note FQDN filtering with categories happens for:

1. SNI in TLS client hello
2. DNS queries for FQDN lookups
3. HTTP hostname header (for cleartext HTTP traffic)

Malicious Categories

Multicloud Defense considers the following categories to be particularly malicious:

Table 6: Malicious Categories Multicloud Defense considers the following categories to be particularly malicious

Category Name	Category Description
Malware Sites	Siteshosting malicious content including executables, drive-by infection sites, malicious scripts, viruses, trojans, and code.
Phishingand Other Frauds	Phishing, pharming, and other sites that pose as a reputable site, usually to harvest personalinformation from a user. These sites are typically quite short-lived, so they don’t last long in terms of uptime.
Proxy Avoidance and Anonymizers	Proxyservers and other methods to gain access to URLs in any way that bypasses URL filtering or monitoring. Web-based translation sites that circumvent filtering.
Keyloggers and Monitoring	Softwareagents that track a user's keystrokes or monitor their web surfing habits. Often used for collecting sensitive data such as usernames and passwords.
SPAM URLs	Sites known to distribute unsolicited email (spam) messages.
Spywareand Adware	Spywareor Adware sites that provide or promote information gathering or tracking that is unknown to, or without the explicit consent of, the end user or the organization, also unsolicited advertising popups and programs that may be installed on a user's computer.
Bot Nets	These are URLs, often IP addresses, which are determined to be part of a Bot network, fromwhich network attacks are launched. Attacks may include SPAM messages, DOS, SQL injections, proxy jacking, and other unsolicited contacts.

Multicloud Defense offers traffic analysis when viewing traffic via **Discover** > **Traffic** > **DNS** and **Investigate** > **Flow Analytics** > **Traffic Summary**, where a pre-defined *Malicious Categories* filter can be selected to show instances and VPCs communicating with these Malicious Category FQDNs and URLs.

The full list of categories is shown below.

Full List of Categories

Category Name	Category Name	Category Name	Category Name
Abortion	Games	Motor Vehicles	Sex Education
Abused Drugs	Government	Music	Shareware and Freeware
Adult and Pornography	Gross	News and Media	Shopping
Alcohol and Tobacco	Hacking	Nudity	Social Networking
Auctions	Hate and Racism	Online Greeting Cards	Society
Bot Nets	Health and Medicine	Open HTTP Proxies	SPAM URLs
Business and Economy	Home and Garden	Parked Domains	Sports
Cheating	Hunting and Fishing	Pay to Surf	Spyware and Adware
Computer and Internet Info	Illegal	Peer to Peer	Streaming Media
Computer and Internet Security	Image and Video Search	Personal sites and Blogs	Swimsuits and Intimate Apparel
Confirmed SPAM Sources	Individual Stock Advice and Tools	Personal Storage	Training and Tools
Content Delivery Networks	Internet Communications	Philosophy and Political Advocacy	Translation
Cult and Occult	Internet Portals	Phishing and Other Frauds	Travel
Dating	Job Search	Private IP Addresses	Uncategorized
Dead Sites	Keyloggers and Monitoring	Proxy Avoidance and Anonymizers	Unconfirmed SPAM Sources
Dynamically Generated Content	Kids	Questionable	Violence
Educational Institutions	Legal	Real Estate	Weapons
Entertainment and Arts	Local Information	Recreation and Hobbies	Web Advertisements
Fashion and Beauty	Malware Sites	Reference and Research	Web Hosting
Financial Services	Marijuana	Religion	Web-based Email
Gambling	Military Search Engines	Services	

Associating a Filtering Profile with a Policy Ruleset Rule

- Refer to Fully Qualified Domain Name Filter Profile to create/edit FQDN Filtering Profiles
- Refer to URL (Uniform Resource Locator) Filter Profile to create/edit URL Filtering Profiles

BrightCloud URL / IP Lookup Tool

BrightCloud offers an online URL / IP Lookup Tool (https://www.brightcloud.com/tools/url-ip-lookup.php) that can be used to understand what category a particular FQDN / URL is classified as along with its Web Reputation.

PART IX

Investigate and Analysis

Investigate summary page

The Investigate tab of the Multicloud Defense Controller offers a collection of traffic, events, and logs that can assist in diagnosing policy effectiveness and threats.

Flow Analytics

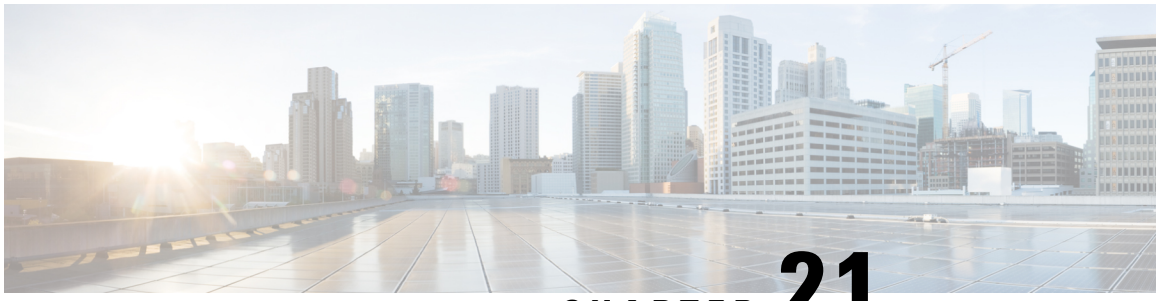
Flow Analytics provides overall visibility into the traffic seen, processed and protected by the Multicloud Defense Gateway. The traffic is organized into two main categories: traffic summary logs and security events. Traffic summary logs provide information related to each traffic session that is being processed by the gateways. Security events provide information related to how the gateway datapath protects each traffic session.

Network Analytics

Network Stats provides information on the performance of the gateway. The generated graph has the potential to display how gateways and instances associated with the gateways autoscale to combat with the capacity threshold. This can be a useful tool in troubleshooting gateway behavior, trends or spikes, and gateway management.

System Status

System Logs detail which user logged into the Multicloud Defense Controller by time and time range, as well as actions performed.



CHAPTER 21

Flow Analytics

Flow Analytics - Traffic Summary

This view provides detailed visibility, filtering and analysis for events recorded by Multicloud Defense from either a forward or reverse gateway proxy. Traffic Summary events contribute to one of three event types: `Firewall Events`, `Network Events` and `Web Attacks`.

Traffic Summary

Tables and Fields available in Session Summary are as follows:

Event Details	Description
Date and Time	ISO 8601 format: YYYY-MM-DD T HH:MM:SS:S Example: `2020-11-22T10:58:46.820`
CSP Account	Multicloud Defense CSP Account
Gateway	Multicloud Defense Gateway
Region	Region of the Multicloud Defense Gateway
Level	INFO
Session ID	..

Client-side Connection	Description
Src IP	Source IP Address

Client-side Connection	Description
Src Port	Source Port
Dest IP	Destination IP Address
Dest Port	Destination Port
Protocol	UDP, TCP

Client-side Stats	Traffic between client and Multicloud Defense Gateway
Received Bytes	Number of bytes received from client
Transmitted Bytes	Number of bytes sent to client
Received Packets	Number of packets received from client
Transmitted Packets	Number of packets sent to client

Policy Match Info	Description
Dest Address Group	Destination Address Group configured in the matched policy rule
Src Address Group	Source Address Group configured in the matched policy rule
Request SNI	Server Name Indication in the request
Service Type	Service Type. Example: `PROXY`
Src Country	Country that the request originated from on the client-side
Dest Country	Country that the request was destined to on the server-side. Example: `United States`

Server-side Connection	Description
Src IP	Source IP Address
Src Port	Source Port
Dest IP	Destination IP Address
Dest Port	Destination Port
Protocol	UDP, TCP

Server-side Stats	Traffic between Multicloud Defense Gateways and server
Received Bytes	Number of bytes received from server
Transmitted Bytes	Number of bytes sent to server

Server-side Stats	Traffic between Multicloud Defense Gateways and server
Received Packets	Number of packets received from server
Transmitted Packets	Number of packets sent to server

Application Info	Description
Client App Name	Application name associated with client side of the session. Example: `Advanced Packaging Tool`
Payload App Name	HTTP application name associated with webserver host. Example: `Facebook`
Service App Name	Application name associated with server side of the session. Example: `HTTP`

Action	Description
Action	ALLOW, DENY

Cloud Service	Description
Cloud Service	Name of the destination cloud service accessed with the request. Example `AMAZON, EC2`

Src Instance Info	Description
Instance ID	Client instance ID
Instance Name	Client instance name (and provides ability to see tags)
VPC ID	Client VPC ID

HTTP Request	Description
Host	Host portion of URL
Method	GET, PUT, POST, HEAD, DELETE, PATCH, OPTIONS
URI	URI Identifier RFC 3986

Rule	Description
ID	ID number/description of Multicloud Defense Rule. Example `59 (egress-prod-apt-80).`

FQDN	Description
FQDN	Fully Qualified Domain Name
Category Name	Category classification of the FQDN. Example: `Social Media`

FQDN	Description
Reputation	Reputation score of the FQDN

Flow Analytics - All Events

Flow Analytics - All Events provides overall visibility into network and security events from the entire Multicloud Defense solution.

Tables and Fields available in All Events are as follows:

Event Details	Description
Date and Time	ISO 8601 format: YYYY-MM-DD T HH:MM:SS:S Example: `2020-11-22T10:58:46.820`.
Type	APPID, AV, DLP, DPI, FLOW_LOG, FQDNFILTER, L4_FW, L7DOS, MALICIOUS_SRC, SNI, TLS_ERROR, TLS_LOG, URLFILTER.
CSP Account	Multicloud Defense CSP Account.
Gateway	Multicloud Defense Gateway.
Region	Region of the Multicloud Defense Gateway.
Level	DEBUG, INFO, NOTICE, WARNING, ERROR, CRITICAL, ALERT, EMERGENCY.
Session ID	..

Service	Description
Src IP	Source IP Address.
Src Port	Source Port.
Dest IP	Destination IP Address.
Dest Port	Destination Port.
Protocol	UDP, TCP.

Application Info	Description
Client App Name	Application name associated with client side of the session. Example: `Advanced Packaging Tool`.
Payload App Name	HTTP application name associated with webserver host. Example: `Facebook`.

Application Info	Description
Service App Name	Application name associated with server side of the session. Example: `HTTP`.

Action	Description
Action	ALLOW, DENY.
State	ESTABLISHED, CLOSE, CLOSED, CLOSE_WAIT, TIME_WAIT, FIN_WAIT, LAST_ACK.

HTTP Request	Description
Host	Host portion of URL.
Method	GET, PUT, POST, HEAD, DELETE, PATCH, OPTIONS.
URI	URI Identifier RFC 3986.

Rule	Description
ID	ID number/description of Multicloud Defense Rule. Example `59 (egress-prod-apt-80).`

FQDN	Description
FQDN	Fully Qualified Domain Name.
Category Name	Category classification of the FQDN. Example: `Social Media`.
Reputation	Reputation score of the FQDN.

Flow Analytics - Firewall Events

This view provides detailed visibility, filtering and analysis for events recorded by the Multicloud Defense Firewall configuration and summarized in `Firewall Events` category.

Tables and Fields available in Firewall Events are as follows:

Event Details	Description
Date and Time	ISO 8601 format: YYYY-MM-DD T HH:MM:SS:S Example: `2020-11-22T10:58:46.820`
Type	APPID, L4_FW, MALICIOUS_SRC, SNI
CSP Account	Multicloud Defense CSP Account
Gateway	Multicloud Defense Gateway

Event Details	Description
Region	Region of the Multicloud Defense Gateway
Level	DEBUG, INFO, NOTICE, WARNING, ERROR, CRITICAL, ALERT, EMERGENCY
Session ID	..

Service	Description
Src IP	Source IP Address
Src Port	Source Port
Dest IP	Destination IP Address
Dest Port	Destination Port
Protocol	UDP, TCP

Application Info	Description
Client App Name	Application name associated with client side of the session. Example: `Advanced Packaging Tool`
Payload App Name	HTTP application name associated with webserver host. Example: `Facebook`
Service App Name	Application name associated with server side of the session. Example: `HTTP`

Action	Description
Action	ALLOW, DENY
State	ESTABLISHED, CLOSE, CLOSED, CLOSE_WAIT, TIME_WAIT, FIN_WAIT, LAST_ACK

HTTP Request	Description
Host	Host portion of URL
Method	GET, PUT, POST, HEAD, DELETE, PATCH, OPTIONS
URI	URI Identifier RFC 3986

Rule	Description
ID	ID number/description of Multicloud Defense Rule. Example 59 (egress-prod-apt-80)

FQDN	Description
FQDN	Fully Qualified Domain Name
Category Name	Category classification of the FQDN. Example: `Social Media`
Reputation	Reputation score of the FQDN

Flow Analytics - Network Threats

This view provides detailed visibility, filtering and analysis for threats recorded by the Multicloud Defense threat analysis engine and summarized in `Network Threats`.

Network Threats

Tables and Fields available in Network Threats are as follows:

Event Details	Description
Date and Time	ISO 8601 format: YYYY-MM-DD T HH:MM:SS:S Example: `2020-11-22T10:58:46.820`
Type	AV, DLP, DPI
CSP Account	Multicloud Defense CSP Account
Gateway	Multicloud Defense Gateway
Region	Region of the Multicloud Defense Gateway
Level	DEBUG, INFO, NOTICE, WARNING, ERROR, CRITICAL, ALERT, EMERGENCY
Session ID	..

Service	Description
Src IP	Source IP Address
Src Port	Source Port
Dest IP	Destination IP Address
Dest Port	Destination Port
Protocol	UDP, TCP

Application Info	Description
Client App Name	Application name associated with client side of the session. Example: `Advanced Packaging Tool`

Application Info	Description
Payload App Name	HTTP application name associated with webserver host. Example: `Facebook`
Service App Name	Application name associated with server side of the session Example: `HTTP`

Action	Description
Action	ALLOW, DENY
State	ESTABLISHED, CLOSE, CLOSED, CLOSE_WAIT, TIME_WAIT, FIN_WAIT, LAST_ACK

HTTP Request	Description
Host	Host portion of URL
Method	GET, PUT, POST, HEAD, DELETE, PATCH, OPTIONS
URI	URI Identifier RFC 3986

FQDN	Description
FQDN	Fully Qualified Domain Name
Category Name	Category classification of the FQDN. Example: `Social Media`
Reputation	Reputation score of the FQDN

Rule	Description
ID	ID number/description of Multicloud Defense Rule. Example 59 (egress-prod-apt-80)

Flow Analytics - Web Attacks

This view provides detailed visibility, filtering and analysis for threats recorded by the Multicloud Defense web protection engine. The `Web Attacks` event types include WAF and L7DOS.

Web Attacks

Tables and Fields available in Web Attacks are as follows:

Event Details	Description
Date and Time	ISO 8601 format: YYYY-MM-DD T HH:MM:SS:S Example: `2020-11-22T10:58:46.820`
Type	L7DOS, WAF

Event Details	Description
CSP Account	Multicloud Defense CSP Account
Gateway	Multicloud Defense Gateway
Region	Region of the Multicloud Defense Gateway
Level	DEBUG, INFO, NOTICE, WARNING, ERROR, CRITICAL, ALERT, EMERGENCY
Session ID	..

Service	Description
Src IP	Source IP Address
Src Port	Source Port
Dest IP	Destination IP Address
Dest Port	Destination Port
Protocol	UDP, TCP

Application Info	Description
Client App Name	Application name associated with client side of the session. Example: `Advanced Packaging Tool`
Payload App Name	HTTP application name associated with webserver host. Example: `Facebook`
Service App Name	Application name associated with server side of the session Example: `HTTP`

Action	Description
Action	ALLOW, DENY
State	ESTABLISHED, CLOSE, CLOSED, CLOSE_WAIT, TIME_WAIT, FIN_WAIT, LAST_ACK

HTTP Request	Description
Host	Host portion of URL
Method	GET, PUT, POST, HEAD, DELETE, PATCH, OPTIONS
URI	URI Identifier RFC 3986

FQDN	Description
FQDN	Fully Qualified Domain Name

FQDN	Description
Category Name	Category classification of the FQDN. Example: `Social Media`
Reputation	Reputation score of the FQDN

Rule	Description
ID	ID number/description of Multicloud Defense Rule. Example 59 (egress-prod-apt-80)

Flow Analytics - URL Filtering

This view provides detailed visibility, filtering and analysis for events recorded by the Multicloud Defense URL Filtering configuration. URL Filtering events contribute to one of three event types: `Firewall Events`, `Network Events` and `Web Attacks`.

URL Filtering

Tables and Fields available in URL Filtering are as follows:

Event Details	Description
Date and Time	ISO 8601 format: YYYY-MM-DD T HH:MM:SS:S Example: `2020-11-22T10:58:46.820`
Type	URLFILTER
CSP Account	Multicloud Defense CSP Account
Gateway	Multicloud Defense Gateway
Region	Region of the Multicloud Defense Gateway
Level	DEBUG, INFO, NOTICE, WARNING, ERROR, CRITICAL, ALERT, EMERGENCY
Session ID	..

Service	Description
Src IP	Source IP Address
Src Port	Source Port
Dest IP	Destination IP Address
Dest Port	Destination Port
Protocol	UDP, TCP

Application Info	Description
Client App Name	Application name associated with client side of the session. Example: `Advanced Packaging Tool`.
Payload App Name	HTTP application name associated with webserver host. Example: `Facebook`
Service App Name	Application name associated with server side of the session Example: `HTTP`

Action	Description
Action	ALLOW, DENY
State	ESTABLISHED, CLOSE, CLOSED, CLOSE_WAIT, TIME_WAIT, FIN_WAIT, LAST_ACK

HTTP Request	Description
Host	Host portion of URL
Method	GET, PUT, POST, HEAD, DELETE, PATCH, OPTIONS
URI	URI Identifier RFC 3986

Rule	Description
ID	ID number/description of Multicloud Defense Rule. Example 59 (egress-prod-apt-80)

FQDN	Description
FQDN	Fully Qualified Domain Name
Category Name	Category classification of the FQDN. Example: `Social Media`
Reputation	Reputation score of the FQDN

Flow Analytics - FQDN Filtering

This view provides detailed visibility, filtering and analytical options for events recorded from the FQDN Filtering configuration. FQDN Filtering events contribute to one of three event types: `Firewall Events`, `Network Events` and `Web Attacks`.

FQDN Filtering

Tables and Fields available in FQDN Filtering are as follows:

Event Details	Description
Date and Time	ISO 8601 format: YYYY-MM-DD T HH:MM:SS:S Example: `2020-11-22T10:58:46.820`.
Type	FQDNFILTER.
CSP Account	Multicloud Defense CSP Account.
Gateway	Multicloud Defense Gateway.
Region	Region of the Multicloud Defense Gateway.
Level	DEBUG, INFO, NOTICE, WARNING, ERROR, CRITICAL, ALERT, EMERGENCY.
Session ID	..

Service	Description
Src IP	Source IP Address.
Src Port	Source Port.
Dest IP	Destination IP Address.
Dest Port	Destination Port.
Protocol	UDP, TCP.

Action	Description
Action	ALLOW, DENY.
State	ESTABLISHED, CLOSE, CLOSED, CLOSE_WAIT, TIME_WAIT, FIN_WAIT, LAST_ACK.

HTTP Request	Description
Host	Host portion of URL.
Method	GET, PUT, POST, HEAD, DELETE, PATCH, OPTIONS.
URI	URI Identifier RFC 3986.

FQDN	Description
FQDN	Fully Qualified Domain Name.
Category Name	Category classification of the FQDN. Example: `Social Media`.
Reputation	Reputation score of the FQDN.

Rule	Description
ID	ID number/description of Multicloud Defense Rule. Example 59 (egress-prod-apt-80).

Flow Analytics - HTTPS Logs

This view provides detailed visibility, filtering and analytical options for events recorded from HTTPS Logs. HTTPS logs may contribute to one of three event types: `Firewall Events`, `Network Events` and `Web Attacks`.

HTTPS Logs

Tables and Fields available in HTTPS Logs are as follows:

Event Details	Description
Date and Time	ISO 8601 format: YYYY-MM-DD T HH:MM:SS:S Example: `2020-11-22T10:58:46.820`
Type	TLS_ERROR, TLS_LOG.
CSP Account	Multicloud Defense CSP Account.
Gateway	Multicloud Defense Gateway.
Region	Region of the Multicloud Defense Gateway.
Level	DEBUG, INFO, NOTICE, WARNING, ERROR, CRITICAL, ALERT, EMERGENCY.
Session ID	..

Service	Description
Src IP	Source IP Address.
Src Port	Source Port.
Dest IP	Destination IP Address.
Dest Port	Destination Port.
Protocol	UDP, TCP.

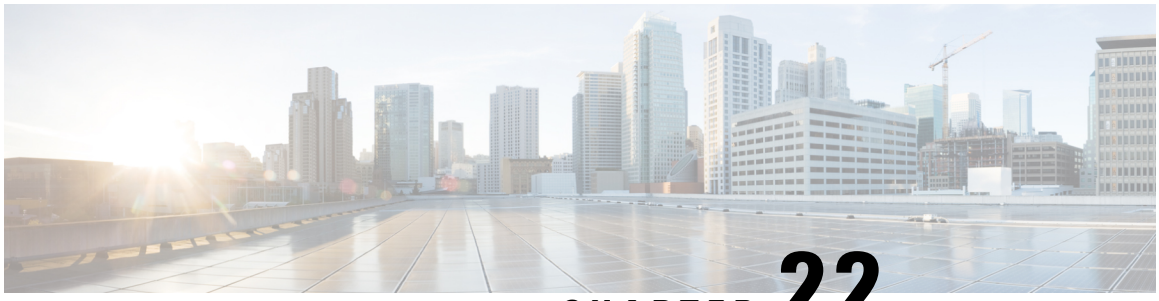
Application Info	Description
Client App Name	Application name associated with client side of the session. Example: `Advanced Packaging Tool`.
Payload App Name	HTTP application name associated with webserver host. Example: `Facebook`.

Application Info	Description
Service App Name	Application name associated with server side of the session Example: `HTTP`.

Action	Description
Action	ALLOW, DENY.
State	ESTABLISHED, CLOSE, CLOSED, CLOSE_WAIT, TIME_WAIT, FIN_WAIT, LAST_ACK.

HTTP Request	Description
Host	Host portion of URL.
Method	GET, PUT, POST, HEAD, DELETE, PATCH, OPTIONS.
URI	URI Identifier RFC 3986.

FQDN	Description
FQDN	Fully Qualified Domain Name.
Category Name	Category classification of the FQDN. Example: `Social Media`.
Reputation	Reputation score of the FQDN.



CHAPTER 22

Network Analytics

Stats

This view provides detailed visibility into the bandwidth and connections of selected Multicloud Defense gateway/s, both instantaneously, and over selected timeframes.

Step 1 Navigate to **Investigate** > **Network Analytics** > **Stats**.

Step 2 Initially, statistics are displayed for `All CSP Accounts` and `All Gateways` with timeframe default to `Last 1 hour`.

Step 3 Graphically, the X and Y axis are auto-scaled based on timeframe selection / bandwidth, and auto- updated while viewing. Statistics are refreshed every 5 seconds while viewing this page.

Step 4 Use the drop-down options in the filter bar to finesse the display and view the stats of a specific **Account**, **CSP Type**, or **Instance Type**.

Note that if you select **Instance Type**, you see two additional stats: CPU usage and memory usage.

Step 5 Select a **Timeframe** from the pulldown as shown below. Options are: `Last 15 mins` `Last 1 hour` `Last 1 day` `Last 7 Days` `Last 30 days`.

Total Bandwidth

The total network bandwidth is a measurement indicating the maximum capacity of a wired or wireless communications link to transmit data over a network connection in a given amount of time. This value is a compilation of **total speed** (addition of Inbound and Outbound bandwidth of selected gateways), **inbound** bandwidth (bandwidth ingressing a gateway), and **outbound** bandwidth (bandwidth egressing a gateway).

CPU Usage

Note This statistic is only available if you include an **Instance Type** in your selection from the filter bar located at the top of the page.

This view provides information about gateway instances that may have higher than normal memory use. You can use this information to monitor and optimize the performance of the gateway activities based on CPU capacity. You can also use these stats to help asses trends in traffic and the effort expressed by the CPU over the behaviors.

Memory Usage

Note This statistic is only available if you include an **Instance Type** in your selection from the filter bar located at the top of the page.

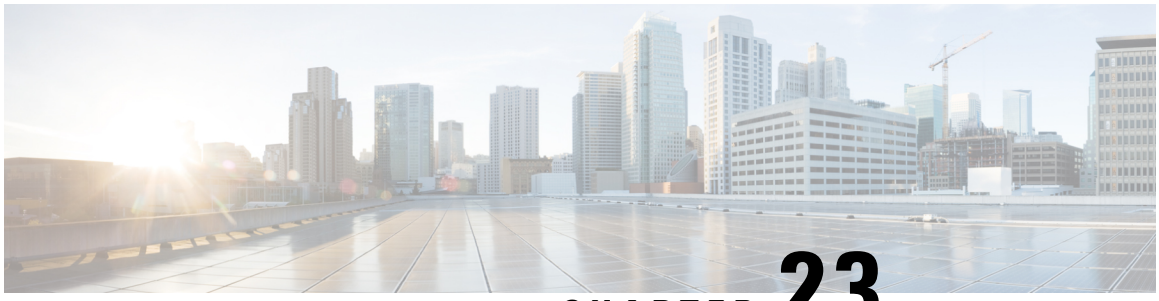
This view provides information about gateway instances that may have higher than normal memory use. You can use this information to monitor and optimize the performance of the gateway activities based on memory usage capacity.

Connection Rate

Connection rates refers to the percentage of successfully connected calls out of the total attempted calls. Specifically, it equates to the **connection** (total number of current active connections) and **connections per second** (bandwidth of both inbound and outbound connections to a gateway).

HTTP Request Rate

An **HTTP request rate** typically measures of how much demand is being placed on your system, measured in a high-level system-specific metric. For a web service, this measurement is usually HTTP requests per second.



CHAPTER 23

System Status

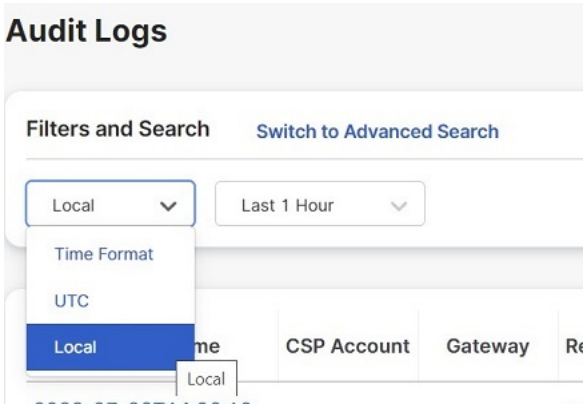
Audit Logs

Audit logs contain details of actions performed by Users. This includes, but not limited to, actions of login/logout activity, creating, deleting, updating, enabling, disabling etc. of Profiles, Rules, Gateways or any User activity that relates to the configuration and operation of the Multicloud Defense solution.

Time Format

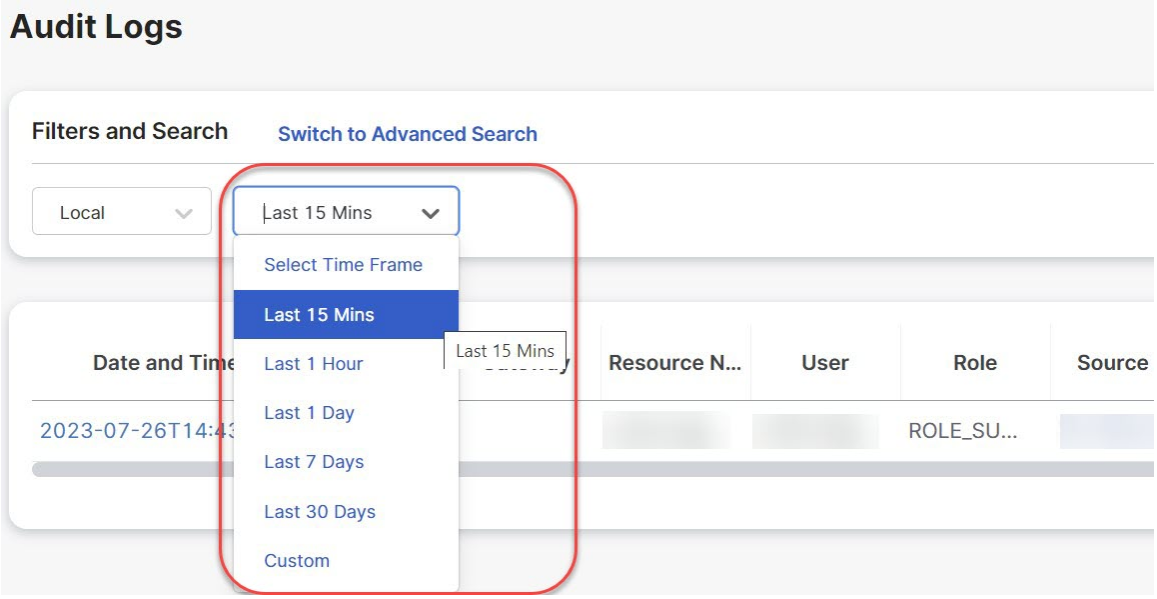
Logs can be displayed in UTC (Coordinated Universal Time) or Local time format. Local means the time zone of the user as configured e.g. USA/Pacific. Date and Time of logs will be displayed in ISO 8601 format (Complete date plus hours, minutes, seconds and a decimal fraction of a second - YYYY-MM-DD T HH:MM:SS:S). Example: `2020-11-22T10:58:46.820`

To select, or switch between, different Time Formats, click the radio button as shown:



Timeframe

Logs can be displayed in increment options from 15 minutes to 30 days, or Custom timeframes. To select, or switch between, timeframes, click the pulldown and select timeframe as shown:



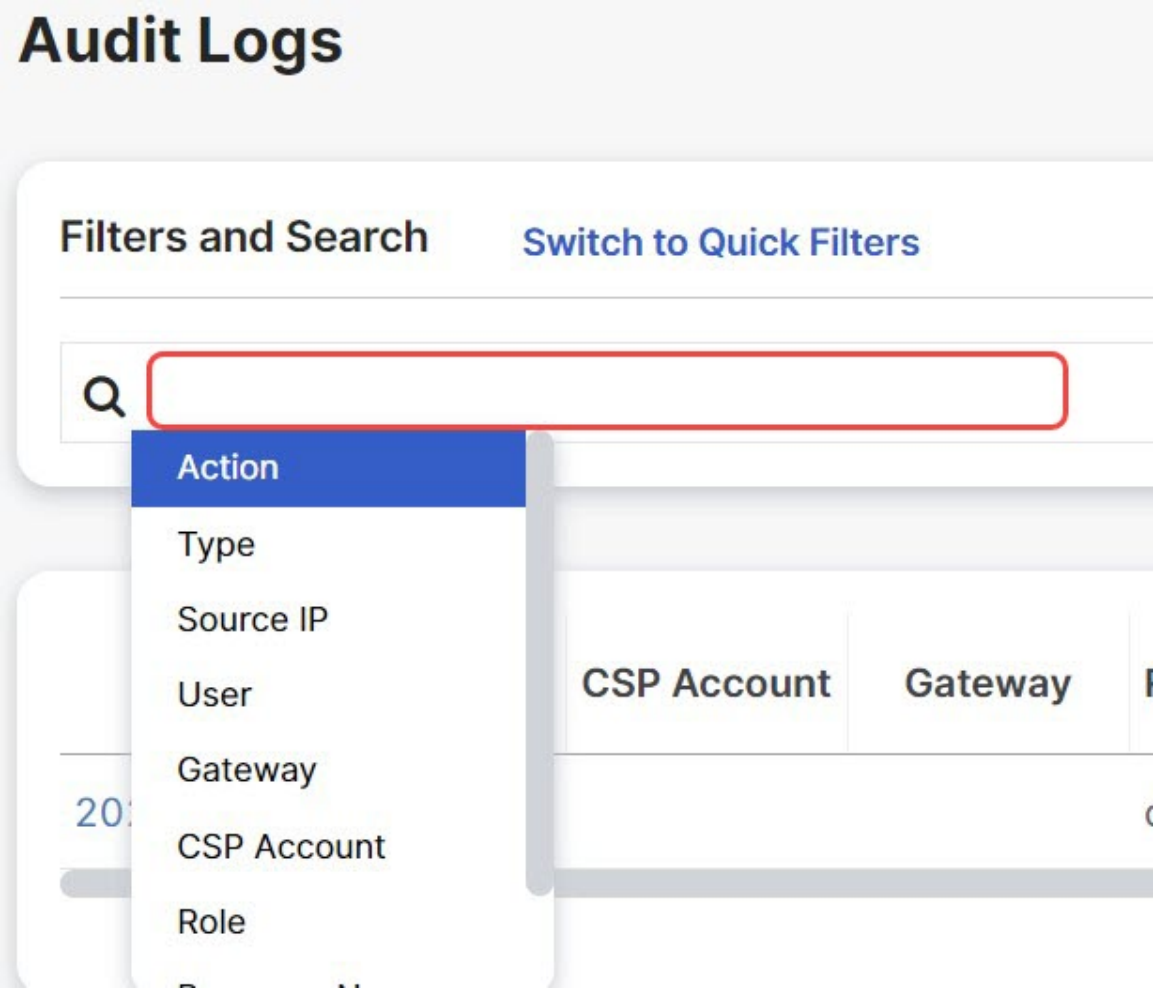
For Custom timeframes, select **Custom**, the **Start** and the **End** date or time by clicking the calender objects followed by **Save**.

Search Filter

Logs can be filtered using the Search function and audit log fields. The audit log fields are `Action` `Type` `Source IP` `User` `Gateway` `CSP Account` `Role`

To filter audit logs on one, or multiple, fields:

Step 1 Left mouse-click in the Search field to access the pull down menu.



Step 2 Select a field e.g. `Action`.

Step 3 Type a desired search string e.g. `DELETE`.

Step 4 Add additional fields to the search criteria as required.

Example: Filter for Actions = **"DELETE"** and performed by user with string containing **"steve"** would appear in the filter criteria and results.

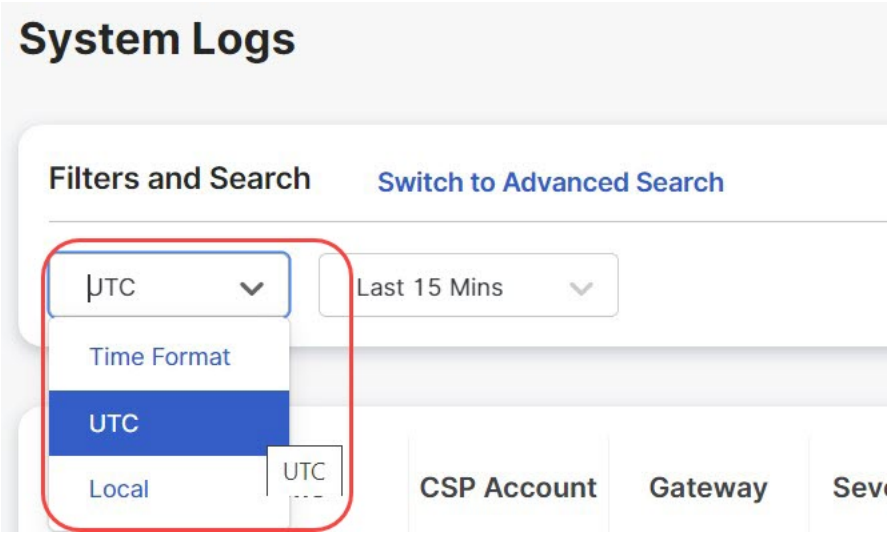
System Logs

System logs contain details of actions performed by the Multicloud Defense solution. This includes, but not limited to, system messages, gateway events, instance creation/deletion and other configuration and operation modifications of the Multicloud Defense solution (system).

Time Format

Logs can be displayed in UTC (Coordinated Universal Time) or Local time format. Local means the time zone of the user as configured e.g. USA/Pacific. Date and Time of logs will be displayed in ISO 8601 format (Complete date plus hours, minutes, seconds and a decimal fraction of a second - YYYY-MM-DD T HH:MM:SS:S). Example: `2020-11-22T10:58:46.820`

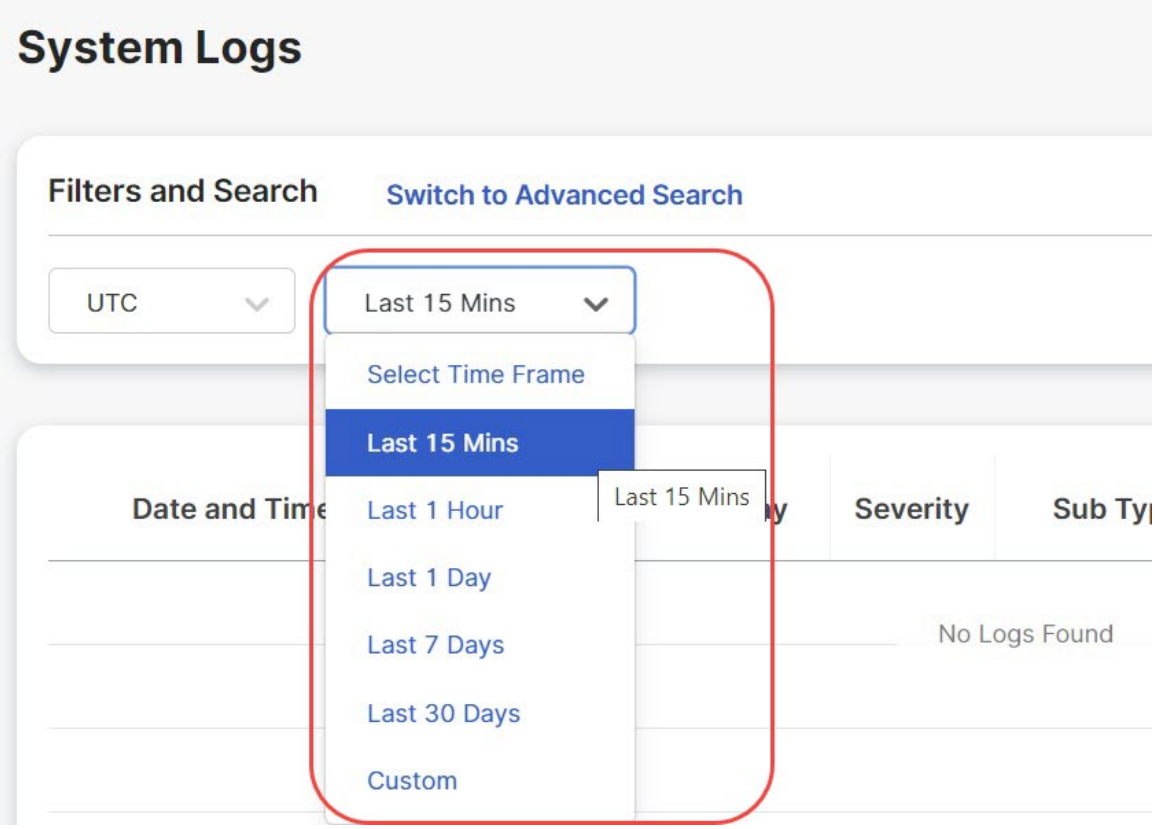
To select, or switch between, different Time Formats, click the radio button as shown:



Timeframe

Logs can be displayed in increment options from 15 minutes to 30 days, or Custom timeframes.

To select, or switch between, timeframes, click the pulldown and select timeframe as shown:



For Custom timeframes, select **Custom**, the **Start** and the **End** date or time by clicking the calender objects followed by **Save**.

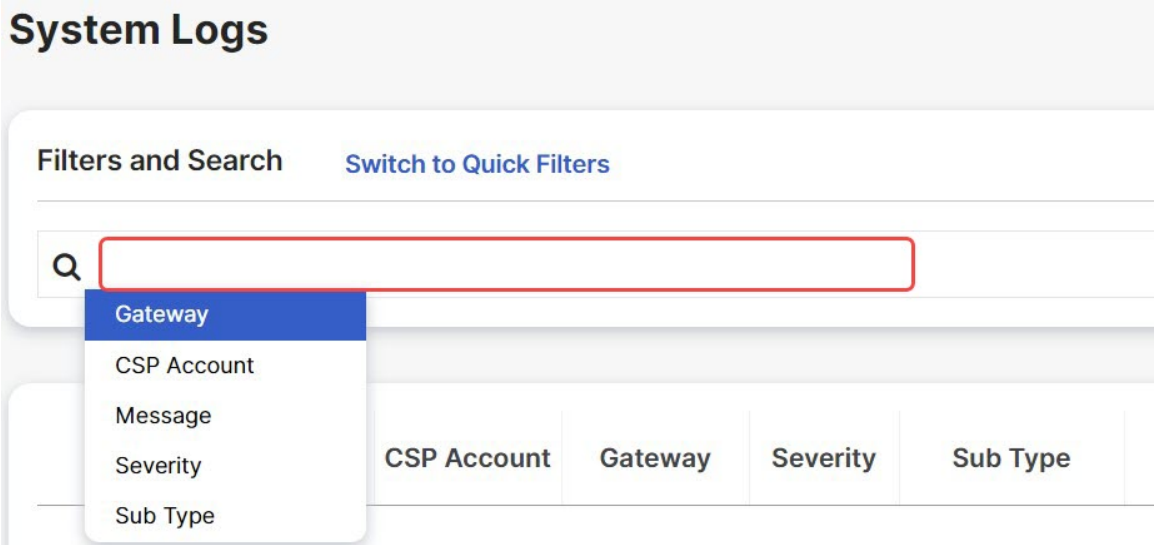
Search Filter

Logs can be filtered using the Search function and System log fields.

The System log fields are `Gateway` `CSP` `Account` `Message`

To filter System logs on one, or multiple, fields:

Step 1 Left mouse-click in the Search field to access the pull down menu.



Step 2 Select a field e.g. `Gateway`.

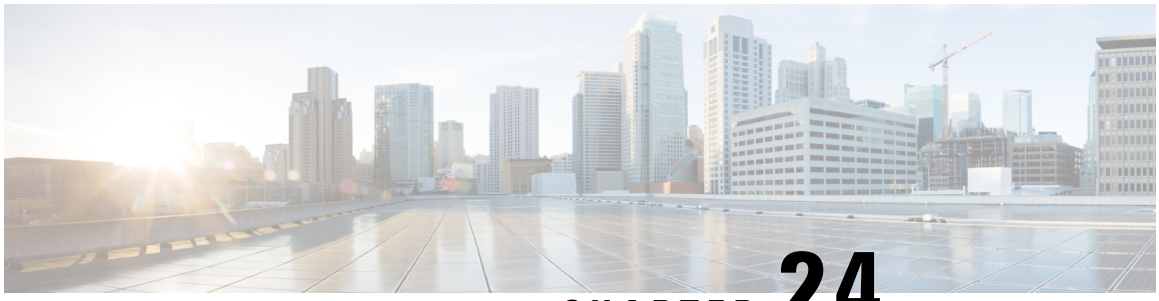
Step 3 Type a desired search string e.g. `ingress`.

Step 4 Add additional fields to the search criteria as required.

Example: Filter for a Gateway = **"ingress"** and Messages containing **"created"** would appear in the filter criteria and results.

PART X

Threat Research



CHAPTER 24

Threat Research

Threat Research is generated from a set of rules that are applied to the inspection engine to detect threats and malicious activity. This page allows you to view these rules. Once a day, Multicloud Defense searches for new or modified rules for network intrusion and includes or removes rules and known malicious sources from the internal library. This action is automated. Included in this function is the act of downloading and validating the new list of IP addresses as sources and implementing them in new rulesets. These rulsesets are then deployed.

The rules have a variety of ways in which they are organized such as policy, class, application, ruleset library date, and other parameters. If you are interested in understanding more about a rule that has tripped (e.g., detected a threat or malicious activity), use the **Threat Research** page to view more details about the rule. The following parts of each of the page are available for your use:

Search Bar

The search bar at the top of the window allows you to search each page under threat research for any singular dientifying facet: a known IP address, action, rule name, gateway name, attack type, or profile name. If you find a specific field value by scrolling, you can **Add to Search** to facilitate an easier search experience.

Note that the searches are isolated to each page, and you cannot cross-search the different types of threat research. See the section below for more details.

View Details

Each of the facets under threat research offer the ability to **View Details** of a singular incident or attack. The values provided in these details differ between the types of threat research, but can be valuable if you want to finetune your policies, security profiles, rules or rulesets.

Add to Search

For any of the types of research available here, you can click on any one value within a row and automatically have the option to **Add to Search**. This automatically applies the selected value to the search bar at the top of the window and filteres the viewing window to the content in the search bar. You can do this multiple times and the values you select compound into a complex search request.

- Network Intrusion, on page 180
- Web Protection, on page 180
- Malicious Sources, on page 181

Network Intrusion

Network intrusion refers to any unauthorized activity on your network. Note that this tabl does not include the built-in rules to the IDS/IPS engine or any affiliated information from these rules; these rules are designated for detection only; the remainder of the IDS/IPS rules are configured to protect and perform actions based on the varying levels of intrusion or attack.

The Network Intrusion page displays the following:

- **Gateway Names** - the names of the affected gateways that processed the malicious source.
- **Profile Names** - the names of the security profiles triggered by the malicious source.
- **IPS Policy** - the policy within Multicloud Defense triggered by the event or attack.
- **IPS Class** - the type of attack as deteremined by the database of attack signatures traffic is compared against.
- **IPS Category** - the IPS signature category triggered by the event or attack.
- **Rule ID** - the rule ID as documented internally within Multicloud Defense that was triggered by the event or attack.
- **Services Impacted** - the type of web service affected by the event or attack.
- **Impact** - the severity level of impact, known or assumed, by the event or attack.
- **Message** - the contents of the event that has been identified as an attack.
- **Rule Content** - content of the rule triggered by the event or attack.
- **CVSS Score** - Common Vulnerability Scoring System (CVSS) is a framework that assigns a numerical score to the severity of an information security vulnerability. CVSS scores range from 0 to 10, with 10 being the most severe.
- **CVEs** - Common Vulnerabilities and Exposures (CVE) is a glossary that classifies vulnerabilities. Is there is a CVE associated with the type of attack or event, the internal library automatically generates its value here.
- **References** - If publicly available, this link directs you to the original announcement and categorization of the CVE.

Web Protection

The Web Application Firewall (WAF) research is displayed as "Web Protection" This lets you secure your devices against web threats and helps you regulate unwanted content. The Web Protection page displays the following:

- **Gateway Names** - the names of the affected gateways that processed the malicious source.
- **Profile Names** - the names of the security profiles triggered by the malicious source.
- **CRS Category** - the Core Rule Set (CRS) category identified per set of generic attack detection rules.

- **Inspection Type** - the type of inspection Multicloud Defense peformed on the traffic that encapsulated the attack or event.
- **Attack Type** - the type of unauthorized attack traversed over a network.
- **Platform** - the platform type identified from the attack or event.
- **Lanuage** - the noted web developtment language detected from the event.

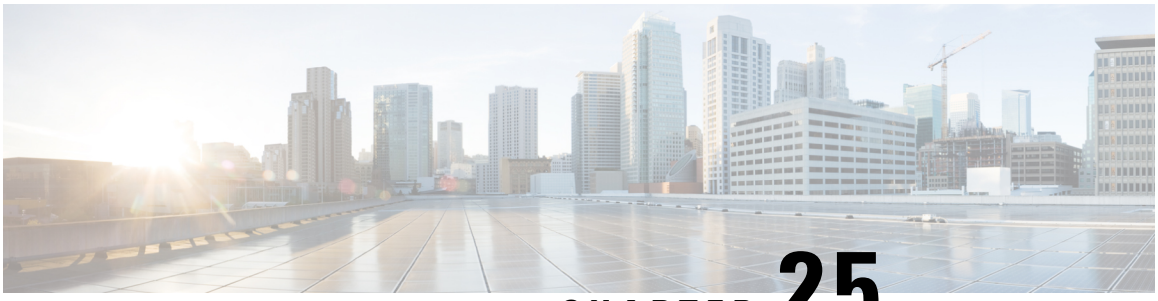
Malicious Sources

Malicious sources are any type of code or packet that causes harm to a network. The Malicious Sources page dispalys the following:

- **Gateway Names** - the names of the affected gateways that processed the malicious source.
- **Profile Names** - the names of the security profiles triggered by the malicious source.
- **Malicious Sources Action** - the action taken when the malicious source was identified.
- **Impact** - the impact of the malicious material deteremined by how it is ranked within the library.
- **Malicious Source IP** - the IP address where the malicious source originates from.

PART XI

Cloud Visibility Reports



CHAPTER 25

Cloud Visibility Reports

Reports provide valuable statistical information that you can use as insight to the network and its genereal health, and make decisions accordingly. Multicloud Defense provides the ability to generate the following types of reports:

Discovery

The Generate a Discovery Report is generated by taking out-of-band traffic information from DNS queries and VPC flow logs, and correlating the data with threat intelligence and cloud inventory information. These logs are only available if you configure the VPC of your cloud service provider to send logs to an S3 bucket, which are then transferred directly to the Multicloud Defense Controller.

Threat Indicators Snapshot

The Generate a Threat And Cloud Analytics Report report is a compilation of data on the gateway instance. You can use this report to determine the gateway's endurance under duress by examining traffic patterns, when and how thresholds are met, trends of attacks, and specific instances. The report includes the following points:

- **IDS/IPS Detection** - This data is how many attacks detected, the type of attack, the time of the detected attacks, and the top ten IDS/IPS signatures over the time range selected.
- **WAF Detection** - This data is how many attacks detected by WAF rule(s), the time of the detected attacks, and the top ten WAF signatures over the time range selected.
- **Gelocation of Threats by Volume** - This choropleth map that shows the volume of attacks for both WAF and IDS/IPS events by country in volume.
- **Top Ten Attacking Countries by Volume and Time** - This horizontal bar chart depicts the volume of the top 10 countries that during the entirety of the timespan produced the most events, then displayed breaking that volume across the time increments for which the events occurred during the timespan.
- **Policy and Prevention** - This data chart shows the action taken by the gateway security type in whichever CSP environment it is deployed in. This includes the type of action, how many events generated from the action, the gateway security type and more.

Note that you **must** have Web Application Firewall (WAF), intrusion detection and protention (IDS/IPS) rules enabled in your policy in order for the Multicloud Defense Gateway to collect and poll data.

For Additional Information:

- Generate a Discovery Report, on page 186

• Generate a Threat And Cloud Analytics Report, on page 186

Generate a Discovery Report

A discovery report is generated by taking DNS queries and VPC flow logs that have been sent to an S3 bucket prior to getting processed by the Multicloud Defense Controller.

Use the following procedure to generate a Discovery Report:

Step 1 In the Multicloud Defense Controller page, navigate to **Reporting**.

Step 2 Select **Discovery**.

Step 3 Click on the **Generate** button. The report is generated in a new tab.

Step 4 The report is generated. To save the report locally, click **Print Report** and navigate to where you want the report saved on your local server.

Generate a Threat And Cloud Analytics Report

The Threat and Cloud Analytics Report is a **Threat Indicator Snapshot** that is generated by using the traffic collected and inspected by Multicloud Defense Gateway. This provides a more comprehensive report as Multicloud Defense is now in the datapath and compliments the discovery report.

Note that reports cannot be generated for the day of, since a qualitative summarization of events cannot be made until end of day, end of month, end of quarter, or end of year.

Note You **must** have Web Application Firewall (WAF), intrusion detection and protection (IDS/IPS) rules enabled in your policy in order for the Multicloud Defense Gateway to collect and poll data. For more information, see the following links respecitvely:

- Web Application Firewall (WAF) Profile
- Network Intrusion (IDS/IPS) Profile, on page 125

Use the following procedure to generate a Threat And Cloud Analytics with the threat indicators snapshot:

Step 1 In the Multicloud Defense Controller page, navigate to **Reporting**.

Step 2 Select **Threat Indicators Snapshot**.

Step 3 Use the drop-down menu to select the **Frequency** the data is pulled: daily, weekly, monthly, quarterly, or yearly.

- **Daily** - From 12AM for 24 hours. This is in UTC time.
- **Weekly** - From Monday to Sunday.
- **Monthly** - Generally from the beginning to the end of the month.

- **Quarterly** - From the beginning to end of a quart. Quarters are generally defined as from January 1 - March 31, April 1 - June 30, July 1 - September 30, and October 1 - December 31.
- **Yearly** - From January 1 to December 31 of the year selected.

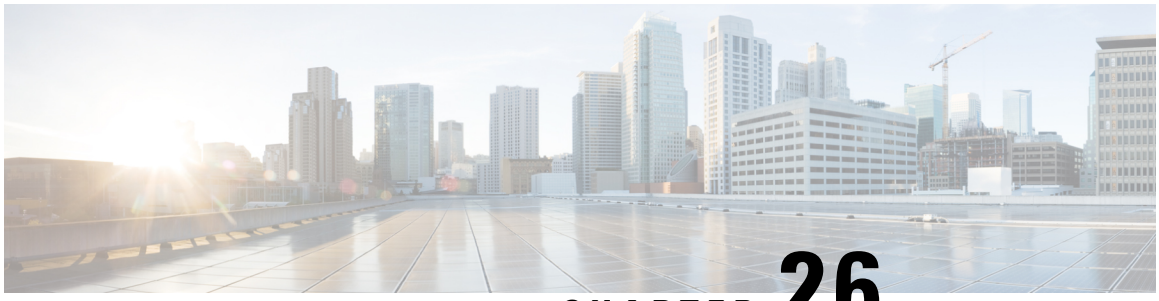
Step 4 Use the drop-down **Calendar** to select the time range, or specific days, that you want to collect data on. Days that are grayed out have no data to compile. If you have no data available to generated a report, confirm your policies contain WAF and IDS/IPS rules.

Step 5 Click **Generate Report**.

Step 6 The report is generated. To save the report locally, click **Print Report** and navigate to where you want the report saved on your local server.

PART XII

Alerting, Log Forwarding, and Reports



CHAPTER 26

Alerting Overview

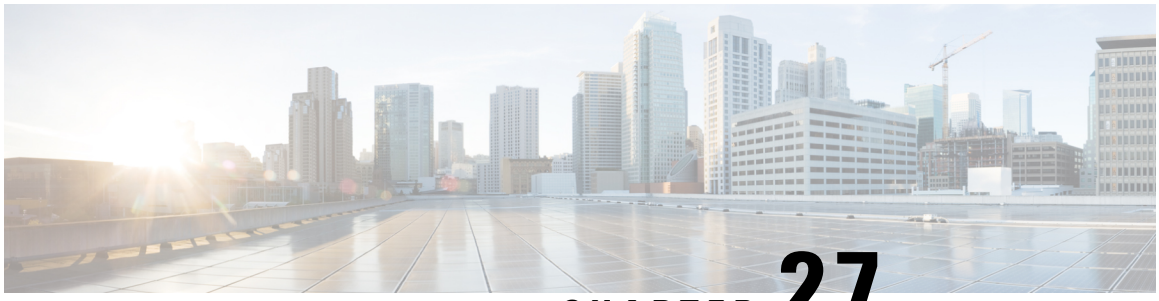
Alert Services Overview

To integrate with widely deployed alerting services, Multicloud Defense integrates with Microsoft Sentinel, PagerDuty, ServiceNow and Slack to forward critical system level alerts. This enables cloud operations teams to be alerted, and respond to, user-defined system events and severity levels detected by the Multicloud Defense Cloud Controller. This is accomplished within Multicloud Defense Controller using an Alert Service Profile, together with an Alert Rule, for a given integration.

To configure integrations with supported alerting services, navigate to: **Administration** > **Alert Profiles** > **Services**

Integration with these services require either an API URL, API key, or both. Generally, the API Keys and URLs need to be generated by your Organization's Administrator of these services.

Note For ServiceNow integrations, a Webhook must be configured to enable ServiceNow to receive and display alerts from the Multicloud Defense Controller.



CHAPTER 27

Alert Destinations / SIEMs

Datadog Integration

Once configured, Multicloud Defense alerts will sent to Datadog using the defined Alert Service Profile and Alert Rule.

Create an Alert Profile Service

Before you begin

In order to send alerts to Datadog, the following information is required:

- Datadog account
- API Key

Tip

- To Sign up for a Datadog account, refer to Datadog Account (https://www.datadoghq.com/).
- To create a Datadog API Key, refer to Datadog API Key (https://app.datadoghq.com/account/login?next=%2Faccount%2Fsettings#api).

Step 1 Navigate to **Administration** > **Alert Profiles** > **Services**.

Step 2 Click **Create**.

Step 3 **Name** - Enter unique name for the alert integration. Example `multicloud defense-Datadog-profile`.

Step 4 **Description** (optional) - Enter a description for the alert integration.

Step 5 **Type** - Using the pulldown, choose **Datadog**.

Step 6 **API Key** - Specify the Datadog API Key used to authenticate the communication.

Step 7 Click **Save**.

What to do next

Create an alert rule with this new profile.

Create an Alert Rule

Before you begin

In order to send alerts to Datadog, the following information is required:

- Datadog account
- API Key

Tip

- To Sign up for a Datadog account, refer to Datadog Account (https://www.datadoghq.com/).
- To create a Datadog API Key, refer to Datadog API Key (https://app.datadoghq.com/account/login?next=%2Faccount%2Fsettings#api).

Step 1 Navigate to **Settings** > **Alert Profiles** > **Alert Rules**.

Step 2 Click **Create**.

Step 3 **Profile Name** - Enter unique name for the integration. Example `multicloud defense-Datadog-alert-rule`.

Step 4 **Description** (optional) - Enter a description for the alert rule.

Step 5 **Alert Profile** - Using the pulldown, choose a PagerDuty Alert Profile. As example, select profile created above `multicloud defense-Datadog-profile`.

Step 6 **Type** - Using the pulldown, select either **System Logs** or **Discovery**.

Step 7 **Sub Type** - For Type **System Logs**, the Sub Type pulldown options are either: **Gateway** or **Account**. For Type **Discovery**, the Sub Type pulldown optionis: **Insights Rule**.

Step 8 **Severity** - For selected Type **System Logs**, and using the pulldown, select a Severity level from options: `Info Warning Medium High` or `Critical`. For Type **Discovery**, select a Severity level from options: `Info Medium Critical`.

Step 9 **Enabled** - Using the checkbox, check to enable this alert profile.

Step 10 Click **Save**.

Microsoft Sentinel Integration

Once configured, Multicloud Defense alerts will sent to Microsoft Sentinel using the defined Alert Service Profile and Alert Rule.

Create an Alert Profile Service

Before you begin

In order to send alerts to Microsoft Sentinel, the following information is required:

- Create an Azure Log Analytics Workspace.
- Define an Azure Log Table.

Step 1 Navigate to **Administration** > **Alert Profiles** > **Services**.
Step 2 Click **Create**.
Step 3 **Name** - Enter unique name for the alert integration. Example `mcd-mssentinel-profile`.
Step 4 **Description** (optional) - Enter a description for the alert integration.
Step 5 **Type** - Using the pulldown, choose **Microsoft Sentinel**.
Step 6 **API Key** - Specify the Shared Key created in Azure for the Azure Log Analytics Workspace.
Step 7 **Azure Log Table Name** - Specify the name of the Azure Log defined when creating the Azure Log Analytics Workspace.
Step 8 **Azure Log Analytics Workspace ID** - Specify the ID of the Azure Log Analytics Workspace.
Step 9 Click **Save**.

What to do next

Create an alert rule with this new profile.

Create an Alert Rule

Before you begin

In order to send alerts to Microsoft Sentinel, the following information is required:

- Create an Azure Log Analytics Workspace.
- Define an Azure Log Table.

Step 1 Navigate to **Settings** > **Alert Profiles** > **Alert Rules**.
Step 2 Click **Create**.
Step 3 **Profile Name** - Enter unique name for the integration. Example `mcd-mssentinel-alert-rule`.
Step 4 **Description** (optional) - Enter a description for the alert rule.

Step 5 **Alert Profile** - Using the pulldown, choose a PagerDuty Alert Profile. As example, select profile created above `mcd-mssentinel-profile`.

Step 6 **Type** - Using the pulldown, select either **System Logs** or **Discovery**.

Step 7 **Sub Type** - For Type **System Logs**, the Sub Type pulldown options are either: **Gateway** or **Account**. For Type **Discovery**, the Sub Type pulldown optionis: **Insights Rule**.

Step 8 **Severity** - For selected Type **System Logs**, and using the pulldown, select a Severity level from options: `Info Warning Medium High` or `Critical`. For Type **Discovery**, select a Severity level from options: `Info Medium Critical`.

Step 9 **Enabled** - Using the checkbox, check to enable this alert profile.

Step 10 Click **Save**.

PagerDuty Integration

Once configured, Multicloud Defense alerts will sent to a PagerDuty API gateway using the defined Alert Service Profile and Alert Rule.

Create an Alert Profile Service

Before you begin

In order to complete the steps in this guide, you will need:

- A PagerDuty account with an API Key configured.

Tip

- Sign up for a PagerDuty account (https://www.servicenow.com/my-account/sign-up.html).
- Setup the API Key (https://developer.pagerduty.com/api-reference).

Step 1 Navigate to **Administration** > **Alert Profiles** > **Services**.

Step 2 Click **Create**.

Step 3 **Name** - Enter unique name for the alert integration. Example `mcd-pagerduty-profile`.

Step 4 **Description** (optional) - Enter a description for the alert integration.

Step 5 **Type** - Using the pulldown, choose **PagerDuty**.

Step 6 **API Key** - Copy the PagerDuty API key generated above, or other PagerDuty API Key as desired.

Step 7 Click **Save**.

What to do next

Create an alert rule with this new profile.

Create an Alert Rule

Before you begin

In order to complete the steps in this guide, you will need:

A PagerDuty account with an API Key configured.

Tip

- Sign up for a PagerDuty account (https://www.servicenow.com/my-account/sign-up.html).
- Setup the API Key (https://developer.pagerduty.com/api-reference).

Step 1 Navigate to **AdministrationAlert ProfilesAlert Rules**.

Step 2 Click **Create**.

Step 3 **Profile Name** - Enter unique name for the integration. Example `mcd-pagerduty-alert-rule`.

Step 4 **Description** (optional) - Enter a description for the alert rule.

Step 5 **Alert Profile** - Using the pulldown, choose a PagerDuty Alert Profile. As example, select profile created above `mcd-pagerduty-profile`.

Step 6 **Type** - Using the pulldown, select either **System Logs** or **Discovery**.

Step 7 **Sub Type** - For Type **System Logs**, the Sub Type pulldown options are either: **Gateway** or **Account**. For Type **Discovery**, the Sub Type pulldown optionis: **Insights Rule**.

Step 8 **Severity** - For selected Type **System Logs**, and using the pulldown, select a Severity level from options: `Info Warning Medium High or Critical`. For Type **Discovery**, select a Severity level from options: `Info Medium Critical`.

Step 9 **Enabled** - Using the checkbox, check to enable this alert profile.

Step 10 Click **Save**.

ServiceNow Integration

Once configured, Multicloud Defense alerts will sent to a ServiceNow API gateway using the defined Alert Service Profile and Alert Rule.

Create an Alert Profile Service

Before you begin

In order to complete the steps in this guide, you will need:

- A ServiceNow account with an Incoming Webhook URL.
- API Key configured.

Tip

- Sign up for a ServiceNow account (https://www.servicenow.com/my-account/sign-up.html)
- Setup Webhook and API Key (https://docs.servicenow.com/search?q=setup%20webhook)

Step 1 Navigate to **Administration** > **Alert Profiles** > **Services**.
Step 2 Click **Create**.
Step 3 **Name** - Enter unique name for the alert integration. Example `mcd-servicenow-profile`.
Step 4 **Description** (optional) - Enter a description for the alert integration.
Step 5 **Type** - Using the pulldown, choose **ServiceNow**.
Step 6 **API Key** - Specify the ServiceNow API key generated above, or other ServiceNow API Key as desired.
Step 7 **API URL** - Specify the ServiceNow Webhook URL generated above, or other ServiceNow Webhook URL as desired.
Step 8 Click **Save**.

What to do next

Create an alert rule with this new profile.

Create an Alert Rule

Before you begin

In order to complete the steps in this guide, you will need:

- A ServiceNow account with an Incoming Webhook URL.
- An API Key configured.

Tip

- Sign up for a ServiceNow account (https://www.servicenow.com/my-account/sign-up.html)
- Setup Webhook and API Key (https://docs.servicenow.com/search?q=setup%20webhook)

Step 1 Navigate to **Administration** > **Alert Profiles** > **Alert Rules**.
Step 2 Click **Create**.
Step 3 **Profile Name** - Enter unique name for the integration. Example `mcd-servicenow-alert-rule`.
Step 4 **Description** (optional) - Enter a description for the alert rule.
Step 5 **Alert Profile** - Using the pulldown, choose a ServiceNow Alert Profile. As example, select profile created above `mcd-servicenow-profile`.
Step 6 **Type** - Using the pulldown, select either **System Logs** or **Discovery**.
Step 7 Select the **Sub Type**.

- For Type **System Logs**, the options are either **Gateway** or **Account**.
- For Type **Discovery**, the only option is **Insights Rule**.

Step 8 Select the **Severity**.

- For selected Type **System Logs**, and using the pulldown, select a Severity level from options: **Info Warning Medium High or Critical**.
- For Type **Discovery**, select **Info Medium Critical**.

Step 9 **Enabled** - Using the checkbox, check to enable this alert profile.

Step 10 Click **Save**.

Slack Integration

Once configured, Multicloud Defense alerts will sent to a Slack Incoming Webhook URL using the defined Alert Service Profile and Rule.

Create an Alert Profile Service

Before you begin

In order to complete the steps in this guide, you will need:

- A Slack account with an incoming webhook URL configured.

Tip

1. Create a Slack account (https://slack.com/get-started#/create).
2. Create an incoming Webhook (https://slack.com/help/articles/115005265063-Incoming-webhooks-for-Slack#set-up-incoming-webhooks).

Step 1 Navigate to **Administration** > **Alert Profiles** > **Services**.

Step 2 Click **Create**.

Step 3 **Name** - Enter unique name for the alert integration. Example `mcd-slack-profile`.

Step 4 **Description** (optional) - Enter a description for the alert integration.

Step 5 **Type** - Using the pulldown, choose **Slack**.

Step 6 **API URL** - Specify the Slack Webhook URL generated above, or other Slack Webhook URL as desired.

What to do next

Create an alert rule with this new profile.

Create an Alert Rule

Before you begin

In order to complete the steps in this guide, you will need:

A Slack account with an Incoming Webhook URL configured.

Tip

1. Create a Slack account (https://slack.com/get-started#/create).
2. Create an incoming Webhook (https://slack.com/help/articles/115005265063-Incoming-webhooks-for-Slack#set-up-incoming-webhooks).

Step 1 Navigate to **Administration** > **Alert Profiles** > **Alert Rules**.

Step 2 Click **Create**.

Step 3 **Profile Name** - Enter unique name for the integration. Example `mcd-slack-alert-rule`.

Step 4 **Description** (optional) - Enter a description for the aler trule.

Step 5 **Alert Profile** - Using the pulldown, choose a Slack Alert Profile. As example, select profile created above `mcd-slack-profile`.

Step 6 **Type** - Using the pulldown, select either **System Logs** or **Discovery**.

Step 7 **Sub Type** - For Type **System Logs**, the Sub Type pulldown options are either: **Gateway** or **Account**. For Type **Discovery**, the Sub Type pulldown optionis: **Insights Rule**.

Step 8 **Severity** - For selected Type **System Logs**, and using the pulldown, select a Severity level from options: `Info Warning Medium High or Critical`. For Type **Discovery**, select a Severity level from options: `Info Medium Critical`.

Step 9 **Enabled** - Using the checkbox, check to enable this alert profile.

Step 10 Click **Save**.

Webex Integration

Once configured, Multicloud Defense alerts will sent to a Webex API gateway using the defined Alert Service Profile and Alert Rule.

Create an Alert Profile Service

Before you begin

In order to complete the steps in this guide, you will need:

- A Webex account with an Incoming Webhook URL.
- API Key configured.

Note

1. Create or access a Webex account.
2. Create a Webex Incoming Webhook.
3. Accept the Incoming Webhook permissions.
4. Provide a Name and select a Webex Space.
5. Copy the Webex Webhook URL to use in the configuration of the Alert Service Profile.

Step 1 Navigate to **Administration** > **Alert Profiles** > **Services**.

Step 2 Click **Create**.

Step 3 **Name** - Enter unique name for the alert integration. An example would be `mcd-servicenow-profile`.

Step 4 (Optional) **Description** - Enter a description for the alert integration.

Step 5 **Type** - Using the pulldown, choose **Webex**.

Step 6 **API URL** - Specify the Webex Webhook URL generated as part of the prerequisites, or other Webex Webhook URL as desired.

What to do next

Create an alert rule with this new profile.

Create an Alert Rule

Step 1 Navigate to **Administration** > **Alert Profiles** > **Alert Rules**.

Step 2 Click **Create**.

Step 3 **Profile Name** - Enter unique name for the integration. An example is `mcd-servicenow-alert-rule`.

Step 4 (Optional) **Description** - Enter a description for the alert rule.

Step 5 **Alert Profile** - Using the pulldown, choose a **Webex Alert Profile**. As example, select profile created above mcd-servicenow-profile.

Step 6 **Type** - Using the pulldown, select either **System Logs** or **Discovery**.

Step 7 Select the **Sub Type**.

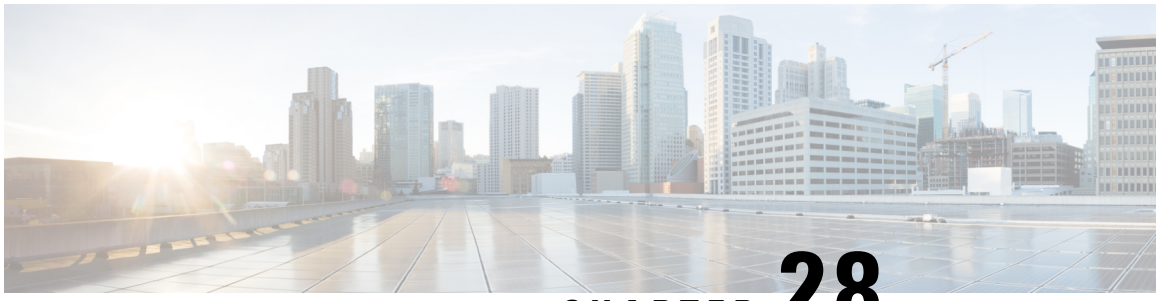
- For Type System Logs, the options are either **Gateway** or **Account**.
- For Type Discovery, the only option is **Insights Rule**.

Step 8 Se;ect the **Severity**.

- For selected Type System Logs, and using the pulldown, select either **Info Warning Medium High** or **Critical**.
- For Type Discovery, select **Info Medium Critical**.

Step 9 **Enabled** - Using the checkbox, check to enable this alert profile.

Step 10 Click **Save**.



CHAPTER 28

Log Forwarding Overview

Log Forwarding - Security Events and Traffic Logs

Security Information Event Management (SIEM) systems are solutions that specialize in combining security information and security event information together into a single management platform. The security and event information will originate from 3rd party security solutions that are configured to forward this information to the SIEM.

Multicloud Defense supports viewing security event information directly within the UI. These events are available under the **Investigate** > **Flow Analytics** section. The events are categorized and viewable as follows:

Category	Type	Description
Flow Logs	FLOW_LOG	Information related to the different stages of a traffic flow
Firewall Events	APPID	Traffic matched based on Application ID (OpenAppID)
	GEOIP	Traffic sourced from or destined to a Geo IP (MaxMind)
	L4_FW	Traffic matched based on layer4 information (Source/Dest IP/Port and Protocol)
	MALICIOUS_IP	Traffic sourced from or destined to a malicious IP (Trustwave)
	SNI	Traffic matched based on SNI information

Category	Type	Description
Network Threats	AV	Traffic where a virus has been detected (ClamAV)
	DPI	Traffic where an IDS/IPS threat has been detected (TALOS)
	DLP	Traffic where sensitive data is being exfiltration
Web Protection	WAF	Traffic where a web application threat has been detected (ModSecurity)
	L7DOS	Traffic that is contributing to a layer7 DOS attack
URL Filtering	URLFILTER	Traffic that matches a URL category or URL (BrightCloud)
FQDN Filtering	FQDNFILTER	Traffic that matches a FQDN category or FQDN (BrightCloud)
HTTPS Logs	HTTP_REQUEST	Information related to web-based traffic (HTTP)
	TLS_ERROR	Information related to TLS errors
	TLS_LOG	Information related to TLS behavior
Traffic Summary Logs	SESSION_SUMMARY	Summary information on each processed traffic session

Note Flow Logs are deprecated in 2.10 and later gateway releases. The information contained within each flow Log is made available as part of the session information available in **Traffic Summary** > **Logs**.

Each of the event categories can be sent to a SIEM using a log forwarding profile. The SIEMs currently supported by Multicloud Defense are:

- Log Forwarding - AWS S3 Bucket
- Log Forwarding - Datadog
- Log Forwarding - GCP Logging
- Log Forwarding - Microsoft Sentinel
- Log Forwarding - Splunk
- Log Forwarding - Sumo Logic
- Log Forwarding - Syslog

A log forwarding profile can be operated on using the steps outlined below:

Create a Standalone Event or Traffic Log Profile

Step 1 Navigate to **Manage** > **Profiles** > **Log Forwarding**.
Step 2 Click **Create**.
Step 3 Specify a Profile Name and Description.
Step 4 Specify *Type* as Standalone.
Step 5 Fill in the appropriate parameters (refer to the SIEM-specific documentation).
Step 6 Click **Save**.
Step 7 Add the desired Gateway Associations (refer to Add an Event, Traffic Log Forwarding Profile, or Metrics Forward Profile to a Gateway).

Edit a Standalone Event or Traffic Log Profile

Step 1 Navigate to **Manage** > **Profiles** > **Log Forwarding**.
Step 2 Check the box next to the Profile you want to *Edit*.
Step 3 Click **Edit**.
Step 4 Modify the parameters as desired (refer to the SIEM-specific documentation).
Step 5 Click **Save**.

Create a Group Event or Traffc Log Profile

Step 1 Navigate to **Manage** > **Profiles** > **Log Forwarding**.
Step 2 Click **Create**.
Step 3 Specify a Profile Name and Description.
Step 4 Specify *Type* as Group.
Step 5 Add as many rows as needed to accommodate for the number of standalone profiles you want to group.
Step 6 Click **Save**.
Step 7 Add the desired **gateway associations** (refer to Add an Event, Traffic Log Forwarding Profile, or Metrics Forward Profile to a Gateway).

Edit a Group Event or Traffc Log Profile

Step 1 Navigate to **Manage** > **Profiles** > **Log Forwarding**.
Step 2 Check the box next to the Profile you want to *Edit*.

Step 3 Click **Edit**.
Step 4 Modify, Add or Remove Standalone Profiles.
Step 5 Click **Save**.

View an Event or Traffic Log Forwarding Profile

Step 1 Navigate to **Manage** > **Profiles** > **Log Forwarding**.
Step 2 Select the Profile link you want to view the *Details*.
Step 3 View the *Details* information.

Delete an Event or Traffc Log Profile

Use the following procedure to delete the profile from your dashboard:

Before you begin

You **must** remove the association between the event or profile and the gateway before you delete the profile from your dashboard. See Remove an Event, Traffic Log Forwarding Profile, or Metrics Forward Profile from a Gateway for more information.

Step 1 Navigate to **Manage** > **Profiles** > **Log Forwarding**.
Step 2 Check the box next to the Profile you want to *Delete*.
Step 3 Click **Delete**.
Step 4 Confirm the *Delete* operation by clicking **Yes** or **No**.

Gateway Metrics Forwarding Profile

This profile is intended to forward gateway metrics generated by the Multicloud Defense Gateway for data monitoring and analysis.While the metrics are generated by the gateway, it is the Multicloud Defense Controller that forwards the metrics to the third party analysis application. With this forwarding profile you are able to monitor, analyze, and organize your gateway metrics without logging into Multicloud Defense. Use this information to gauge the performance and behavior of your gateway environment; you can also utilize this information for environmental troubleshooting.

Note As of Multicloud Defense Controller version 23.09, only Datadog is supported as a third party analytics application.

For the majority of analytics applications available, for example, Datadog, you must already be an authorized user to access the tool's APIs and rendered data.

Create a Standalone Metrics Forwarding Profile

Use the following procedure to create a standalone profile and forward metrics to be processed by a third party:

Before you begin

You must have at least one third party application to forward the metric to prior to creating this profile.

Step 1 Navigate to **Manager** > **Profiles** > **Metrics Forwarding**.

Step 2 Click **Create**.

Step 3 Enter a unique profile **Name**.

Step 4 (Optional) Enter a **Description**. This may help differentiate from other profiles with a similar name.

Step 5 Expand the **Type** drop-down menu and select **Standalone**.

Step 6 Expand the **Destination** drop-down menu and select the third-party application to process and analyze the metrics.

Step 7 Enter the **Endpoint** to be used as the endpoint location for the metrics.

Step 8 Click **Save**.

If you select Datadog as your analyitics application, the **Endpoint** is filled in by default with an HTTPs webhook. This entry, if defaulted, can be modified prior to saving the profile.

What to do next

- View a Profile Details, on page 145
- Add a Gateway Association to a Profile, on page 146

Edit a Standalone Metrics Forwarding Profile

Use the following procedure to edit a standalone profile that has already been created.

Step 1 Navigate to **Manage** > **Profiles** and select the appropriate profile **Type**.

Step 2 Check the box next to the profile you want to edit.

Step 3 Click **Edit**.

Step 4 Modify the parameters as desired.

Step 5 Click **Save**.

Create a Group Metrics Forwarding Profile

In this process, you create a profile and then assign it to a specific gateway. A group profile combines up to five standalone metrics forwarding profile that can then be assigned to a single gateway. Use the following procedure to create a grouped metrics forward profile:

Before you begin

- You must have at least one third party application to forward the metric to prior to creating this profile.
- You must have at least two standalone metrics forwarding profiles already created. See Create a Standalone Metrics Forwarding Profile, on page 142 for more information.

Step 1 In the Multicloud Defense Controller interface navigate to **Manager** > **Profiles** > **Metrics Forwarding**.
Step 2 Click **Create**.
Step 3 Enter a unique **Profile Name**
Step 4 (Optional) Enter a **Description**. This may help differentiate between profiles with a similar name.
Step 5 Expand the **Type** drop-down menu and select **Group**.
Step 6 Under **Group Details**, click **Add** for every new row you need to add to the profile.
Step 7 Expand the drop-down menus for each row to select a profile to add to the group. If you want to remove a profile at any point prior to saving, select the profile's checkbox so it is highlighted and select **Remove**.
Step 8 Click **Save**.

What to do next

- View a Profile Details, on page 145
- Add a Gateway Association to a Profile, on page 146

Edit a Group Profile

Use the following procedure to edit a set of grouped profiles that has already been created:

Step 1 Navigate to **Manage** > **Profiles** and select the appropriate profile **Type**.
Step 2 Check the box next to the profile you want to *Edit*.
Step 3 Click **Edit**.
Step 4 Modify, add or remove group profiles.
Step 5 Click **Save**.

Delete a Profile

Use the following procedure to delete the profile from your dashboard:

Before you begin

You **must** remove the association between the profile and the gateway before you delete the profile from your dashboard. See Remove an Event, Traffic Log Forwarding Profile, or Metrics Forward Profile from a Gateway for more information.

Step 1 Navigate to **Manage** > **Profiles** and select the appropriate profile **Type**.
Step 2 Check the box next to the profile you want to delete.
Step 3 Click **Delete**.
Step 4 Click **Yes** or **No** to either confirm or cancel the delete action.

Add an Event, Traffic Log Forwarding Profile, or Metrics Forward Profile to a Gateway

Step 1 Navigate to **Manage** > **Gateways**.
Step 2 Check the box next the gateway you want to associate the *Profile*.
Step 3 Click **Edit**.
Step 4 For the *Log Profile* parameter, select the desired *Profile* from the menu.
Step 5 Click **Save**.

Remove an Event, Traffic Log Forwarding Profile, or Metrics Forward Profile from a Gateway

Step 1 Navigate to **Manage** > **Gateways**.
Step 2 Check the box next the gateway you want to de-associate the *Profile*.
Step 3 Click **Edit**.
Step 4 For the *Log Profile* parameter, click the 'X' next to the *Profile* to remove it.
Step 5 Click **Save**.

Note A Log Forwarding Profile can also be associated with a gateway at time of gateway creation. The *Log Profile* parameter is available during the gateway creation process, where the desired *Profile* can be selected from the menu.

Log Forwarding - Discovery Logs

Discovery logs may be forwarded to Security Information Event Management (SIEM) systems to aggregate into a single management platform.

Multicloud Defense supports viewing security event information directly within the UI. These events are available under the **Investigate** > **Traffic** section. The events are categorized and viewable as follows:

Category	Type	Description
DNS Logs	DNS_LOG	Correlation of Threat Intelligence with DNS Log information gathered from cloud provider
VPC Logs	VPC_LOG	Correlation of Threat Intelligence with VPC/VNet Flow Log information gathered from cloud provider

Each of the categories can be sent to a SIEM using a Log Forwarding Profile and attaching the Profile to the onboarded Cloud Account. The Log Forwarding destinations currently supported by Multicloud Defense are:

- Log Forwarding - AWS S3 Bucket
- Log Forwarding - Datadog
- Log Forwarding - GCP Logging
- Log Forwarding - Microsoft Sentinel
- Log Forwarding - Splunk
- Log Forwarding - Sumo Logic
- Log Forwarding - Syslog

To forward Discovery Logs, use the steps below:

Create a Standalone Discovery Log Profile

Step 1 Navigate to **Manage** > **Profiles** > **Log Forwarding**.
Step 2 Click **Create**.
Step 3 Specify a Profile Name and Description.
Step 4 Specify *Type* as Standalone.
Step 5 Fill in the appropriate parameters (refer to the SIEM-specific documentation).
Step 6 Click **Save**.
Step 7 Associate the Log Profile to the desired Cloud Accounts (refer to Add a Discovery Log Profile with a Cloud Account).

Edit a Standalone Discovery Log Profile

Step 1 Navigate to **Manage** > **Profiles** > **Log Forwarding**.
Step 2 Check the box next to the profile you want to *Edit*.
Step 3 Click **Edit**.
Step 4 Modify the parameters as desired (refer to the SIEM-specific documentation).
Step 5 Click **Save**.

Create a Group Discovery Log Profile

Step 1 Navigate to **Manage** > **Profiles** > **Log Forwarding**.
Step 2 Click **Create**.
Step 3 Specify a Profile Name and Description.
Step 4 Specify *Type* as Group.
Step 5 Add a row for to associate a Standalone Profile.
Step 6 Click **Save**.
Step 7 Add the desired Gateway Associations (refer to Add an Event, Traffic Log Forwarding Profile, or Metrics Forward Profile to a Gateway).

Edit a Group Discovery Log Profile

Step 1 Navigate to **Manage** > **Profiles** > **Log Forwarding**.
Step 2 Check the box next to the Profile you want to *Edit*.
Step 3 Click **Edit**.
Step 4 Modify, Add or Remove Standalone Profiles.
Step 5 Click **Save**.

View a Discovery Log Profile Details

Step 1 Navigate to **Manage** > **Profiles** > **Log Forwarding**.
Step 2 Select the Profile link you want to view the *Details*.
Step 3 View the *Details* information.

Add a Discovery Log Profile with a Cloud Account

Step 1 Navigate to **Manage** > **Cloud Accounts** > **Accounts**.
Step 2 Check the box next the cloud account you want to associate the *Profile*.
Step 3 Click **Actions** > **Update Log Profile**.
Step 4 Select the **Log Profile** object for cloud logs forwarding profile.
Step 5 Click **Save & Continue**.

Remove a Discovery Log Profile from a Cloud Account

Step 1 Navigate to **Manage** > **Cloud Accounts** > **Accounts**.
Step 2 Check the box next the Cloud Account you want to disassociate the *Profile*.
Step 3 Click **Actions** > **Update Log Profile**.
Step 4 For the *Cloud Logs Forwarding Profile* parameter, click the 'X' next to the *Profile* to remove it.
Step 5 Click **Save & Continue**.

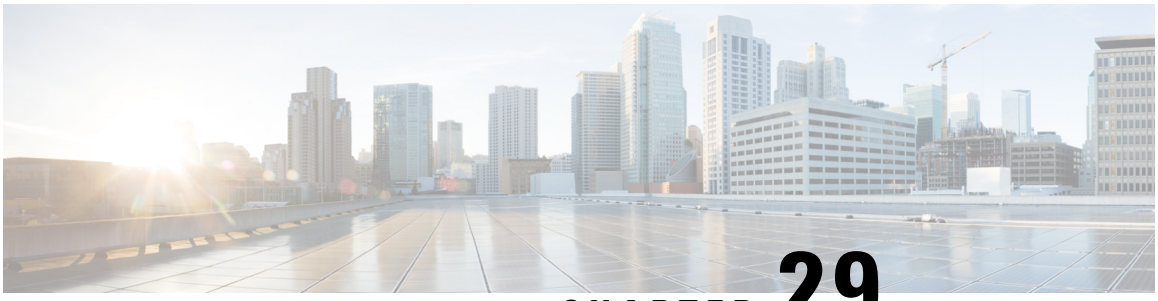
Delete a Discovery Log Profile

Use the following procedure to delete the profile from your dashboard:

Before you begin

You **must** remove the association between the profile and the gateway before you delete the profile from your dashboard. See Remove a Discovery Log Profile from a Cloud Account for more information.

Step 1 Navigate to **Manage** > **Profiles** > **Log Forwarding**.
Step 2 Check the box next to the Profile you want to *Delete*.
Step 3 Click **Delete**.
Step 4 Confirm the *Delete* operation by clicking **Yes** or **No**.



CHAPTER 29

Log Forwarding Destinations / SIEMs

Log Forwarding - AWS S3 Bucket

Multicloud Defense supports forwarding Security Events and Traffic Logs to an AWS S3 Bucket to send Security Events and Traffic Log information for processing, storage, access and correlation. The information sent is in a semi- structured JSON format where the attribute-value pairs can be accessed and processed.

Requirements

In order to forward Events/Logs to the AWS S3 Bucket, the following is required:

1. Create a new or use an existing AWS S3 Bucket.
2. Apply the following policy to the AWS S3 Bucket to permit the Multicloud Defense Controller to access and write to the bucket:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "<controller-role-arn>"
      },
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::<s3bucketname>/*",
        "arn:aws:s3:::<s3bucketname>"
      ]
    }
  ]
}
```

Profile Parameters

Parameter	Deonticity	Default	Description
Profile Name	Required		A unique name to use to reference the Profile.
Description	Optional		A description for the Profile.
Destination	Required	AWS S3	AWS S3 Bucket.
CSP Account	Required		The CSP Account where the AWS S3 Bucket resides.
S3 Bucket	Required		The AWS S3 Bucket name where Events/Logs will be forwarded.

Log Forwarding - Datadog

Datadog is a very common and powerful SIEM that is used by many companies. Multicloud Defense supports Log Forwarding to Datadog to send Security Events and Traffic Log information for processing, storage, access and correlation. The information sent is in a semi-structured JSON format where the attribute-value pairs can be accessed and processed.

Requirements

In order to forward logs to Datadog, the following information is required:

- Datadog account
- Endpoint URL
- API Key

Tip

- To Sign up for a Datadog account, refer to **Datadog Account** (https://www.datadoghq.com/).
- To create a Datadog API Key, refer to **Datadog API Key** (https://app.datadoghq.com/account/login?next=%2Faccount%2Fsettings#api).

Profile Parameters

Parameter	Deonticity	Default	Description
Profile Name	Required		A unique name to use to reference the Profile.

Parameter	Deonticity	Default	Description
Description	Optional		A description for the Profile.
Destination	Required	Datadog	The SIEM used for the Profile.
Skip Verify Certificate	Optional	Unchecked	Whether to skip verifying the authenticity of the certificate.
API Key	Required		The Datadog API Key to authenticate the communication.
Endpoint	Required	https://http-intake.logs.datadoghq.com/	The URL endpoint used to receive the forwarded Events/Logs.

Log Forwarding - GCP Logging

GCP Stackdriver Logging is a service offer by Google Cloud Provider (GCP) for collecting and storing logs from applications and services. Multicloud Defense supports Log Forwarding to GCP Stackdriver Logging to send Security Events and Traffic Log information for processing, storage, access and correlation. The information sent is in a semi- structured JSON format where the attribute-value pairs can be accessed and processed.

Requirements

The GCP *multicloud defense-firewall* Service Account must be assigned **Logs Writer** role in order for the Gateway to write events to the GCP Stackdriver Log.

Profile Parameters

Parameter	Deonticity	Default	Description
Profile Name	Required		A unique name to use to reference the Profile.
Description	Optional		A description for the Profile.
Destination	Required	GCP Logging (From Gateway)	The SIEM used for the Profile.
Log Name	Required	ciscomcd -gateway-logs	The name of the Stackdriver Log used to store events.

Field Integer to String Mappings

When events are forwarded from the Controller, the Controller introduces mappings of event field values to friendly names. When events are forwarded directly from the Gateway (e.g., GCP Logging), the Controller is not involved and thus the event field values are not mapped to friendly names. In order to interpret these fields, the user is responsible for performing the field value to friendly name mapping.

The fields, sub-fields and their value to friendly mapping are provided below:

Field	Integer	String
action	0	DUMMY_ACTION
	1	ALLOW
	2	DENY
	3	DROP
	4	REDIRECT
	5	PROXY
	6	LOG
	7	OTHER
	8	DELAY
	9	DETECT_SIG

Field	Integer	String
gatewaySecurityType	1	INGRESS_FIREWALL
	2	EAST_WEST_AND_EGRESS_FIREWALL

Field	Integer	String
level	1	DEBUG
	2	INFO
	3	NOTICE
	4	WARNING
	5	ERROR
	6	CRITICAL
	7	ALERT
	8	EMERGENCY

Field	Integer	String
policyMatchInfo.serviceType	0	UNKNOWN
	1	PROXY
	2	FORWARDING
	3	REVERSE_PROXY
	4	FORWARD_PROXY

Field	Integer	String
protocol **sessionSummaryInfo.egressConnection.protocol** **sessionSummaryInfo.ingressConnect.protocol**	0	DUMMY
	1	ICMP
	6	TCP
	17	UDP
	252	HTTP

Field	Integer	String
rule.type	0	DUMMY_RULE_TYPE
	1	THIRD_PARTY
	2	USER_DEFINED

Field	Integer	String
statusText **ingressConnectionStates.state**	0	CLOSED
	1	SYN_SENT
	2	SYN_RECV
	3	ESTABLISHED
	4	FIN_WAIT
	5	CLOSE_WAIT
	6	LAST_ACK
	7	TIME_WAIT
	8	CLOSE

Field	Integer	String
type	1	WAF
	2	DPI
	3	HTTP_REQUEST
	4	L4_FW
	5	FLOW_LOG
	6	MALICIOUS_IP
	7	TLS_ERROR
	8	TLS_LOG
	9	L7DOS
	10	SNI
	11	APPID
	12	URLFILTER
	13	SESSION_SUMMARY
	14	DLP
	15	FQDNFILTER
	16	AV

Log Forwarding - Microsoft Sentinel

Microsoft Sentinel is a powerful SIEM that is used by many companies. Multicloud Defense supports Log Forwarding to Microsoft Sentinel to send Security Events and Traffic Log information for processing, storage, access and correlation. The information sent is in a semi-structured JSON format where the attribute-value pairs can be accessed and processed.

Requirements

In order to forward logs to Microsoft Sentinel, the following information is required:

- Create an Azure Log Analytics Workspace.
- Define an Azure Log Table.

Profile Parameters

Parameter	Deonticity	Default	Description
Profile Name	Required		A unique name to use to reference the Profile.
Description	Optional		A description for the Profile.
Destination	Required	Microsoft Sentinel	The SIEM used for the Profile.
Azure Log Analytics Workspace ID	Required		The ID of the Azure Log Analytics Workspace.
Shared Key	Required		The Shared Key used to authenticate the communication.
Azure Log Table Name	Required		Name of the Azure Log Table where the logs/events will be stored.

Log Forwarding - Splunk

Splunk is a very common and powerful SIEM that is used by many companies. Multicloud Defense supports Log Forwarding to Splunk to send Security Events and Traffic Log information for processing, storage, access and correlation. The information sent is in a semi-structured JSON format where the attribute-value pairs can be accessed and processed.

Requirements

In order to forward logs to Splunk, the following information is required:

- Splunk account
- Splunk Collector URL
- Event Collector Key
- Index Name

Tip For information on the Splunk Event Collector, refer to **Splunk HTTP Event Collector** (https://docs.splunk.com/Documentation/Splunk/8.1.0/Data/UsetheHTTPEventCollector).

Profile Parameters

Parameter	Deonticity	Default	Description
Profile Name	Required		A unique name to use to reference the Profile.
Description	Optional		A description for the Profile.
Destination	Required	Datadog	The SIEM used for the Profile.
Skip Verify Certificate	Optional	Unchecked	Whether to skip verifying the authenticity of the certificate.
Endpoint	Required		The URL used to access the HTTP Event Collector.
Token	Required		The Splunk Token to allow Multicloud Defense to communicate with Splunk.
Index	Required	main	The name of the Splunk index used to store events.

Log Forwarding - Sumo Logic

Sumo Logic is a very common and powerful SIEM that is used by many companies. Multicloud Defense supports Log Forwarding to Sumo Logic to send Security Events and Traffic Log information for processing, storage, access and correlation. The information sent is in a semi-structured JSON format where the attribute-value pairs can be accessed and processed.

Requirements

In order to forward logs to Sumo Logic, the following information is required:

- Sumo Logic account
- Sumo Logic collector endpoint

Tip For information on how to setup Sumo Logic Collector, refer to **Sumo Logic Setup Guide** (https://help.sumologic.com/docs/send-data/setup-wizard/).

Profile Parameters

Parameter	Deonticity	Default	Description
Profile Name	Required		A unique name to use to reference the Profile
Description	Optional		A description for the Profile
Destination	Required	Sumo Logic	The SIEM used for the Profile
Endpoint	Required		The URL endpoint used to receive the forwarded Events/Logs

Log Forwarding - Syslog

A syslog server is a common log collector that accepts a standard formatted syslog message. Each syslog message contains fields for facility, severity and message. Almost any SIEM can accept syslog formatted messages, although most SIEMs support other message formats. Multicloud Defense supports sending security events and traffic logs to a syslog server. The following are a list of events and logs that can be forwarded:

- Flow Logs (Traffic Summary)
- Firewall Events (AppID, L4FW, GeoIP, MaliciousIP, SNI)
- HTTPS Logs (HTTP, TLS)
- Network Threats (AV, DLP, IDS/IPS)
- Web Protection (WAF, L7 DoS)

Note Flow logs are deprecated in gateway version 2.10 and later releases. The information contained within each flow log is made available as part of the session information available in **Traffic Summary** > **Logs**.

Events can be forwarded to a syslog server using a log forwarding profile. Once created, the profile needs to be associated with a new or existing gateway in order for the events to be sent to the syslog Server. To create, modify or change the gateway association of a log forwarding profile, refer to Log Forwarding - Security Events and Traffic Logs.

Profile Parameters

Parameter	Deonticity	Default	Description
Profile Name	Required		A unique name to use to reference the Profile.

Parameter	Deonticity	Default	Description
Description	Optional		A description for the Profile.
SIEM Vendor	Required	Syslog	The SIEM used for the profile.
Server IP	Required		The IP address of the syslog server.
Protocol	Required	UDP	The protocol to use when sending messages (TCP / UDP).
Port	Required		The port to use when sending messages.
Format	Required	IETF	The format of the messages (only IETF is supported).
Flow Logs	Required	No	Whether to send flow logs (Yes / No).
Firewall Events	Required	No	Whether to send firewall events (Yes / No).
HTTPS Logs	Required	No	Whether to send HTTPS logs (Yes / No).
Network Threats	Required	Emergency	The lowest severity level to send network threats.
Web Attacks	Required	Emergency	The lowest severity level to send web attacks.

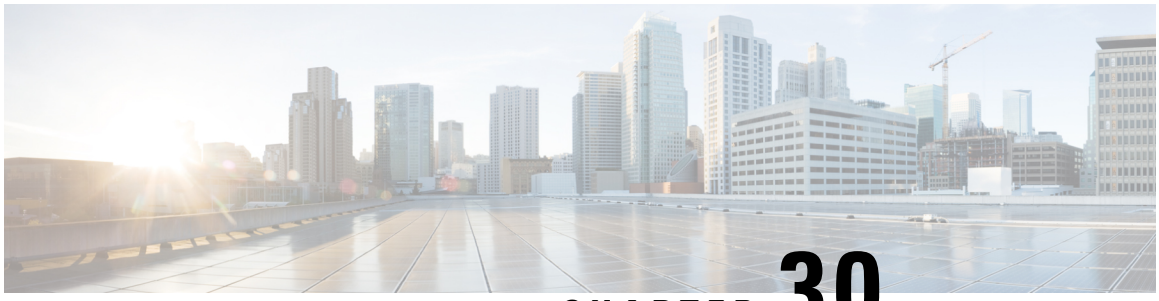
Note The following levels of severity (highest to lowest) are available:

- Emergency
- Alert
- Criticial
- Error
- Warning
- Notice
- Info
- Debug

All events for the category that contain the severity level specified or higher will be sent to the syslog server.

PART XIII

Administration



CHAPTER 30

Management

The **Administration** page offers opporutnities to watch the state of your account and the overall status of the cloud service providers affiliated with your account.

Management

The **Administration** page offers opporutnities to watch the state of your account and the overall status of the cloud service providers affiliated with your account.

API Keys

Navigate to **Administration** > **Management** > **API Keys** to view this page.

Search

Use the search bar to seek or filter the list of API keys with key words. You must use at least three characters for the search to qualify.

API Key Table and Actions

This table lists all the API keys that are created by Multicloud Defense components for your cloud service providers. View the role, key ID, the date the key was added to Multicloud Defense, and the date the key expires.

From here you can create or delete API keys. Note that these keys are generated by Multicloud Defense and not related to the keys your cloud service provider might create to maintain communication. Continue reading for more information.

Create an API Key in Multicloud Defense

Use the following procedure to create an API Key:

Step 1 Navigate to Navigate to **Administration** > **Management** > **API Keys**.

Step 2 Click **Create API Key**.

Step 3 Enter a unique **Name**.

Step 4 Confirm the **Email Address** that Multicloud Defense automatically generates. You cannot change this option.

Step 5 Use the drop-down menu to select one of the key roles:

- **admin_read_only** - This role restricts interactions so you cannot modify or action anything, and can only “view” the available data.
- **admin_read_rw** - This role allows you to read and modify available data.

Step 6 Enter an appropriate value for **API Key Lifetime (days)**. The deafult value is 365 days.

Step 7 Click **Save**.

Delete an API Key from Multicloud Defense

Use the following procedure to delete a API Key:

Step 1 Navigate to **Administration** > **Management** > **API Keys**.

Step 2 Select the API Key from the table and check the box so it is highlighted.

Step 3 Click **Delete**.

Step 4 Confirm you want to delete the key and click **Yes**. The key is immediately removed from Multicloud Defense.

Account Level Settings

This page displays some of the tags used in Multicloud Defense, including application tags and custom tags. Continue reading for more information.

Application Tags

The application tag is a string of characters and is used as one of the classification criteria for the automatic classification of processes or threads. Tagging allows you to group apps based on your unique requirements so that you can search for apps and find vulnerabilities. Note that not all cloud service providers support the use of application tags.

Note You can only create one appication tag at a time. If you need to create a new tag, you **must** delete the existing tag and then create a new application tag.

Create an Application Tag

Use the following procedure to create an application tag. Note that these tags are for internal use only and may not be recognized or available from your cloud ervice provider's interface.

Step 1 Navigate to **Administration** > **Management** > **Account**.

Step 2 In the **Application Tag** table, click **Create**.

Step 3 The type of application tag is `APPLICATION_TAG_KEYS` by default.

Step 4 Enter a brief **Description** of the tag. This can help identify or differentiate between other tags that might have a similar name or concept.

Step 5 Enter at least one **Value**. Hit `Enter` after each value to create more than one. Note that these values are case sensitive.

Step 6 Click **Save**. The tag is created and available in the table.

Edit an Application Tag

Use the following procedure to edit an existing application tag that has been created in Multicloud Defense. You cannot use this procedure to modify tags that were created in your cloud service provider's interface.

Step 1 Navigate to **Administration** > **Management** > **Account**.

Step 2 In the **Application Tag** table, locate the application tag you want to edit and check its box on the left so it is highlighted.

Step 3 Click **Edit**.

Step 4 Modify the following parameters:

- **Description** - You can edit or delete the description.
- **Tag Values** - You can add or remove tags here.

Step 5 Click **Save**. Alternatively, you can cancel at any time without saving changes.

Delete an Application Tag

Use the following procedure to delete an existing application tag:

Step 1 Navigate to **Administration** > **Management** > **Account**.

Step 2 In the **Application Tag** table, locate the application tag you want to edit and check its box on the left so it is highlighted.

Step 3 Click **Delete**.

Step 4 Confirm you want to delete the application tag and click **Yes**.

Custom Tags

Custom tags are simple pieces of data that provide details about an item and make it easy to locate related items that have the same tag. You can use a tag to easily identify or differentiate an object, policy, rule, and more.

Create a Custom Tag

Use the following procedure to create a custom tag in Multicloud Defense. Note that these tags are for internal use only and may not be recognized or available from your cloud ervice provider's interface.

Step 1 Navigate to **Administration** > **Management** > **Account**.

Step 2 In the **Custom Tag** table, click **Create**.

Step 3 Enter the **Value** of the tag. This can help identify or differentiate between other tags that might have a similar name or concept

Step 4 Enter at least one **Value**.

Step 5 Click **Save**. The tag is created and available in the table.

Edit a Custom Tag

Use the following procedure to modify an existing custom tag:

Step 1 Navigate to **Administration** > **Management** > **Account**.

Step 2 In the **Custom Tag** table, locate the application tag you want to edit and check its box on the left so it is highlighted.

Step 3 Click **Edit**.

Step 4 Modify the following parameters:

- Key.
- Values.

Step 5 Click **Save**. Alternatively, you can cancel at any time without saving changes.

Delete a Custom Tag

Use the following procedure to delete an existing custom tag:

Step 1 Navigate to **Administration** > **Management** > **Account**.

Step 2 In the **Custom Tag** table, locate the application tag you want to edit and check its box on the left so it is highlighted.

Step 3 Click **Delete**.

Step 4 Confirm you want to delete the application tag and click **Yes**.

System

The **System** page is a historical document that catalogues at least a year's worth of updates. You can use these details for general knowledge, locating the correct Release Notes version, and when you contact Cisco Support for product help. The following information collections are displayed here:

Component

This section displays the current versions for both the Multicloud Defense Controller and the user interface. Note that you cannot force an update or rollback to a previous version from this page.

Gateway Images

The gateway images table denotes when your Multicloud Defense Gateway was upgraded, which version of the gateway was in place and for how long, and what time zone the gateway is established in.

Talos/Network Intrusion

This table displays all the updates from Cisco's Talos Intelligence Group. These updates are pushed to Cisco products separate from a normal product software release.

Web Protection

This table displays all the Web Application Firewall (WAF) core and trustwave rule updates against the latest Web application vulnerabilities and threats.

Metering

The **Metering** page displays graphs of usage, both for the overall useage of Multicloud Defense and the gateway instances created for your cloud service providers.

Filters

Use the filters located at the top of the page to determine the data displayed in the page. You can change this view by selecting the month and year. You can use these filter settings to generate a usage report.

Generate a Usage Report

You can generate a usage report for either of the two options from this page. Navigate to **Administration** > **Mangement** > **Metering** and expand the **Download** drop-down option in the **Filter** section of the page to select either usage or instances. The file is downloaded locally as an .csv file. Use the filtering options to determine the timespan the report should generate from.

Usage Records

The **Usage Records** table details the number of accounts associated with your tenant, how many hours the accounts were interacted with, and on what days of the month selected in the Filter section. You can determine from the usage/month ratio what days were the most active.

Instance Records

The **instance Records** table displays the following instance statistics:

- Account Name.
- Account type by cloud service provider.
- Instance ID.
- Instance Type.
- Availablilty zone.
- Gateway.
- Started - When the gateway instance was created.

- Ended - When the gateway instance expired or was terminated.

Alert Profiles

Access the following Management views by navigating to **Administration** > **Alert Profiles**.

Both the **Services** and **Alerts** page focus on alerts from Multicloud Defense. The **Alerts** page focuses on *where* alerts are sent to and the **Alerts** page details *what* alerts are sent to the endpoints configured. For ideal configuration, spend time setting up entries in both pages to successfully and wholly optimze the alert opportunity within the dashboard.

Services

Navigate to **Administration** > **Management** > **Service** to view this page.

Services focuses on **where** you want to send alerts to. Note that you must provide criteria from the third-party application in order to successfully configure any options on this page.

Search

Use the search bar to seek or filter the list of services with key words. You must use at least three characters for the search to qualify.

Services Table and Actions

This table lists all the services that are created by Multicloud Defense components for your cloud service providers. View the name, type of service, the date the service was updated.

From here you can create or delete services. Note that these services are generated by Multicloud Defense and not related to the services your cloud service provider might provide.

Create a Service

Use the following procedure to create a service:

Before you begin

You must have service notifications or integrations enabled or allowed on your third party messaging application.

Step 1 Navigate to Navigate to **Administration** > **Management** > **Services**.

Step 2 Click **Create**.

Step 3 Enter a unique **Name**.

Step 4 (Optional) Enter a **Description**. This may help differentiate between other services that may have a similar name.

Step 5 Use the drop-down menu to select the service **Type**:

- Pager Duty.
- ServiceNow.

- Slack.
- Datadog.
- Microsoft Sentinel.
- Microsoft Teams.
- Webex.
- Splunk.

Step 6 Depending on the service type, complete the following entries when prompted:

- API Key.
- API URL.
- Azure Log Table Name.
- Azure Log Analytics Workspace ID
- (Optional for Splunk) Index.

Step 7 Click **Save**.

Edit a Service

Use the following procedure to edit an existing service:

Step 1 Navigate to Navigate to **Administration** > **Management** > **Services**.
Step 2 Locate and select the service within the table so it is highlighted.
Step 3 Expand the Actions drop-down menu and click **Edit**.
Step 4 Modify the following aspects of the service:

- Name.
- Description.
- Type.
- Type-specific configuration criteria.

Step 5 Click **Save** to confirm the changes. At any point, click **Cancel** to close the window and cancel the changes.

What to do next

You may have to **Refresh** the page to see any changes.

Clone a Service

Use the following procedure to clone an existing service:

Step 1 Navigate to Navigate to **Administration** > **Management** > **Services**.

Step 2 Locate and select the service within the table so it is highlighted.

Step 3 Expand the Actions drop-down menu and click **Clone**.

Step 4 A clone of the service is generated. By default, only the service **Type** and any service-specific configuration criteria is retained.

Step 5 Enter a unique **Name**.

Step 6 (Optional) Enter a description.

Step 7 Click **Save** to confirm the changes. At any point, click **Cancel** to close the window and cancel the changes.

What to do next

You may have to **Refresh** the page to see changes or additions to the table.

Export a Service

Use the following procedure to export an existing service:

Step 1 Navigate to Navigate to **Administration** > **Management** > **Services**.

Step 2 Locate and select the service within the table so it is highlighted.

Step 3 Expand the Actions drop-down menu and click **Export**.

Step 4 Multicloud Defense generates an export wizard.

Step 5 Either click **Download** to download the terrform locally or click **Copy Code** to copy the JSON resource to manually paste into the terroform script.

Step 6 Within the terrform prompt, execute the command provided in the lower half of the window: `terraform import "ciscomcd_alert_profile". "servicename" <number in table>`

Step 7 Follow the prompts within terraform to complete the task. There are no more steps in the dashboard.

Delete a Service

Use the following procedure to delete an existing service:

Step 1 Navigate to Navigate to **Administration** > **Management** > **Services**.

Step 2 Locate and select the service within the table so it is highlighted.

Step 3 Expand the Actions drop-down menu and click **Delete**.

Step 4 Confirm you want to delete the service and click **Yes**.

Step 5 The service is removed from Multicloud Defense.

Alerts

The Alerts page focuses on **what** alerts are sent to the third-party endpoints.We strongly recommend configuring both alerts and services to take advantage of the alerts opportunity.

Create an Alert

Use the following procedure to create an alert:

Step 1 Navigate to Navigate to **Administration** > **Management** > **Services**.

Step 2 Click **Create**.

Step 3 Enter a unique **Name**.

Step 4 (Optional) Enter a **Description**. This may help differentiate between other services that may have a similar name.

Step 5 Select the **Alert Profile**. At this time, `Pagerduty` is the only option available.

Step 6 Use the drop-down menu to select the alert **Type**.

- System Logs.
- Audit Logs.
- Discovery.

Step 7 (Optional) Use the drop-down menu to select the **Sub Type**. Note that these options may change or may not be available depending on the Type you selected in step 6:

- Gateway.
- Account.
- Controller.
- Insights Rule.

Step 8 Use the drop-down menu and select the level of **Severity**:

- Info.
- Warning.
- Medium.
- High.
- Critical.

Step 9 The **Enabled** checkbox is checked by default. This option designates whether the alert profile is active and usable or not. If it is disabled, Multicloud Defense does not include it when issuing alerts.

What to do next

Services to designate where these alerts are sent to.

Edit an Alert

Use the following procedure to edit an existing alert:

Step 1 Navigate to Navigate to **Administration** > **Management** > **Alert**.
Step 2 Locate and select the alert within the table so it is highlighted.
Step 3 Expand the Actions drop-down menu and click **Edit**.
Step 4 Edit any of the fields and selections of the alert proile. Note that some of the available fields may change depending on the selections you make.
Step 5 Click **Save** to confirm the changes. At any time, click **Cancel** to cancel the changes and close out the edit window.

Clone an Alert

Use the following procedure to clone an existing alert:

Step 1 Navigate to Navigate to **Administration** > **Management** > **Alert**.
Step 2 Locate and select the alert within the table so it is highlighted.
Step 3 Expand the Actions drop-down menu and click **Edit**.
Step 4 A clone of the alert is generated. By default, only the **Alert Profile** and **Type** is retained.
Step 5 Edit any of the remaining fields and selections of the alert. Note that some of the available fields may change depending on the selections you make.
Step 6 Click **Save** to confirm the changes. At any time, click **Cancel** to cancel the changes and close out the edit window.

Export an Alert

Use the following procedure to export an existing alert:

Step 1 Navigate to Navigate to **Administration** > **Management** > **Alert**.
Step 2 Locate and select the alert within the table so it is highlighted.
Step 3 Expand the Actions drop-down menu and click **Export**.
Step 4 Multicloud Defense generates an export wizard.
Step 5 Either click **Download** to download the terraform locally or click **Copy Code** to copy the JSON resource.
Step 6 Manually paste into the terraform script.
Step 7 Within the terraform prompt, execute the command provided in the lower half of the window: `terraform import "ciscomcd_alert_rule"."alertname" <number in table>`
Step 8 Follow the prompts within the terraform prompt to complete the task. **Close** the export window in Multicloud Defense. There are no more steps in the dashboard.

Delete an Alert

Use the following procedure to delete an existing alert:

Step 1 Navigate to Navigate to **Administration** > **Management** > **Alert**.

Step 2 Locate and select the alert within the table so it is highlighted.

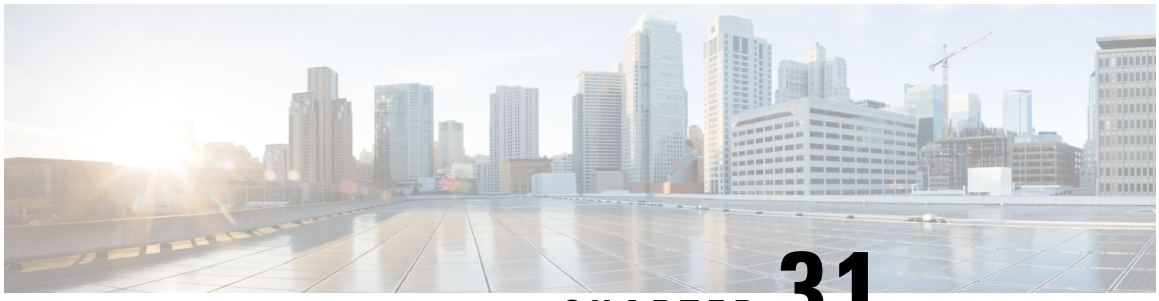
Step 3 Expand the Actions drop-down menu and click **Delete**.

Step 4 Confirm you want to delete the service and click **Yes**.

Step 5 The alert is removed from Multicloud Defense.

PART XIV

Manage Your Mutlicloud Account



CHAPTER 31

Manage Your Multicloud DefenseAccount

Account (Multicloud Defense Tenant)

The Account information is used by the Administrator to create and edit the following functions.

Navigate to **Administration** > **Management** > **Account**.

User Roles in CDO

There are a variety of user roles in Cisco Defense Orchestrator (CDO): Read-Only, Edit-Only, Deploy-only, Admin, and Super Admin. User roles are configured for each user on each tenant. If a CDO user has access to more than one tenant, they may have the same user ID but different roles on different tenants. A user may have a read-only role on one tenant and a Super Admin role on another. When the interface or the documentation refers to a Read-only user, an Admin user, or a Super Admin user we are describing that user's permission level on a particular tenant.

Roles in Multicloud Defense

Roles play an important part of what a user is allowed to do when accessing the Multicloud Defense tenant through the Multicloud Defense portal. A role is a privilege that grants the user a set of permissions.

There are three available roles:

- Super Admin (admin_super) .
- Edit-only Admin (admin_rw).
- Read-only Admin (admin_read-only) .

There are two permission definitions:

- Modify - Read, write, edit, and delete.
- Read - Read-only.

The permissions for each setting associated with each role are outlined in the following table:

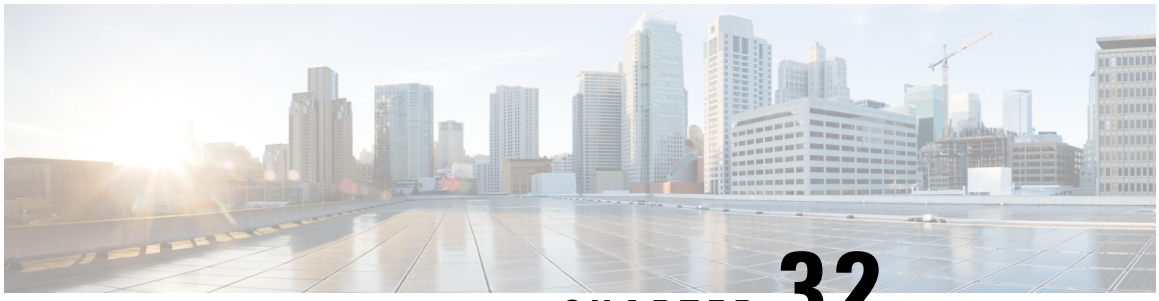
Setting	Super Admin(admin_super)	Edit-Only (admin_rw)	Read-Only (admin_read-only)
Management			
Users	Modify	Modify (except Super Admin)	Read
MFA Enable / Disable	Modify	Modify (except Super Admin)	Read
Reset MFA	Modify	Modify (except Super Admin)	Read
API Keys	Modify	Modify	Read
Roles	Read	Read	Read
Account > Application Tags	Modify	Modify	Read
Account > Email Domains	Modify	Read	Read
System	Read	Read	Read
Metering	Read	Read	Read
Alert Profiles			
Services	Modify	Modify	Read
Alert	Modify	Modify	Read

Only one (1) user within a Multicloud Defense tenant can be assigned the super admin role. This user is seen as the **owner** of the account and is synonymous with the owner of an AWS account or a linux root account. All other users should be assigned a read/write admin or read-only admin role.

The super admin role is assigned by Multicloud Defense and is granted to the first user created when the Multicloud Defense tenant is created. If any changes are required to a super admin user, please contact Multicloud Defense Support.

PART XV

Troubleshoot Your Account



CHAPTER 32

Troubleshoot Connecting Your Account

Manually Onboard an Account

In cases where onboarding a cloud service provider account to Multicloud Defense with the methods provided in Account Onboarding, on page 21, you may need to onboard your account manually. Use the following options as an alternative.

Manually Onboard a GCP Project

GCP Overview

GCP Project and GCP Folders

Multicloud Defense currently supports both GCP projects and GCP folders although these components are supported separately. Note the following limitations and exceptions for both of these options.

A GCP project has to potential to contain GCP resources like virtual machines, storage buckets, databases, and more. It can be used to create, enable, and use all Google Cloud services.

- Projects can be onbarded with terraform, manual onboarding, and scripted onboarding.
- Projects are ideal for environments that require orchestration, including discovery and investigation.
- You can interact with each project indvidually through the Multicloud Defense dashboard.

As of Version 23.10 you can connect a GCP folder with terraform. A GCP folder contains projects, other folders, or a combination of both. Organization resources can use folders to group projects under the organization resource node in a hierarchy.

- Folders that do not have the `roles/compute.admin` permission enabled are considered empty and are not used.
- Projects associated with onboarded folders are used for asset and traffic discovery only.
- Projects associated with onboarded folders do not accommodate orchestrating service VPC or gateway creation.

- Permissions made to folders from the GCP console must be made at the folder level. As such, Multicloud Defense actions are also made at the folder level.

If you want to onboard a GCP folder, see Terraform Repository.

Overview Proecdure

The following is an overview of how to connect your GCP project. An shell **script** is provided by Multicloud Defense and facilitates an easy connective process as part of a wizard. The script automates the following steps so you don't have to:

1. Create two service accounts.
2. Enable the following APIs (Compute Engine, Secret Manager).
3. Create the two following VPCs (management, datapath).
4. Create firewall rules to allow traffic to the Multicloud Defense Gateway (app traffic) in the datapath VPC.
5. Create firewall rules to allow management traffic from Multicloud Defense Gateway to the Multicloud Defense Controller in the management VPC.

If you find that the script does not work, or if you need to manually change your settings, these actions can be executed using the GCP cloud console web UI, or using the gcloud CLI. See the alternative method of connecting your project Manually Onboard a GCP Project.

Service Accounts

Multicloud Defense requires two service accounts created in your GCP project:

- **multicloud defense-controller**: This account is used by theMulticloud Defense Controller to access your GCP project to create resources (Multicloud Defense Gateways), load balancers for Multicloud Defense Gateways, and read information about the VPCs, Subnets, Security Group tags etc.
- **multicloud defense-gateway**: This account is assigned to the Multicloud Defense Gateways (Compute VM instances). The account provides access to the secret manager (private keys for TLS decryption) and storage.

You can create these service accounts in one of two ways: by using the service available in the UI or by using the the cloud service provider's CLI.

Create Multicloud Defense Controller Service Account Using GCP Cloud Console

The Multicloud Defense Controller service account is used by the Multicloud Defense Controller to access and manage resources in your GCP project. You must create the account and generate a key. The key is added to the Controller as part of Account onboarding to the Controller.

Step 1 Open **IAM** in your GCP project.

Step 2 Click **Service Accounts**.

Step 3 Create **Service Account**.

Step 4 Provide a name and ID (e.g multicloud defense-controller) and click **Create**.

Step 5 Add **Compute Admin** and **Service Account User roles**.

Step 6 Click **Continue**.

Step 7 Click **Done**.

Note There is no requirement to add any users.

Step 8 Click on the newly created account, scroll down to **Keys** and in the dropdown for **Add Key** and select **Create New Key**.

Step 9 Choose JSON (default option) and click **Create**.

Step 10 A file is downloaded to your computer. Save this file.

Create a Multicloud Defense Firewall Service Account Using the GCP Cloud Console

The multicloud defense firewall service account is used by the Multicloud Defense Gateway instances running inside your GCP project. The Gateways may need to access the private keys stored in the SecretManager for TLS decryption and access storage to store PCAP files etc. (if configured by the user). Also, the Gateways many need Log Writer permissions to send logs from Multicloud Defense Gateway to the GCP logging instance (if configured by the user).

Below are two (2) methods of creating this service account.

Step 1 Open **IAM** in your GCP project.

Step 2 Click **Service Accounts**.

Step 3 Create **Service Account**.

Step 4 Provide a name and ID (e.g multicloud defense-firewall) and click **Create**.

Step 5 Add **Secret Manager**, **Secret Accessor** and **Logs Writer roles**.

Step 6 Click **Continue**.

Step 7 Click **Done**.

Note There is no requirement to add any users.

Enable API

You can enable the API for communication between Multicloud Defense Controller and your GCP account with either GCP console or the cloud service provider's CLI.

Enable API-Using the GCP Cloud Console

Enable the APIs in your project/account so that the Multicloud Defense Controller can create Multicloud Defense Gateways (Virtual Machines, Load Balancers).

Step 1 Search for **Compute Engine API** in the searchbar.

Step 2 Click **Enable**.

Step 3 Search for **Secret Manager API** in the searchbar.

Step 4 Click **Enable**.

Step 5 Search for **Identity and Access Management (IAM) API** in the searchbar.

Step 6 Click **Enable**.

Step 7 Search for **Cloud Resource Manager API** in the searchbar.

Step 8 Click **Enable**.

VPC Setup

Multicloud Defense Gateway instances can be deployed in edge or hub mode. In edge mode, the gateway instances run in the same VPC as your applications. This document focuses on preparing you to deploy the Multicloud Defense Gateway deployment in edge mode.

VPC and Subnets

When deploying the Multicloud Defense Gateway, the Multicloud Defense Controller will prompt for the **management** and **datapath** VPC information. Multicloud Defense Gateway instances require two network interfaces. In GCP, the network interfaces of a VM instance need to be in different VPCs unlike other cloud providers where they can be in just different subnets. If you already have a VPC where the application is running, you have the **datapath** VPC and the subnet. You must create another VPC (or use an another existing VPC) for management purposes. You can either use the auto-created subnets or create them manually.

The datapath vpc is the VPC where your applications are running and will be referred to as such in the following sections

In each of the VPCs, Multicloud Defense requires one subnet for datapath and one subnet for management.

The **management** subnet is a public subnet that must be associated with the route table that has a default route to the Internet. The Multicloud Defense Gateway instance has an interface attached to this subnet that it uses to communicate with the Multicloud Defense Controller. This interface is used for policy pushes and other management and telemetry activities between the Multicloud Defense Controller and the Multicloud Defense Gateway instances. Customer application traffic **does not** flow through this interface and subnet. The interface is associated with the **multicloud defense- management** network tag (or any tag based on your team requirements), which is described in the network tags section below.

The **datapath** subnet is a public subnet that must be associated with the route table that has a default route to the Internet. The Multicloud Defense Controller creates a network load balancer (NLB) in this subnet. In addition, a Multicloud Defense Gateway instance has an interface attached to this subnet. The customer applications traffic **flows** through this interface. A security policy is applied to the traffic ingressing through this interface. The interface is associated with the **multicloud defense-datapath** network tag (or any tag based on your team requirements), which is described in the network tags section below.

Sample VPC and Subnets using CLI

Use the following commands as an example when executing your own commands to create VPCs for your GCP account. Open the Google Cloud Shell windows for these particular commands:

Step 1 Create VPC **apps** and subnet **apps-us-east1**

Step 2 Create VPC `multicloud defense-mgmt` and subnet `multicloud defense-mgmt-us-east1`:

Step 3 Create at least two Firewall rules for VPC `multicloud defense-mgmt` with target-tags as `multicloud defense-mgmt`:

a. Egress rule to allow all the outbound traffic:

b. Ingress rule to allow SSH into the firewall instances:

Step 4 Create at least three Firewall rules for VPC **apps**. Use the following as examples:

a. One egress rule to allow all the outbound traffic with target-tags as `multicloud defense-datapath`:

b. One ingress rule to allow HTTP and HTTPS into the gateway instances through the non-load balancerwith target-tags as `multicloud defense-datapath`:

c. Once egress rule to allow all the outbound traffic with target-tags as `app-instance`:

d. One ingress rule to allow `tcp:8000` with `target-tags` as `app-instance`:

```
gcloud config set project <project-name> # incase the project is not set in the gcloud cli shell
gcloud compute networks create apps --subnet-mode custom
gcloud compute networks subnets create apps-us-east1 --network apps --range 10.0.0.0/24 --region
us-east1
gcloud compute networks create ciscomcd-mgmt --subnet-mode custom
gcloud compute networks subnets create ciscomcd-mgmt-us-east1 --network ciscomcd-mgmt --range
172.16.0.0/24 --region us-east1
gcloud compute firewall-rules create ciscomcd-mgmt-out --direction EGRESS --network ciscomcd-mgmt \
    --target-tags ciscomcd-mgmt --allow tcp,udp
gcloud compute firewall-rules create ciscomcd-mgmt-in --direction INGRESS --network ciscomcd-mgmt \
    --target-tags ciscomcd-mgmt --allow tcp:22
gcloud compute firewall-rules create ciscomcd-datapath-out --direction EGRESS --network apps \
    --target-tags ciscomcd-datapath --allow tcp,udp
gcloud compute firewall-rules create ciscomcd-datapath-in --direction INGRESS --network apps \
    --target-tags ciscomcd-datapath --allow tcp:80,tcp:443
gcloud compute firewall-rules create app-instance-out --direction EGRESS --network apps \
    --target-tags app-instance --allow tcp,udp
gcloud compute firewall-rules create app-instance-in --direction INGRESS --network apps \
    --target-tags app-instance --allow tcp:8000,tcp:22
```

Once you run the above commands, you can create a VM instance in the **apps** VPC and launch a test web application on port 8000.

```
gcloud compute instances create app-instance1 \
  --zone=us-east1-b \
  --image-project=ubuntu-os-cloud \
  --image-family=ubuntu-2004-lts \
  --network apps \
  --subnet=apps-us-east1 \
  --tags=app-instance
gcloud compute ssh app-instance1 --zone us-east1-b
echo hello world > index.html
python3 -m http.server 8000
```

Network Tags (for GCP Gateways)

The management and datapath network tags are associated with the respective interfaces on the Multicloud Defense Gateway instance, as described in the subnets section above.

Create a gateway rule in the **management** VPC and associate that with **multicloud defense-management** network tag. This must allow all outbound traffic that makes the gateway instance communicate with the controller. Optionally, for inbound rules, enable port 22 (SSH) to allow SSH access to the gateway instance. SSH is **not required** for the Multicloud Defense firewall to function properly.

Create a gateway rule in the **datapath** VPC and associate that with **multicloud defense-datapath** network tag. This must allow the traffic to the Multicloud Defense Gateway for all the services that you enable (are going to enable).

For example, if an application is running on port 3000 and is proxied by the Multicloud Defense Gateway on port 443, port 443 must be opened on the multicloud defense-datapath network security tag.

Gateway Creation

Using the Multicloud Defense Gateway creation page use the following parameters:

1. Datapath VPC: **apps**.
2. Datapath Network Tag: **multicloud defense-datapath**.
3. Management VPC: **multicloud defense-mgmt**.
4. Management Network Tag: **multicloud defense-mgmt**.
5. Use **us-east1-b** zone.
6. Management Subnet: **multicloud defense-mgmt-us-east1**.
7. Datapath Subnet: **apps-us-east1**.

You can create subnets in other regions to test the Multicloud Defense Gateway in multi-AZ mode.

Manually Onboard an Azure Subscription

If you cannot directly connect an Azure subscription with the script provided in the Multicloud Defense Controller dashboard, use the procedures below to manually connect your subscription

(Optional) User-assigned Managed Identity for Key Vault and Blob Storage access

Multicloud Defense Gateways can optionally integrate with Azure Key Vault to retrieve TLS certificates and with Blob Storage for saving PCAP (packet capture) files. User-assigned managed identities are used to grant access to these services.

In the Azure portal, navigate to **Managed Identities** to create an identity.

Alternatively in Azure Cloud Shell, run the following command:

```
az identity create -g <RESOURCE GROUP> -n <USER ASSIGNED IDENTITY NAME>
```

For information on creating TLS certificate secrets in Azure Key Vault, see Azure Key Vault, on page 106.

Register Application in Azure Active Directory

Step 1 Navigate to **Azure Active Directory**.

Step 2 Select **App registrations**.

Step 3 Click **New registration**.

Step 4 Provide a name to reference the new app registration e.g. Multicloud Defense Controller In the *Supported account types* choose the second option *Accounts in any organizational directory*.

Step 5 Choose the option appropriate to your organization. Note that the **Redirect URI** is not needed for the creation of the App registration.

Step 6 Click **Register**.

Step 7 In the left navigation bar under the newly created application, click **Certificates & secrets**.

Step 8 Click **+ New client secret**, and then enter the required information in the *Add a client secret* dialog

- **Description** - Add a description (e.g multicloud defense-controller-secret1)
- **Expires** - Choose **Never**. You can also make this selection at your convenience. You will need to create new secrets when the current one expires)

Step 9 Click **Add**. The client secret is populated under the **Value** column.

Step 10 Copy the **Client secret** into a notepad, as this is shown only once and is never displayed again.

Step 11 In the left navigation bar click **Overview**.

Step 12 Copy the **Application (client) ID** and **Directory (tenant) ID** into a notepad.

Create a custom role to assign to the Application

Create a **custom role** that will be assigned to the application created for the Multicloud Defense Controller. The custom role gives the application permissions to read inventory information and create resources (e.g., VMs, load balancers, etc.) The custom role can be created in multiple ways.

Step 1 Navigate to **Subscription** and click **Access Control (IAM)**.

Step 2 Click on **Roles** and on the top menu bar navigate to click **+Add** > **Add Custom Role**.

Step 3 Give a name to the custom role (e.g., `multicloud defense-controller-role`).

Step 4 Keep clicking **Next** until you get to the JSON editing screen.

Step 5 Click **Edit** on the screen and in the JSON text, under the **permissions > actions** section, copy and paste the following content between the square brackets (no need to maintain the indentation):

```
"Microsoft.ApiManagement/service/*",
"Microsoft.Compute/disks/*",
"Microsoft.Compute/diskEncryptionSets/read",
"Microsoft.Compute/images/read",
"Microsoft.Compute/sshPublicKeys/read",
"Microsoft.Compute/virtualMachines/*",
"Microsoft.ManagedIdentity/userAssignedIdentities/read",
"Microsoft.ManagedIdentity/userAssignedIdentities/assign/action",
"Microsoft.Network/loadBalancers/*",
"Microsoft.Network/locations/serviceTags/read",
"Microsoft.Network/networkinterfaces/*",
"Microsoft.Network/networkSecurityGroups/*",
"Microsoft.Network/publicIPAddresses/*",
"Microsoft.Network/routeTables/*",
"Microsoft.Network/virtualNetworks/*",
"Microsoft.Resources/subscriptions/resourcegroups/*",
"Microsoft.Storage/storageAccounts/blobServices/*",
"Microsoft.Storage/storageAccounts/listkeys/action",
"Microsoft.Network/networkWatchers/*",
"Microsoft.Network/applicationSecurityGroups/*",
"Microsoft.Compute/diskEncryptionSets/read",
"Microsoft.Insights/Metrics/Read"
```

Step 6 **Optional** - If you plan to use multiple subscriptions with Multicloud Defense, you must edit the JSON at `assignableScopes` to add another subscription line or change it to ***** (star) so the custom role can be used with all subscriptions.

Step 7 Click **Save** at the top of the text box.

Step 8 Click **Review + Create** and create the role.

Step 9 Once the custom role is created return to **Access Control (IAM).**

Step 10 On the top menu bar, click **Add** > **Add role assignment**.

Step 11 In the **Role** dropdown, select the custom role created above.

Step 12 In the **Assign access to** dropdown leave it as the default (Azure AD user, group, service principal).

Step 13 In the **Select** text box, type in the name of the application created earlier (e.g. `multicloud defensecontrollerapp`) and click **Save**.

Step 14 In the **Subscription** page, click on the **Overview** in the left menu bar and copy the subscription ID to the notepad.

Required Values For Multicloud Defense Controller Onboarding

Make sure you have the following information before proceeding further:

- Subscription ID (*from subscription overview page*)
- Directory (Tenant) ID (*from the Azure AD app overview page*)
- Application (client) ID (*from the Azure AD app overview page*)
- Client Secret (*Copied when the Client secret was created*)

Accept Marketplace Terms

Multicloud Defense Controller creates Gateway instances using a Multicloud Defense virtual machine (VM) image from the Azure marketplace. The Terms and Conditions must be accepted for each subscription. Open the Azure cloud shell from the Azure portal website (on the top menubar towards the right side). Choose or switch to bash shell and execute the following command (replace the subscription-id with your subscription id copied in the previous section):

```
az vm image terms accept --publisher valtix --offer datapath --plan valtix_dp_image
--subscription subscription-id
```

Terraform Onboarding Scripts for Cloud Accounts

You an use the terraform script to onboard your cloud service provider account instead of using the onboarding wizard or the manual process.

About Terraform

Multicloud Defense customers can use the **Terraform Provider** to: **discover** - onboard public cloud accounts, gain continuous asset visibility and detect indicators of compromise (IoC); **deploy** - Multicloud Defense Gateways to protect ingress, egress and east-west traffic; and **defend** - with multi-cloud (AWS, Azure, GCP, OCI) dynamic policies with continuously discovered cloud assets.

Attention As of Multicloud Defense Controller version 23.10, you can connect a GCP folder as well as a GCP project using the terraform provider. See Terraform Repository, on page 253 for more information.

The Multicloud Defense terraform provider is a “Verified” provider available from the terraform registry. Customers can now use the terraform provider for Multicloud Defense to bake security into their operations, i.e. on-board their cloud accounts into Multicloud Defense, deploy Multicloud Defense Gateways and specify security policies to protect against ingress attacks from the Internet (WAF, IDS/IPS, Geo-IP), stop exfiltration on egress traffic (TLS decryption, IDS/IPS, AV, DLP, FQDN/URL filtering), and prevent east-west attacks between VPCs/VNets. The security policies can be specified based on cloud asset tags (e.g., “dev”, “test”, “prod”, “pci”, “web”, “app1” etc.)

For more information, refer to:

- Download the Terraform Provider for Multicloud Defense.
- Examples in GitHub.
- Multicloud Defense Blog on Terraform.

Terraform Repository

Use case	Description	Github Repository
AWS onboarding	This is for onboarding AWS account using Terraform.	Github Repo
AWS discovery CFT	This CFT deployment will include all necessary privileges needed to use Multicloud Defense's discovery feature. For full feature set, please use the in product CFT.	Github Repo
AWS discovery	This is for onboarding AWS account for discovery only mode using Terraform.	Github Repo
Azure onboarding	This is for onboarding Azure Subscription using Terraform.	Github Repo
GCP Project onboarding	This is for onboarding GCP project using Terraform.	Github Repo
GCP Folder onboarding	This is for onboarding GCP folder using Terraform.	Github Repo

Exporting Configuration as Terraform Block

Customers can export security profiles into terraform resource blocks from Multicloud Defense Controller. To export configuration into Terraform block, navigate and select the intended security profile and click on **Export** button. This will download a file that has the terraform block for the selected object/security profile.

All objects and profiles support terraform export with the exception of:

- Gateways
- Service VPCs/VNets

- Diagnostics