

Cisco Multicloud Defense Getting Started Guide

First Published: 2025-03-05

Last Modified: 2025-03-26

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

© 2025 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1 **Introduction to Cloud Security** 1

Cloud Security Overview 1

CHAPTER 2 **About Multicloud Defense** 3

About Multicloud Defense 3

CHAPTER 3 **Provisioning Multicloud Defense** 5

Prerequisites for Multicloud Defense 5

Licensing and Support in Multicloud Defense 5

Set up Multicloud Defense 6

Architecture of Multicloud Defense 7

Multicloud Defense Workflow 8

CHAPTER 4 **Onboarding Accounts in Multicloud Defense** 11

Set up AWS Account 11

Set up Azure Account 12

Set up GCP Account 13

Set up OCI Account 13

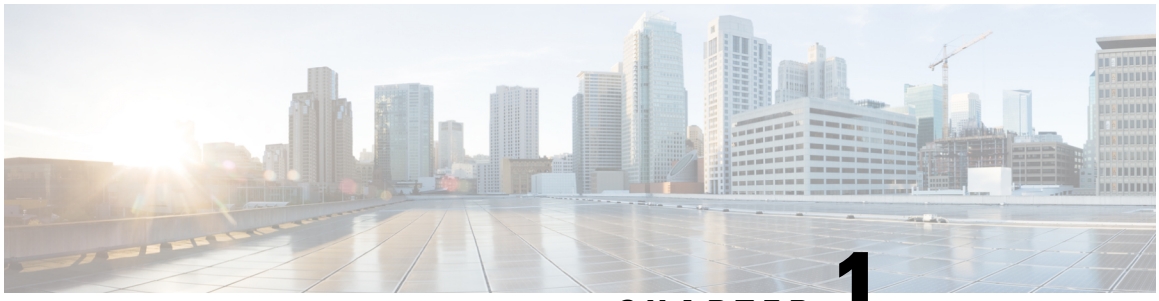
Discover Assets and Inventory 14

CHAPTER 5 **Configuring and Deploying Gateways** 15

Configure and Deploy Gateways in Multicloud Defense 15

CHAPTER 6 **Resources for Multicloud Defense** 17

Resources for Multicloud Defense 17



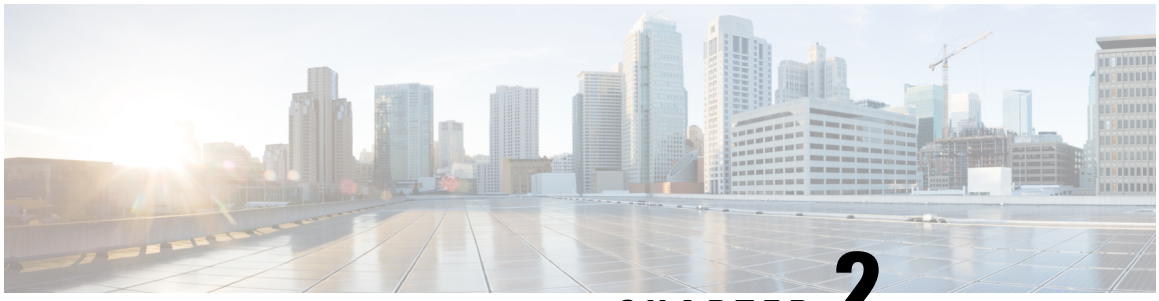
CHAPTER 1

Introduction to Cloud Security

• Cloud Security Overview, on page 1

Cloud Security Overview

In today's digital world, businesses are increasingly moving their operations to the cloud. Organizations are turning to cloud computing for several key reasons such as cost savings, scalability, improved performance, and enhanced collaboration. The cloud also presents unique security challenges such as data security, privacy, and complexity of management. Tools with advanced features, custom solutions, and multi-cloud management platforms help address these challenges.



CHAPTER 2

About Multicloud Defense

- About Multicloud Defense, on page 3

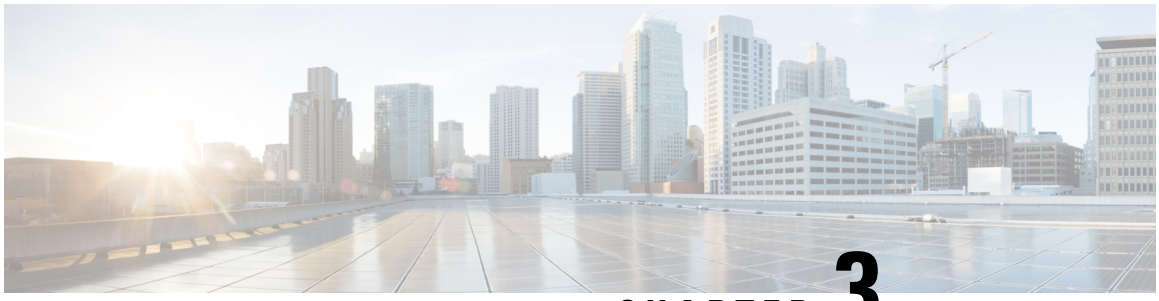
About Multicloud Defense

Cisco Multicloud Defense is a cloud-native, multi-cloud network security solution designed to secure traffic entering and leaving your cloud environment. It functions as a perimeter security solution, inspecting network traffic for threats and enforcing access control policies to protect your cloud resources. Cisco Multicloud Defense, also known as Multicloud Defense, offers an array of security features such as intrusion detection and prevention, application-layer firewall, SSL/TLS decryption, and content filtering across AWS, Azure, and Google Cloud Platform (GCP), and OCI.

Multicloud Defense caters to:

- Users of platforms such as AWS, Azure, GCP, OCI who are looking at protecting their assets over the cloud.
- Cloud Service providers.
- Administrators – Customer administration teams and administrators both external and internal to Cisco.
- Development Operations (DevOps and DevSecOps).
- Security Operation Centers (SOCs).
- Security and Cloud Architects.

About Multicloud Defense



CHAPTER 3

Provisioning Multicloud Defense

Once you enrol for Multicloud Defense, Security Provisioning and Administration creates an account for your tenancy. Security Provisioning and Administration is a web application that provides centralized management of Cisco Secure product instances, user identity, and user access management across Cisco Security Cloud.

Refer to the Cisco Security Provisioning and Administration User Guide for more information for any of these steps for:

- Purchasing and claiming a subscription license.
- Activating the account or cloud instance on Security Cloud Control.

- Prerequisites for Multicloud Defense, on page 5
- Licensing and Support in Multicloud Defense, on page 5
- Set up Multicloud Defense, on page 6
- Architecture of Multicloud Defense, on page 7
- Multicloud Defense Workflow, on page 8

Prerequisites for Multicloud Defense

To use Multicloud Defense, you need to:

- Install and use a Chrome browser to view the Multicloud Defense controller dashboard.
- Upgrade to a Multicloud Defense Gateway version that specifically supports IMDSv2 in the **Required** mode for optimal security with Amazon EC2 instances.
- Activate Multicloud Defense in Security Cloud Control.

Licensing and Support in Multicloud Defense

When you log into your Security Cloud tenant, you will see a wizard that guides you through connecting your cloud accounts to Multicloud Defense so that you can manage them with a free 90-day trial of Multicloud Defense Controller. The 90-day trial experience offers the full functionality of a paid-subscription to Multicloud Defense Controller.

For paid licensing, see the Cisco Multicloud Defense Ordering Guide.

When you enrol with Multicloud Defense, you can provision and activate Multicloud Defense in Security Cloud Control. For more information, see the Cisco Security Provisioning and Administration User Guide.

Set up Multicloud Defense

Click **Get Started** to begin your 90-day trial. This begins the process of provisioning the Multicloud Defense Controller.

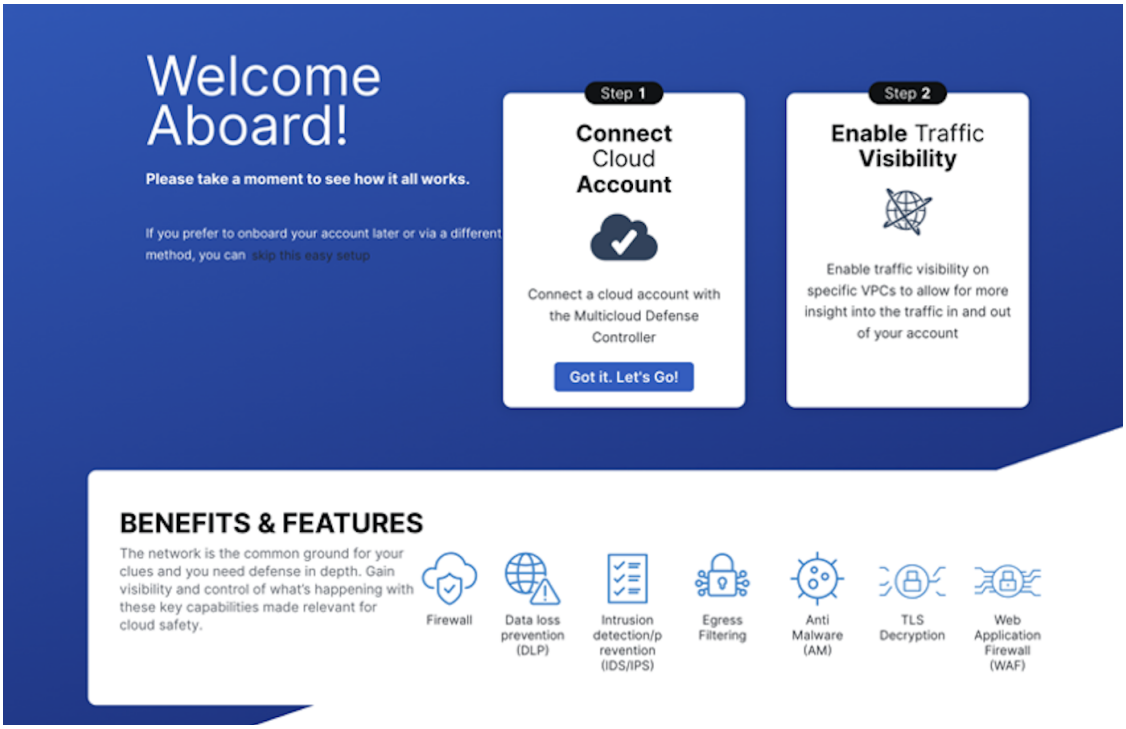
Easy Setup supports the following features for Cloud Providers:

- Account Onboarding: AWS, Azure, GCP, OCI.
- Enable Traffic Visibility: AWS (Flow Logs, DNS Query Logs), Azure (Flow Logs), GCP (VPC flow logs, DNS Query Logs).
- Create Services VPC/VNet: AWS, Azure, GCP.
- Create Gateways: AWS, Azure, GCP.

Cloud Account Easy Setup

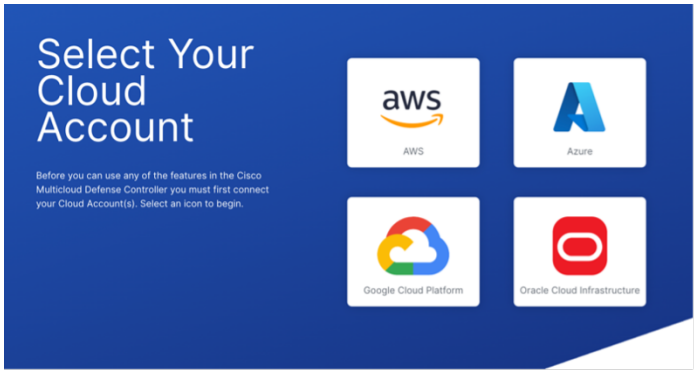
Once you log into Security Cloud Control, you can follow the on-screen guided wizard to set up your cloud account in Multicloud Defense.

Figure 1: On-screen guided wizard



Select your cloud account and provide details.

Figure 2: Select Your Cloud Account



The process of setting up Multicloud Defense security is a series of these simple steps:

- **Connect your Account:** Onboard your cloud service provider account to Multicloud Defense and simultaneously discover regions and additional inventory and assets affiliated with your account.
- **Enable Traffic Visibility:** Utilize the easy setup method to enable the collection of logs to understand the flow of traffic.
- **Secure Your Account:** -Set up a VNet or VPC, depending on the cloud account that you have, and a Multicloud Defense Gateway to secure your account.

Architecture of Multicloud Defense

Cisco Multicloud Defense has two main components:

- Multicloud Defense Gateways
- Multicloud Defense Controller.

Multicloud Defense Gateways

Multicloud Defense Gateway is a network-based security platform that contains network load balancers with a cluster of Multicloud Defense Gateway instances. Some of the key features are:

- Autoscaling and Self-healing: Operate as autoscaling, self-healing Platform-as-a-Service (PaaS), serving as inline network-based security enforcement nodes.
- Simplified Management: Eliminate the need for constructing virtual firewalls, configuring high-availability setups, or managing software installations.
- Advanced Security Profiles: Implement granular security profiles within a single pass datapath pipeline, without the need for traffic offloading to third-party engines.

Multicloud Defense supports these gateway use cases:

- Egress
- Ingress
- East-West

- Distributed
- Centralized / Hub
- Advanced Gateway Configuration: Use Your Own Load Balancer

To manage gateways, see the Multicloud Defense User Guide.

Multicloud Defense Controller

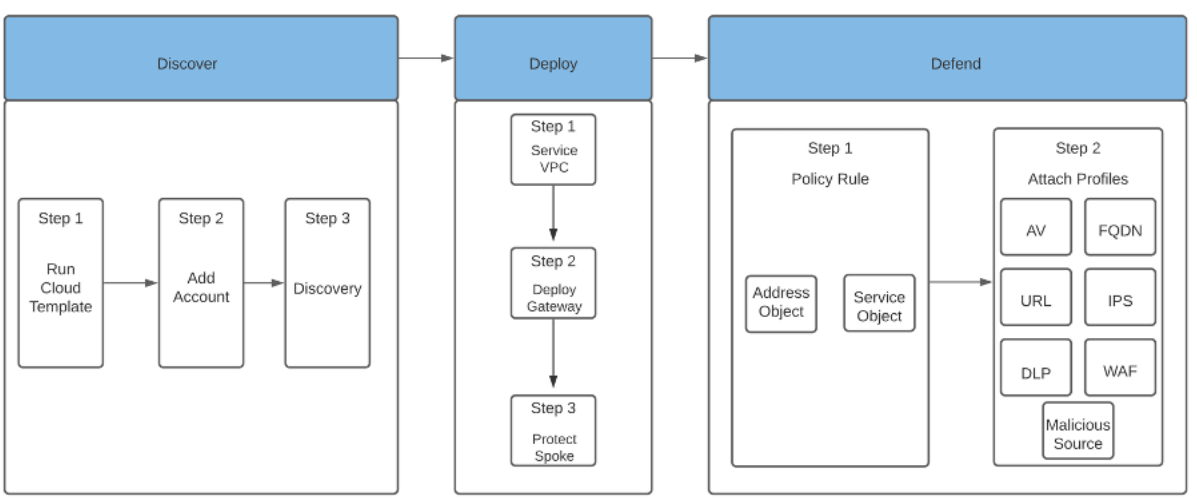
The Multicloud Defense Controller uses an architecture that contains:

- SaaS-based management: The Software-as-a-Service (SaaS) controller manages the Gateway stack and includes an API Server for orchestration of CSP load balancers (LBs) and Gateway Instances.
- Dynamic scaling: Facilitates dynamic horizontal scaling through instance additions and removals from the load balancer's "target pool," monitored for high availability.
- Continuous communication: Engages in continuous communication with Cloud Service Provider (CSP) accounts to keep security policies up-to-date.
- Dynamic policy and cloud-to-controller communication.
- Dynamic address objects: Uses cloud-native constructs to define dynamic address objects, automatically updating them as cloud resources change.
- Tag-based policy rules: Allows for granular policy rules based on instance tags, automatically inheriting security policies for new instances with appropriate tags.
- Full decryption using CSP-native key stores.
- Ensuring chain-of-custody: Multicloud Defense Gateways can directly access private keys stored in CSP-native key stores, such as Azure Key Vault, ensuring chain-of-custody, data sovereignity, and PKI adherence.
- Secure key management: Private keys remain within the organization's perimeter and are actively maintained by the key store.
- Proxies: These serve as intermediaries between clients and servers, facilitating various types of network communications. Cisco Multicloud Defense performs both reverse proxy and forward proxy functions.

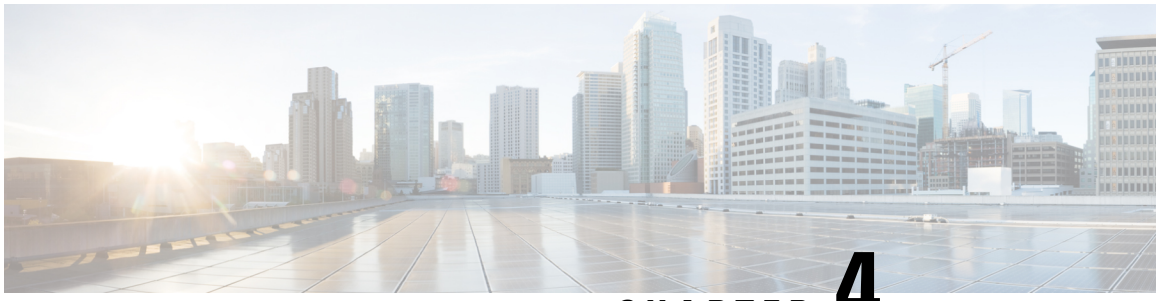
Multicloud Defense Workflow

In Multicloud Defense, follow these series of steps to Discover, Deploy, and Defend your cloud securely.

Figure 3: Workflow of Discover, Deploy, and Defend



Discover contains the first phase of connecting your cloud accounts, by onboarding them and discovering all your cloud inventory and traffic. Deploy contains setting up your VPCs and Gateways and deploying them. Defend contains the final phase of creating and managing policies using rules, rulesets, and profiles, to enable protection.



CHAPTER 4

Onboarding Accounts in Multicloud Defense

Based on your provider that you use, ensure that you complete the prerequisites prior to onboarding your account.

- Set up AWS Account, on page 11
- Set up Azure Account, on page 12
- Set up GCP Account, on page 13
- Set up OCI Account, on page 13
- Discover Assets and Inventory, on page 14

Set up AWS Account

Before you begin

Before connecting your AWS cloud account to Multicloud Defense Controller you need to:

- Ensure you have an active Amazon Web Services (AWS) account.
- Ensure you have an Admin or Super Admin user role in your Security Cloud Control tenant.
- You must have Multicloud Defense enabled for your Security Cloud Control tenant.

For more information on the steps to prepare your AWS account for integration with Multicloud Defense using a CloudFormation template, see AWS Overview. You can watch a video on how to onboard an AWS Account here.

Procedure

Step 1 Set up your account using the easy setup wizard. For more details, see Connect AWS Account

Step 2 Connect and deploy to AWS Account from the Multicloud Defense Dashboard with a CloudFormation template, (which is part of the easy setup wizard). For more details, see Account Onboarding - AWS.

Step 3 Enable traffic visibility. For more details, see Enable traffic for AWS.

Step 4 Enable CloudFormation outputs. For more details, see CloudFormation Outputs.

Step 5 Create or add Controller, Gateway, and Inventory roles. You can set permissions for these roles based on your needs. For more details, see Roles Created by Multicloud Defense.

What to do next

- Secure your account using the easy setup wizard. For more details, see Secure Your Account.
- Monitor the traffic and manage policies and resources.

Set up Azure Account

Before you begin

Get your Azure account and subscriptions ready before you connect and onboard them to the Multicloud Defense Controller. For more details, see the steps outlined in Prepare your Azure account. You can watch a video on how to onboard an Azure account here.

Procedure

Step 1 Set up your account using the easy setup wizard. For more details, see Connect Azure Account.

Step 2 Connect and deploy your Azure Account. For more details, see Connect an Azure Subscription to the Multicloud Defense Controller from the Multicloud Defense Dashboard.

Step 3 Discover assets in your account using the easy setup wizard.

Step 4 Create a policy in the Azure portal.

Step 5 Enable traffic visibility. For more details, see Enable traffic visibility for Azure.

Step 6 (Optional) Based on your needs, you can configure:

a) VNet Route Tables for your Azure Subscription.
b) Post-Onboarding Procedures.
c) VNet Route Tables for your Azure Subscription.
d) Roles Created by Multicloud Defense.
e) Set up Azure VNet – Subnets, Security Groups, Launch ARM Template.

What to do next

- Secure your account using the easy setup wizard. For more details, see Secure Your Account.
- Monitor the traffic and manage policies and resources.

Set up GCP Account

Multicloud Defense supports both set up of accounts using GCP projects and GCP folders, although these components are supported separately. For more details, see GCP Overview. You can watch a video on how to onboard a GCP account here.

Before you begin

Ensure you have:

- An active project for GCP.
- Relevant permissions to create service accounts, VPC, subnets etc.
- Super Admin or Admin access in Security Cloud Control.
- Enabled your tenant for Multicloud Defense in Security Cloud Control.

Procedure

Step 1 Create a Controller Service Account.

Step 2 Create a GCP Firewall Service Account.

Step 3 Set up your account using the easy setup wizard. For more details, see Connect Google Cloud Platform Account.

Step 4 Connect and deploy a GCP Project. For more details, see Connect a GCP Project to the Multicloud Defense Controller from the Multicloud Defense Dashboard.

Step 5 Enable Traffic Visibility. For more details, see Enable Traffic for a GCP Project.

Step 6 (Optional) Set up roles and permissions based on your needs. For more details, see Roles Created by Multicloud Defense.

What to do next

- Secure your account using the easy setup wizard. For more details, see Secure Your Account.
- Monitor the traffic and manage policies and resources.

Set up OCI Account

Prepare your OCI environment using these steps to successfully connect with Multicloud Defense. For OCI-specific documentation on how to accomplish these requirements, see OCI documentation on oracle.com. Watch a video on how to onboard an OCI account here.

- You can use the automated method to prepare your OCI account. For more details, see Overview of Automated Steps.
- You can also use the manual method to prepare your OCI account. For more details, see Overview of Manual Steps.

Before you begin

Before you onboard an OCI tenant to Multicloud Defense, you need to set up your OCI account.

- Ensure you have an active OCI account.
- Ensure you have a Super Admin or Admin role in Security Cloud Control.
- Ensure that Multicloud Defense is enabled in Security Cloud Control.
- To onboard the OCI tenant, you need to subscribe to the US West (San Jose) region. If you do not subscribe to this region, 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 cause an unauthorized error.



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

Procedure

Step 1 Set up account using the easy setup wizard – Connect Oracle Acount.

Step 2 Connect and deploy the OCI account to your Multicloud Defense - Connect the Oracle OCI Tenant to the Multicloud Defense Controller from the the Multicloud Defense Dashboard.

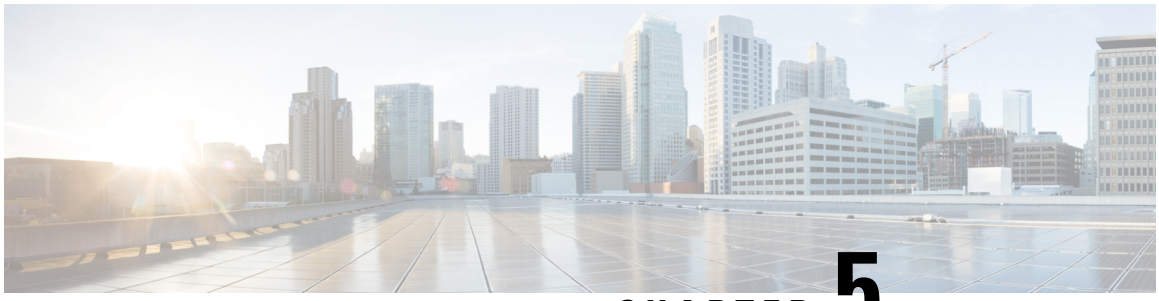
Step 3 Enable traffic visibility using the easy setup wizard.

What to do next

- Secure your account using the easy setup wizard. For more details, see Secure Your Account.
- Monitor the traffic and manage policies and resources.

Discover Assets and Inventory

Once you onboard your accounts, you can get 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 controller periodically crawls and keeps tabs on changes to maintain a fresh inventory model of the resources. In the **Discovery** tab, you can see the attributes of your resources and how they are interconnected. For more information about inventory, discovery, security insights, and rules and findings, see Assets and Inventory Discovery.



CHAPTER 5

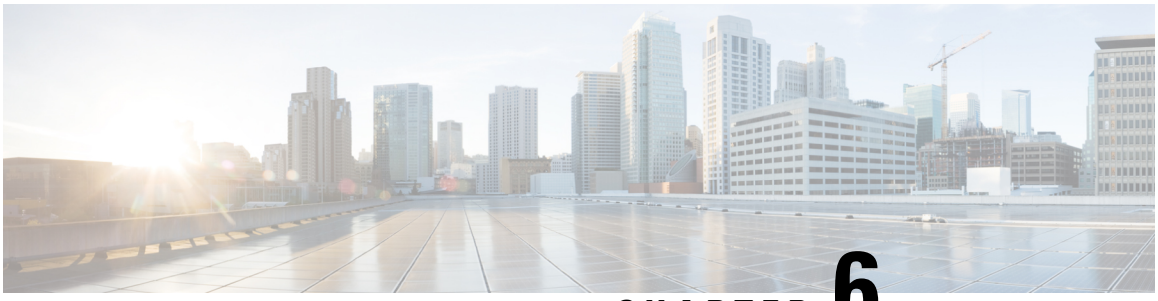
Configuring and Deploying Gateways

- Configure and Deploy Gateways in Multicloud Defense, on page 15

Configure and Deploy Gateways in Multicloud Defense

View the content in these specific sections, to configure, deploy, and manage Multicloud Defense Gateways and VPC/VNets:

- Orchestrate a gateway - Before You Begin.
- Create a Service VPC or VNet.
- Secure a Spoke VPC or VNet.
- Add a Multicloud Defense Gateway.
- Manage a Multicloud Defense Gateway.



CHAPTER 6

Resources for Multicloud Defense

- Resources for Multicloud Defense, on page 17

Resources for Multicloud Defense

Here is a list of resources that you can access to know more about Multicloud Defense:

- Multicloud Defense in Cisco Security Provisioning and Administration
- Recommended Versions of Multicloud Defense Components
- Multicloud Defense User Guide
- Multicloud Defense Release Notes
- Multicloud Defense Naming Conventions
- Supported Regions
- Terraform documentation
- Troubleshooting

Resources for Multicloud Defense