# Cisco Multicloud Defense – Terminology

**First Published:** 2026-07-01

## Cisco Multicloud Defense

Cisco Multicloud Defense is a cloud-native, multi-cloud network security solution for inspecting and securing traffic entering, leaving, and moving within cloud environments. It combines a SaaS controller with cloud-deployed gateways to deliver visibility, policy enforcement, threat prevention, and segmentation across AWS, Azure, Google Cloud, and OCI.

## Cisco Multicloud Defense terminology

**account onboarding**

The process of connecting a cloud account, subscription, project, folder, or tenancy to Multicloud Defense so the controller can discover cloud resources, enable traffic visibility, and deploy security infrastructure. Onboarding supports AWS, Azure, GCP, and OCI, with cloud-specific prerequisites and permission models.

**advanced security profile**

A collection of granular inspection and enforcement capabilities applied through the Multicloud Defense Gateway data path. Examples include IDS/IPS, WAF, antivirus, TLS decryption, DLP, URL filtering, FQDN filtering, and application-layer controls.

**application layer firewall**

A security capability that evaluates application traffic at Layer 7 rather than only using IP address, port, or protocol. In Multicloud Defense, application layer firewalling is used for cloud workload protection and is commonly associated with ingress protections such as WAF and Layer-7 threat defense.

**asset discovery**

The capability that discovers cloud resources and inventory in onboarded cloud accounts and maintains a current view of how resources are deployed and interconnected. Asset discovery helps teams understand cloud exposure and place controls where needed.

**auto-scaling**

Auto-scaling is an automated capability that can add or remove gateway instances to match traffic demand. It is applicable for both Multicloud Defense Gateway and FTDv Gateway. Auto-scaling is managed by the controller and is designed to maintain security enforcement while adapting to cloud workload changes.

**centralized security model**

A deployment model in which security services are placed in a central service VPC, VNet, or security VPC that acts as an enforcement hub for multiple spoke networks. Centralized designs are used for ingress, egress, and east-west inspection across connected cloud networks.

**CIDR**

In Multicloud Defense, Classless Inter-Domain Routing (CIDR) is the foundational method used to define network boundaries. It identifies workload subnets, segments traffic, and builds security policies across disparate environments like AWS, Azure, GCP, and OCI.

**cloud account**

A cloud-provider administrative scope that is connected to Multicloud Defense. Examples include an AWS account, Azure subscription, GCP project or folder, and OCI tenancy.

**cloud-native key store**

A cloud-provider key management service, such as Azure Key Vault, used to keep private keys inside the customer-controlled cloud perimeter while enabling TLS inspection use cases.

**cloud service provider**

A public cloud platform such as AWS, Azure, Google Cloud Platform, or Oracle Cloud Infrastructure. Multicloud Defense integrates with Cloud Service Provider (CSP) networking and logging constructs to deploy gateways, discover assets, and collect traffic visibility.

**combined security model**

A deployment approach that uses both centralized and distributed security enforcement. This model can centralize shared inspection while placing gateways closer to specific applications or cloud networks where needed.

**content filtering**

Inspection and enforcement that controls or blocks traffic based on content, URLs, FQDNs, categories, malware verdicts, or data-loss-prevention logic.

**controller service account**

A cloud identity or service account used to grant the Multicloud Defense Controller the permissions it needs to discover resources, orchestrate infrastructure, and manage security workflows in a cloud account.

**Data Loss Prevention**

A security capability that detects or prevents sensitive or confidential data from leaving approved boundaries. Cisco documentation describes Data Loss Prevention (DLP) as supporting compliance and security for data types such as PII and PHI.

**data plane**

The traffic-processing side of the architecture, represented by Multicloud Defense Gateways. The data plane inspects and enforces policy on traffic while the controller provides the control plane.

**Discover, Deploy, Defend**

The Multicloud Defense workflow. Discover connects cloud accounts and inventories resources and traffic. Deploy sets up VPCs, VNets, and gateways. Defend creates and manages policies, rulesets, and profiles for protection.

**distributed security model**

A deployment model that places security enforcement closer to applications, workloads, or individual cloud networks rather than only in a central hub. It is useful when teams need application-local inspection, scale, or segmentation.

**dynamic address object**

A policy object based on cloud-native resource attributes that updates as cloud resources change. Dynamic address objects help keep policy aligned to cloud resources without constant manual updates.

**east-west security**

Inspection and enforcement for traffic moving laterally between workloads, subnets, VPCs, VNets, or cloud networks. It helps limit lateral movement and implement segmentation or least-privileged access between applications and tiers.

**egress gateway**

A gateway used to protect outbound and east-west traffic. It can provide FQDN filtering, URL filtering, DLP, IDS/IPS, antivirus, forward proxy, TLS decryption, and related controls.

**egress security**

Controls for traffic leaving cloud workloads or networks toward the Internet, SaaS services, other networks, or other cloud environments. Egress security helps prevent data exfiltration, command-and-control traffic, malware communication, and unauthorized destinations.

**enforcement point**

A gateway instance or gateway cluster where traffic policies are applied. The controller defines and orchestrates policy, while gateways enforce that policy inline.

**forward proxy**

A proxy function for outbound client traffic. In Multicloud Defense, forward proxy capabilities are commonly associated with egress inspection, TLS decryption, URL/FQDN filtering, DLP, and threat prevention.

**forwarding mode**

A gateway operating mode that performs access control based on source and destination communication without inspecting full packet or content payloads. It is commonly used for east-west flows and egress filtering based on IP address, Layer 4 information, tags, or FQDN.

**gateway**

The Multicloud Defense data-plane component deployed into a customer cloud account as a PaaS component. Gateways inspect traffic inline and enforce policy for ingress, egress, and east-west use cases.

**gateway instance**

A cloud compute instance that forms part of a Multicloud Defense Gateway deployment. Multiple instances can be placed behind a cloud load balancer to provide scale and high availability.

**hub-and-spoke architecture**

A network design in which a central service network or security hub connects to multiple spoke VPCs, VNets, or VPC networks. Multicloud Defense uses this design for centralized inspection and enforcement.

**ingress gateway**

A gateway used to protect inbound traffic destined for applications or workloads. It can provide WAF, Layer-7 DoS protection, IDS/IPS, antivirus, reverse proxy, TLS decryption, geo-IP controls, and malicious-IP filtering.

**ingress security**

Controls for traffic entering cloud environments from the Internet or external networks. Ingress security protects web and non-web applications against exploits, bots, malware, malicious IPs, DoS attempts, and other inbound threats.

**inline inspection**

Traffic inspection performed while traffic is passing through a gateway in the data path. Inline inspection allows policies to allow, deny, decrypt, scan, or otherwise enforce controls before traffic reaches its destination.

**inventory**

The model of discovered cloud resources, their attributes, and their relationships. Inventory is periodically refreshed by the controller so administrators can view current resources and how they are connected.

**least-privileged access**

A segmentation principle that allows only authorized communication between workloads, tiers, environments, or cloud networks. Multicloud Defense uses segmentation to help enforce least-privileged lateral access.

**Multicloud Defense Controller**

The SaaS control plane for Cisco Multicloud Defense. The controller provides centralized management, cloud account onboarding, discovery, gateway lifecycle automation, policy orchestration, logging, alerting, metering, and integrations with third-party operations tools.

**Multicloud Defense Gateway**

The inline enforcement component of Cisco Multicloud Defense. It is deployed in the customer cloud account, receives policy from the controller, inspects traffic, and enforces protections such as WAF, IDS/IPS, DLP, URL filtering, TLS decryption, and antivirus.

**Multicloud Defense Terraform provider**

An infrastructure-as-code interface for deploying and managing Multicloud Defense resources. It enables DevOps and DevSecOps teams to instantiate security infrastructure and policies through Terraform workflows.

**northbound traffic**

Traffic flowing inbound from the Internet or external networks toward cloud-hosted applications and workloads. In Multicloud Defense documentation, northbound traffic is commonly associated with ingress protection and reverse proxy inspection.

**north-south traffic**

Traffic flowing outbound from cloud workloads toward the Internet or external services. Multicloud Defense documentation associates this direction with egress protection and forward proxy or forwarding operation.

**OCI**

Oracle Cloud Infrastructure (OCI) is a cloud computing platform. It natively integrates with Cisco Multicloud Defense to provide unified, consistent defense across distributed environments.

**policy**

A set of security rules and profiles that expresses what traffic is allowed, denied, decrypted, inspected, or logged. In Multicloud Defense, policy is created centrally and applied to enforcement points across cloud environments.

**proxy mode**

A gateway operating mode that terminates and re-establishes connections to inspect application content more deeply. Proxy mode supports reverse and forward proxy use cases, TLS decryption, WAF, DLP, and other content inspection functions.

**reverse proxy**

A proxy function for inbound application traffic. In Multicloud Defense, reverse proxy capabilities are used by ingress gateways to inspect and protect traffic before it reaches applications.

**ruleset**

A grouped set of rules that can be applied to traffic or resources as part of a policy. Rulesets help administrators organize enforcement logic for profiles and protected flows.

**security profile**

A reusable configuration that defines specific inspection or protection behavior, such as threat prevention, web application firewall behavior, URL filtering, TLS decryption, or DLP.

**service VPC / service VNet / security VPC**

A cloud network used as the centralized hub for Multicloud Defense gateways and supporting services. It connects to spoke networks and steers traffic through inspection points.

**spoke VPC / spoke VNet**

An application or workload network connected to a centralized service network. Traffic from spoke networks can be routed to Multicloud Defense gateways for inspection.

**tag-based policy**

A policy method that uses cloud resource tags and workload identity to apply rules dynamically. Tag-based policy helps newly deployed resources inherit the correct security controls as cloud environments change.

**traffic visibility**

The use of traffic and DNS data, such as flow logs and DNS query logs, to understand communication patterns, destinations, risk categories, and exposure across cloud environments.

**TLS decryption**

The capability to decrypt encrypted traffic for inspection and then re-encrypt it when forwarding traffic. Multicloud Defense supports TLS decryption in proxy and gateway use cases while using cloud-native key stores for key custody in supported designs.

**VPC flow logs / DNS query logs**

Cloud logging data sources used for visibility into network flows and DNS activity. They help Multicloud Defense discover resources, understand traffic, and generate security insights.

**Web Application Firewall**

A Layer-7 inspection capability used to protect web applications from application-layer attacks. Multicloud Defense includes Web Application Firewall (WAF) as part of ingress security capabilities.

**workload identity**

Attributes that describe a workload, such as tags, cloud metadata, deployment type, environment, or application tier. Multicloud Defense uses workload identity and discovery to build dynamic policies across cloud resources.

© Cisco Systems, Inc. All rights reserved.