Cisco Multicloud Defense

Embrace the future of multicloud network security with confidence

Table of Contents

Abstract

Applications and workloads are no longer limited to the data center. Today, organizations also deploy workloads and applications to public and private cloud environments, oftentimes more than one cloud, for greater agility, flexibility, and scale. As organizations continue to expand their multicloud footprint, the need for consistent visibility and unified security controls across clouds becomes critical for achieving a successful multicloud security strategy. With Cisco® Multicloud Defense, organizations can embrace the future of multicloud network security with confidence by leveraging highly scalable and agile security infrastructure for protecting workloads and applications deployed in a multicloud environment from malicious traffic or insider threats.

Target Audience

This document provides a technical overview of the design principles, architecture, and use cases for Cisco Multicloud Defense. It also covers best practices, and highlights the capabilities of Cisco Multicloud Defense, such as flexible and scalable security, distributed enforcement, network automation, and orchestration.

The target audience for this document is Cloud Architects, Security Architects, System Engineers, and Network Engineers.

Scope

This document covers Cisco Multicloud Defense architecture and outlines the various security capabilities and the use cases.

“For greater agility, flexibility and scale, organizations also deploy workloads and applications to public and private cloud environments – often times more than one cloud.”

Overview

In the cloud, everything is dynamic. Everything is connected, everything is encrypted, and everything should be automated. Most organizations leverage the cloud because of the economic benefits it offers their businesses and applications. In the ever-evolving threat landscape, organizations need to ensure their environments, workloads, and applications are secure and maintain compliance. Cisco Multicloud Defense provides a platform that enables organizations to focus on applications and policy, without having to worry about infrastructure and the dynamic nature of the cloud.

Multicloud Defense provides solution for the following use-cases:

- Ingress Security (IPS/IDS/WAF): Given the volume of exploits in the wild and the time it takes to fix apps, organizations implement detection and prevention rules to protect web and nonweb apps against threats.
- Egress Security: With the advancement of cloud apps and those apps' ability to initiate connections for themselves (updates, maintenance, 3rd-party services, etc.), organizations need to ensure those apps are communicating with the right/appropriate services.
- East/West Segmentation: Enterprises want to have sustainable and manageable macro-segmentation with cloud-native network security capability.
- Data Loss Prevention (DLP): DLP helps organizations with both compliance and security for sensitive and confidential data such as personally identifiable information (PII) and protected health information (PHI).
- Multicloud Networking: Enterprises want to have secure connectivity between different cloud infrastructures.

The relevant metrics of value for customers are:

- Accelerate time to value – Multicloud Defense enables teams to quickly onboard new cloud accounts, deploy security faster, and map existing policies consistently across clouds through automation and orchestration.
- Increase efficiency and accuracy – Reduce labor-intensive tasks, minimize misconfigurations, and gain efficiencies with security that is automatically applied and continuously enforced as new VPCs or workloads are deployed. Scale securely on demand with auto-scaling capabilities that enable you to meet traffic demands in near real time.
- Reduce overhead – Multicloud Defense consolidates solutions to reduce vendor sprawl and enables teams to stand up security in new cloud environments with minimal training.

Multicloud Defense Architecture

Cisco Multicloud Defense is a multicloud security as a service designed to provide highly scalable, agile, and robust security for multicloud environments. Multicloud Defense works in both highly distributed and centralized deployment architectures and scales to match ever-changing application demand. Cisco Multicloud Defense uses a common principle in public clouds and software-defined networking (SDN) that decouples the control and data plane, translating to two solution components: the Multicloud Defense Controller and the Multicloud Defense Gateways.

Customers can quickly onboard their cloud environments to begin protecting their infrastructure using distributed and/or centralized security architecture. This solution enables organizations to build unified security policies for multicloud infrastructure where the policy (per app, as opposed to per enforcement point) is created once and applied to the various enforcement points (Multicloud Defense Gateways) running in different cloud infrastructures.

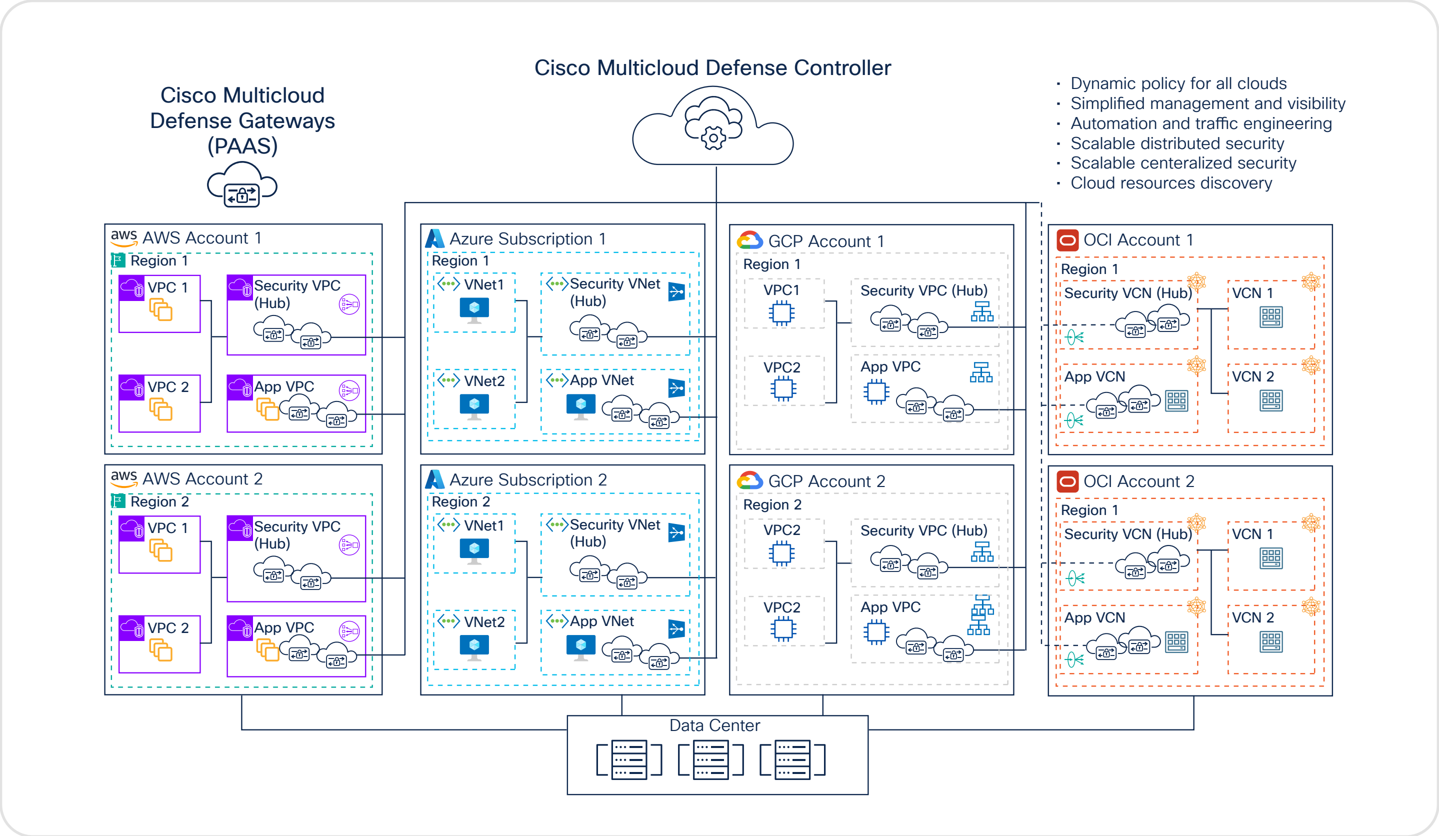


Figure 1. Cisco Multicloud Defense – Scalable distributed security architecture

Multicloud Defense Controller

The Multicloud Defense Controller is a multitenant service built using scalable and resilient microservices architecture and is delivered as a software as a service (SaaS). The Multicloud Defense Controller is a centralized control plane that automates and orchestrates infrastructure with enforcement points (gateways) to secure the applications across multiple clouds (AWS, Azure, GCP, and OCI). Customers can access the Multicloud Defense Controller through a web portal or may choose to use Terraform to instantiate security into the DevOps/DevSecOps processes.

- Modern cloud-native, microservices-based architecture for geo-scale and multitenancy
- Automated lifecycle management of Multicloud Defense Gateway(s)
- Logging and alerting
- Integration with 3rd-party SIEMs and alerting services like Syslog, Splunk, PagerDuty, Slack, and ServiceNow

Capabilities of Multicloud Defense Controller

Real-time discovery of multicloud networks and workloads regardless of scale.

Cloud-native gateway management with built-in self-healing and auto-scaling. This frees customers from having to maintain network security infrastructure and they can focus on security policies.

Cloud-native, microservices-based architecture delivered as a multi-tenant SaaS removes management plane upkeep and complexity.

Architecture meets SOC2 Type2, PCI DSS compliance, and well-architected design patterns of 3rd-party cloud providers. Customers' traffic also stays within their cloud account boundaries.

Continuously ingests security intelligence feeds from Cisco Talos® to keep Multicloud Gateways up to date with the latest protections against threats.

Integration with cloud-native networking to enable automation of highly distributed and/or centralized (hub-n-spoke) architectures for ingress, egress, east-west, and hybrid cloud.

Define dynamic multicloud policies using the workload identity provided by real-time discovery – security policies can be granular based on deployment type (dev, test, prod) and application tier (web-tier, app-tier, db-tier).

The controller uses continuous discovery in near real time to detect and apply tag-based policies on application architectures including virtualized, containerized, and serverless. The controller leverages the discovery capability to detect tags for application architectures including virtualized, containerized, and serverless. This discovery is continuous and in real time.

Built-in metering of customer usage for Multicloud Defense Gateways.

Multicloud Defense Gateway

Multicloud Defense Gateways are auto-scaling, with a patented single-pass pipelined architecture. These flexible gateways are deployed as platform as a service (PaaS) into the customer's public cloud account(s) by the Multicloud Defense Controller. This provides advanced inline security protections to defend against external attacks, block egress data exfiltration, and prevent the lateral movement of attacks. The Multicloud Defense Controller is SaaS-based, providing delivery, management, and orchestration of the gateways.

The Multicloud Gateway does inline traffic inspection and is the enforcement point for customer-configured policy. Located closer to the application in the customer's account, it supports all the necessary security services required to enforce the policy it receives from the controller. With this approach, organizations save on data transfer costs and preserve the PII data within the cloud account boundaries.

The Multicloud Defense Gateway uses a single pass architecture to provide:

- High throughput and low latency
- TLS decryption with reverse and forward proxies, and forwarding mode
- Flexibility in selecting relevant advanced network security inspection engines, including TLS decryption and re-encryption, web application firewall (WAF), HTTP and WebSocket, Layer 7 DoS protection, IDS/IPS, antivirus/antimalware, FQDN and URL filtering, DLP
- Multi-cloud support for AWS, Azure, GCP, and OCI

Highly Scalable Ingress and Egress Gateways

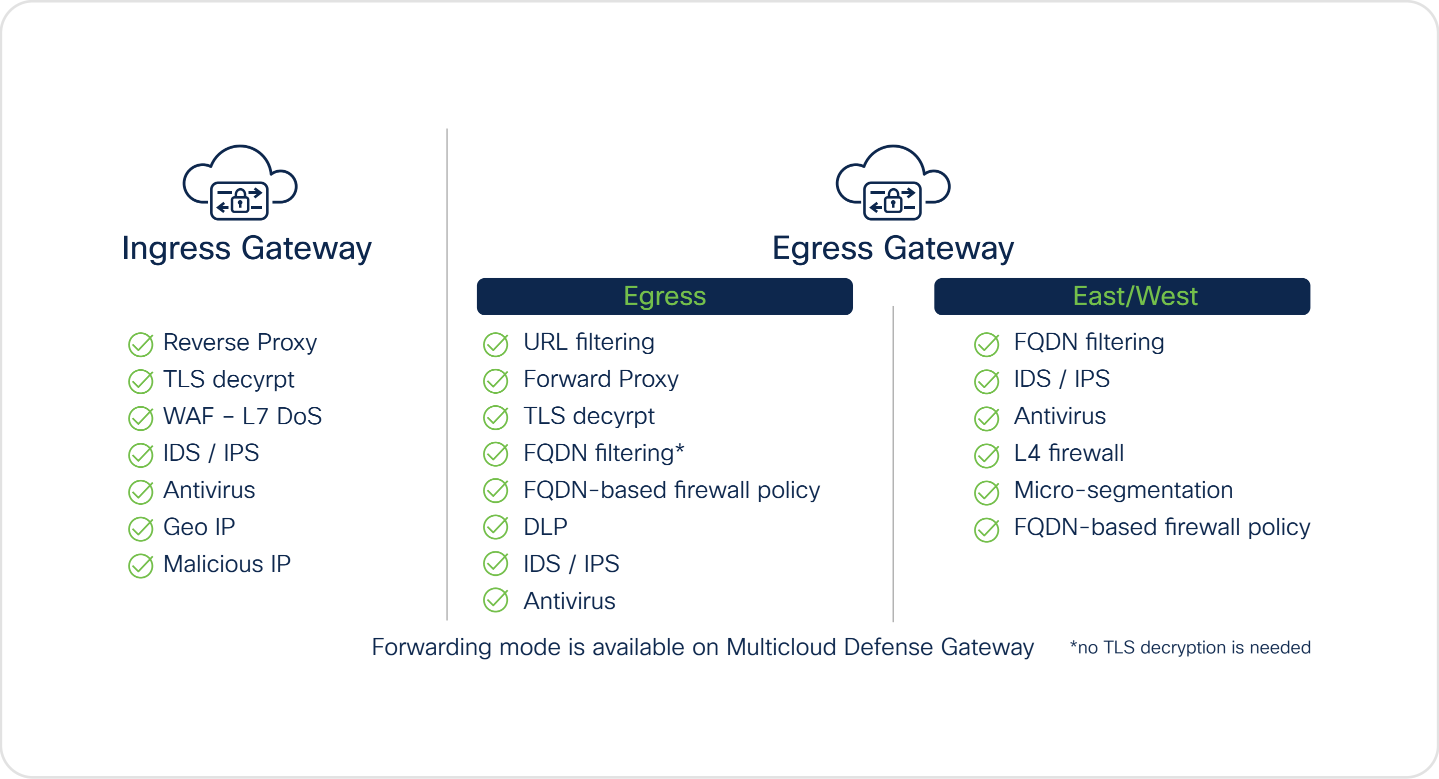
Customers can use the controller to deploy highly scalable and resilient egress gateways or ingress gateways into their public cloud account(s).

Egress Gateway(s)

Protect outbound and east/west traffic. This gateway provides security capabilities like FQDN filtering, URL filtering, DLP IPS/IDS, antivirus, forward proxy, and TLS decryption.

Ingress Gateway(s)

Protects inbound traffic and provides security capabilities like WAF, Layer 7 DoS, IDS/IPS, antivirus, reverse proxy, and TLS decryption.



Ingress Gateway

- ✓ Reverse Proxy
- ✓ TLS decyrpt
- ✓ WAF – L7 DoS
- ✓ IDS / IPS
- ✓ Antivirus
- ✓ Geo IP
- ✓ Malicious IP

Egress Gateway

Egress

- ✓ URL filtering
- ✓ Forward Proxy
- ✓ TLS decyrpt
- ✓ FQDN filtering*
- ✓ FQDN-based firewall policy
- ✓ DLP
- ✓ IDS / IPS
- ✓ Antivirus

East/West

- ✓ FQDN filtering
- ✓ IDS / IPS
- ✓ Antivirus
- ✓ L4 firewall
- ✓ Micro-segmentation
- ✓ FQDN-based firewall policy

Forwarding mode is available on Multicloud Defense Gateway

*no TLS decryption is needed

Figure 2. Multicloud Defense Gateway capabilities

Capabilities of the Multicloud Defense Gateway

- Full proxy support for reverse and forward proxy enables a comprehensive defense-in-depth content inspection of traffic flows including TLS with perfect forward secrecy (PFS).
- Advanced web traffic inspection is comparable to WAFs for advanced inspection of HTTPS.
- Packet capture (PCAP) of live attacks into a cloud storage bucket without significant performance degradation enables a rule-based capture on a per-session and per-attack basis.
- High throughput decryption and re-encryption in the range of multiple Gbps per gateway instance. This combined with auto-scaling of gateway instances, managed by the Multicloud Defense Controller, provides a highly scalable network security service that can inspect all traffic flows.
- Hardware offload for greater Multicloud Defense Gateway throughput.
- Multicloud Defense supports FPGA instances like AWS EC2 F1 and Azure N-series.

Forwarding Mode and Proxy Mode

The Multicloud Defense Gateway supports forwarding and proxy modes.

Forwarding Mode

The Multicloud Defense Gateway performs access control (allowing or denying) in forwarding mode without inspecting the actual packet/traffic contents. Access control at the gateway is based on communication occurring at the source and destination. Forwarding mode is commonly used for east-west flows and for egress where customers only want filtering based on options like IP address, Layer 4, tags, and FQDN (for FQDN filtering).

Proxy Mode

The Multicloud Defense Gateway also serves as a reverse proxy or forward proxy when performing content inspection of encrypted flows in addition to access control. The decryption of encrypted traffic ensures that attackers cannot exploit vulnerabilities in TLS-encrypted applications and cannot exfiltrate data (DLP) or connect to inappropriate URLs for well-known sites (i.e., AWS S3 buckets or Google Docs). Proxy mode is required for inspecting encrypted traffic (TLS Decrypt) to provide an advanced content inspection such as Layer 7 firewall, User ID, WAF, IDS/IPS, App ID, DLP, antivirus, antimalware, URL filtering, reverse proxy, and forward proxy.

Security Models

This solution provides flexible security insertion for the customer's infrastructure using three highly scalable and automated deployment models. These models include distributed, centralized, and combined.

Distributed Security Model

In the distributed security model, the Multicloud Defense Controller seamlessly adds gateways in each VPC/VNet/VCN. In this architecture, ingress and egress traffic stay local in the VPC/VNet/VCN.

Based on direction, traffic flow is inspected by egress or ingress gateways. This deployment ensures scalability, resiliency, and agility using cloud deployment best practices.

Figure 3 shows egress and ingress gateways in each VPC/VNet/VCN.

- For scalability, autoscaling is supported.
- For resiliency, auto-scaled instances are deployed in multi-availability zones.

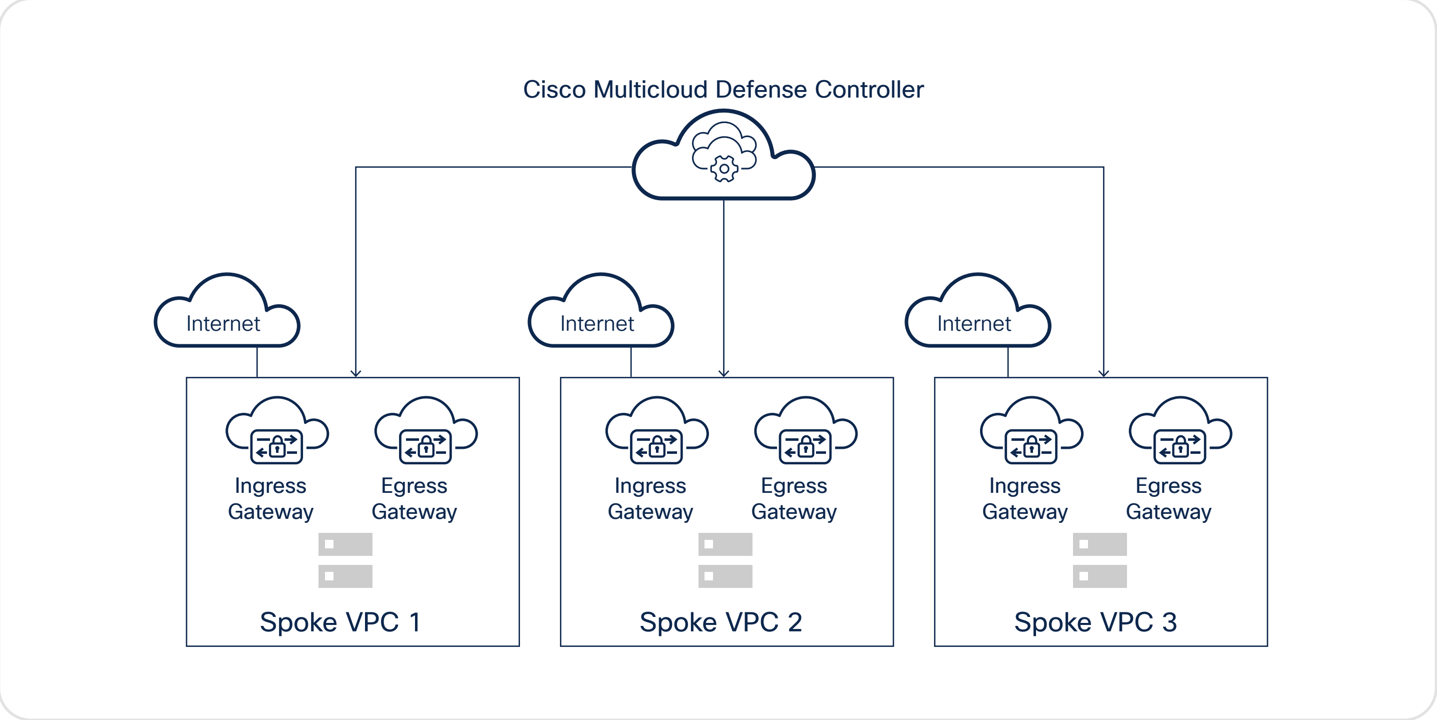


Figure 3. Distributed security model

Centralized Security Model

In the centralized security model, the Multicloud Defense Controller seamlessly adds gateways in the centralized security VPC/VNet/VCN. In this architecture, ingress and egress traffic is sent to a centralized security VPC/VNet/VCN for inspection before it is sent to the destination. This architecture ensures scalability, resiliency, and agility using cloud deployment best practices.

Figure 4 shows egress and ingress gateways in a security VPC/VNet/VCN.

- For scalability, autoscaling is supported.
- For resiliency, auto-scaled instances are deployed in multi-availability zones.
- Cloud service provider networking is automated by the controller as well to ensure traffic from the applications in the spokes is routed via gateways in the central security VPC.

In a centralized security model, gateways are deployed in a hub inside the customer's cloud account. However, customers can choose to have multiple hubs across accounts/subscriptions.

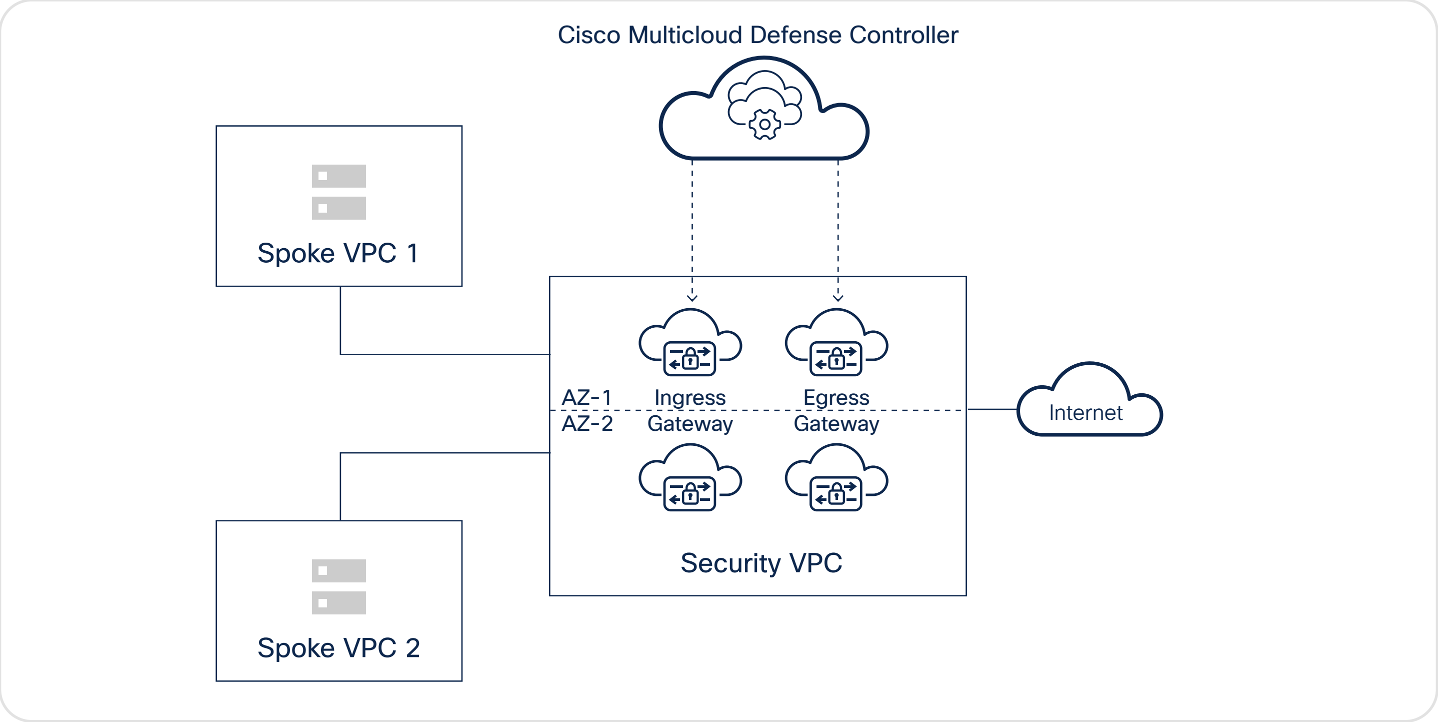


Figure 4. Centralized security mode

Combined Security Model (Centralized + Distributed)

This security model uses centralized and distributed models. In this case, some flows are protected by gateways deployed in the security VPC/VNet/VCN, and some flows are protected by gateways in the VPC/VNet/VCN.

Based on the traffic flow, traffic is inspected by egress or ingress gateways. This deployment ensures scalability, resiliency, and agility using cloud deployment best practices.

Figure 5 shows egress and ingress gateways in a centralized security VPC/VNet/VCN in addition to gateways deployed in the application VCPs/VNets/VCNs.

- For scalability, autoscaling is supported.
- For resiliency, auto-scaled instances are deployed in multi-availability zones.

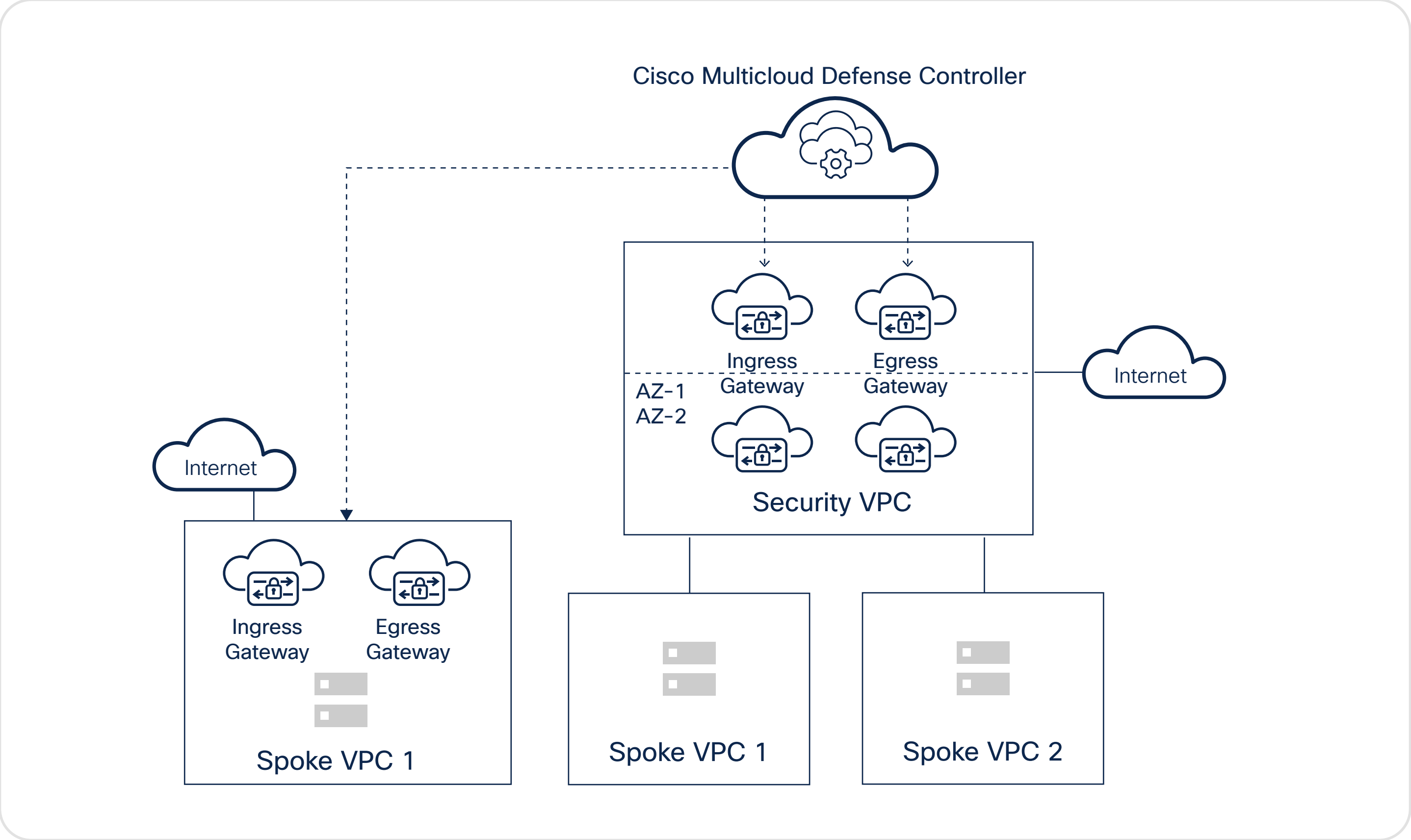


Figure 5. Centralized + distributed security model

Conclusion

We live in a multicloud world, and organizations need a cloud-agnostic solution that unifies security controls across all environments while protecting workloads at cloud speed and scale. With Cisco Multicloud Defense, customers can leverage a simplified and unified security experience to navigate their multicloud future with confidence

For more information on Cisco Multicloud Defense, visit: cisco.com/go/multicloud-defense.