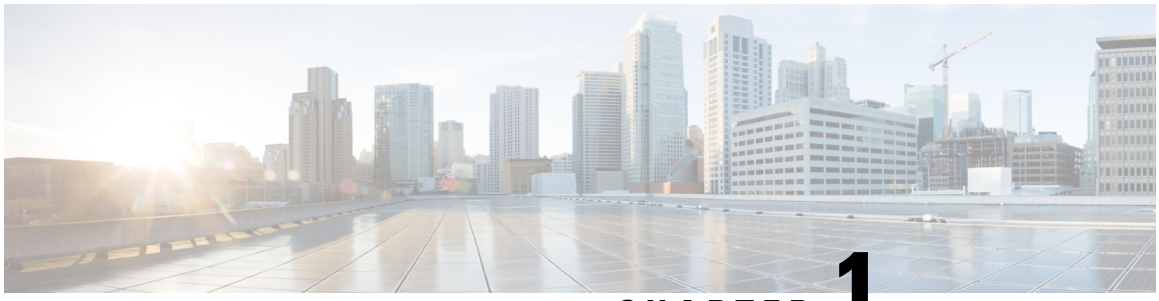
Cisco Multicloud Defense Release Notes

First Published: 2023-08-25

Last Modified: 2024-04-18

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



CHAPTER 1

Welcome

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

We strongly recommended using the following releases for each Multicloud Defense component:

Multicloud Defense Controller

Version 24.02, February 26, 2024

Multicloud Defense Gateway

Version 23.08-15, March 27, 2024

Multicloud Defense Terraform Provider

Verison 24.2.1, February 31, 2024

Supported Versions

The following versions are currently supported by Multicloud Defense components:

Multicloud Defense Controller Versions

- Version 24.02, February 26, 2024
- Verison 23.12, December 14, 2023

Multicloud Defense Gateway

- Version 23.10-03, January 11, 2024
- Verison 23.08-14, January 25, 2024
- Verison 23.06-14, November 12, 2023

Multicloud Defense Terraform Provider

- Version 23.10.1, November 6, 2023
- Version 23.8.1, August 22, 2023
- Version 23.7.2, July 27, 2023
- Version 23.6.1 July 17, 2023

Additional Resources and Assistance

Online Resources

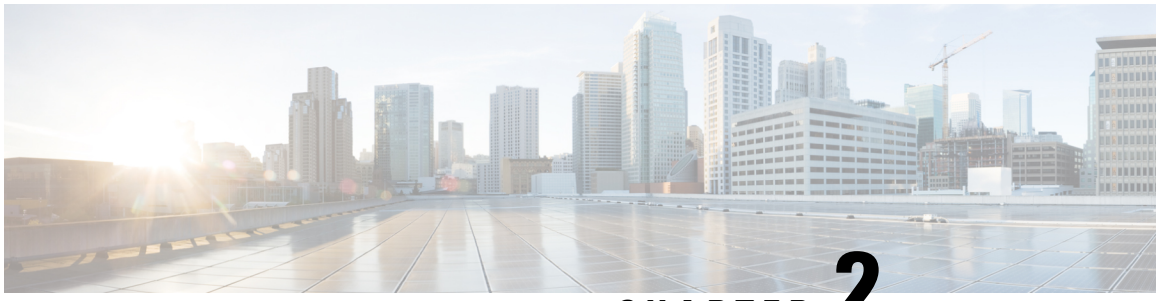
Cisco provides this additional documentation:

- Cisco Multicloud Defense User Guide
- Cisco Multicloud Defense FAQs

Contact Cisco

If you cannot resolve an issue using the online resources listed above, contact Cisco TAC:

- Email Cisco TAC: tac@cisco.com
- Call Cisco TAC (North America): 1.408.526.7209 or 1.800.553.2447
- Call Cisco TAC (worldwide): Cisco Worldwide Support Contacts



CHAPTER 2

Multicloud Defense Components

The following components make up the Multicloud Defense experience.

Multicloud Defense Controller

The Multicloud Defense Controller is a Software as a Service (SaaS) component delivered with CDO. It operates as the control plane of the Multicloud Defense and provides administrators the ability to deploy, configure and manage all aspects of Multicloud Defense. It is also the translation layer between operations performed in the Multicloud Defense Controller or terraform provider, and the orchestration of those operations within the cloud service provider.

Capabilities that are provided through the Multicloud Defense Controller include the following:

- Cloud service provider account on-boarding.
- Cloud service provider asset and traffic visibility discovery.
- Services VPC/VNet creation and management.
- Spoke VPC/VNet protection management.
- Gateway deployment, auto-scaling and updates.
- Security policy definition and deployment.
- 3rd party SIEM and Alert integrations.
- Traffic and security event investigation and analysis.
- Discovery and threat awareness report generation.

CDO operations is responsible for updating the Multicloud Defense Controller. Enhancements and updates are provided frequently and can be delivered regularly based on planned release updates, or deployed by way of hot fixes to address critical fixes rapidly.

Multicloud Defense Gateway

The Multicloud Defense Gateway is a platform as a service (PaaS)-delivered component that operates as the data plane deployed in the cloud service provider account to protect public cloud workloads. The Multicloud Defense Gateway is deployed and operates entirely within the cloud service provider account. All traffic processing and security protections reside within the cloud service provider.

Capabilities offered by the Multicloud Defense Gateway include the following:

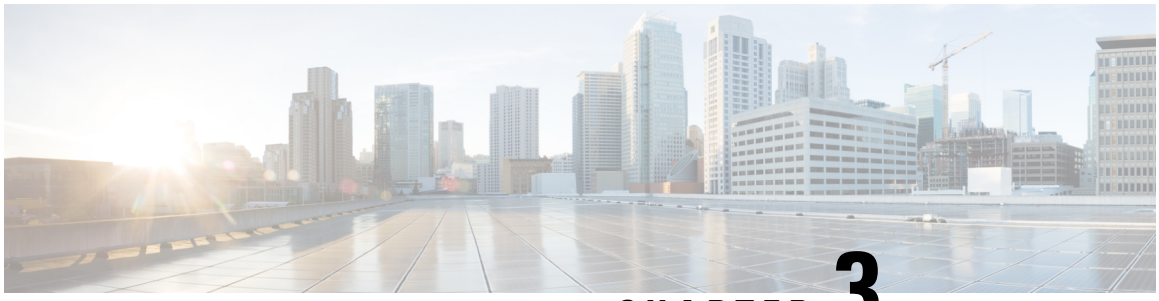
- Cloud native architecture for protecting workloads.
- Ingress, egress and east-west use-cases.
- Forwarding and proxy-based processing.
- Full decryption for traffic payload inspection.
- Advanced security from a web application firewall (WAF), IDS/IPS, DLP and L7 DOS.
- Filtering via L4, URL/URI, and malicious and geographical IP.
- Orchestration via the Multicloud Defense Controller and terraform provider.
- Multi-cloud, multi-region and multi-availability zone deployment.
- Dynamic auto-scaling based on workload demands.
- Dynamic multi-cloud security policy using cloud constructs.

The customer is responsible for updating the Multicloud Defense Gateway through an upgrade process that is simple, hitless and is completed in minutes. Gateway enhancements and updates are provided frequently.

Multicloud Defense Terraform Provider

The Multicloud Defense terraform provider is a multi-cloud service provider infrastructure-as-code (IaC) orchestration language used to deploy, configure and manage an entire Multicloud Defense deployment via a continuous integration, continuous deployment (CICD) pipeline. It can be used exclusively or in conjunction with the Multicloud Defense Controller and accommodates most operations that are available using the controller.

The customer is responsible for updating their Multicloud Defense terraform provider through referencing the desired terraform release and running a `terraform update` command that loads the referenced version.



CHAPTER 3

Enhancements and Fixes

The following entries include all features, enhancements, and bug fixes that have occurred in each component at the time of each release.

Multicloud Defense Controller Enhancements

Version 24.02 February 26, 2024 (Recommended)

Features

The following features are included in this release:

Hybrid Cloud

- (Private Preview) Site-to-site VPN (requires Multicloud Defense Gateway version 24.02 or later).

Orchestration

- Cross-Subscription Spoke VNet protection (Azure).
- Route table creation for Spoke VPC/VNet protection.
- LB Health Check Security Group orchestration.

Gateway

- Reduced disk size for all Gateway instance types.
- Enable/Disable Gateway SSH access.
- Upgrade Gateway from Details page.
- Cancel Gateway upgrade.
- Instance level actions (terminate protect, replace instance, restart datapath).

Integrations

- Dynamically track changes to cloud service provider-certificates.
- User management with Azure Active Directory.

Miscellaneous

- Performance improvements.
- Operational improvements.
- Bug fixes and stability improvements.

Enhancements

The following enhancements are included in this release:

- (Private Preview) Added support for site-to-site VPN. This includes VPN tunnel configuration, including IPSec and BGP. The VPN is terminated directly on the gateway to process and protect traffic flowing across the VPN. This enhancement requires Multicloud Defense Gateway version 24.02 or later.
- Adds support for orchestrating route tables in spoke VPCs and VNets to ensure traffic originating or returning from the spoke VNet/VPC and route to the service VPC/VNet containing the Multicloud Defense Gateway. This enhancement includes a workflow for create route tables and route entries, and associating the route tables with subnets.
- Adds support for cross-subscription spoke VNet protection by orchestrating spoke VNet peering to route traffic from the spoke VNet to the services VNet containing Multicloud Defense. This ensures the orchestration in Azure is parity with similar orchestrations in AWS and GCP.
- Adds support for orchestrating the security group, network security group, and firewall rules CIDRs related to health checks from the cloud service provider load balancer (Azure, GCP, OCI) or heath check service (GCP).
- Adds support for enabling and disabling SSH from the **Gateway Details** page to accommodate reverse SSH using Teleport. Requires Multicloud Defense Gateway version 23.10 or later, which supports Teleport integration.
- Adds support for upgrading the Multicloud Defense Gateway from the **Gateway Details** page.
- Adds the ability to cancel (abort) a Multicloud Defense Gateway upgrade.
- Adds gateway instance-level actions (terminate protect, replace instance, restart datapath).
- Reduces the disk size for all instances in all cloud service providers from 256GB to 128GB.
- Adds support to dynamically track changes to certificate objects where the private key is stored in the cloud service provider and retrieved by the Multicloud Defense Gateway. When changes take place to the cloud service provider resource, the controller instructs the gateway to reread the private key from the cloud service provider resource to ensure that it is accessible and the updated content is used. If there are any issues with accessing the certificate, a system log message will be generated.
- When selecting a region for gateway deployment, a region friendly name should be displayed for all regions along with the true region name (lowercase name). This enhancement ensures that all regions are displayed with both the friendly and true region names.

- Adds support for configuring the Multicloud Defense Controller to integrate with Azure Active Directory for authentication.
- Improves performance of various resource view pages to reduce number of API calls and improve overall load times.
- Adds pagination support for **Traffic Summary** page to improve performance.
- Adds pagination support for **Stats** page to improve performance.

Fixes

The following fixes are included in this release:

- Fixes an issue where the Inventory and Discovery views would not display asset information if the region does not include a gateway deployment.
- Fixes an issue where deployment of an ingress gateway Azure would not be successful if the ingress policy rule set is empty.
- Fixes an issue where log forwarding to an S3 bucket would not work if the log forward profile is used in a group log forwarding profile.
- Fixes an issue where deleting the gateway from the UI does not fully delete the gateway on the backend inhibiting deploying a replacement gateway with the same name.
- Fixes an issue where disabling assign public IP addresses for a gateway deployed in Azure performs a blue/green gateway replacement, but does still assigns public IPs.
- Fixes an issue where the first category and FQDN Row of an FQDN filter profile could not be deleted.
- Fixes an issue to ensure the gateway names in the gateway filter are sorted alphabetically.
- Fixes an issue with export to Terraform for account and gateway resources where the resulting exported Terraform was empty.
- Fixes an issue where the policy rule set Status would show as **Updating** even though the gateway policy Status is shown as **Updated**.
- Fixes an issue where a scale out would be unsuccessful due to a health check failure even though the instance is healthy.
- Changes the health check unhealthy time period to 120 seconds. When a new gateway is deployed, the load balancer heath check or health check service will be orchestrated to evaluate an instance health over a 2 minute (120 second) period. The previous orchestration would evaluate over a 20 second period.
- Fixes an issue to ensure the time zone select defaults to **Local** rather than **UTC**.
- Fixes an issue in the **Stats** page where CPU metric was always showing an order of magnitude less than what should be shown.
- Fixes an issue with deleting a spoke VPC peering in GCP where the spoke VPC would not be deleted. This issue occurs only when the VPC ID was used instead of the self-link.
- Fixes consistency issues with the display of **Last Modified** information across resources.
- Fixes various UI-related resource links where the link would not redirect to the linked resource.
- Fixes various UI-related issues related to advanced search.

- Fixes various UI workflows to ensure proper behavior

Version 23.12 December 14, 2023

Features

The following features are included in this release:

Orchestration

- User-supplied NLB IP for gateway creation in GCP.
- GCP health check CIDRs in datapath firewall rule.

Policy

- Apply ICMP policy to gateways across cloud service providers.

Integrations

- Multiple Syslog Servers in log forwarding group.

Usability

- Additional fields for filtering and advanced search.
- SNAT configuration display in policy rule set.

Miscellaneous

- Performance improvements.
- Operational improvements.
- Bug fixes and stability improvements.

Enhancements

The following enhancements are included in this release:

- Adds fields to Advanced Search that were initially not available.
- Enhances the gateway creation in GCP to allow a user-provided IP resource to be used as the load balancer frontend IP. This can only be supplied when using Terraform.
- Adds display of the service object SNAT setting in the policy rule set view.
- Relaxes the hard requirement for a cloud service provider to support ICMP to apply an ICMP policy to a gateway that is deployed in that cloud service provider. A policy rule set that contains an ICMP policy can now be applied to any gateway that resides in any cloud service provider, whether or not the cloud service provider supports ICMP.
- Adds support for more than one Syslog Server configuration in a log forwarding group.
- Adds GCP health check CIDRs when orchestrating datapath firewall rule.

Fixes

The following fixes are included in this release:

- Fixes an issue where the log forwarding profile for Splunk was showing unreachable even though the Splunk endpoint was reachable.
- Fixes an issue where de-orchestrating an AWS Service VPC would not fully clean up all VPC resources, including the VPC itself.
- Fixes an issue where all address objects would be displayed when a user is creating or editing a reverse proxy service object. Only reverse proxy service objects are now being displayed.
- Fixes an issue where the controller was using an incorrect Project ID when orchestrating a gateway into a GCP shared VPC scenario.
- Fixes an issue where the list of address objects was not showing in the drop down when creating or modifying a group address object.
- Fixes the typeahead search for cloud service provider account in the create gateway workflow.
- Fixes an issue when adding a rule within the policy rule set to improve the performance and ensure the operation is quick.
- Fixes an issue where adding an AWS account through the CDO page could result in a timeout.
- Fixes the count issue for FQDN match and FQDN filtering objects. The counts were representing both types of objects in each view.
- Fixes various advanced search and filter issues.
- Fixes an issue where deploying a gateway into Azure when Azure has no available capacity would fail deployment and not clean up the created resources. When Azure has no capacity, it does not inhibit creating a virtual machine and its associated resources. It creates the VM, but brings up the VM in a failed state with an error message. This scenario needed to be handled in a specific way to ensure that it is recognized, the proper action is taken to clean up the resources and the user is made aware of the cloud service provider issue through a system log message.
- Fixes an issue where the cloud service provider resource and capacity information is not displayed when deploying a gateway in Azure.
- Improves the performance of displaying the list of rules in a policy rule set.
- Fixes an issue where deleting the GCP-based account would not delete all of the inventory objects related to inventory discovery.
- Addresses an issue with gateway instance per-zone rows that would inhibit a user from removing the first row. This only applies to scenarios where the gateway is deployed into a user-managed VPC or VNet.
- Fixes an issue where deploying a gateway into GCP would not orchestrate the egress route into the orchestrated service VPC.
- Fixes an issue where orchestrating spoke VPC protection could fail.
- Corrects an issue where the SNI and L7 DOS profiles would not be displayed when editing a reverse proxy service object.

- Fixes an issue where a UI change operation to the assign public IPs settings could trigger an unnecessary blue/green gateway replacement.
- Fixes an issue where orchestrating a gateway into multiple GCP regions could result in a race condition that would inhibit the gateway from becoming active.
- Fixes an issue where a new gateway deployment would become immediately inactive due to an internal error.
- Fixes an issue where a forwarding or forward proxy policy rule set that was created by Terraform would be displayed in the UI as a reverse proxy rule.
- Fixes an issue where rules could not be reordered when editing a policy rule set.
- Fixes an issue where a service object that contained more than 20 rows would be accepted and pushed to the gateway resulting in a gateway crash. The service object is now limited to 20 rows. This limit validation is performed by both the controller and gateway.
- Fixes an issue to ensure the Gateway Details page displays the date modified and data created times.
- Fixes an issue with proper sorting for views containing objects and profiles that span multiple pages.
- Improves performance of various object creation pages.
- Improves the user experience through fixes and enhancements throughout the UI.
- Ensures the user-specified time setting of local or UTC is honored across views and persists across portal invocations. The persistence across portal invocations is achieved by storing this setting in the browser cache.
- Fixes a UI issue where the tooltip information was missing for custom managed Encryption Key gateway configuration.
- Ensures the controller generates System Log messages when the gateway fails to become active due to cloud service provider errors.

Multicloud Defense Gateway Enhancements

Version 24.02

Version 24.02-02 April 18, 2024

Fixes

The following fix is included in this release:

- Fixes an issue related to memory buffer access during gateway initiatlization that would inhibit a new gateway instance from becoming active.

Version 24.02-01 February 28, 2024

Enhancements

The following enhancements are included in this release:

- [Private Preview] Adds support for site-to-site VPN. This includes VPN tunnel configuration, including IPSec and BGP. The VPN is terminated directly on the Multicloud Defense Gateway to process and protect traffic flowing across the VPN. This enhancement requires Multicloud Defense Gateway version 24.02 or later.
- Adds support to dynamically track changes to certificate objects where the private key is stored in the cloud service provider and retrieved by the Multicloud Defense Gateway. When changes take place to the cloud service provider resource, the Multicloud Defense Controller will instruct the gateway to reread the private key from the cloud service provider resource to ensure that it is accessible and the updated content is used. If there are any issues with accessing the certificate, a system log message is generated.
- Adds a message to the management Linux shell when logging in via SSH. The message emphasizes that the device is a Cisco-managed device (e.g., a device managed by the Multicloud Defense Controller).
- Adds support for more than one syslog server configuration in a log forwarding group.

Fixes

The following fixes are included in this release:

- Addresses the CVE-2023-4863 vulnerability related to libwebp version 1.2.0-3.el9.
- Fixes an issue where a policy change that results in a datapath hitless restart could cause high latencies that impact traffic processing, including load balancer health checks, under light or moderate load.
- Fixes an issue addressed in version 23.08-12 that still impacted 4-core instance types. The issue addresses high CPU utilization caused by debug I/O activity. The previous fix now addresses all instance types across all cloud service providers.
- Fixes an issue related to high CPU utilization that was caused by I/O related debug activity.
- Fixes an issue related to intermittent load balancer healthcheck failures. The fix enhances the gateway by prioritizing heathchecks to ensure the load balancer does not incorrectly mark instances as unhealthy.
- Fixes an egress gateway memory leak that would be automatically corrected by triggering a self-healing preemptive datapath restart.
- Fixes an issue where a generated gateway diagnostic bundle would be larger than what would be permitted to send to the Multicloud Defense Controller resulting in the inability to analyze gateway logs. This fix addresses the restrictive limit so generated diagnostic bundles will be successfully sent to the Multicloud Defense Controller.
- Fixes an issue where more than one SNI event was being recorded for each session processed by forward proxy rule.
- Improvements to the stability of the Multicloud Defense Gateway.
- Fixes a traffic processing issue where traffic would stop being processed after TCP and TLS due to a race condition related to DNS-based FQDN caching.

- Fixes an issue where the Multicloud Defense Gateway might not successfully build the IP cache when either an active or inactive rule has DNS-based FQDN caching configured. When the cache is not properly built, policy could fail to match traffic. This fix ensures the IP cache is properly built in order for the policy match and process traffic properly.
- Changes the timeout for waiting for a SYN ACK after receiving a SYN. The original timeout was 120 seconds. In certain scenarios (e.g., port scanning) where a SYN ACK is never returned, a long timeout will consume an entry in the session pull long that desired. For scenarios where many sessions do not respond with a SYN ACK, the session pool could be exhausted. This is often referred to as a SYN flood. By reducing the timeout, the session will be released sooner in order to free up the session pool for use in processing valid sessions. The timeout has been reduced to 30s and is configurable via a Multicloud Defense Gateway setting.
- Fixes an issue related with DNS-based FQDN Address Object resources where enabling DNS caching could result in a race condition between policy change and the DNS resolution interval that would result in the cache for a domain to be reset to a value of 0 (no cache). When this situation occurs, the domain resolution will never be cached and any existing cache values will be flushed as their TTL expire. The end result is the Multicloud Defense Gateway will eventually not match traffic for that domain. This fix addresses the race condition such that the cache will operate as expected.
- Fixes an issue where the DPI (IDS/IPS) Security Event sent to a syslog server did not have the **Action** field present. The **Action** field was present, but the values were not consistent with the Action values present in the UI or the event information sent to other SIEMs. The fix addresses this universally across all security events to ensure the **Action** field has values of `ALLOW` or `DENY`.
- Fixes an issue where a change to a security profile auto-update to manual where the ruleset version is not changed would result in an unnecessary datapath restart. The fix ensures that the change is applied without requiring a datapath restart.
- Improvements to the stability of the Multicloud Defense Gateway.
- Improvements to the performance of the Multicloud Defense Gateway.
- Fixes an issue with the SNI Security Event where the domain that is obtained from the SNI field of a TLS hello message would populate the text field for the event rather than the FQDN field. The change to populate the FQDN field provides consistency across logs and events when viewing and filtering by domain using the FQDN field.
- Fixes an issue with the datapath process that could result in a session pool leak. When this situation occurs, the datapath will evaluate the session pool consumption and self heal before the leak becomes operationally impactful. This fix corrects the leak to avoid the datapath needing to self-heal.
- Improves performance of the Multicloud Defense Gateway by optimizing API calls to the Multicloud Defense Controller to retrieve gateway profile information.
- Fixes an issue where setting the policy rule set action to a `No Log` value would still generate a log message.

Version 23.10

Version 23.10-03 January 11, 2024

Fixes

The following fixes are included in this release:

- Fixes an issue where a generated gateway diagnostic bundle would be larger than what would be permitted to send to the controller resulting in the inability to analyze gateway logs. This fix addresses the restrictive limit so generated diagnostic bundles will be successfully sent to the controller.
- Fixes an issue where the gateway might not successfully build the IP cache when either an active or inactive rule has DNS-based FQDN caching configured. When the cache is not properly built, policy could fail to match traffic. This fix ensures the IP cache is properly built in order for the policy match and process traffic properly.
- Changes the timeout for waiting for a SYN ACK after receiving a SYN. The original timeout was 120 seconds. In certain scenarios (e.g., port scanning) where a SYN ACK is never returned, a long timeout will consume an entry in the session pull long that desired. For scenarios where many sessions do not respond with a SYN ACK, the session pool could be exhausted. This is often referred to as a SYN flood. By reducing the timeout, the session will be released sooner in order to free up the session pool for use in processing valid sessions. The timeout has been reduced to 30s and is configurable via a gateway setting.
- Improvements to the stability of the gateway.

Version 23.10-02 November 16, 2023

Fixes

The following fix is included in the upgrade:

- Fixes an issue related with DNS-based FQDN address object resources where enabling DNS caching could result in a race condition between policy change and the DNS resolution interval that would result in the cache for a domain to be reset to a value of 0 (no cache). When this situation occurs, the domain resolution will never be cached and any existing cache values will be flushed as their TTL expire. The end result is the gateway will eventually not match traffic for that domain. This fix addresses the race condition such that the cache will operate as expected.

Version 23.10-01 November 3, 2023

Enhancements

The following enhancements are included in this upgrade:

- Moves the policy type mismatch message generated for each session that is processed by two rules that have mismatched policy type (forwarding and forward proxy) to an event related to each session. This eliminates many system log messages when this scenario occurs and generates error as an event associated with each session. When this scenario occurs, the session will be denied and the event will report the reason. The deny will also be represented in the traffic summary log.

- Enhances the forward proxy policy to validate the server certificate when negotiating the backend TLS session. The certificate validation is disabled by default, but can be configured in a decryption profile for all TLS sessions and in an FQDN match object on a per-domain (or set of domains) basis.
- Integrates with teleport to accommodate reverse SSH making it easier to SSH to the gateway instance management interface especially when the gateway is orchestrated without public IPs. The requirements to SSH is rare and only necessary for advanced troubleshooting purposes. Inbound communication is inhibited by default using cloud service provider restrictions (security groups, network security groups, firewall rules).

Fixes

The following fixes are included in this upgrade:

- Fixes an issue related to a forward proxy rule that uses an FQDN match object for decryption exception could result in traffic processing issues.
- Fixes an issue where traffic would be incorrectly denied by a forward proxy rule configured with an FQDN match profile due to delays in certificate validation. The deny will be seen as an `FQDNFILTER` security eent even though an FQDN filtering profile is not applied.
- Fixes an issue where a rule that uses an FQDN match object would incorrectly process traffic for an uncategorized domain.
- Fixes an issue related to dynamic address objects where a large number of IPs and a large number of changes to those IPs could result in the datapath not accepting changes, causing matching issues resulting in traffic being processed incorrectly.
- Fixes an issue with DNS-based FQDN caching where setting the DNS resolution interval would not change the frequency of DNS resolution.
- Fixes an issue with packet collection that could cause the gateway to become unhealthy.
- Fixes an issue where certain logs from the gateway could contain private key information.
- Fixes various gateway stability issues.
- Fixes a gateway memory leak that could also cause a CPU issue resulting in traffic processing issues.
- Fixes an issue where the URI information is not shown in traffic summary log.
- Fixes an issue where L7DOS event does not properly show the URI.

Version 23.08

Version 23.08-15-b1 April 12, 2024

This is a hotfix.

Fixes

The following fix is included in this hotfix:

- Fixes an issue with log rotation for gateways in OCI. The fix ensures that the logs are properly rotated to not consume unnecessary disk space.

Version 23.08-15-a1 April 11, 2024

This is a hotfix.

Fixes

The following fix is included in this hotfix:

- Fixes an issue related to blue/green policy change. When the policy change occurs and the new datapath becomes active, the gateway begins draining current sessions off the old datapath. If the datapath cannot properly drain the sessions, it treats the datapath as unhealthy and will employ a datapath restart. This will terminate both old and new datapaths, which could cause disruption to old and new sessions. The fix ensures that the session draining completes properly and eliminates the situation where the datapath is seen as unhealthy.

Version 23.08-15 March 27, 2024 (Recommended)

Fixes

The following fixes are included in this release:

- Fixes an issue where HTTP traffic passing through an ingress gateway was not using the proper domain specified in the reverse proxy target associated with the matched policy rule set.
- Fixes an issue where HTTP traffic passing through an ingress gateway was not properly matching the proper policy rule set.
- Fixes an issue related to forwarding and how the datapath protocol stack handles timings with TCP FINs and RSTs. A FIN from the server and a RST from the client could occur in a sequence such that the protocol stack would inhibit accepting (and forwarding) the RST after it has already seen a FIN. The change relaxes the protocol stacks acceptance of the RST so it can be forwarded to the server and not dropped by the protocol stack. The RST drop occurs due to a mismatch in the expected sequence number since the protocol stack has already received a FIN from the server.
- Fixes an issue where the datapath could restart due to a policy change taking too long to apply.
- Fixes an issue that results in increased CPU usage during a blue/green policy update where two datapaths would be running at the same time. Each datapath would consume CPU in a way that assumes it is the only datapath running. When the second datapath is instantiated to accommodate the new policy, the CPU would not be shared properly and the CPU metrics would not be recorded properly.
- Fixes an issue related to a memory leak for that would result in a preemptive datapath self-heal.
- Addresses the CVE-2023-4863 vulnerability related to libwebp version 1.2.0-3.el9.
- Fixes an issue related to a lost write event after a write operation to the backend server returns EAGAIN. This lost event causes the gateway to think it has sent the request body to the backend server and is awaiting a response that will never arrive. This is a timing issue related to the speed of the gateway vs. the speed of the backend server.
- Fixes an issue with generating diagnostic bundles for gateways deployed in OCI.
- Fixes an issue related to active connection reset where the TCP RST was being sent with the wrong sequence number and not actively resetting the connection.

- Fixes a traffic processing issue during a policy change where traffic passing through the datapath running the old policy would be unnecessarily delayed.
- Fixes an issue with large request body traffic where the WAF component would consume the client request body. This causes thevgateway to keep expecting the request body from the client, while the client is expecting a response from the gateway, leading to a client timeout.

Version 23.08-14-e1 March 28, 2024

This is a hotfix.

Fixes

The following fixes are included in this hotfix:

- Fixes an issue where a policy rule that uses DNS-based FQDN cache could become corrupted causing the gateway to not properly process traffic.
- Addresses the CVE-2023-4863 vulnerability related to libwebp version 1.2.0-3.el9.

Version 23.08-14-a2 March 20, 2024

This is a hotfix.

Fixes

The following fixes are included in this hotfix:

- Fixes an issue related to forwarding and how the datapath protocol stack handles timings with TCP FINs and RSTs. A FIN from the server and a RST from the client could occur in a sequence such that the protocol stack would inhibit accepting (and forwarding) the RST after it has already seen a FIN. The change relaxes the protocol stacks acceptance of the RST so it can be forwarded to the server and not dropped by the protocol stack. The RST drop occurs due to a mismatch in the expected sequence number since the protocol stack has already received a FIN from the server.
- Fixes an issue that results in increased CPU usage during a blue/green policy update where two datapaths would be running at the same time. Each datapath would consume CPU in a way that assumes it is the only datapath running. When the second datapath is instantiated to accommodate the new policy, the CPU would not be shared properly and the CPU metrics would not be recorded properly.

Version 23.08-14-d1 March 13, 2024

This is a hotfix.

Fixes

The following fixes are included in this hotfix:

- Fixes an issue where HTTP traffic passing through an ingress gateway was not using the proper domain specified in the reverse proxy Target associated with the matched policy rule set.
- Fixes an issue where HTTP traffic passing through an ingress gateway was not matching the proper policy rule set.

Version 23.08-14-c1 February 20, 2024

This is a hotfix.

Fixes

The following fix is included in this hotfix:

- Addresses the CVE-2023-4863 vulnerability related to libwebp version 1.2.0-3.el9.

Version 23.08-14-b1 February 21, 2024

This is a hotfix.

Fixes

The following fixes are included in this hotfix:

- Fixes an issue related to a lost write event after a write operation to the backend server returns EAGAIN. This lost event causes the Multicloud Defense Gateway to think it has sent the request body to the backend server and is awaiting a response that will never arrive. This is a timing issue related to the speed of the gateway vs. the speed of the backend server.
- Fixes an issue with generating diagnostic bundles for gateways deployed in OCI.
- Fixes an issue with large request body traffic where the WAF component would consume the client request body. This causes the Multicloud Defense Gateway to keep expecting the request body from the client, while the client is expecting a response from the Multicloud Defense Gateway, leading to a client timeout.

Version 23.08-14-a1 February 17, 2024

This is a hotfix.

Fixes

The following fixes are included in this hotfix:

- Fixes an issue related to active connection reset where the TCP RST was being sent with the wrong sequence number and not actively resetting the connection.
- Fixes a traffic processing issue during a policy change where traffic passing through the datapath running the old policy would be unnecessarily delayed.

Version 23.08-14 January 25, 2024

Fixes

The following fixes are inluded in this release:

- Fixes an issue addressed in 23.08-12 that still impacted 4-core instance types. The issue addresses high CPU utilization caused by debug I/O activity. The previous fix now addresses all instance types across all cloud service providers.

- Fixes an issue where a policy change that results in a datapath hitless restart could cause high latencies that impact traffic processing, including load balancer health checks, under light or moderate load.

Version 23.08-12 January 18, 2024

Fixes

The following fixes are included in this release:

- Fixes an issue related to high CPU utilization that was caused by I/O related debug activity.
- Fixes an issue related to intermittent load balancer healthcheck failures. The fix enhances the gateway by prioritizing heathchecks to ensure the load balancer does not incorrectly mark instances as unhealthy.
- Improves performance of the gateway by optimizing API calls to the controller to retrieve gateway profile information.

Version 23.08-11 January 11, 2024

Enhancements

The following enhancement is included in this release:

- Moves the policy type mismatch message generated for each session that is processed by two rules that have mismatched policy type (gorwarding and gorward proxy) to a security event log related to each session. This eliminates a large volume of per-session system log messages without eliminating the per-session log. When this scenario occurs, the session will be denied and the event associated with the session will report the reason. The deny will also be represented in the traffic summary log.

Version 23.08-10 December 18, 2023

Fixes

The following fixes are included in this release:

- Changes the timeout for waiting for a SYN ACK after receiving a SYN. The original timeout was 120 seconds. In certain scenarios (e.g., port scanning) where a SYN ACK is never returned, a long timeout will consume an entry in the session pull long that desired. For scenarios where many sessions do not respond with a SYN ACK, the session pool could be exhausted. This is often referred to as a SYN flood. By reducing the timeout, the session will be released sooner in order to free up the session pool for use in processing valid sessions. The timeout has been reduced to 30s and is configurable via a gateway setting.
- Fixes an issue where the gateway might not successfully build the IP cache when either an active or inactive rule has DNS-based FQDN caching configured. When the cache is not properly built, policy could fail to match traffic. This fix ensures the IP cache is properly built in order for the policy match and process traffic properly.
- Fixes an issue where a generated gateway diagnostic bundle would be larger than what would be permitted to send to the controller resulting in the inability to analyze gateway logs. This fix addreses the restrictive limit so generated diagnostic bundles will be successfully sent to the controller.
- Improvements to the stability of the gateway.

Version 23.08-09 November 16, 2023

Fixes

This following fix is included in the upgrade:

- Fixes an issue related with DNS-based FQDN address object resources where enabling DNS caching could result in a race condition between policy change and the DNS resolution interval that would result in the cache for a domain to be reset to a value of 0 (no cache). When this situation occurs, the domain resolution will never be cached and any existing cache values will be flushed as their TTL expire. The end result is the gateway will eventually not match traffic for that domain. This fix addresses the race condition such that the cache will operate as expected.

Version 23.08-08 November 8, 2023

Fixes

The following fix is included in the upgrade:

- Improves gateway stability for all use-cases.

Version 23.08-07 October 18, 2023

Fixes

The following fix is included in this upgrade:

- Fixes an issue to ensure log forwarding to GCP logging sends logs as a JSON structure rather than a JSON-encoded string.

Version 23.08-06 October 7, 2023

Fixes

The following fix is included in this update:

- Fixes an issue related to a forward proxy rule that uses an FQDN match object for decryption exception could result in traffic processing issues.

Version 23.08-05 October 3, 2023

Fixes

The following fix is included in this update:

- Fixes an issue where traffic would be incorrectly denied by a forward proxy rule configured with an FQDN match profile due to delays in certificate validation. The deny will be seen as an FQDNFILTER security event even though an FQDN filtering profile is not applied.

Version 23.08-04 September 19, 2023

Fixes

The following fix is included in this upgrade:

- Fixes an issue where a rule that uses an FQDN match object would incorrectly process traffic for an uncategorized domain.

Version 23.08-03 September 10, 2023

Fixes

The following fixes are included in this upgrade:

- Fixes an issue related to dynamic address objects where a large number of IPs and a large number of changes to those IPs could result in the datapath not accepting changes, causing matching issues resulting in traffic being processed incorrectly.
- Fixes a slow session pool leak related to UDP traffic that would result in the DP detecting the leak and restarting the datapath.

Version 23.08-02 September 3, 2023

Fixes

The following fixes are included in this upgrade:

- Fixes an issue with teverse proxy where sending a HTTP POST with a payload greater than 200KB would cause the traffic to be dropped.
- Fixes an issue where a DNS-based address object that contains static IPs would fail to properly match.
- Removes the dependency on SNI or Host header for TCP forward proxy.

Version 23.08-01 August 25, 2023

Enhancements

The following enhancements are included in this upgrade:

- Enhances the datapath to generate a session summary event when the gateway connection and proxy timers are exceeded. This enhancement will help in troubleshooting when a session is closed by the gateway due to timer settings.
- Enhances the gorward proxy service object to accommodate L4 (TCP) and L5 (TLS) proxies. This is achieved by specifying either TCP or TLS as a valid value for the `transport_mode` argument.
- Enhances the gateway datapath to track session performance.
- Enhances the gateway datapath process to generate a TCP reset to actively close the connections during a datapath restart.

Fixes

The following fixes are included in this upgade:

- Fixes an issue where URL encoded characters of [`and`] in an HTTP object name where decoded by the gateway, but not re-encoded before sending the request to the server. This results in the server not being able to properly locate the object, returning a 400 response code. This fix properly re-encodes the characters prior to sending the request to the server.
- Fixes an issue where the presence of underscores in an SNI would cause the proxy to not pass traffic. This change enables the proxy configuration to accommodate the use of underscores in domain names.
- Fixes an issue where traffic is matched to a correct policy, but an incorrect certificate is issued.
- Fixes an issue where traffic is matched to a correct policy, but an incorrect certificate is issued.
- Fixes an issue with large file transfers related to HTTP commands (e.g., Github repository cloning) where a proxy timeout would result in a 408 status code.
- Fixes an issue where URL Filtering category query timeout expires causing the traffic to be denied.
- Fixes a stability issue with the ingress gateway where the datapath could self heal due to an issue with the upstream proxy.
- Fixes an issue where the gateway could introduce additional latency when processing certain types of traffic.
- Fixes an unnecessary datapath restart that is triggered when enabling memory profiling.
- Fixes an issue where the gateway could intermittently generate a 502 due to a datapath restart triggered by a policy change.
- Fixes an issue with CPU-based auto-scale could result in an unnecessary scale out.
- Fixes a proxy connection leak.
- Improvements to the stability of the Multicloud Defense Gateway.

Terraform Provider Enhancements

Version 24.2.1 February 31, 2024 (Recommended)

Enhancements

The following enhancements are included in this release:

- Adds arm64 support for Windows, Linux and MacOS.
- Enhances the Multicloud Defense Gateway `ciscomcd_gateway` resource creation in GCP to allow a user-provided IP resource to be used as the load balancer frontend IP.
- Adds support for cross-subscription Spoke VNet peering orchestration in Azure `ciscomcd_spoke_vpc`. This ensures feature parity across cloud service providers.

- Adds support for account (Tenant/Compartment) onboarding `ciscomcd_account` and Multicloud Defense Gateway deployment `ciscomcd_gateway` resources for orchestration in OCI.

Fixes

The following fixes are included in this release:

- Fixes an issue where attempting to create an FQDN filtering `ciscomcd_profile_fqdn` resource would result in an error message: `"unknown action Inherit from decryption profile for profile type FQDN_FILTER"`.
- Fixes an issue where a change to a decryption profile `ciscomcd_profile_decryption` resource would not recognize the change producing the message: `"No changes. Your infrastructure matches the configuration"`.
- Fixes an issue with deleting a spoke VPC `ciscomcd_spoke_vpc` peering in GCP where the spoke VPC peering would not be deleted. This issue occurred only when the VPC ID was used instead of the self-link.

Version 23.10.1 November 6, 2023

Enhancements

The following enhancements are included in this release:

- Adds support in a cloud service provider account `ciscomcd_cloud_account` resource for onboarding GCP folder hierarchies to accommodate asset and traffic discovery of all projects that are contained within a Folder hierarchical structure. Onboarding GCP folders permits asset and traffic discovery, but does not permit full orchestration. Discovery is beneficial and necessary for creating a dynamic policy that adapts in real time to changes made within the GCP projects. In order to orchestrate within a project, each project where orchestration is required should be onboarded individually.
- Adds support for sending Multicloud Defense Gateway metrics to 3rd-party SIEMs. This introduces a new metrics forwarding profile `ciscomcd_profile_metrics_forwarding` resource that can be configured and assigned to Multicloud Defense Gateway `ciscomcd_gateway` resources in order for gateway metrics to be sent to the SIEM. The first implementation supports Datadog as a SIEM. Support for other SIEMs will follow in future releases.
- Changes the Multicloud Defense Gateway `ciscomcd_gateway` resource `aws_gateway_lb` argument default value from false to true. When deploying an AWS egress gateway, the supported transit architecture is an AWS gateway load balancer (GWLB) architecture. This argument is optional and if not specified should default to the appropriate value.
- Adds support for sending audit and system logs to Splunk. This introduces an update to the alert profile `ciscomcd_alert_profile` resource by adding Splunk as a new value for the type argument.
- Adds support for sending audit and system logs to Microsoft Teams. This introduces an update to the alert profile `ciscomcd_alert_profile` resource by adding Microsoft Teams as a new value for the type argument.
- Enhances the forward proxy policy to validate the server certificate when negotiating the backend TLS session. The certificate validation is disabled by default, but can be configured in a decryption profile `ciscomcd_profile_decryption` resource for all TLS sessions and in an FQDN match object `ciscomcd_profile_fqdn` resource on a per-domain (or set of domains) basis.

- Adds support for creating an Azure Resource Group (RG) as part of the service VNet `ciscomcd_service_vpc` resource. The RG is required such that all resources orchestrated by the Multicloud Defense Controller will be associated within the specified (or newly created) RG.

Fixes

The following fix is included in this release:

- Fixes an issue where validation was not being performed when configuring a forward or reverse proxy service object `ciscomcd_service_object` resource to require a decryption profile `ciscomcd_profile_decryption` to be assigned to the tls_profile argument when using a secure proxy (TLS, HTTPS, WEBSOCKETS) value assigned to the `transport_mode` argument. If a secure proxy is configured, it must have a decryption profile assigned otherwise the proxy will not operate as a secure proxy and TLS encrypted traffic will be denied.

Version 23.8.1 August 22, 2023

Enhancements

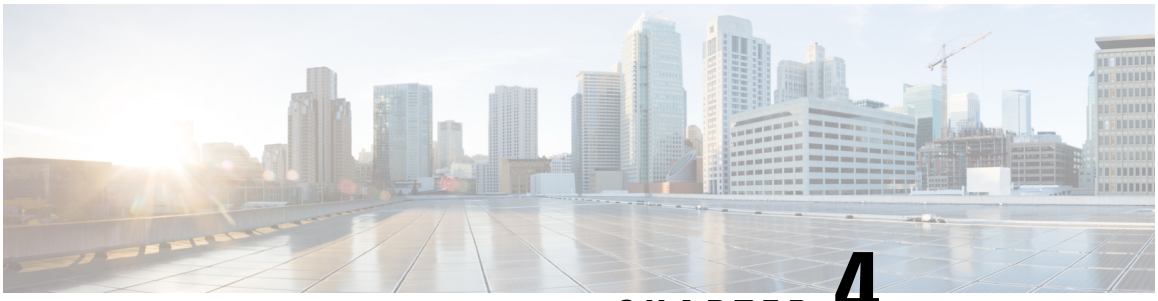
The following enhancements are included in this release:

- Enhances the forward proxy service object `ciscomcd_service_object` resource to accommodate L4 (TCP) and L5 (TLS) proxies. This is achieved by specifying either TCP or TLS as a valid value for the `transport_mode` argument.
- Enhances the Multicloud Defense Gateway `ciscomcd_gateway` resource to perform a blue/green gateway replacement when a change to assign_public_ip setting is made.

Fixes

The following fixes are included in this release:

- Fixes an issue where an FQDN Profile `ciscomcd_fqdn_profile` resource with `mode=MATCH` argument without a policy argument would result in traffic that matches to be denied. The policy argument does not need to be specified and is not listed as an argument in the Terraform Provider documentation.
- Fixes an issue where an update to the policy rules `ciscomcd_policy_rule_set` resource could take a longtime and generate an RPC error.



CHAPTER 4

Release and Service Policies

Release Versioning and Schedule

Release Versioning

Multicloud Defense release versioning is defined as X.Y-Z or X.Y.Z, where X is the major release (denoted by a calendar year), Y is the minor release (denoted by a calendar month), and Z is the maintenance release (denoted by an integer starting at a value of 1).

Major Release

A major version is a release by Multicloud Defense and will contain major enhancements, stability improvements and bug fixes.

Minor Release

A minor version is a release by Multicloud Defense that contains minor enhancements, stability improvements and bug fixes.

Maintenance Release

A maintenance version is a frequent update release by Multicloud Defense and will contain stability improvements and bug fixes, and occasionally (although rare) enhancements.

Hotifx Release

A hotfix release is a prioritized release that contains bug fixes that address an operational issue that impacts a small number of deployments (usually a single deployment).

Hotfixes are enhancements to the corresponding Major, Minor and Maintenance release. Each hotfix release does not contain cumulative enhancements across hotfix releases denoted by a letter (e.g., hotfix B does not contain enhancements from hotfix A). However, each hotfix release within a hotfix release letter, denoted by a number, will contain cumulative enhancements (e.g., hotfix A2 will contain enhancements from hotfix A1).

Release notes for each hotfix release will contain information on the specific enhancements beyond the Major, Minor and Maintenance release enhancements.

The hotfix release enhancements will eventually be rolled into a maintenance release. Upgrade to a hotfix release should only occur under the guidance of Cisco Support.

Release Schedule

Multicloud Defense will make every attempt to issue major or minor releases every three months. Maintenance releases will occur periodically for each major or minor release per the End-of-Support and End-of-Life policy.

Release Life and Support

The definitions and process for announcing and enforcing the life of a release from release date, through End-of-Support, to End-of-Life.

End-of-Life/Support Policy

The definitions and process for announcing and enforcing the life of a release from release date, through End-of-Support, to End-of-Life.

End-of-Support (EoS)

The last day after which a major or minor release, including all maintenance releases, will no longer be supported to troubleshoot or fix issues. No new maintenance releases will be issued. Multicloud Defense will assist in upgrading to a recommended major or minor, and maintenance release, determine if the issue is still present, and work towards providing a fix or workaround.

A major or minor release will be marked as End-of-Support 6 months from release date.

Announcements

- 1-month prior
- 1-week prior
- Day of

End-of-Life (EoL)

The last day after which a major or minor release, including any associated maintenance releases, will no longer be available to install. Multicloud Defense will assist in upgrading to a recommended major or minor, and maintenance release, determine if the issue is still present, and work towards providing a fix or workaround.

A major or minor release (and all maintenance releases) will be marked as End-of-Life 2 months after the major or minor release is marked End-of-Support.

Announcements

- 1-month prior
- 1-week prior
- Day of

Accelerated EoS/EoL

Multicloud Defense reserves the right to accelerate the End-of-Life and/or End-of-Support for a major or minor release (and all associated maintenance releases). Multicloud Defense will give notice to customers and assist with upgrading to a recommended release.

Announcements

- Defined on a case-by-case basis