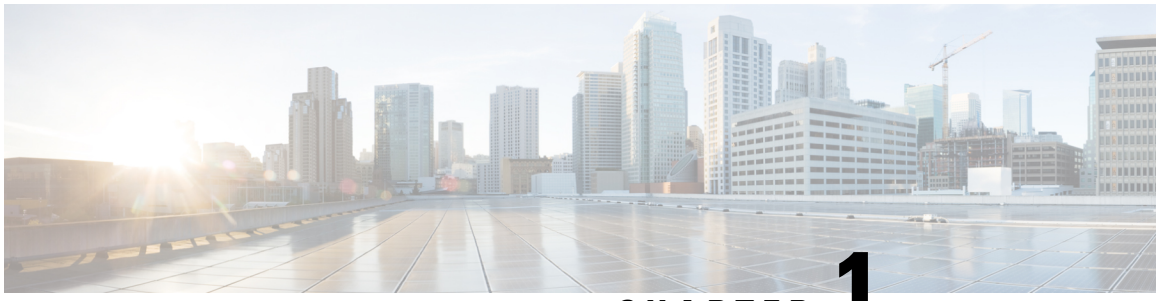
Cisco Multicloud Defense Release Notes

First Published: 2023-08-25

Last Modified: 2024-11-08

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

Additional Multicloud Defense Documentation

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 Gateway

Version 23.08-17, September 4, 2024

Multicloud Defense Terraform Provider

Version 24.10.1 November 7, 2024

Additional Resources and Assistance

Online Resources

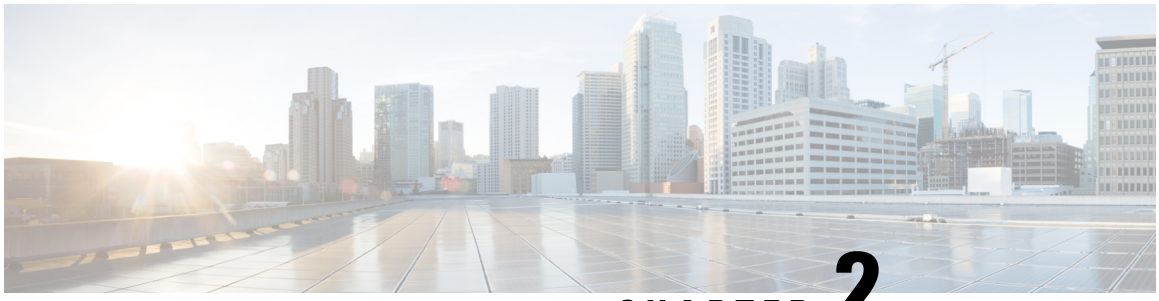
Cisco provides this additional documentation:

- 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 Controller Features and Enhancements

Version 24.10 October 29, 2024

The following features and enhancements are included in this release:

Features

AWS CloudWAN

Multicloud Defense now provides the option to utlize AWS CloudWAN in tandem with service VPCs and network segments. AWS CloudWAN simplifies the process of building, managing, and monitoring a global network that connects your data centers, branch offices, and cloud resources. See Create a Service VPC or VNet for more information.

Log Forwarding Profile with Webhooks

You can now create a log forwarding profile with a generic webhook as the destination. Webhooks can enable real-time data transfer, are ideal for an event-driven architecture or centralized logging, as well as support automation and integration with other third-party services. See Webhook for more information.

Enhancements

Integration with Cisco Talos Intelligence

Multicloud Defense now uses Cisco Talos Intelligence for FQDN and URL lookups. Cisco Talos is one of the most trusted threat intelligence research teams on the globe, comprised of world-class researchers, analysts, incident responders, and engineers. See Intelligence Categories for more information.

Dashboard and Navigation Display

Starting with Version 24.10, the Multicloud Defense Controller is updating and improving the general look and feel of the dashboard appearance as well as the navigation to certain functions with Magnetic. This helps unify the dashboard with other Cisco products and creates a universally streamlined display. This is an ongoing effort.

Version 24.09 September 30, 2024

The following features and enhancements are included in this release:

Feature

Beta: AWS CLoudWAN Support

Enhancements

Network Visibility Report

The network visibility report now includes a summary of activity.

GCP Load-Balancer

GCP now uses a single load-balancer for both TCP and UDP traffic. By streamlining the the work to a single load balancer, configuration and maintenance tasks are simplified which reduces the complexity of your network infrastructure and improved resource utilization.

Version 24.08 September 3, 2024

Fixes

The following fixes are included in this release:

- Improves FQDN object matching functionality.
- Improves general performance.

Version 24.07 August 17, 2024

Features

The following feature is included in this release:

- Support for OCI real-time discovery events.

Fixes

The following fixes are included in this release:

- Improved report generation in event batching to support up to 250K for pagination.

- Fixes an issue where session summary events configured for **No Log Action** continued to generate a logged event. With this fix there is no event logged when this configuration is selected.
- Fixes an issue where syslog forwarding did not include all logging types.
- Updated the list of permissions required for connecting to an OCI account.

Version 24.06 June 26, 2024

Features

The following features are included in this release:

Site-to-Site VPN Tunnel Connections

You can now create site-to-site VPN tunnel connections with the following cloud service providers and platforms:

- Amazon Web Services (AWS)
- Microsoft Azure
- Google Cloud Platform (GCP)
- Cisco ASA managed by , formerly known as "Cisco Defense Orchestrator"

  Multicloud Defense Gateways
- Extranet devices

Use a Multicloud Defense Gateway as either endpoint, or create an environment where Multicloud Defense Gateway acts as both endpoints. Secure your gateways with either a BGP or IPSec profile to finetune the configuration for your specific environmnent. See Site-to-Site VPN Tunnel Connection for more information.

Dynamic Object Sharing

You can now share, create and deploy, and modify objects that are shared with different platforms and immediately have any changes identifed and updated. See Shared Objects for more informaiton.

Azure NAT Gateways

You can now create a service VPC with the intention of attaching it to a Network Address Translation (NAT) gateway in an egress Azure deployment. See Egress Gateways for more information.

Use an Azure Load Balancer in Your Gateway

You can now opt to use a load balancer created in the Azure dashboard instead of the the load balancer that Multicloud Defense provides when you create a gateway. See Advanced Gateway Configuration: Use Your Own Load Balancer for more information.

Miscellaneous

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

Version 24.02 February 26, 2024

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.

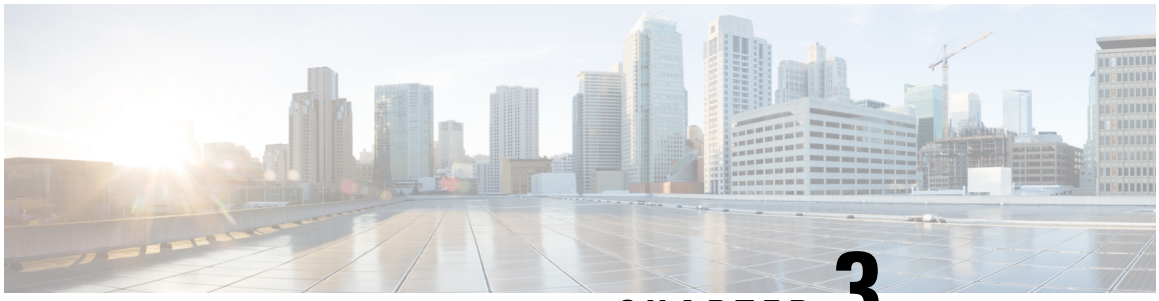
Fixes

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 page, formerly known as "Cisco Defense Orchestrator", 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.



CHAPTER 3

Multicloud Defense Gateway Fixes and Enhancements

Version 24.06

Version 24.06-04 October 25, 2024

Fixes

The following fix is included in this release:

- Fixes an issue where a gateway could unnecessarily consume CPU in a proxy scenario where the backend connection is unresponsive causing delays in processing traffic.

Version 24.06-03 October 20, 2024

Enhancements

The following enhancements are inlcuded in this release:

- Provides an enhanced gateway image that supports the BoringCrypto required for use for gateways deployed in a FedRamp environment. This is a continued effort towards Multicloud Defense being FedRamp compliant.
- Adds support for a custom banner to be displayed when an SSH session to the gateway is established through Teleport.

Fixes

The following fixes are inlcuded in this release:

- Fixes an issue where a TLS session that contains Kyber cipher suites could cause increased CPU usage resulting in the inability to process traffic.
- Fixes an issue where the connection drain time was not being honored when a gateway instance was replaced.
- Fixes a stability issue where the gateway datapath could self-heal when proxied sessions are actively terminated during policy change or gateway instance replacement.
- Fixes an issue where the generation of a Diagnostic Bundle could fail.
- Fixes an issue where the gateway could not retrieve the SNI from a TLS Client Hello message causing the gateway to close the connection with a TCP RST. This is caused by a change made in Chrome in April 2024 to shift to Post-Quantum Cryptography. With this change, the Client Hello is larger than 1415 bytes, which can result in an inability to retrieve the Server Name Indication (SNI), which is used by the proxy to determine what certificate to issue. The fix ensures the proxy can support Client Hello sizes greater than 1415 bytes.
- Fixes various stability issues.
- Fixes an issue where a change to DNS for a domain used in an FQDN-based address object would be received by the gateway datapath agent, but not applied to the datapath workers. This would result in the DNS change not being applied to the dynamic nature of the address object, impacting proper traffic processing.
- Fixes an issue where the gateway-side cipher suites used in a gateway SSH session were potentially flagged as weaker cipher suites. The fix accommodates only the most secure GCM-based cipher suites.

Version 24.06-02-a2 October 2, 2024

This release is a hotfix.

Fixes

The following fixes are included in this hotfix:

- Fixes an isuse where the Multicloud Defense Gateway temporarily crashes when a new gateway image is deployed.
- The Multicloud Defense Gateway now honors the drain time value configured in the Multicloud Defense Controller when terminating a gateway instance.

Version 24.06-02 September 18, 2024

Enhancements

The following enhancement is included in this release:

- Continued enhancements to the gateway to accommodate FedRAMP CIS Level-2 hardening.

Fixes

The following fixes are included in this release:

- Fixes and issue where the gateway will self-heal if an empty FQDN/URL Filtering profile is assigned to the policy rule set.
- Fixes a deny rule action issue related to the use of domains as a 6-tuple match. If the first rule match is a 6-tuple match (includes an assigned FQDN Match Profile) and the policy action is set to **Deny**, the deny action will be based on the 5-tuple match and will not include the domain for match consideration. This fix ensures that all 6-tuples are considered when evaluating the rule and its action. If the traffic does not match the rule based on the 6-tuple match, then it will refine its match to a subsequent rule and take action based on the matched rule's configuration.
- Fixes an issue where an Azure ingress gateway will get stuck in `Health Checking Pending` state after a policy update is applied. This issue also includes new gateway deployments .
- Fixes an allow rule match issue related to the use of domains as a 6-tuple match. If the first rule match is a 6-tuple match (includes an assigned FQDN Match profile), the policy action is set to **Allow** and there are no subsequent rules that are consistent with the 5-tuple match of the first rule, then all domains will be allowed and domains will be denied. This fix ensures that only the domains that are matched in the rule will be allowed and all other domains will be denied
- Fixes an issue where a egress policy rule set that uses an decryption-based forward proxy (TLS, HTTPS, WebsocketS) is initially matching on 5-tuple and retrieving the domain from the SNI, but not performing a match refinement based on the 6th tuple resulting in a TLS error. The fix ensures that 6-tuple match refinement occurs such that the traffic can be successfully processed by the proper decryption rule.
- Fixes an issue where sessions with TLS negotiation errors where not recording the SNI as a **Traffic Summary** > **Event**.
- Fixes an issue where multiple SNI events were being recorded for each forward proxy full decrypted session.
- Fixes an issue where the address group size could be exceeded, causing all IPs/CIDRs in excess of the size to not be included in the address group. The address group size has been increased to 20k IPs/CIDRs.
- Adds a System Log message if the GeoIP limitations of the gateway are exceeded.
- Fixes an issue where the wrong action would be taken for URL filtering category matching if a timeout occurs when attempting to retrieve the URL filtering category if the URL is not found in the cache.
- Ensures that an user with administrator access to configure a URL Filtering profile cannot use the custom URL response to inject Javascript. The fix enforces HTML encoding in the custom URL response.

Version 24.06-01 July 10, 2024

-

Enhancements

The following enhancements are included in this release:

- Adds support for inspecting content within a GRE tunnel that passes through the gateway. The gateway will decapsulate the traffic, perform inspection on the encapsulated traffic to apply proper policy and protection, then re-encapsulate that traffic back into the GRE tunnel.

- Adds support for active connection resets during gateway upgrade, scale-in and connection timeout scenarios. When these scenarios occur and the gateway is processing long running connections that are not closed by the client or server, the gateway will take action by sending a TCP RST to active close the connection when reaping the old instance or a connection timeout is exceeded.
- Support ability to specify a custom banner when logging into a gateway instance through Teleport (SSH access). This is a requirement for gateways deployed into FedRamp environments where any method of SSH access requires a customer-defined banner to be displayed.

Fixes

The following fixes are included in this release:

- Fixes an issue where specifying an Validate Certificate action other than "Default" in a Decryption profile will cause the gateway to become unhealthy.
- Fixes an issue for user-generate diagnostic bundles where the gateway would fail to generate the diagnostic bundle and send to the Multicloud Defense Controller.
- Fixes an issue related to the use of GeoIP. Countries with many providers have a very large number of advertised prefixes. When those country codes are used in a GeoIP address group, the address group will contain a large number of CIDR blocks. The GeoIP address group was restricted to 64k CIDRs where exceeding this limit would result in a partial set of CIDRs applied to the policy. This fix relaxes the limit to ensure the full set of CIDRs will be applied to the policy. It is recommended to use an 8-core instance type due to the additional memory requirements imposed by GeoIP.
- Fixes an issue where the gateway could issue the wrong certificate when a Chrome browser is connecting to the gateway using TLS 1.3. This is caused by a change made in Chrome in April 2024 to shift to Post-Quantum Cryptography. With this change, the Client Hello is larger than 1415 bytes, which can result in an inability to retrieve the Server Name Indication (SNI), which is used by the proxy to determine what certificate to issue. The fix ensures the proxy can support Client Hello sizes greater than 1415 bytes.
- Fixes an issue where the gateway was producing the correct statistics for display in the**Investigate** > **Network Analytics** > **Stats** page.
- Fixes various stability issues.
- 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.
- Fixes an issue where a VPN tunnel state transition was not generating a System Log message to provide troubleshooting and debugging information on the tunnel setup and negotiation.
- Fixes a slow memory leak for an ingress gateway that eventually results in a datapath self heal. The memory leak is related to traffic that contains files that are gzip compressed.
- Fixes an issue where an ingress gateway could drop a connection when back-to-back POST commands contain a payload greater than 160k.

Version 24.04

Version 24.04-01 May 16, 2024

Enhancements

The following enhancement is included in this release:

- Adds support for site-to-site VPN for gateways running in AWS, Azure and GCP. This includes VPN tunnel configuration, including IPSec and BGP profiles. The VPN is terminated directly on the Gateway to process and protect traffic flowing across the VPN. This enhancement requires gateway version 24.04 or later.

Fixes

The following fixes are included in this release:

- Ensures the gateway limits address objects to no more than 63 characters.
- 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.
- Fixes an issue where the gateway policy update status could be stuck in updating.
- Fixes various issues that improve the stability of the gateway.

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 23.08-17-b1 September 27, 2024

This is a hotfix.

Fixes

The following fix is included in this hotfix:

- Fixes an issue where the gateway could not retrieve the SNI from a TLS Client Hello message causing the gateway to close the connection with a TCP RST. This is caused by a change made in Chrome in April 2024 to shift to Post-Quantum Cryptography. With this change, the Client Hello is larger than 1415 bytes, which can result in an inability to retrieve the Server Name Indication (SNI), which is used by the proxy to determine what certificate to issue. The fix ensures the proxy can support Client Hello sizes greater than 1415 bytes.

Version 23.08-17-a1 September 4, 2024

This is a hotfix.

Fix

The following fix is included in this hotfix:

- Fixes an issue where a policy rule that uses DNS-based FQDN cache could become corrupted causing the Multicloud Defense Gateway to not properly process traffic.

Version 23.08-17 September 4, 2024 (Recommended)

Fixes

The following fixes are included in this release:

- Fixes an issue related to the use of GeoIP. Countries with many providers have a very large number of advertised prefixes. When those country codes are used in a GeoIP address group, the address group will contain a large number of CIDR blocks. The GeoIP address group was restricted to 64k CIDRs where exceeding this limit would result in a partial set of CIDRs applied to the policy. This fix relaxes the limit to ensure the full set of CIDRs will be applied to the policy. It is recommended to use an 8-core instance type due to the additional memory requirements imposed by GeoIP.
- Fixes an issue where an egress gateway would silently close TCP connections at 240s even though the TCP established timeout was changed to a value greater than 240s.
- Fixes an issue where the datapath of an ggress gateway could self heal when filtering traffic using a URL filtering profile.

Version 23.08-16-a1 August 6, 2024

This is a hotfix.

Fixes

The following fix is included in this hotfix:

- Fixes an issue where a Policy Rule that uses a DNS-based FQDN cache could become corrupted causing the Gateway to not properly process traffic.

Version 23.08-16 June 25, 2024

Fixes

The following fixes are included in this release:

- Fixes an issue where the Multicloud Defense Gateway could issue the wrong certificate when a Chrome browser is connecting to the Gateway using TLS 1.3. This is caused by a change made in Chrome in April 2024 to shift to Post-Quantum Cryptography. With this change, the Client Hello is larger than 1415 bytes, which can result in an inability to retrieve the Server Name Indication (SNI), which is used by the proxy to determine what certificate to issue. The fix ensures the proxy can support Client Hello sizes greater than 1415 bytes.
- Fixes an issue where sending a TCP RST by the datapath to close a session could cause the datapath to self heal.
- Fixes an issue related to receive buffer exhaustion that could impact the ability of the Multicloud Defense Gateway to process traffic. For the Gateway to accommodate resetting connections (TCP RST), information from the last packet received must be retained (receive buffer). If the active session volume is high, there is a risk that the receive buffer can become exhausted, causing the Multicloud Defense Gateway to not receive new packets. This scenario can occur more commonly from half-opened connections related to SYN floods (intentional or unintentional). This fix extracts the necessary information from the last packet of each active session and stores this information in a buffer that is large enough to accommodate the Gateway active session limits, eliminating the possibility of buffer exhaustion.
- Fixes an issue related to blue/green policy change. When the policy change occurs and the new datapath becomes active, the Multicloud Defense 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.
- Fixes an issue with log rotation for Multicloud Defense Gateway in OCI. The fix ensures that the logs are properly rotated to not consume unnecessary disk space.
- 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 slow memory leak for an ingress gateway that eventually results in a datapath self heal. The memory leak is related to traffic that contains files that are gzip compressed.

Version 23.08-15-a3 June 22, 2024

This is a hotfix.

Fixes

The following fix is included in this hotfix:

- Fixes an issue related to the use of GeoIP. Countries with many providers have a very large number of advertised prefixes. When those country codes are used in a GeoIP address group, theaddress group will contain a large number of CIDR blocks. The GeoIP address group was restricted to 64k CIDRs where exceeding this limit would result in a partial set of CIDRs applied to the policy. This fix relaxes the limit

to ensure the full set of CIDRs will be applied to the policy. It is recommended to use an 8-core instance type due to the additional memory requirements imposed by GeoIP.

Version 23.08-14-c3 June 8, 2024

This is a hotfix.

Fixes

The following fixes are included in this hotfix:

- Fixes an issue where the gateway could issue the wrong certificate when a Chrome browser is connecting to the gateway using TLS 1.3. This is caused by a change made in Chrome in April 2024 to shift to Post-Quantum Cryptography. With this change, the Client Hello is larger than 1415 bytes, which can result in an inability to retrieve the Server Name Indication (SNI), which is used by the proxy to determine what certificate to issue. The fix ensures the proxy can support Client Hello sizes greater than 1415 bytes.
- Fixes a slow memory leak for an ingress gateway that eventually results in a datapath self heal. The memory leak is related to traffic that contains files that are gzip compressed.

Version 23.08-15-c1 May 9, 2024

This is a hotfix

Fixes

The following fixes are included in this hotfix:

- Fixes an issue related to receive buffer exhaustion that could impact the ability of the gateway to process traffic. For the gateway to accommodate resetting connections (TCP RST), information from the last packet received must be retained (receive buffer). If the active session volume is high, there is a risk that the receive buffer can become exhausted, causing the gateway to not receive new packets. This scenario can occur more commonly from half-opened connections related to SYN floods (intentional or unintentional). This fix extracts the necessary information from the last packet of each active session and stores this information in a buffer that is large enough to accommodate the gateway active session limits, eliminating the possibility of buffer exhaustion.

Version 23.08-15-a2 May 1, 2024

This is a hotfix.

Fixes

The following fix is included in this hotfix:

- Fixes an issue where sending a TCP RST by the datapath to close a session could cause the datapath to self heal.

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

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:

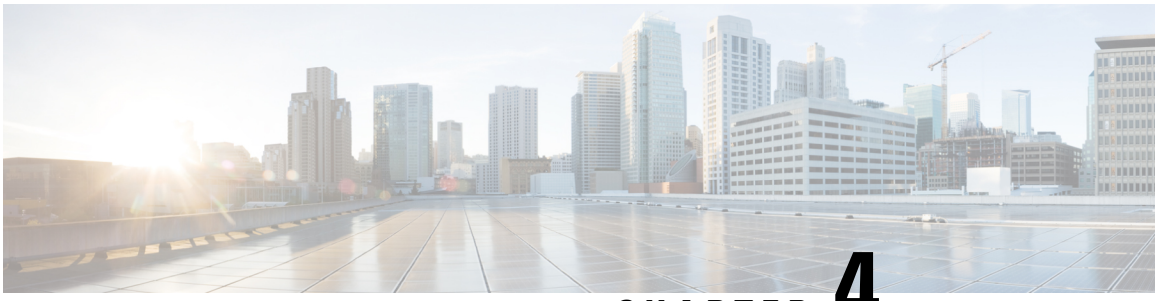
- Enhances the datapath to generate a session summary event when the gateway connection and proxy timers are exceeded. This enhancement will help in troubleshooting when a session is closed by the gateway due to timer settings.
- Enhances the gorward proxy service object to accommodate L4 (TCP) and L5 (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.



CHAPTER 4

Multicloud Defense Terraform Provider Enhancements

Version 24.10.1 November 7, 2024 (Recommended)

Enhancements

The following enhancement is included in this release:

- Changes the default value for the argument `aws_gateway_lb` from false to true of a gateway (`valtix_gateway`) resource with `security_type` argument set to **EGRESS**.

Fixes

The following fixes are included in this release:

- Fixes an issue where changing the name argument of a policy rule set (`valtix_policy_rule_set`) resource would not result in a change to the name.
- Fixes an issue where changing the name argument of an address object (`valtix_address_object`) resource would not result in a change to the name.
- Fixes an issue where attaching an ICMP rule to a policy rule (`valtix_policy_rules`) resource will result in a feature compliant error message.
- Fixes an issue where a forwarding profile (`valtix_profile_log_forwarding`) resource that is configured with a reference to a dynamic IP address value would throw an error requiring an IP address to be specified.
- Fixes an issue where a BGP Profile (`valtix_profile_bgp`) cannot be created without BGP neighbor blocks being specified.

- Fixes an issue where the CIDR argument for a service VPC (`valtix_service_vpc`) resource was not being validated properly, allowing CIDRs that are not applicable when creating a service VPC.
- Fixes an issue where both an address object (`valtix_address_object`) resource and a policy rule (`valtix_policy_rules`) resource are created in the same apply operation where the rule references the address object, but throws an error due to the address object ID being **0**. The creation of the address object is not returning the ID and thus the ID is 0 when applying to the rule. This fixes the issue such that the address object and rule can both be created and referenced in the same apply.

Version 24.2.2 August 21, 2024

Fixes

The following fix is included in this release:

- Fixes an issue related to ordering of the `instance_details` blocks for a Gateway (`ciscodmcd_gateway`) resource deployed in Edge mode. The block order in a multi-zone deployment could be random, causing the Terraform apply to incorrectly detect an infrastructure change. This fix ensures a consistent order based on the user specified Terraform code such that no infrastructure change is detected if there is no change to the order in the code.

Version 24.2.1 February 31, 2024

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

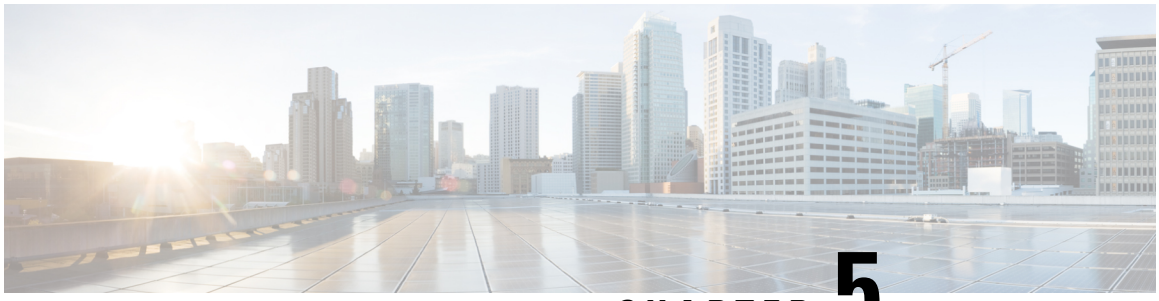
The following enhancements are included in this release:

- 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 5

Legacy Versions

The following legacy versions are not recommended, but are still supported.

Legacy Multicloud Defense Gateway Versions

Version 23.06

Version 23.06-14 November 12, 2023

Fixes

The following fix is included in this 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 23.06-13 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 23.06-12 October 6, 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 23.06-11 September 27, 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 23.06-10 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 23.06-09 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 23.06-08 September 3, 2023

Fixes

The following fix is included in this upgrade:

- Fixes an issue where a DNS-based address object that contains static IPs would fail to properly match.

Version 23.06-07 August 29, 2023

Fixes

The following fix is inlcuded in this upgrade:

- Fixes an issue with Forward Proxy where sending a HTTP POST with a payload greater than 200KB would cause the traffic to be dropped.

Version 23.06-06 August 23, 2023

Fixes

The following fixes are included in this upgrade:

- 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.
- Improvements to the stability of the Gateway.
- Fixes an additional 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 traffic is matched to a correct policy, but an incorrect certificate is issued.
- Fixes an issue where URL Filtering category query timeout expires causing the traffic to be denied.
- Fixes a proxy connection leak Fix: 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.

Version 23.06-05 August 4, 2023

Fixes

The following fixes are included in this upgrade:

- Fixes an issue where HTTP headers that use underscores would not be passed by a proxy Rule. This change enables the proxy configuration to accommodate headers with underscores.
- 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 HTTP traffic processed initially by a Forward Proxy Rule, then subsequently processed by a Forwarding Rule due to refined matching, would be allowed when it should be denied.

Version 23.06-04 July 27, 2023

Fixes

The following fix is included in this upgrade:

- Fixes an issue where certain types of traffic processed by the anti-malware engine could result in high CPU causing delays in traffic processing.

Version 23.06-03 July 21, 2023

Fixes

The following fix is included in this upgrade:

- Fixes an issue where a new Gateway deployment could result in a bring-up failure if a Policy Rule Set contains Address Objects that utilize a mix of IP/CIDR inclusion and exclusion.

Version 23.06-02 July 19, 2023

Fixes

The following fixes are included in this upgrade:

- Fixes an issue where an update to a CIDR-based Address Object is not properly applied to the datapath workers, resulting in incorrect Rule matching.
- Fixes an issue with a DNS-based FQDN Address Object where a DNS cache is properly established, but not properly applied to the datapath workers, resulting in incorrect Rule matching.
- Fixes a datapath processing behavior where a Forward Proxy Rule preceded by a Forwarding Rule for the same L3/L4 (IP/port/protocol) matching criteria, but distinct L5 (SNI) matching would result in traffic processed as Forwarding even though proper Rule matching occurs. A similar behavior would be seen if the Forwarding and Forward Proxy Rules order were reversed. The reason this behavior occurs is that in order to accommodate L5 (SNI) matching, the TCP handshake must be fully established to receive the TLS hello message to obtain the SNI. Once the TCP handshake has completed, the traffic has already been processed by the Rule type of the first Rule. Once the session has been established, it is not possible to change the traffic processing from Forwarding to Forward Proxy (or vice versa). If a Policy Rule Set has been configured with this conflict, the datapath will detect the conflict and generate a System Log message. The traffic will be denied as it cannot successfully be processed by the conflicting Rule.
- 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 a datapath restart would result in a spike in CPU that could cause an unnecessary auto-scale.

Version 23.06-01 July 6, 2023

Fixes

The following fixes are included in this upgrade:

- Fixes an issue where a GCP Gateway could not generate support-related diagnostic bundles.
- Fixes an issue where an NTP Profile was repeatedly applied to a Gateway even though no Profile change was introduced.

- Fixes an issue where an empty Address Object applied to a Gateway would result in a traffic processing issue.
- Fixes an issue where an unnecessary datapath self-heal would occur when simultaneously applying both an NTP Profile and Log Forwarding Profile to a Gateway. This issue would only surface if the Profiles are applied using orchestration since the operations are independent, would occur sequentially and all within a very short separation in time.
- Fixes an issue where an Ingress Gateway could issue an incorrect certificate when a Rule has been configured with a domain that contains more than 3 levels.
- Fixes an issue where frequent changes to an Address Object could result in the datapath not accepting further changes.
- Fixes an issue where a Reset on Deny (TCP Reset) would not be issued when traffic is processed by a Ruleset that uses FQDN Match.
- Fixes an issue where an L4_FW event was not consistently produced when for traffic processed by the Gateway.
- Fixes an issue where changing the WAF action from "Allow Log" to "Rule Default" could cause the datapath to restart multiple times.
- Fixes an issue where HTTP traffic with chunked Transfer-Encoding could cause large memory consumption in WAF that would trigger a datapath self heal Fix: Fixes a slow memory leak that results in a silent datapath restart that could disrupt traffic.
- Fixes a memory issue that could result in a datapath self heal.

Version 23.04

Version 23.04-18 September 3, 2023

Fixes

The following fixes are included in this upgrade:

- Fixes an issue with reverse 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.

Version 23.04-17 August 23, 2023

Fixes

The following fix is included in this upgrade:

- 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.

Version 23.04-16 August 22, 2023

Fixes

The following enhancements are included in this upgrade:

- 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 additional 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 traffic is matched to a correct policy, but an incorrect certificate is issued.
- Fixes an issue where URL Filtering category query timeout expires causing the traffic to be denied.
- Fixes a proxy connection leak.
- Improvements to the stability of the Gateway.

Version 23.04-14 July 27, 2023

Fixes

The following fix is included in this upgrade:

- Fixes an issue where certain types of traffic processed by the anti-malware engine could result in high CPU causing delays in traffic processing.

Version 23.04-13 July 27, 2023

Fixes

The following fix is included in this upgrade:

- Fixes an issue where certain types of traffic processed by the anti-malware engine could result in high CPU causing delays in traffic processing.

Version 23.04-12 July 19, 2023

Fixes

The following fixes are included in this upgrade:

- Fixes an issue where an update to a CIDR-based Address Object is not properly applied to the datapath workers, resulting in incorrect Rule matching.
- Fixes an issue with a DNS-based FQDN Address Object where a DNS cache is properly established, but not properly applied to the datapath workers, resulting in incorrect Rule matching.
- Fixes a datapath processing behavior where a Forward Proxy Rule preceded by a Forwarding Rule for the same L3/L4 (IP/port/protocol) matching criteria, but distinct L5 (SNI) matching would result in traffic processed as Forwarding even though proper Rule matching occurs. A similar behavior would be seen if the Forwarding and Forward Proxy Rules order were reversed. The reason this behavior occurs is that

in order to accommodate L5 (SNI) matching, the TCP handshake must be fully established to receive the TLS hello message to obtain the SNI. Once the TCP handshake has completed, the traffic has already been processed by the Rule type of the first Rule. Once the session has been established, it is not possible to change the traffic processing from Forwarding to Forward Proxy (or vice versa). If a Policy Rule Set has been configured with this conflict, the datapath will detect the conflict and generate a System Log message. The traffic will be denied as it cannot successfully be processed by the conflicting Rule.

- 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 a datapath restart would result in a spike in CPU that could cause an unnecessary auto-scale.

Version 23.04-11 July 10, 2023

Fixes

The following fixes are included in this upgrade:

- Fixes a stability issue in the Snort engine that could cause the Gateway to self heal.
- Fixes an issue where Ingress traffic containing a long header will cause the Reverse Proxy to generate a 400 response code.
- Fixes an issue where traffic is not processed properly by a Forward Proxy Rule when the Rule uses a FQDN Match Profile with multiple rows containing a mixture of Decryption Exception settings.

Version 23.04-10 June 28, 2023

Fixes

The following fix is included in this upgrade:

- Fixes an issue where applying a DNS-based cache setting to a Gateway will cause the Gateway instance to become unhealthy.

Version 23.04-09 June 25, 2023

Fixes

The following fixes are included in this upgrade:

- Removes 15-day periodic Gateway datapath self-heal that was in place to help ensure consistent Gateway health. This was incorporated more than 2 years ago to address an issue that was challenging to catch and fix. That issue has since been addressed, but the periodic self-heal was never removed. It is no longer needed and has now been removed.
- Fixes an issue where a GCP Gateway could not generate support-related diagnostic bundles.
- Fixes an issue where an NTP Profile was repeatedly applied to a Gateway even though no Profile change was introduced.
- Fixes an issue where a Policy Rule Set could be in a persistent "Updating" state when an FQDN Filtering Profile is applied.

- Fixes an issue where an empty Address Object applied to a Gateway would result in a traffic processing issue.
- Fixes an issue where an unnecessary datapath self-heal would occur when simultaneously applying both an NTP Profile and Log Forwarding Profile to a Gateway. This issue would only surface if the Profiles are applied using orchestration since the operations are independent, would occur sequentially and all within a very short separation in time.

Version 23.04-07 June 14, 2023

Fixes

The following fixes are included in this upgrade:

- Fixes an issue where changing the WAF action from "Allow Log" to "Rule Default" could cause the datapath to restart multiple times.
- Provides an update to revert a change that was made in 23.04-05 related to a slow session pool leak addressed by a preemptive datapath self-heal. The previous update has the potential to cause datapath self-heals that cannot be preempted. This release ensures stability while the initial issue is fully addressed.

Version 23.04-06 June 8, 2023

Fixes

The following fixes are included in this upgrade:

- Fixes an issue where an L4_FW event was not consistently produced when for traffic processed by the Gateway.
- Fixes an issue where HTTP traffic with chunked Transfer-Encoding could cause large memory consumption in WAF that would trigger a datapath self heal.

Version 23.04-05 June 1, 2023

Fixes

The following enhancements are included in this upgrade:

- Fixes a slow memory leak that results in a silent datapath restart that could disrupt traffic.
- Fixes a very slow session pool leak that would result in a preemptive datapath self-heal.
- Fixes an issue where a Reset on Deny (TCP Reset) would not be issued when traffic is processed by a Ruleset that uses FQDN Match.
- Fixes an issue where an Ingress Gateway could issue an incorrect certificate when a Rule has been configured with a domain that contains more than 3 levels.
- Fixes an issue where frequent changes to an Address Object could result in the datapath not accepting further changes.
- Fixes various Gateway stability issues that would result in a datapath self-heal.

Version 23.04-04 May 19, 2023

Fixes

The following fix is included in this upgrade:

- Fixes an issue with traffic processing for a Policy Ruleset Rule that uses FQDN Match. Sessions containing a TLS SNI that would match the FQDN would initially be denied, but subsequent sessions would be incorrectly allowed.

Version 23.04-03 May 16, 2023

Fixes

The following fix is included in this upgrade:

- Provides an enhanced memory profiling mode enabled as a Gateway setting. This is useful for advanced troubleshooting to understand memory consumption.

Version 23.04-02 May 2, 2023

Fixes

The following fixes are included in this upgrade:

- Fixes an issue where establishing an SSH session to an OCI Gateway management interface would fail with a permission denied due to invalid user account.
- Fixes an issue where a user-defined NTP Profile associated with a Gateway would not properly configure the NTP settings when applied to the Gateway.

Version 23.04-01 April 20, 2023

Enhancements

The following enhancements are included in this upgrade:

- Enhances the error message reporting by the Gateway when a TLS session cannot be negotiated due to no shared cipher suite. The error message for Security Events of type "TLS_ERROR" have been enhanced to be more descriptive.
- Enhances the hardening of the Centos base image used in the Valtix Gateway. The base image has now been moved to Centos9 and is hardened to accommodate environments that have strict compliance requirements.
- Provides support for configuring the NTP settings of a Gateway. The Gateway NTP settings can be configured using an NTP Profile that can be assigned to the Gateway.
- Support for Azure GWLB-based architectures for Ingress protection.

Fixes

The following fixes are included in this upgrade:

- Fixes an issue with FQDN Match Object where the traffic would be processed by an incorrect Rule when no SNI is present in the traffic.
- Fixes an issue where DLP and IDS/IPS Profiles that were created prior to IDS/IPS and WAF Custom Rule support might not operate as expected unless the Profile was modified and saved.
- Fixes an Ingress Gateway issue related to large-volume bursty TLS traffic where the Gateway could issue an incorrect certificate to the client. This scenario is rare and is a downstream issue that could occur in Gateway releases 22.12-04 and earlier. This fix addresses the downstream issue by ensuring it is never reached and is a safeguard to ensure the issue never occurs.
- Fixes an issue where the same certificate could be issued when the policy is specified with two or more unique listener ports, with each sharing the same SNI and backend configuration.
- Fixes an issue where the datapath engine would not start after failing to load an updated package. This issue has been addressed with the new CentOS 9 base image where package updates are handled by Valtix and not by the Linux kernel itself.
- Fixes an issue where FQDNFILTER Events where showing a reversed source and destination IP/Port information.
- Fixes an issue related to URL Filter Profile where the a Profile created using an older Controller version would not properly deny URLs when the action is configured as deny.
- Fixes a traffic processing issue related to L7DOS Profile configuration. When the Profile is configured with a Request Rate or Burst Size of 1, the datapath would not limit the traffic properly.
- Fixes a traffic processing issue related to L7DOS Profile configuration. When the Profile is configured with Request Rate or Burst Size values of 0, the datapath should inhibit any traffic related to the specified URL/URI. Even though the L7DOS Profile can be used to block URLs/URIs by using this method, the recommended method is to create a URL Filter Profile and apply the Profile to the Policy Ruleset Rules that are processing traffic related to the URL.
- Fixes an issue with Traffic Summary Logs and Events that are sent directly from the Gateway to CSP storage systems (S3 Bucket, GCP Logging) where the friendly name to field values were represented by an integer. This would require a documented integer to friendly name translation by the user. The Logs and Events will now contain the friendly name and not the integer value.
- Fixes a stability issue in an Egress Gateway related to various traffic patterns.
- Fixes an issue related to Websockets Proxy where a duplicate host header would be added to the backend connection. In general, this is not an issue as the RFC states that multiple (and duplicate) host headers are allowed. But there are some application frameworks that do not accept multiple host headers. Ngnix as an application server is one of those systems. When Nginx receives HTTP traffic with multiple host headers, it will reject the session and respond back with a 400 Bad Request.
- Fixes OS vulnerabilities related to Gateway Management Centos Linux container that would result in information notices in vulnerability scanners.
- Fixes an issue with MLX4 DPDK driver for Azure Gateway that could cause an infrequent datapath self-heal.
- Changes the auto-scaling CPU threshold from 75% to 95% to reduce the CPU-based auto-scaling sensitivity.

Version 23.02

Version 23.02-10 June 28, 2023

Fixes

The following fix is included in this upgrade:

- Fixes an issue where applying a DNS-based cache setting to a Gateway will cause the Gateway instance to become unhealthy.

Version 23.02-09 June 25, 2023

Fixes

The following fixes are included in this upgrade:

- Removes 15-day periodic Gateway datapath self-heal that was in place to help ensure consistent Gateway health. This was incorporated more than 2 years ago to address an issue that was challenging to catch and fix. That issue has since been addressed, but the periodic self-heal was never removed. It is no longer needed and has now been removed.
- Fixes an issue where a GCP Gateway could not generate support-related diagnostic bundles.
- Fixes an issue where an NTP Profile was repeatedly applied to a Gateway even though no Profile change was introduced.
- Fixes an issue where a Policy Rule Set could be in a persistent "Updating" state when an FQDN Filtering Profile is applied.
- Fixes an issue where an empty Address Object applied to a Gateway would result in a traffic processing issue.
- Fixes an issue where an unnecessary datapath self-heal would occur when simultaneously applying both an NTP Profile and Log Forwarding Profile to a Gateway. This issue would only surface if the Profiles are applied using orchestration since the operations are independent, would occur sequentially and all within a very short separation in time.

Version 23.02-08 June 15, 2023

Fixes

The following fixes are included in this upgrade:

- Fixes an issue where changing the WAF action from "Allow Log" to "Rule Default" could cause the datapath to restart multiple times.
- Provides an update to revert a change that was made in 23.04-05 related to a slow session pool leak addressed by a preemptive datapath self-heal. The previous update has the potential to cause datapath self-heals that cannot be preempted. This release ensures stability while the initial issue is fully addressed.

Version 23.02-07 June 8, 2023

Fixes

The following fixes are included in this upgrade:

- Fixes an issue where an L4_FW event was not consistently produced when for traffic processed by the Gateway.
- Fixes an issue where HTTP traffic with chunked Transfer-Encoding could cause large memory consumption in WAF that would trigger a datapath self heal

Version 23.02-06 June 2, 2023

Fixes

The following fixes are included in this upgrade:

- Fixes a slow memory leak that results in a silent datapath restart that could disrupt traffic.
- Fixes a very slow session pool leak that would result in a preemptive datapath self-heal.
- Fixes an issue where a Reset on Deny (TCP Reset) would not be issued when traffic is processed by a Ruleset that uses FQDN Match.
- Fixes an issue where an Ingress Gateway could issue an incorrect certificate when a Rule has been configured with a domain that contains more than 3 levels.
- Fixes an issue where frequent changes to an Address Object could result in the datapath not accepting further changes.
- Fixes various Gateway stability issues that would result in a datapath self-heal.

Version 23.02-05 May 22, 2023

Enhancements

The following enhancement is included in this upgrade:

- Provides an enhanced memory profiling mode enabled as a Gateway setting. This is useful for advanced troubleshooting to understand memory consumption.

Fixes

The following fix is included in this upgrade:

- Fixes an issue with traffic processing for a Policy Ruleset Rule that uses FQDN Match. Sessions containing a TLS SNI that would match the FQDN would initially be denied, but subsequent sessions would be incorrectly allowed.

Version 23.02-04 April 14, 2023

Fixes

The following fixes are included in this upgrade:

- Fixes an issue related to Websockets Proxy where a duplicate host header would be added to the backend connection. In general, this is not an issue as the RFC states that multiple (and duplicate) host headers are allowed. But there are some application frameworks that do not accept multiple host headers. Ngnix as an application server is one of those systems. When Nginx receives HTTP traffic with multiple host headers, it will reject the session and respond back with a 400 Bad Request.
- Moved the TLS renegotiation configuration to a configurable setting. Changed the renegotiation back to a default state of enabled due to potential issues with older clients that rely on renegotiation.
- Changes the auto-scaling CPU threshold from 75% to 95% to reduce the CPU-based auto-scaling sensitivity.

Version 23.02-03 March 7, 2023

Fixes

The following fix is included in this upgrade:

- Fixes an issue where DLP and IDS/IPS Profiles that were created prior to IDS/IPS and WAF Custom Rule support might not operate as expected unless the Profile was modified and saved.

Version 23.02-02 February 20, 2023

Fixes

The following fixes are included in this upgrade:

- Fixes an Ingress Gateway issue related to large-volume bursty TLS traffic where the Gateway could issue an incorrect certificate to the client. This scenario is rare and is a downstream issue that could occur in Gateway release 23.02-01. This fix addresses the downstream issue by ensuring it is never reached and is a safeguard to ensure the issue never occurs.
- Disabled TLS renegotiation to address vulnerability related to CVE-2009-3555.
- Fixes an issue where the FQDN Filtering Events would show reversed source/destination IP/Port information.

Version 23.02-01 February 15, 2023

Enhancements

The following enhancements are included in this upgrade:

- Enhances the DNS-based FQDN Address Object to accommodate IP Address caching. The enhancement provides a configurable set of Gateway settings related to DNS resolution frequency (update interval), IP Address TTL (entry TTL) and IP Address cache size (cache). These settings can be applied using

Terraform only. When not applied, default values are: 60 (seconds) for DNS resolution frequency, 0 (seconds) for IP Address TTL (no caching), and 0 (address count) for IP Address cache size (no caching).

- Enhances the Egress/East-West Policy Ruleset Rule matching criteria to introduce a new variation of an FQDN Profile called an FQDN Match Profile. The FQDN Profile variant is a set of PCRE-defined FQDNs that can be applied to TLS encrypted traffic such that the policy can match on SNI. This enhances the segmentation policy with added flexibility for policies that need to have finer-grained control based on FQDNs.

Fixes

The following fixes are included in this upgrade:

- Fixes an Ingress Gateway issue related to the session upstream connection where the connection being null could result in a datapath self heal.
- Fixes a stability issue in WAF related to large POST commands with chunked encoding enabled.
- Fixes an Ingress Gateway session pool exhaustion issue related to HTTP Keepalives where frontend (Client to Gateway) has KA enabled and backend (Gateway to Server) has KA disabled.
- Fixes an issue related to a dynamic policy that leverages a GCP service where the service does not exist resulting in a policy that contains an empty IP/CIDR. The configuration is valid requiring the Gateway to handle cases where a policy might contain an empty IP/CIDR.
- Fixes an issue related to Rule matching that could result in a datapath self-heal.
- Removes an Azure-generated message that is presented as a System Log message related to Gateway provisioning where Azure assigns a different interface type than requested and posts a warning message suggesting potential performance degradation. The message is seen as `TYPE_AZURE_DEGRADED_PERFORMANCE`. There is no performance impact related to the assigned interface type.
- Enhances Gateway stability for all use cases to eliminate any potential session pool exhaustion.

Legacy Multicloud Defense Terraform Provider Versions

Version 23.7

Version 23.7.2 July 27, 2023

Fixes

The following fix is included in this version:

- Fixes an issue where an FQDN profile (`valtix_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.

Version 23.7.1 July 24, 2023

Fixes

The following fixes are included in this release:

- Fixes an issue when creating a Dynamic VPC address object (`valix_address_object`) resource for an Azure VNet would result in a "'region' parameter is not supported" error.
- Fixes an issue where an FQDN Profile (`valtix_fqdn_profile`) resource with `mode=MATCH` argument incorrectly requires 'policy' argument.

Version 23.6

Version 23.6.1 July 17, 2023

Enhancements

The following enhancements are included in this release:

- Enhanced the Alert profile (`valtix_alert_profile`) resource to support sending alerts (System Logs, Audit Logs) to Webex Teams.
- Adds support for including a Subnet resource as a scope in a Dynamic User Defined Tag address object (`valtix_address_object`) resource.

Fixes

The following fix is included in this release:

- Fixes an issue when creating a Dynamic VPC Address object (`valix_address_object`) resource for an Azure VNet would result in a "'region' parameter is not supported" error.
- Fixes an issue when deploying a gateway (`valtix_gateway`) resource in Azure would throw an error when attempting to deploy in south central/US region.

Version 23.5

Version 23.5.1 June 12, 2023

Enhancements

The following enhancement is included in this release:

- Published a Multicloud Defense Terraform Provider that mirrors the Valtix Terraform Provider. The new Provider is called `ciscomcd` and will be available publicly in the near future. The providers will be updated simultaneously and will represent mirrors of each other unless announced otherwise. In the near future, the Valtix provider will be deprecated and fully replaced by the Cisco provider.

Fixes

The following fixes are included in this release:

- Fixes an issue where deploying a gateway (`valtix_gateway`) resource into Azure zone 1 south central/US region would result in an error.
- Enhances the attributes of a gateway (`valtix_gateway`) resource to output the Azure gateway load balancer frontend resource ID when deploying the ingress gateway in an Azure gateway load balancer-based architecture. The output is specified as part of the gateway endpoint (`gateway_gwlb_endpoints`) attribute.
- Fixes the example in the policy rule set (`valtix_policy_rule_set`) group resource to reference the appropriate member resource argument.

Verison 23.4

Version 23.4.3 May 23, 2023

Fixes

The following fix is included in this release:

- Enhances the attributes of a gateway (`valtix_gateway`) resource to output the Azure gateway load balancer frontend resource ID when deploying the ingress gateway in an Azure gateway load balancer-based architecture. The output is specified as part of the gateway endpoint (gateway_gwlb_endpoints) attribute.

Version 23.4.2 May 11, 2023

Fixes

The following fixes are included in this section:

- Fixes an issue with the NTP profile (`valtix_ntp_profile`) data source where attempting to access the resource would generate an invalid data source error.
- Updates to the Terraform documentation to include the NTP profile (`valtix_ntp_profile`) resource and data source information.

Version 23.4.1 April 20, 2023

Enhancements

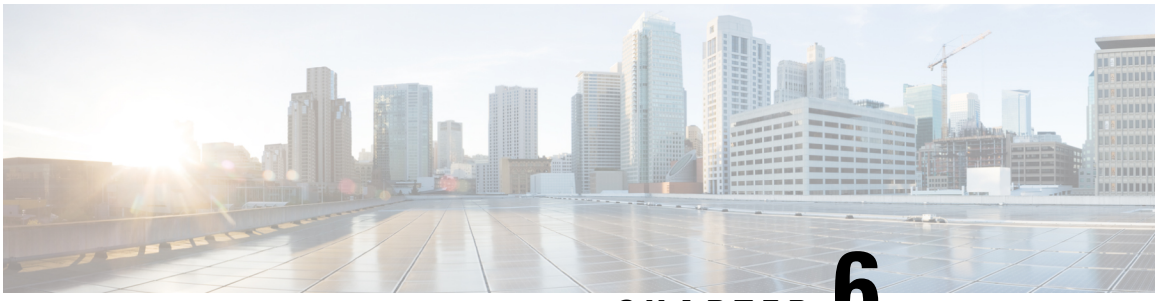
The following enhancements is included in this release:

- Changes the policy rule set (`valtix_policy_rule_set`) resource to include `group_member_ids` argument replacing `child_rule_set_ids` argument that is now deprecated.

Fixes

The following fixes are included in this release:

- Fixes an issue with Terraform **Import** operation related to the gateway resource (`valtix_gateway`).
- Fixes an issue in the gateway resource (') where specifying an SSH Key Pair (`ssh_key_pair)` for an Azure gateway would result in an error stating the argument is not supported.
- Fixes an issue related to suppression of WAF rule IDs 949110 and 959100. These rule IDs are informational and define security events stating the WAF anomaly scores (request and response, respectively) have been exceeded along with the action taken based on the WAF profile resource (`valtix_profile_application_threat`) configuration. When these rule IDs are suppressed, the information Events will not be generated. The fix prohibits the ability to suppress these rule IDs resulting in the informational events will always be generated.
- Fixes an issue with Terraform Import operation related to the policy rules resource (`valtix_policy_rules`).



CHAPTER 6

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