

Cisco Multicloud Defense Release Notes

First Published: 2023-01-25

Last Modified: 2026-09-11

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

© 2023–2026 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1

Welcome 1

Multicloud Defense 1

Recommended Versions 1

Additional Resources and Assistance 2

CHAPTER 2

Multicloud Defense Controller and Gateway Releases 3

Version 26.08 Multicloud Defense Controller, September 18, 2026 4

Version 26.08 Multicloud Defense Controller, September 11, 2026 4

Version 26.08 Multicloud Defense Controller, September 8, 2026 4

Version 26.08 Multicloud Defense Controller, September 1, 2026 5

Version 26.07 Multicloud Defense Controller, August 21, 2026 5

Version 26.07 Multicloud Defense Controller, August 7, 2026 6

July 26, 2026 Gateway 25.02-10 (Recommended) 6

Version 26.06 Multicloud Defense Controller, July 8, 2026 6

June 17, 2026 Gateway 25.02-09 7

June 3, 2026 Gateway 25.02-08 7

Version 26.05 Multicloud Defense Controller, May 19, 2026 7

May 7, 2026 Gateway 24.06-21 8

May 1, 2026 Gateway 25.02-07 8

May 1, 2026 Gateway 25.02-07-a1 9

Version 26.04 Multicloud Defense Controller, April 21, 2026 9

April 21, 2026 Gateway 26.03 10

Version 26.03 Multicloud Defense Controller, April 1, 2026 10

March 24, 2026 Gateway 25.02-06-a1 10

March 24, 2026 Gateway 25.02-06 10

Version 26.03 Multicloud Defense Controller, March 18, 2026 11

February 21, 2026, Gateway 25.02-05 11
Version 26.02 Multicloud Defense Controller 12
February 13, 2026 Gateway 24.06-20 13
December 12, 2025 Gateway 24.06-19 13
Version 25.12 Multicloud Defense Controller, December 12, 2025 13
November 18, 2025 Gateway 24.06-18 13
Version 25.10 Multicloud Defense Controller, November 5, 2025 14
October 15, 2025 Gateway 25.02-03 15
Version 25.09 Multicloud Defense Controller, October 7, 2025 17
October 3, 2025 Gateway Hotfix 24.06-17-a1 17
September 24, 2025 Gateway 24.06-17 17
August 22, 2025 Gateway Hotfix 24.06-16-a1 18
August 2025 Gateway Version 24.06-16 and Controller Version 25.08 18
Version 25.07 Multicloud Defense Controller, July 31, 2025 19
July 17, 2025 Gateway Hotfix 24.06-15-a1 19
June 2025 Gateway Version 24.06-15 and Controller Version 25.06 20
July 3, 2025 Gateway Hotfix 24.06-14-b1 21
July 3, 2025 Gateway 25.02-02 21
February 28, 2025 Gateway 25.02-01 24
June 5, 2025 Gateway Hotfix 24.06-14-a1 28
May 2025 Gateway Version 24.06-14 and Controller Version 25.05 29
May 23, 2025 Gateway Hotfix 24.06-13-a1 29
May 23, 2025 Gateway 24.06-13 30
May 9, 2025 Gateway Hotfix 24.06-12-a1 30
May 9, 2025 Gateway 24.06-12 31
May 7, 2025 Gateway Hotfix 24.06-11-a1 31
April 2025 Gateway Version 24.06-11 and Controller Version 25.04 32

CHAPTER 3 **Multicloud Defense Controller Features and Enhancements (Archives)** 33
Version 25.03 March 28, 2025 33
Version 25.02 February 28, 2025 33
Version 25.01 January 6, 2025 34
Version 24.12 December 2, 2024 34

CHAPTER 4 Multicloud Defense Gateway Fixes and Enhancements (Archives) 35

Version 24.06 35

Version 24.06-10-a1 March 31, 2025 35

Version 24.06-10 March 31, 2025 35

Version 24.06-09-a1 February 14, 2025 36

Version 24.06-09 February 14, 2025 37

Version 24.06-08-a1 January 16, 2025 37

Version 24.06-08 January 16, 2024 37

Version 24.06-07-a1 December 18, 2024 38

Version 24.06-07 December 18, 2024 38

Version 24.06-06-a1 November 28, 2024 39

Version 24.06-06 November 26, 2024 39

Version 24.06-05 November 22, 2024 39

Version 24.06-04 October 25, 2024 40

Version 24.06-03 October 20, 2024 40

Version 24.06-02-a2 October 2, 2024 41

Version 24.06-02 September 18, 2024 41

Version 24.06-01 July 10, 2024 42

Version 24.04 43

Version 24.04-01 May 16, 2024 43

Version 24.02 44

Version 24.02-02 April 18, 2024 44

Version 24.02-01 February 28, 2024 44

Version 23.08 46

Version 23.08-17-b1 September 27, 2024 46

Version 23.08-17-a1 September 4, 2024 46

Version 23.08-17 September 4, 2024 47

Version 23.08-16-a1 August 6, 2024 47

Version 23.08-16 June 25, 2024 47

Version 23.08-15-a3 June 22, 2024 48

Version 23.08-14-c3 June 8, 2024 48

Version 23.08-15-c1 May 9, 2024 49

Version 23.08-15-a2 May 1, 2024 49

Version 23.08-15-b1 April 12, 2024 49
Version 23.08-15-a1 April 11, 2024 49
Version 23.08-15 March 27, 2024 50
Version 23.08-14-e1 March 28, 2024 50
Version 23.08-14-a2 March 20, 2024 51
Version 23.08-14-d1 March 13, 2024 51
Version 23.08-14-c1 February 20, 2024 51
Version 23.08-14-b1 February 21, 2024 52
Version 23.08-14-a1 February 17, 2024 52
Version 23.08-14 January 25, 2024 52
Version 23.08-12 January 18, 2024 53
Version 23.08-11 January 11, 2024 53
Version 23.08-10 December 18, 2023 53
Version 23.08-09 November 16, 2023 54
Version 23.08-08 November 8, 2023 54
Version 23.08-07 October 18, 2023 54
Version 23.08-06 October 7, 2023 54
Version 23.08-05 October 3, 2023 54
Version 23.08-04 September 19, 2023 55
Version 23.08-03 September 10, 2023 55
Version 23.08-02 September 3, 2023 55
Version 23.08-01 August 25, 2023 55

CHAPTER 5 **Multicloud Defense Terraform Provider Enhancements** 57

Multicloud Defense Terraform Provider Version 25.8.1 September 16, 2025 (Recommended) 57
Multicloud Defense Terraform Provider Version 0.3.3 June 20, 2025 58
Multicloud Defense Terraform Provider Version 0.3.2 June 20, 2025 58
Multicloud Defense Terraform Provider Version 0.3.1 May 7, 2025 58
Multicloud Defense Terraform Provider Version 0.3.0 March 3, 2025 59
Multicloud Defense Terraform Provider Version 0.2.9 November 15, 2024 59
Multicloud Defense Terraform Provider Version 0.2.8 November 7, 2024 59
Multicloud Defense Terraform Provider Version 0.2.7 August 21, 2024 60
Multicloud Defense Terraform Provider Version 0.2.6 March 1, 2024 60
Multicloud Defense Terraform Provider Version 0.2.5 November 6, 2023 61

Multicloud Defense Terraform Provider Version 0.2.4 August 22, 2023 62

CHAPTER 6 **Legacy Versions** 63

Legacy Multicloud Defense Gateway Versions 63

Version 23.10 63

Version 23.10-03 January 11, 2024 63

Version 23.10-02 November 16, 2023 64

Version 23.10-01 November 3, 2023 64

Version 23.06 65

Version 23.06-14 November 12, 2023 65

Version 23.06-13 October 18, 2023 65

Version 23.06-12 October 6, 2023 65

Version 23.06-11 September 27, 2023 66

Version 23.06-10 September 19, 2023 66

Version 23.06-09 September 10, 2023 66

Version 23.06-08 September 3, 2023 66

Version 23.06-07 August 29, 2023 66

Version 23.06-06 August 23, 2023 67

Version 23.06-05 August 4, 2023 67

Version 23.06-04 July 27, 2023 67

Version 23.06-03 July 21, 2023 67

Version 23.06-02 July 19, 2023 68

Version 23.06-01 July 6, 2023 68

Version 23.04 69

Version 23.04-18 September 3, 2023 69

Version 23.04-17 August 23, 2023 69

Version 23.04-16 August 22, 2023 69

Version 23.04-14 July 27, 2023 70

Version 23.04-13 July 27, 2023 70

Version 23.04-12 July 19, 2023 70

Version 23.04-11 July 10, 2023 71

Version 23.04-10 June 28, 2023 71

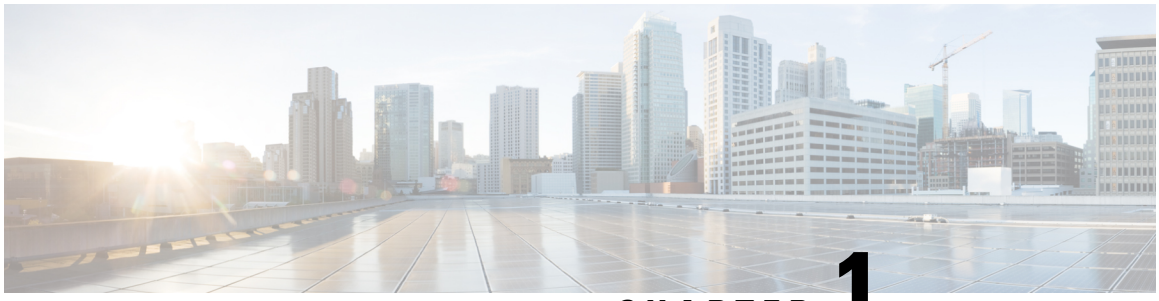
Version 23.04-09 June 25, 2023 71

Version 23.04-07 June 14, 2023 72

Version 23.04-06 June 8, 2023 72
Version 23.04-05 June 1, 2023 72
Version 23.04-04 May 19, 2023 72
Version 23.04-03 May 16, 2023 73
Version 23.04-02 May 2, 2023 73
Version 23.04-01 April 20, 2023 73
Version 23.02 75
Version 23.02-10 June 28, 2023 75
Version 23.02-09 June 25, 2023 75
Version 23.02-08 June 15, 2023 75
Version 23.02-07 June 8, 2023 76
Version 23.02-06 June 2, 2023 76
Version 23.02-05 May 22, 2023 76
Version 23.02-04 April 14, 2023 77
Version 23.02-03 March 7, 2023 77
Version 23.02-02 February 20, 2023 77
Version 23.02-01 February 15, 2023 77
Legacy Multicloud Defense Terraform Provider Versions 78
Version 23.7 78
Version 23.7.2 July 27, 2023 78
Version 23.7.1 July 24, 2023 79
Version 23.6 79
Version 23.6.1 July 17, 2023 79
Version 23.5 79
Version 23.5.1 June 12, 2023 79
Verison 23.4 80
Version 23.4.3 May 23, 2023 80
Version 23.4.2 May 11, 2023 80
Version 23.4.1 April 20, 2023 80

CHAPTER 7 **Release and Service Policies** 83
Release Versioning and Schedule 83
Release Life and Support 84

87



CHAPTER 1

Welcome

Welcome to the Multicloud Defense Release Notes. This document provides a comprehensive collection of features, enhancements, major fixes, and any hotfixes that are included in each release. Note that there are significant sections that address the releases for the Controller, the Gateway, and the Terraform Provider.

- Multicloud Defense, on page 1
- Recommended Versions, on page 1
- Additional Resources and Assistance, on page 2

Multicloud Defense

Multicloud Defense 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 varies.

Multicloud Defense offers a sophisticated, streamlined security framework harmonizing controller orchestration, gateway communication, and optimized datapath processing for robust and efficient multicloud protection.

Recommended Versions

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

Multicloud Defense Gateway

Version 25.02-10, July 26, 2026

Multicloud Defense Terraform Provider

Version 25.8.1, September 16, 2025

Additional Resources and Assistance

Online Resources

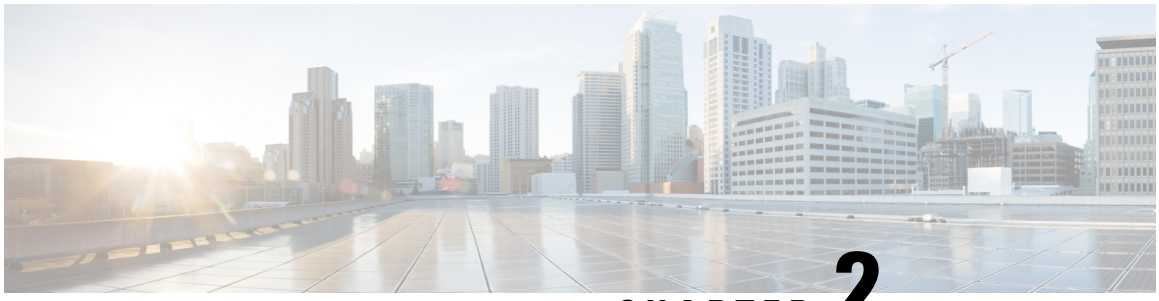
Cisco provides this additional documentation:

- Cisco Multicloud Defense User Guide
- Cisco Multicloud Defense Getting Started 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 and Gateway Releases

While Multicloud Defense Controller and Multicloud Defense Gateway releases are not packaged together, updates are typically released within the same timeframe. The controller is updated automatically so your URL-hosted controller dashboard is always up-to-date; the gateway is updated at your preference to minimize security and traffic inspection interruptions that could affect the state of your environment.

- Version 26.08 Multicloud Defense Controller, September 18, 2026, on page 4
- Version 26.08 Multicloud Defense Controller, September 11, 2026, on page 4
- Version 26.08 Multicloud Defense Controller, September 8, 2026, on page 4
- Version 26.08 Multicloud Defense Controller, September 1, 2026, on page 5
- Version 26.07 Multicloud Defense Controller, August 21, 2026, on page 5
- Version 26.07 Multicloud Defense Controller, August 7, 2026, on page 6
- July 26, 2026 Gateway 25.02-10 (Recommended), on page 6
- Version 26.06 Multicloud Defense Controller, July 8, 2026, on page 6
- June 17, 2026 Gateway 25.02-09, on page 7
- June 3, 2026 Gateway 25.02-08, on page 7
- Version 26.05 Multicloud Defense Controller, May 19, 2026, on page 7
- May 7, 2026 Gateway 24.06-21, on page 8
- May 1, 2026 Gateway 25.02-07, on page 8
- May 1, 2026 Gateway 25.02-07-a1, on page 9
- Version 26.04 Multicloud Defense Controller, April 21, 2026, on page 9
- April 21, 2026 Gateway 26.03, on page 10
- Version 26.03 Multicloud Defense Controller, April 1, 2026, on page 10
- March 24, 2026 Gateway 25.02-06-a1, on page 10
- March 24, 2026 Gateway 25.02-06, on page 10
- Version 26.03 Multicloud Defense Controller, March 18, 2026, on page 11
- February 21, 2026, Gateway 25.02-05, on page 11
- Version 26.02 Multicloud Defense Controller, on page 12
- February 13, 2026 Gateway 24.06-20, on page 13
- December 12, 2025 Gateway 24.06-19, on page 13
- Version 25.12 Multicloud Defense Controller, December 12, 2025, on page 13
- November 18, 2025 Gateway 24.06-18, on page 13
- Version 25.10 Multicloud Defense Controller, November 5, 2025, on page 14

- October 15, 2025 Gateway 25.02-03, on page 15
- Version 25.09 Multicloud Defense Controller, October 7, 2025, on page 17
- October 3, 2025 Gateway Hotfix 24.06-17-a1, on page 17
- September 24, 2025 Gateway 24.06-17, on page 17
- August 22, 2025 Gateway Hotfix 24.06-16-a1, on page 18
- August 2025 Gateway Version 24.06-16 and Controller Version 25.08, on page 18
- Version 25.07 Multicloud Defense Controller, July 31, 2025, on page 19
- July 17, 2025 Gateway Hotfix 24.06-15-a1, on page 19
- June 2025 Gateway Version 24.06-15 and Controller Version 25.06, on page 20
- July 3, 2025 Gateway Hotfix 24.06-14-b1, on page 21
- July 3, 2025 Gateway 25.02-02, on page 21
- February 28, 2025 Gateway 25.02-01, on page 24
- June 5, 2025 Gateway Hotfix 24.06-14-a1, on page 28
- May 2025 Gateway Version 24.06-14 and Controller Version 25.05, on page 29
- May 23, 2025 Gateway Hotfix 24.06-13-a1, on page 29
- May 23, 2025 Gateway 24.06-13, on page 30
- May 9, 2025 Gateway Hotfix 24.06-12-a1, on page 30
- May 9, 2025 Gateway 24.06-12, on page 31
- May 7, 2025 Gateway Hotfix 24.06-11-a1, on page 31
- April 2025 Gateway Version 24.06-11 and Controller Version 25.04, on page 32

Version 26.08 Multicloud Defense Controller, September 18, 2026

The following fix is included in this release:

- Fixes an issue where the **HTTP2** checkbox was incorrectly missing from the Service object creation and editing screens in the UI.

Version 26.08 Multicloud Defense Controller, September 11, 2026

The following fix is included in this release:

- Fixes an issue where amplitude pods were failing due to SQL syntax errors. This fix updates amplitudecli to avoid stacked queries by qualifying table names with tenant schemas and using separate connections, resolving the pod failures without re-enabling multiStatements=true.

Version 26.08 Multicloud Defense Controller, September 8, 2026

The following fixes are included in this release:

- Fixes an issue with parsing controller logs in Splunk for Global Payment. Controller logs are not encoded but have concatenated event values, making rule creation difficult. The fix will expose the destination IP and message fields at the top level in IPS events for better analytics.
- Fixes an issue where inventorylogsserver pods in US prod1 are crashing due to out-of-memory errors caused by high memory usage when processing Azure VNet flow logs. Recommended fixes include skipping records with missing NICs, streaming flow tuples individually, incremental chunk flushing, and rate-limiting error logging. Temporary memory limit increases and inventory sync investigations are suggested mitigations.

Version 26.08 Multicloud Defense Controller, September 1, 2026

The following fix is included in this release:

- Support for features such as AI Guardrail and L7 Denial-of-Service is being deprecated.

Version 26.07 Multicloud Defense Controller, August 21, 2026

The following fixes are included in this release:

- Fixes an issue where the usagecli gRPC interceptor bug causes inactive accounts to be wrongly reactivated during billing because the system activates accounts without checking if they have valid CSP accounts. This fix ensures accounts are only reactivated if they have one or more active CSP accounts, preventing unintended reactivation.
- Fixes an issue where the billing pipeline runs the `accountutils -cmd` list command without filtering by account state, causing it to include inactive accounts. This results in inactive accounts being processed and inadvertently reactivated. This fix adds support for filtering to include only active accounts, preventing unintended reactivation.
- Adds support for selecting and configuring the internal load balancer option directly through the UI, simplifying deployment and management of cloud ingress gateways. This update introduces a new UI option to enable the use of an internal load balancer for Azure and AWS Firewall Threat Defense Virtual (FTDv) ingress gateways. While this feature was previously functional via Terraform, it was not available in the UI.
- Adds support for LegacyVMNVA Tag in Azure Deployments. Multicloud Defense and Firewall Threat Defense Virtual (FTDv) gateways now include the LegacyVMNVA tag to prevent deployment on unsupported Microsoft Azure Network Adapter (MANA) hardware. This configuration ensures continued stability for existing VM series and serves as a temporary exception valid until the Microsoft-defined sunset date of May 31, 2027.
- Fixes an issue where gateway or account names containing underscores prevented VPN tunnel configuration. DNS labels now sanitize these names by replacing underscores with hyphens, ensuring compliance with RFC 1123 hostname standards and allowing for successful tunnel setup with external peer systems.

Version 26.07 Multicloud Defense Controller, August 7, 2026

The following fixes are included in this release:

- Fixes an issue where the `api/v1/gateway/get` API call failed when selecting the **create new** option from the **Policy Rule Set** drop-down during the creation of AWS, Azure, and GCP FTDv gateways. This fix addresses the failure that occurred after deployment when navigating to the enforcement view, which previously showed a **Policy ID is empty** error and improves the time taken to create Azure FTDv gateways.
- Fixes an issue where Karpenter fails to deploy correctly on Kubernetes clusters that share subnets due to non-unique tagging of shared resources, causing ownership conflicts and malfunction. This fix ensures unique tagging by appending the cluster name and an arbitrary value to resource tags, enabling proper deployment across multiple clusters.
- Fixes an issue where selecting certain Azure regions like **belgiumcentral**"or **austriaeast** on the **Enable Traffic Visibility** page caused a **Network watcher not enabled** error. This occurred because Network Watcher was not provisioned in those regions if no prior networking resources existed there. This fix improves handling of such cases to prevent API failures during traffic visibility setup.

July 26, 2026 Gateway 25.02-10 (Recommended)

The following fixes and enhancements are included in this release:

- Fixes 403 forbidden errors on S3 Downloads. This issue was caused by a REX failure when TLS ClientHello packets arrived out-of-order (OOO). We have now updated the gateway's OOO drop guard mechanism to correctly detect and handle out-of-order fragments within SNAT-enabled flows.
- Adds support for Teleport labels to facilitate enhanced access control integration. This update allows for more granular resource categorization and improved policy enforcement when managing gateway access.
- Fixes an issue where gateways could become stuck in an "updating" state. Previously, internal ASAC container reboots inadvertently reset host Linux memory-overcommit settings and disabled ZRAM swap. The gateway now maintains the required memory headroom for hitless configuration updates, preventing update failures and ensuring continuous application of security profile updates.
- The integrated Teleport agent has been upgraded to version 18. This update aligns the agent with the latest Teleport server standards, ensuring seamless communication and feature parity.

Version 26.06 Multicloud Defense Controller, July 8, 2026

The following enhancements are included in this release:

- **Firewall Threat Defense virtual (FTDv)**—To deploy FTDv gateway using Multicloud Defense, like AWS, Azure now utilizes a unified gateway for Ingress, Egress, and East-West traffic. GCP requires separate gateways for Ingress or Egress and East-West traffic.

- In the edit gateway workflow for Firewall Threat Defense Virtual (FTDv), the **security_type** field will now be editable. This field is already present in the create gateway workflow. This enhancement applies only to gateways deployed in AWS and Azure environments.

June 17, 2026 Gateway 25.02-09

The following fixes are included in this release:

- Fixes an intermittent crash in certificate validation routine in the Multicloud Defense Gateway datapath.
- Fixes a stability issue where the datapath worker would become unresponsive when handling very large HTTP responses. This fix ensures that the datapath remains performant and stable even when handling responses that significantly exceed configured inspection limits.

June 3, 2026 Gateway 25.02-08

The following fixes are included in this release:

- Fixes an issue where a segmentation fault (SEGV) was identified in the dp-worker process, occurring during response-side IPS packet processing. The dp-worker process crashes upon receiving certain upstream error responses, leading to service disruption and potential packet processing failures during the affected period. This fix treats live nginx connection pairing independently of the flowdata lifetime to prevent premature dereferencing.
- Fixes an issue where packets destined for a Load Balancer (LB) frontend or floating IP in AWS GWLB (Geneve) and Azure GWLB (VXLAN) deployments were not correctly identified as frontend traffic. This misidentification caused the system to skip the required metadata NAT (DNAT) action, resulting in failed forwarding or proxying for the affected traffic. We have now updated the packet processing to ensure correct identification of tunnelled traffic.
- Fixes an issue where AWS EDGE routed ForwardProxy/AppID flows bypassed the proxy/NAT behavior, exposed the original client IP to the backend and rejected the connection. This fix ensures that the MySQL Allow step grants access to the client IP so that the policy or logging semantics are not affected for the routed ForwardProxy traffic.
- Fixes an ingress connectivity issue on FedRAMP gateway. This fix restores the ingress connectivity by triggering a gateway instance replacement.
- Fixes an issue where in version 25.02-07-a1, VPN traffic fails to pass through the Azure Gateway Load Balancer (GWLB) despite successful establishment of the tunnel. Users are advised to upgrade to version 25.02-08 or later to restore proper traffic forwarding.
- Fixes issues in the Gateway datapath related to metadata NAT and iptables configuration. This fix ensures more stable traffic handling and correct packet path processing.

Version 26.05 Multicloud Defense Controller, May 19, 2026

The following enhancement is included in this release:

- **Dynamic Geo IP Support** —We have now enhanced the backend implementation for processing Geo IP regions to better support the growing list of Geo IPs. This update enables the system to manage geographic IP data more dynamically and efficiently.

May 7, 2026 Gateway 24.06-21

The following fixes are included in this release:

- Fixes an issue where GCP gateways could become stuck in an Active pending → Active → Active pending loop with HEARTBEATMISS errors after upgrade (or downgrade/upgrade) to 24.06-20 on version 24.06. The fix aligns the controller's health/heartbeat handling with the CSP instance group health checks so gateways remain stable and active once healthy.
- Fixes a rare issue that could cause the data plane worker process to crash during TLS inspection on gateways. This fix improves internal buffer handling to prevent these crashes and enhances overall gateway stability during secure traffic inspection.
- Fixes an issue where Multicloud Defense gateway instances could briefly enter a health check pending state and disrupt connectivity when short-lived session spikes occurred. The datapath has been hardened so gateways handle these spikes more reliably.
- Fixes an issue where applying an IPS policy to a gateway could cause a datapath crash, trigger instance replacement, and leave the gateway stuck in an "Updating" state. The fix ensures that critical system settings are properly preserved during internal service restarts, preventing the crash and restoring normal policy application behavior.
- Fixes a gateway PCAP handling defect that unnecessarily buffered packets and could deplete RX/TX mbuf pools in deployments with gateway-level PCAP configured.
- Fixes a gateway datapath bug that could exhaust packet buffers and trigger unnecessary instance replacements due to heartbeat missed events.
- Fixes an issue where high DNS traffic and large rule updates could drain datapath flow memory and trigger restarts, improving gateway stability during continuous operations and config changes.
- Fixes an issue where HTTP forward proxy requests with long URLs could be mis-parsed, causing intermittent FQDN mismatches and unexpected traffic denials on FQDN-based policies.
- Fixes an issue where Multicloud Defense gateway instances could remain stuck in ACTIVE_PENDING or HEALTH_CHECK_PENDING state due to a MLX driver crash inside the guest. This fix ensures that updated DPDK versions are used to prevent the crash in the gateway.

May 1, 2026 Gateway 25.02-07

The following fixes are included in this release:

- Fixes an issue where agent crashes when a lot of policy rules are involved in back-to-back configuration updates requiring sync across agent threads, triggering a hitful restart of the datapath, leading to the gateway entering an ACTIVE_PENDING state.
- Fixes an issue where applying an IPS policy to a gateway could cause a datapath crash, trigger instance replacement, and leave the gateway stuck in an "Updating" state.

- Fixes an issue where Multicloud Defense gateway instances could remain stuck in ACTIVE_PENDING or HEALTH_CHECK_PENDING state due to a MLX driver crash inside the guest. This fix ensures that updated DPDK versions are used to prevent the crash in the gateway.
- Fixes a connectivity issue affecting VPN tunnels on Azure V5/V6 VM instances in the US East region.
- Fixes an issue where excessive debug logging caused IO delays within the agent. This fix ensures that agent is properly configured to handle debug logs more efficiently.

May 1, 2026 Gateway 25.02-07-a1

In addition to bug fixes and enhancements in 25.02-07, the following issues are addressed in release 25.02-07-a1:

- Fixes an issue where modifications to large address objects or large number of address objects caused traffic disruption, resulting in a traffic outage.
- Fixes a regression introduced by metadata-mark support that caused backend flowdata collision during SNAT port allocation.
- IMPORTANT: In version 25.02-07-a1, VPN traffic may fail to pass through the VPN tunnel. Users who use the gateway for VPN connectivity should use version 25.02-07. This issue will be addressed in a future release.

Version 26.04 Multicloud Defense Controller, April 21, 2026

Features and Enhancements

The following features and enhancements are included in this release:

- **Cloud Deployment**—The Cloud Deployment for the Cisco Secure Firewall Threat Defense Virtual is a wizard which enables easy deployment of virtual firewalls across multicloud and private cloud environments. This wizard streamlines the deployment process and simplifies the selection of enforcement points.
- **Pay-As-You-Go (PAYG) Licensing**—Multicloud Defense now supports the PAYG licensing for Firewall Threat Defense Virtual. This is a usage-based model which enables you to use the license on demand. This licensing option is available only on AWS.
- **Firewall Threat Defense virtual (FTDv)**—Provides Next-Generation Firewall functionality to virtualized environments, enabling consistent security policies to follow workloads across your physical, virtual, and cloud environments. You can deploy Firewall Threat Defense Virtual gateway using Multicloud Defense. Azure and GCP require separate gateways for Ingress, and Egress or East-West traffic, whereas AWS utilizes a unified gateway for Ingress, Egress, and East-West traffic.
- **Webhook Authentication**—We have now enhanced webhook authentication for inventory monitoring which increases security of our system.

Fix

The following fixes are included in this release:

- Fixes an issue in the AWS log forwarding service where the MCD controller inserted an extra slash (“/”) when forwarding logs to AWS, resulting in destination paths containing double slashes (for example, `ExampleTenant//2026/...`). This issue has been addressed, and destination paths are now normalized to a single-slash format (for example, `ExampleTenant/logs/2026/...`). Please update any existing scripts or integrations that specifically depend on the previous destination path structure.
- Fixes an issue related to traffic failure due to internal IP conflict while creating a new gateway. Users are advised to not use 172.16.0.0/16 subnet when creating a new gateway.

April 21, 2026 Gateway 26.03

The following fix is included in this release:

- Fixes an issue where editing an Azure gateway's instance type could incorrectly fail with "instance type not supported" errors due to stale cached data from a previous operation. The SKU cache now correctly distinguishes between different instance types during validation.

Version 26.03 Multicloud Defense Controller, April 1, 2026

The following fix is included in this release:

- In some GCP environments, newly created VPCs with a large number of subnets were discovered without CIDR information, and their subnets were not visible in Asset Discovery or when deploying gateways. This has been fixed so that all VPCs and their CIDR ranges are correctly discovered and displayed, even at large scale.

March 24, 2026 Gateway 25.02-06-a1

In addition to bug fixes and enhancements in 25.02-06, the following issue is also addressed in release 25.02-06-a1:

- Improved gateway scalability by enhancing support for large number of address groups combined with large number of policy rules, reducing update/processing overhead in high-scale environments.

March 24, 2026 Gateway 25.02-06

The following fixes are included in this release:

- Fixes an issue where GCP gateways could become stuck in an Active pending –> Active –> Active pending loop with HEARTBEATMISS errors after upgrade (or downgrade/upgrade) to 24.06-20 on version 24.06. The fix aligns the controller’s health/heartbeat handling with the Cloud Service Provider's (CSP) instance group health checks so that gateways remain stable and active, once healthy.

- Fixes a rare issue that could cause the data plane worker process to crash during TLS inspection on gateways. This fix improves internal buffer handling to prevent these crashes and enhances overall gateway stability during secure traffic inspection.
- Fixes an issue where Multicloud Defense gateway instances could briefly enter a health check pending state and disrupt connectivity when short-lived session spikes occur. The datapath has been hardened so that gateways can handle these spikes more reliably.
- Fixes a gateway PCAP handling defect that unnecessarily buffered packets and could deplete RX/TX mbuf pools in deployments with gateway-level PCAP configured.
- Fixes a gateway datapath bug that could exhaust packet buffers and trigger unnecessary instance replacements due to heartbeat missed events.
- Fixes an issue where HTTP forward proxy requests with long URLs could be misparsed, causing intermittent FQDN mismatches and unexpected traffic denials on FQDN-based policies.

Version 26.03 Multicloud Defense Controller, March 18, 2026

The following enhancements are included in this release:

- **Microsoft Sentinel Log Forwarding Behavior Change** – Microsoft Sentinel has deprecated the legacy HTTP Data Collector API. Multicloud Defense now supports the Microsoft Sentinel log ingestion API for Log Forwarding, which offers improved processing and greater flexibility for log ingestion. For more information, see Azure Monitor Log Ingestion API.
- **Sumo Logic Support** – Multicloud Defense now provides Sumo Logic support for system and audit logs. For log forwarding, the new format requires a base URL and a separate authToken (with an optional `skip_verify` parameter). While existing profile formats remain functional, you cannot edit them using the previous method. To edit these profile formats, you must use the new method by providing the endpoint (base URL only) and token separately. For alert profiles, you must provide a base URL and an `integration_key` (secret).

February 21, 2026, Gateway 25.02-05

The following fixes are included in this release:

- Fixes an issue where the gateway ipset configuration stops responding after an Address Group update, resulting in a bad gateway response. This fix enables an update in the Address Group to reflect in the update of the ipset also.
- Fixes an issue where SNAT stopped working after upgrading the gateway from 24.06-15 to 24.06-19. This fix ensures that the address translation works properly.

Version 26.02 Multicloud Defense Controller

Version 26.02 Multicloud Defense Controller, February 27, 2026

The following fix is included in this release:

- Fixes an issue related to unhealthy load balancers caused by an update by Microsoft Azure in the backend to the `probeThreshold` parameter and the system no longer considering the `numberofProbes` property. Changes were made to the address objects in Multicloud Defense Controller to fix the issue.

Version 26.02 Multicloud Defense Controller, February 20, 2026

This is a hotfix. The following fix is included in this release:

- Fixes an issue where Azure VNet flow logs with an empty or malformed subnet ID could cause the inventory logs service to crash, preventing some Azure flow logs from being processed.

Version 26.02 Multicloud Defense Controller, February 19, 2026

The following fixes and enhancements are included in this release:

- **Red Hat Enterprise Linux 9 Support** – Multicloud Defense now supports Red Hat Enterprise Linux 9 (RHEL 9) for all gateway versions. We fixed issues related to gateway instances 23.8-15 and earlier, which did not support RHEL 9.
- **Red Hat Enterprise Linux 9 Support for Google Cloud Platform** – Multicloud Defense now supports RHEL 9 for Google Cloud Platform (GCP). Replace your existing gateway instance with the new instance. This new instance uses the RHEL 9 kernel in place of CentOS, offering improved porting of all vulnerability patches and advanced security protection.
- **Firewall Threat Defense Virtual Version 10.0 Support** – Multicloud Defense now supports Firewall Threat Defense Virtual (FTDv) version 10.0.
- **Inventory Page Search Experience** – Multicloud Defense now offers an improved search experience on the Inventory page that is consistent with the overall search experience across the Multicloud Defense application.
- **Grafana Loki Log Forwarding Support** – You can now forward logs to destinations using Grafana Loki. Grafana Loki helps simplify operations and is cost effective.

Version 26.02 Multicloud Defense Controller, February 12, 2026

The following fixes are included in this release:

- **Investigate Page Data Loading** – Improved the page load time on the Investigate page of the Multicloud Defense application.
  - Resolved slow data load times caused by the API calling large data sets instead of user-requested data for a specific date range.
  - Fixed issues related to time filters not synchronizing on the Investigate page and the Audit Logs page. Time range filters now synchronize to show and fetch data for the same period ranges for the Investigate page and the Audit Logs page.

- **IPv6 Configuration Not Supported in Address Groups** – Recent updates to the Multicloud Defense environment caused IPv6 addresses to fail for AWS, Azure, and GCP environments as the Controller inhibits the discovery of IPv6 addresses in address objects. This is addressed through a fallback mechanism where the Controller prevents the insertion of IPv6 addresses in Address Groups. Users are advised to not use IPv6 addresses in Address Groups in their AWS, Azure, and GCP environments until this is resolved.

February 13, 2026 Gateway 24.06-20

The following fixes are included in this release:

- Fixes an issue where SNAT stopped working after upgrading the gateway from 24.06-15 to 24.06-19. This fix ensures that the address translation works properly.
- Fixes an issue where the gateway ipset configuration stops responding after an Address Group update. This fix enables an update in the Address Group to reflect in the update of the ipset also.
- Fixes an issue where a Packet Capture (PCAP) does not show up on a GCP gateway storage when the rule name is long, due to a character limit set for policy names. The fix now removes this set character limit and supports long policy names. However, long policy names will now truncate to 128 bytes for the purpose of session summaries and events.

December 12, 2025 Gateway 24.06-19

The following fix is included in this release:

- Fixes an issue where a Policy Rule Set with a Rule that references an Address Object that contains an IPv6 address would result in the Gateway only loading a partial set of the policy. This issue is due to the IP Set tables currently not supporting IPv6 addresses. This issue has been fixed in the Gateway to ignore IPv6 addresses that are pushed to the Gateway as part of the policy. A subsequent change will occur on the Controller to inhibit the ability to specify IPv6 addresses in static Address Objects and inhibit the discovery of IPv6 addresses in dynamic Address Objects.

Version 25.12 Multicloud Defense Controller, December 12, 2025

The following enhancement is included in this release:

- **Firewall Threat Defense (FTDv) New Version Support** – Multicloud Defense supports new version 7.6.3 for FTDv. The older versions are deprecated.

November 18, 2025 Gateway 24.06-18

The following fixes are included in this release:

- Fixes an issue where a rule description string could cause a memory allocation overrun resulting in the gateway crashing upon instantiation. This issue is addressed by ensuring the description field is character limited.
- Fixes an issue where unencrypted Hypertext Transfer Protocol (HTTP) traffic processed by an HTTP proxy rule that uses a Fully Qualified Domain Name (FQDN) Match policy could improperly generate an HTTP 502 error code, closing the connection.
- Fixes an issue for a Ingress Gateway that is deployed in Azure using GWLB-based architecture where the applied Forwarding policy could not extract the SNI. The issue stems from the tunneling of traffic between Gateway instance and GWLB using Virtual Extensible Local-Area Network (VXLAN). This issue has been addressed and the SNI can be extracted properly.
- Fixes an issue with an Egress Gateway Forwarding policy where the datapath would drop the first application packet after the TCP handshake if that packet arrives from the server rather than from the client. The fix ensures that the first application can arrive from either the client or server and the datapath will process and forward the packet properly.
- Fixes an issue where an Ingress Gateway Reverse Proxy policy operating on Secure File Transfer Protocol (SFTP) traffic would establish the connection, but not fully process the traffic related to the session, causing the client or server to timeout. This fix ensures that the SFTP traffic is properly processed to completion.
- Fixes an issue with Edge-mode Gateway deployments in Azure that could cause a failure to establish the VPN connection. The issue is due to the possibility of an incorrectly assigned secondary interface IP, which could be assigned an IP from a different subnet than required. This fix ensures that the assigned IP is from the datapath subnet, resulting in the VPN being established and becoming active.
- Fixes an issue related to an Egress Forward Proxy policy where the gateway would respond with a 400 Bad Gateway response code when the application is using non-standard HTTP(S) ports. This fix ensures the Forward Proxy will operate properly for all ports that are specified in the policy configuration.
- Fixes an issue with the Data Loss Prevention (DLP) engine that could cause the gateway to not fully initialize upon instantiation.
- Fixes an issue where an Egress Gateway Forward Proxy policy that performs full decryption was not preserving the URL encoding when sending the URL from the front-end connection to the back-end connection.
- Fixes an issue where the Application Info -> Payload App name was being truncated in the Traffic Summary Log.

Version 25.10 Multicloud Defense Controller, November 5, 2025

The following features and enhancements are included in this release:

- **Red Hat Enterprise Linux 9 (RHEL 9) Migration** – Multicloud Defense is now on Red Hat Enterprise Linux 9 (RHEL 9). This is supported on AWS and Azure only. While this migration may likely increase infrastructure costs for some customers, RHEL 9 offers enhanced security against vulnerabilities, with availability of the latest vulnerability patches.
- **Firewall Threat Defense Virtual (FTDv) Support for Azure** – Multicloud Defense now supports Standard_D8s_v5 and Standard_D16s_v5 instance types for FTDv for Azure. The existing instance type will be deprecated. The new instance types offer better performance.

- **Azure Dsv6 Support** – Fixed technical issues related to permissions in the Microsoft Marketplace for Azure Dsv6 instance. Azure Dsv6 is now supported in Multicloud Defense. You can see improved performance, and a likely increase in infrastructure costs as the Azure gateway instance will use Red Hat Enterprise Linux 9 (RHEL 9).
- **Bring Your Own Load Balancer (BYOLB) Support** – Resolved a limitation in Azure that did not allow the configuration of user-defined load balancers due to conflicts in user-configured and managed load balancer policies. You can now customize and enable the floating IP for your load balancer rules and attach the load balancer to the Multicloud Defense Gateway. This is supported for the 25.08 Gateway release.

October 15, 2025 Gateway 25.02-03

Enhancements

The following enhancements are included in this release:

- Adds VPN support for Edge-mode gateway deployments by orchestrating the local VPC/VNet secondary CIDRs into the ASA (VPN) route table to accommodate proper routing across VPN to the destination application or workload. This is an enhancement to orchestrating the primary CIDRs, which was made available in the 24.06-15 release.
- Adds VPN support for Edge-mode gateway deployments by orchestrating the local VPC/VNet CIDR into the ASA (VPN) route table to accommodate proper routing across the VPN to the destination application or workload.
- Adds universal support across commercial and FedRAMP environments to use RHEL 9 as a base image for the gateway in AWS. This ensures the base OS is a commercial OS that has well-maintained and available vulnerability patches to address known CVEs. The licensing for this base OS is a PAYG licensing that is charged to the deployment billing account. It should be expected to see an increase in infrastructure costs within the CSP as a result of the use of the image. For Azure and GCP, the base OS remains as CentOS 9. For OCI, the base image remains as AlmaLinux 9.

Fixes

The following fixes are included in this release:

- Fixes an issue with Edge-mode gateway deployments in Azure that could cause a failure to establish the VPN connection. The issue is due to the possibility of an incorrectly assigned secondary interface IP, which could be assigned an IP from a different subnet than required. This fix ensures that the assigned IP is from the datapath subnet, resulting in the VPN being established and becoming active.
- Fixes an issue related to an Egress Forward Proxy policy where the gateway would respond with a 400 Bad Gateway response code when the application uses non-standard HTTP(S) ports. This fix ensures the Forward Proxy will operate properly for all ports that are specified in the policy configuration.
- Fixes an issue where a gateway could not send heartbeats for a few minutes due to a race condition caused by a VPN lock condition. If this scenario occurs, the Controller could mark the gateway for HB_MISS and initiate a replacement. The fix ensures the race condition will not occur and heartbeats will be sent consistently.
- Fixes an issue where traffic passing through an Egress gateway in AWS could be denied due to the VPC ID that sources the traffic, which is seen in the GENEVE header, has leading '0' characters in the ID.

The gateway was dropping the leading '0' characters, which would not match on a known VPC ID and thus the traffic would be incorrectly denied. This fix ensures that VPC IDs with leading '0' characters retain the leader characters to appropriately match the VPC ID and process the traffic properly.

- Fixes an issue related to traffic processed by a Forwarding policy where a fragmented TLS Hello message sent by the client would not be recognized as a valid TLS Hello message due to out-of-order fragment arrival. This fix ensures that the gateway will properly receive and process all fragments, independent of order, to successfully reassemble the TLS Hello and extract the SNI.
- Fixes an issue where the Log/Event that contains URI information is presenting the URL with ASCII encoding characters rather than replacing the encoding with ASCII characters for proper readability. This fix ensures the characters are ASCII characters. This issue does not affect processing of the traffic by the gateway.
- Fixes an issue where disabling multiple Forward Proxy Rules simultaneously will not properly clean up the proxy configuration, causing the datapath to enter into a restart loop.
- Fixes an issue where a gateway would fail to initialize when more than one Malicious IP Profile has been assigned to different rules in the Gateway Policy Rule Set.
- Fixes a memory leak in an Egress Gateway Forward Proxy policy, which could result in a datapath restart if memory consumption exceeds 80%.
- Fixes an issue that could result in an occasional application socket timeout when processing traffic through an Egress gateway.
- Fixes an issue related to HTTPS Forward Proxy traffic processing that could result in a degradation in connection rate.
- Fixes an issue where the Application Info -> Payload App name was being truncated in the Traffic Summary Log.
- Fixes an issue where the SNI Event `eventText` field was being used differently for traffic that is processed by a policy that uses FQDN match versus one that does not. When an SNI exists and the policy does not use FQDN Match, the field will contain the domain. When a policy uses FQDN Match, the field will contain the domain within addition text about that match. This fix does not change the content of the `eventText` field, but rather leverages a field called `fqdn` to display just the domain, making it possible to use this field to search and display traffic based on the domain.
- Fixes a stability issue in IP tables that could result in a datapath self-heal.
- Fixes a stability issue in the gateway datapath that could cause the datapath to crash and restart.
- Fixes an issue where an Ingress gateway could have a momentarily high CPU resulting in a scale out that is followed by a scale-in. This behavior could continue, resulting in a perpetual scale-out or scale-in behavior.
- Provides a rework of the gateway's capability to retrieve the Service Name Indication (SNI) from the TLS Hello for traffic processed by a Forwarding policy. The original issue, where the gateway could not retrieve the SNI, is caused by a change in TLS libraries to accommodate post-quantum cryptography. With this change, the TLS Hello is larger than 1415 bytes. This can result in an inability to retrieve the SNI, which is used by the policy to match or filter by domain. The original fix could not guarantee the retrieval of the SNI due to inter-packet timing differences. This fix reworks how the gateway processes the TLS Hello packets to ensure the SNI can be successfully retrieved.

Version 25.09 Multicloud Defense Controller, October 7, 2025

The following enhancement is included in this release:

- **Audit and System Logs** – Audit Logs and System Logs are combined into a new page on the Multicloud Defense application. You can find this combined page under **Investigate** > **System Status** > **Audit and System Logs**. The unified page offers advanced search capabilities, clear identification of audit and system logs, and easier correlation of events and logs, all in one place.

October 3, 2025 Gateway Hotfix 24.06-17-a1

The following fix is included in this release:

- Fixes an issue with Edge-mode gateway deployments in Azure that could cause a failure to establish the VPN connection. The issue is due to the possibility of an incorrectly assigned secondary interface IP, which could be assigned an IP from a different subnet than required. This fix ensures that the assigned IP is from the datapath subnet, resulting in the VPN being established and becoming active.

September 24, 2025 Gateway 24.06-17

Enhancement

The following enhancement is included in this release:

- Adds VPN support for Edge-mode gateway deployments by orchestrating the local VPC or VNet secondary CIDRs into the ASA (VPN) route table to accommodate proper routing across VPN to the destination application or workload. This is an enhancement to orchestrating the primary CIDRs, which was made available in the 24.06-15 release.

Fixes

The following fixes are included in this release:

- Fixes an issue where a gateway could not send heartbeats for a few minutes due to a race condition caused by a VPN lock condition. If this scenario occurs, the Controller could mark the gateway for HB_MISS and initiate a replacement. The fix ensures the race condition will not occur and heartbeats will be sent consistently.
- Fixes an issue where traffic passing through an egress gateway in AWS could be denied due to the VPC ID that sources the traffic, which is seen in the GENEVE header, has leading '0' characters in the ID. The gateway was dropping the leading '0' characters, which would not match a known VPC ID and thus the traffic would be incorrectly denied. This fix ensures that VPC IDs with leading '0' characters retain the leader characters to appropriately match the VPC ID and process the traffic properly.
- Fixes an issue related to traffic processed by a Forwarding policy where a fragmented TLS Hello message sent by the client would not be recognized as a valid TLS Hello message due to out-of-order fragment arrival. This fix ensures that the gateway will properly receive and process all fragments, independent of order, to successfully reassemble the TLS Hello and extract the SNI.

- Fixes a memory leak in an egress gateway Forward Proxy policy, which could result in a datapath restart if memory consumption exceeds 80 percent.
- Fixes an issue that could result in an occasional application socket timeout when processing traffic through an egress gateway.
- Fixes an issue in an egress gateway FQDN (domain) match policy where traffic that should be denied is incorrectly allowed if the Service Name Indication (SNI) in the TLS Hello message is not present. If the SNI is not present and a policy expects a domain, no policy rule match should occur and the traffic should be denied by the default deny policy. This fix ensures that the traffic is properly denied.
- Fixes a stability issue in IP tables that could result in a datapath self-heal.
- Provides a rework of the gateway's capability to retrieve the SNI from the TLS Hello for traffic processed by a Forwarding policy. The original issue, where the gateway could not retrieve the SNI, is caused by a change in the TLS libraries to accommodate post-quantum cryptography. With this change, the TLS Hello is larger than 1,415 bytes. This can result in an inability to retrieve the SNI, which is used by the policy to match or filter by domain. The original fix could not guarantee the retrieval of the SNI due to inter-packet timing differences. This fix reworks how the gateway processes the TLS Hello packets to ensure the SNI can be successfully retrieved.

August 22, 2025 Gateway Hotfix 24.06-16-a1

This is a hotfix. The following fixes are included in this hotfix:

- Fixes an issue related to traffic processed by a Forwarding policy where a fragmented TLS Hello message sent by the client would not be recognized as a valid TLS Hello message due to out-of-order fragment arrival. This fix ensures that the gateway will properly receive and process all fragments, independent of order, to successfully reassemble the TLS Hello and extract the Service Name Indication (SNI).
- Provides a rework of the gateway's capability to retrieve the SNI from the TLS Hello for traffic processed by a Forwarding policy. The original issue, where the gateway could not retrieve the SNI, is caused by a change in TLS libraries to accommodate post-quantum cryptography. With this change, the TLS Hello is larger than 1415 bytes. This can result in an inability to retrieve the SNI, which is used by the policy to match or filter by domain. The original fix could not guarantee the retrieval of the SNI due to inter-packet timing differences. This fix reworks how the gateway processes the TLS Hello packets to ensure the SNI can be successfully retrieved.

August 2025 Gateway Version 24.06-16 and Controller Version 25.08

Version 24.06-16 Multicloud Defense Gateway, August 22, 2025

The following fix is included in this release:

- Fixes an issue where the SNI Event `eventText` field was being used differently for traffic that was processed by a policy that uses FQDN match versus one that does not use an FQDN match. When an SNI exists and the policy does not use FQDN match, the field will contain the domain. When a policy uses FQDN match, the field will contain the domain within addition text about that match. This fix does

not change the content of the `eventText` field, but rather leverages a field called `fqdn` to display just the domain, making it possible to use this field to search and display traffic based on the domain.

Version 25.08 Multicloud Defense Controller, September 4, 2025

The following enhancements are included in this release:

- **Azure Cloud Services** – In Multicloud Defense, we have restructured the Azure Cloud Services to align with Microsoft Azure, ensuring a consistent and uniform user experience. You can now use the same nomenclature used in Azure, while configuring regions in Multicloud Defense.
- **Red Hat Enterprise Linux 9 (RHEL 9) Migration** – Multicloud Defense is now on Red Hat Enterprise Linux 9 (RHEL 9). While this migration may likely increase infrastructure costs for some customers, RHEL 9 offers enhanced security against vulnerabilities.
- **System Logs Forwarding to Amazon Web Services (AWS) S3** – You can now select AWS S3 as a destination for system logs forwarding, allowing you to forward these logs to your Security Information and Event Management (SIEM) tool of choice.
- **Azure Dsv6 Support** – Multicloud Defense supports the newer instance type of Azure Dsv6, providing better performance.
- **Talos Malicious IP Integration** – In Multicloud Defense, malicious IP source will now be powered by Cisco Talos to provide security protection.

Version 25.07 Multicloud Defense Controller, July 31, 2025

The following feature and enhancements are included in this release:

- **Virtual Network (VNet) flow log support** – Multicloud Defense will support NSG flow logs until it is deprecated by Microsoft Azure. Microsoft Azure is retiring Network Security Group (NSG) flow logs and replacing it with VNet flow logs. Multicloud Defense will continue to support NSG flow logs until it is deprecated, but users will not be able to create new NSG flow logs. Users can create VNet flow logs instead.
- Bug fixes and enhancements.

July 17, 2025 Gateway Hotfix 24.06-15-a1

This is a hotfix. The following fix is included in this hotfix:

- Provides a rework of the gateway's capability to retrieve the Service Name Indication (SNI) from the TLS Hello for traffic processed by a Forwarding policy. The original issue, where the gateway could not retrieve the SNI, is caused by a change in TLS libraries to accommodate post-quantum cryptography. With this change, the Client Hello is larger than 1415 bytes. This can result in an inability to retrieve the SNI, which is used by the policy to match or filter by domain. The original fix could not guarantee the retrieval of the SNI due to inter-packet timing differences. This fix reworks how the gateway processes the TLS Hello packets to ensure that the SNI can be successfully retrieved.

June 2025 Gateway Version 24.06-15 and Controller Version 25.06

Version 24.06-15 Multicloud Defense Gateway, July 17, 2025

Enhancements

The following enhancements are included in this release:

- Adds VPN support for Edge mode gateway deployments by orchestrating the local VPC/VNet CIDR into the ASA (VPN) route table to accommodate proper routing across VPN to the destination application/workload.
- Adds universal support across commercial and FedRAMP environments to use RHEL 9 as a base image for the gateway in AWS. This ensures the base OS is a commercial OS that has well-maintained and available vulnerability patches to address known CVEs. The licensing for this base OS is a PAYG licensing that is charged to the deployment billing account. It should be expected to see an increase in infrastructure costs within the CSP as a result of the use of the image. For Azure and GCP, the base OS remains as CentOS 9. For OCI, the base image remains as AlmaLinux 9.

Fixes

The following fixes are included in this release:

- Fixes an issue where disabling multiple Forward Proxy Rules simultaneously will not properly clean up the proxy configuration, causing the datapath to enter into a restart loop.
- Fixes a CPU issue for an Egress gateway where the CPU could be 100%, causing traffic processing issues. This could be seen in environments with hundreds or thousands of policy rules, where the initialization of the datapath would result in high CPU and remain in that state, regardless of traffic.
- Fixes an issue where a gateway deployed using the m7i.xlarge instance type could result in higher than expected CPU over time.
- Fixes an issue related to HTTPS Forward Proxy traffic processing that could result in a degradation in connection rate.
- Fixes an issue for traffic processed by a Forwarding policy with Network Intrusion (IDS/IPS) enabled. If a client uses a TCP RST to close the connection, there is a possibility that the RST will not be forwarded by the gateway. This behavior could lead to application slow downs and timeouts. This fix ensures that the RSTs are properly forwarded through the gateway to the destination.
- Fixes an issue where an Ingress gateway could have a momentaryily high CPU resulting in a scale out that is followed by a scale-in. This behavior could continue, resulting in a perpetual scale out/in behavior.
- Fixes an issue where an Ingress policy that uses source IP/CIDR whitelisting would permit traffic from IPs outside of those whitelisted.

Version 25.06 Multicloud Defense Controller, July 2, 2025

The following feature is included in this release:

- **Azure Virtual WAN Route Orchestration** – Multicloud Defense offers integration with Azure Virtual WAN (VWAN) by orchestrating seamless virtual network connectivity between your branch offices, remote users, and on-premises networks in Azure. Multicloud Defense helps connect your on-premises traffic to the cloud through the orchestration of virtual network connections and route propagation between service VNets and vHubs.
- Bug fixes and enhancements.

July 3, 2025 Gateway Hotfix 24.06-14-b1

This is a hotfix. The following fix is included in this hotfix:

- Fixes a CPU issue for an Egress Gateway where the CPU could be 100%, causing traffic processing issues. This could be seen in environments with hundreds or thousands of policy rules, where the initialization of the datapath would result in high CPU and remain in that state, regardless of traffic.

July 3, 2025 Gateway 25.02-02

Enhancements

The following enhancements are included in this release:

- Adds support for M7i (2-core, 4-core, 8-core) instance type when deploying a gateway in AWS. This enhancement accommodates gateway deployments into recently introduced regions that require the latest M-class family.
- Integrates the FIPs Teleport agent into the gateway to accommodate both FIPS (FedRAMP) and non-FIPS (commercial) environments. Teleport is disabled by default. It can only be enabled by the customer when working in conjunction with Cisco Support for advanced troubleshooting.

Fixes

The following fixes are included in this release:

- Fixes a CPU issue for an Egress Gateway where the CPU could be causing 100% traffic processing issues. This could be seen in environments with hundreds or thousands of policy rules, where the initialization of the datapath would result in high CPU and remain in that state, regardless of traffic.
- Fixes an issue where a gateway deployed using the m7i.xlarge instance type could result in higher than expected CPU over time.
- Fixes an issue in an Egress Gateway FQDN (domain) Match policy where traffic that should be denied is incorrectly allowed if the SNI in the TLS Hello message is not present. If the SNI is not present and a policy expects a domain, no policy rule match should occur and the traffic should be denied by the default deny policy. This fix ensures that the traffic is properly denied.
- Fixes an issue for traffic processed by a Forwarding policy with Network Intrusion (IDS/IPS) enabled. If a client uses a TCP RST to close the connection, there is a possibility that the RST will not be forwarded by the gateway. This behavior could lead to application slow-downs and timeouts. This fix ensures that the RSTs are properly forwarded through the gateway to the destination.

- Fixes a stability issue in the gateway datapath that could cause the datapath to crash and restart.
- Fixes an issue where active termination of a long-running flows during a policy change was not being applied properly, resulting in the connections being passively closed. This fix ensures that the long-running sessions are actively terminated through a TCP Reset.
- Fixes an issue with Anti-Malware detection that could cause high CPU, impacting the ability to process sessions. This issue could be seen if the protection is enabled for traffic processed by a Forwarding policy. This fix ensures that the Anti-Malware engine more efficiently processes traffic to properly detect malware without impacting performance.
- Fixes an issue where disabling or enabling a Policy Ruleset Forwarding Rule causes a blue/green datapath replacement. In this scenario, a datapath replacement is not needed and the policy change should apply quickly with no impact to existing sessions. This fix ensures that this type of policy change is accommodated with no requirement for a blue/green datapath replacement.
- Fixes an issue where an update to a certificate object would not apply the update to the gateway. The gateway would continue to use the old certificate until the gateway instance is replaced or the datapath is restarted. This fix ensures the updated certificate is applied to the gateway policy and used for processing traffic.
- Fixes an issue where a policy change that triggers a blue/green datapath replacement could cause longer than expected traffic processing delays that would result in the inability of the datapath to process sessions. This scenario can occur when a policy uses DNS-based FQDN Address Objects with caching enabled on the gateway and/or a diagnostic bundle is generated during the policy change. Each requires the datapath to service these requests in conjunction with processing sessions, causing delays in the latter. The fix ensures that the highest priority is given to the processing of the sessions to ensure no disruptions.
- Fixes an issue where a gateway policy change could become stuck in Updating state because the policy is incomplete due to lack of disk space. This scenario would only occur over a very long period of time when the gateway instance is active. This fix addresses the root cause of the disk space issue so that long-running gateway instances will successfully process policy changes.
- Fixes an issue related to dead connections causing higher than normal CPU and memory consumption. Dead connections are connections that are left open due to the client and server disappearing without actively closing or resetting the connection. The gateway previously held onto these connections for up to 12 minutes, consuming connection pool capacity, causing an increase in CPU and memory, resulting in an unnecessary scale out to accommodate the additional capacity requirements. The fix is to introduce a tunable configuration to reduce the amount of time that dead connections are retained. If this scenario occurs, please contact Cisco Support to evaluate the scenario and adjust the setting to reduce the impact dead connections will have on the gateway capacity.
- Fixes an issue where an upgrade from a Gateway version that does not support VPN to a gateway version that does support VPN could cause the new gateway instances on the new version to not become active due to an instability related to populating route prefixes into the VPN route table.
- Fixes an issue where a Forwarding no SNAT Policy could not retrieve the Service Name Indication (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 SNI, which is used by the policy to match or filter by domain. The fix ensures the forwarding policy can support Client Hello sizes greater than 1415 bytes
- Fixes an issue with an Ingress gateway where a policy with WAF protection enabled could result in a disruption in traffic during a WAF ruleset update. This only occurs when the WAF Profile name is

specified in a particular way. The fix addresses the issue by ensuring the name specified by the user, and permitted by the Controller/UI, is properly accepted by the gateway ensuring no disruption during ruleset updates.

- Fixes an issue where the CPU would be higher than expected for traffic that is processed by a policy with action set to deny.
- Fixes an issue where a gateway datapath could enter a stuck state when processing SMB traffic. When this occurs, the datapath will self-heal. The fix addresses the issue such that the datapath does not enter the state and successfully processes SMB traffic.
- Fixes an issue where an Ingress policy that uses source IP/CIDR whitelisting would permit traffic from IPs outside of those whitelisted.
- Fixes an issue with Data Loss Prevention (DLP) detection in multipart data. If the string being detected is at the file start or end, detection is successful. If anywhere else, then detection would fail. File size could also affect proper detection. This fix ensures that the string is detected in multipart data no matter where the string is located.
- Fixes an issue for traffic processed by an Egress Gateway where DLP protection that has detected a malicious activity would mark the traffic as malicious, but the Events view for the session was missing the DLP event. This fix ensures the DLP event is represented in the session events.
- Fixes an issue with an Ingress Gateway Reverse Proxy Policy where a build-up of CPU could occur for a particular type of session behavior. If a successful end-to-end session is established and the client and server communicate and then each disappear without closing their respective sessions, the proxy will eventually close the sessions, but will not fully clean up the session allocation. This results in a build-up of CPU over time. If the session behavior occurs at a greater volume, the CPU could build-up more rapidly. This fix addresses the session cleanup to ensure the CPU does not build up over time and remains stable.
- Fixes an issue where a UDP session involving UDP fragmentation is not closed and cleaned up if a fragment is never received. [
- Fixes an issue where the Traffic Summary Log would not present the proper number of UDP fragments for a session where fragmentation is seen.
- Fixes an issue with establishing a full end-to-end session for legacy applications when using a TCP Forward Proxy Policy. Examples of legacy applications could include SSHv1 and database management traffic (Oracle). For these types of applications, after the TCP connection is established, the next packet will arrive from the server, not the client. In a TCP Forward Proxy Policy, the Gateway first establishes the frontend TCP connection (client to Gateway) and expects the next packet to arrive from the client, not the server. Since no packet ever arrives, the backend TCP connection (Gateway to server) is never established. This results in no end-to-end session and the application communication will fail.

  This fix addresses the issue in the following two ways: (1) enabling a gateway setting and (2) evaluating the Policy Rule that is processing the traffic to determine if a domain evaluation (FQDN Match, FQDN Filtering) is configured. If both (1) and (2) are configured, the gateway will assume the traffic will be TLS encrypted and the next packet to arrive will be the TLS Hello from the client. If just (1) is configured, the gateway will assume the traffic is not TLS encrypted, therefore it will not expect the next packet to arrive from the client, and will immediately establish the backend connection. The next packet to arrive, whether from the client or server, will have a full end-to-end session to process and send the packet to its intended destination

  In the scenario where (1) is not configured, when the traffic is TLS encrypted and a domain is obtained from the TLS Hello SNI, the Gateway will do a domain resolution and use one of the resolved IPs as the

destination for the backend connection. In the scenario where (1) is configured, or a scenario where traffic is not TLS encrypted, the frontend TCP connection destination IP will be used as the backend TCP connection destination IP since no domain can be obtained and no domain resolution is possible.

In order to employ this fix, a gateway setting is required. If you feel you're running into this issue, please contact Cisco Support to evaluate and obtain information on how this setting can be enabled. In a future release, this behavior will be configurable on a per-rule basis, such that a Rule can be created to segment this type of traffic, where the change described above can apply only to specific traffic.

- Fixes an issue where an Azure Ingress Gateway could crash when the newly instantiated gateway instance is becoming active.
- Fixes an issue where traffic processing on an Ingress Gateway could cause high CPU resulting in an unnecessary auto-scale. The high CPU is a result of moving from a policy that initially processes a connection using an unencrypted HTTP proxy and then moving to an encrypted TCP proxy due to an HTTP redirection.
- Fixes an issue where an Ingress policy that uses source IP/CIDR whitelisting would permit traffic from IPs outside of those whitelisted.

February 28, 2025 Gateway 25.02-01

Enhancements

The following enhancements are included in this release:

- Adds support for UDP fragmentation. This enhancement requires a gateway setting to be enabled, which can be specified in the Terraform Gateway resource.
- Improved session state summary information. Improvements include: Marking sessions that have been closed due to gateway and proxy timeout sessions; Resetting all connections that have been closed by the gateway for any reason (timeouts, datapath restarts); Sending connection reset to both client and server for sessions that have been closed by the gateway; Session summary log generated periodically for long-running sessions.
- Provides an enhanced gateway image that supports the BoringCrypto required for use in Gateways deployed in a FedRAMP. This is 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.
- Added support for logging the duration of a session in the Traffic Summary Log. The duration is from TCP SYN or first UDP packet to the time the session is closed or terminated.
- Enhances the Network Intrusion (IDS/IPS) engine to detect and block HTTP evasion techniques, including HTTP 0.9, deflate compression, gzip compression, double compression (deflate + gzip), chunked transfer and HTTP/1.1 100 ok response code.
- Provides an enhancement to honor the No Log Action of a Policy Rule Set Rule by not sending the log to any destination configured in a gateway-enabled Log Forwarding Profile.
- Continued enhancements to gateway hardening to accommodate STIG and CIS level 2 requirements necessary for deploying into FedRAMP environments.

- Changed the base image from CentOS to RHEL9 to accommodate FedRAMP requirements. This change will eventually be rolled into the non-FedRAMP gateway base image in a future release.
- Adds support for periodically recording Traffic Summary Logs for long-running sessions. Historically, a Traffic Summary Log was recorded only when a session ends. This works well for shorter duration sessions, but not for long-running sessions. The enhancement generates a Traffic Summary Log every 5 minutes with the same session ID and tuple information, but with updated statistics (bytes/packets). A final log will also be generated when the session ends.
- Provides a gateway setting for configuring the drain timeout. The default setting is 2 minutes. When applying this gateway setting, the user can configure the drain timer. If there is a requirement to change the default, please contact Cisco Support.

Fixes

The following fixes are included in this release:

- Fixes an occasional datapath instability when processing client traffic where post-quantum cryptography is enabled. The instability would result in a datapath self-heal. The fix ensures datapath stability, resulting in no need to self-heal.
- Fixes a downstream issue related to obtaining the SNI when a browser-based client has post-quantum cryptography enabled. The post-quantum cryptography scenario causes the TLS hello to be fragmented into multiple packets. If the first packet arrives, but the second packet does not, the Gateway would never release the session-allocated CPU upon session cleanup. This fix ensures that the CPU is released and does not build up over time.
- Fixes an issue with establishing a full end-to-end session for legacy applications when using a TCP Forward Proxy Policy. Examples of legacy applications could include SSHv1 and database management traffic (Oracle). For these types of applications, after the TCP connection is established, the next packet will arrive from the server, not the client. In a TCP Forward Proxy Policy, the Gateway first establishes the frontend TCP connection (client to Gateway) and expects the next packet to arrive from the client, not the server. Since no packet ever arrives, the backend TCP connection (Gateway to server) is never established. This results in no end-to-end session and the application communication will fail.

  This fix addresses the issue in the following two ways: (1) enabling a gateway setting and (2) evaluating the Policy Rule that is processing the traffic to determine if a domain evaluation (FQDN Match, FQDN Filtering) is configured. If both (1) and (2) are configured, the gateway will assume the traffic will be TLS encrypted and the next packet to arrive will be the TLS Hello from the client. If just (1) is configured, the gateway will assume the traffic is not TLS encrypted, therefore it will not expect the next packet to arrive from the client, and will immediately establish the backend connection. The next packet to arrive, whether from the client or server, will have a full end-to-end session to process and send the packet to its intended destination.

  In the scenario where (1) is not configured, when the traffic is TLS encrypted and a domain is obtained from the TLS Hello SNI, the gateway will do a domain resolution and use one of the resolved IPs as the destination for the backend connection. In the scenario where (1) is configured, or a scenario where traffic is not TLS encrypted, the frontend TCP connection destination IP will be used as the backend TCP connection destination IP since no domain can be obtained and no domain resolution is possible.

  In order to employ this fix, a gateway setting is required. If you feel you're running into this issue, please contact Cisco Support to evaluate and obtain information on how this setting can be enabled. In a future release, this behavior will be configurable on a per-rule basis, such that a rule can be created to segment this type of traffic, where the change described above can apply only to specific traffic.

- Fixes an issue with a Group Address Object exclusion list where the IPs/CIDRs specified in the excluded Address Objects were not properly applied to the gateway policy. This ensures that both the included and excluded Address Objects are applied for proper traffic matching.
- Fixes an issue where a gateway in GCP could bounce between healthy and unhealthy due to Health Check Service failing, potentially resulting in instance replacement.
- Fixes an issue where some long-lived active connections would not be properly reset (TCP RST) during gateway replacement, policy change or timeout expiry.
- Fixes an issue related to new Talos Rulesets where a Ruleset change could cause issues with applying the new Rulesets to the gateway. The gateway will become stuck in Policy Ruleset Status "Updating..." state. This issue was caught prior to new Talos Rulesets being published. The issue is resolved with this update such that new Talos Rulesets can be successfully applied.
- Fixes an issue where traffic processing on an Ingress Gateway could cause high CPU resulting in an unnecessary auto-scale. The high CPU is a result of moving from a policy that initially processes a connection using an unencrypted HTTP proxy and then moving to an encrypted TCP proxy due to an HTTP redirection.
- Fixes an issue related to a UDP connection pool leak caused by specific UDP session behavior that could eventually result in a datapath restart. When the datapath restart occurs, the instance will be unhealthy for the duration of the restart. If that unhealthy period is long enough, the Controller will mark the instance for replacement.
- Fixes an issue where an Egress Gateway Forward Proxy policy could get stuck in attempting to match traffic to the proper Policy Rule.
- 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.
- Fixes a gateway crash that is caused by detection of malware in an Ingress Gateway reverse proxy policy.
- 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 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 a Forwarding SNAT Policy could not retrieve the Service Name Indication (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 SNI, which is used by the policy to match or filter by domain. The fix ensures the Forwarding SNAT Policy can support Client Hello sizes greater than 1415 bytes.
- Fixes an issue where a proxy policy 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 policy can support Client Hello sizes greater than 1415 bytes.
- 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 issues in the Anti-Malware engine where known malware was not being detected and blocked. The fix includes updating the anti-malware engine.
- Fixes an issue where properly detecting malware signatures could occur intermittently.
- 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.
- Fixes an issue where a Decryption Profile that is configured differently than the default configuration would not properly apply to the gateway, resulting in TLS negotiation failures due to cipher suite mismatches between the client and the gateway.
- Fixes the recording of Stats related to Active Connections and Connection Rate where UDP sessions were not being properly counted.
- Fixes and issue where the Gateway will self-heal if an empty FQDN/URL Filtering Profile is assigned to the Policy Rule Set rule.
- 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 can get stuck in Health Checking Pending state after a policy update is applied. This issue also includes new gateway deployments.
- 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 64,000 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 Policy Rule Set that uses a 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 were not recording the SNI as a Traffic Summary -> Event.
- 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 TCP reset was not being sent for traffic processed by a Forward policy with a Deny action that uses an FQDN Match Profile when Reset on Deny is enabled.
- 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 20,000 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.
- Updating gateway libraries to address various CVEs.
- Fixes various issues related to update of private key for certificates when the certificate is configured to access the private key from a CSP service like Key Vault, Secrets Manager and KMS. This fix ensures that any update to the resource in the CSP service is detected by the gateway for the gateway to retrieve the update and during traffic processing.
- Ensures that a 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.
- Fixes an issue where changing the PCAP for a Web Protection (WAF) or Network Intrusion (IDS/IPS) Profile would unnecessarily trigger a blue/green datapath replacement.
- Fixes an issue where enabling or disabling PCAP in a Network Intrusion (IDS/IPS) Profile would unnecessarily trigger a blue/green datapath restart.
- Fixes an issue where enabling or disabling SNAT in a Forwarding Service Object would unnecessarily trigger a blue/green datapath restart.
- Fixes an issue where changing the name of an Advanced Security Profile (WAF, IDS/IPS, Anti-Malware, etc.) would unnecessarily trigger a blue/green datapath replacement.

June 5, 2025 Gateway Hotfix 24.06-14-a1

This is a hotfix. The following fixes are included in this hotfix:

- Fixes an issue where a **Forwarding no SNAT Policy** could not retrieve the Service Name Indication (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 SNI, which is used by the policy to match or filter by domain. The fix ensures the Forwarding no SNAT Policy can support Client Hello sizes greater than 1415 bytes.
- Fixes an issue where a **Forwarding SNAT Policy** could not retrieve the Service Name Indication (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 SNI, which is used by the policy to match or filter by domain. The fix ensures the Forwarding SNAT Policy can support Client Hello sizes greater than 1415 bytes.
- Fixes an occasional datapath instability when processing client traffic where post-quantum cryptography is enabled. The instability would result in a datapath self-heal. The fix ensures datapath stability, resulting in no need to self-heal.

May 2025 Gateway Version 24.06-14 and Controller Version 25.05

Version 24.06-14 Multicloud Defense Gateway, June 5, 2025

The following fixes are included in this release:

- Fixes an issue where active termination of long running flows during a policy change was not being applied properly, resulting in the connections being passively closed. This fix ensures that the long running sessions are actively terminated via a TCP Reset.
- Fixes a stability issue in the Gateway datapath that could cause the datapath to crash and restart.
- Fixes an issue where disabling or enabling a Policy Ruleset Forwarding Rule causes a blue/green datapath replacement. In this scenario, a datapath replacement is not needed and the policy change should apply quickly with no impact to existing sessions. This fix ensures that this type of policy change is accommodated with no requirement for a blue/green datapath replacement.
- Fixes an issue where a policy change that triggers a blue/green datapath replacement could cause longer than expected traffic processing delays that would result in the inability of the datapath to process sessions. This scenario can occur when a policy uses DNS-based FQDN Address Objects with caching enabled on the Gateway and/or a diagnostic bundle being generated during the policy change. Each requires the datapath to service these requests in conjunction with processing sessions, causing delays in the latter. The fix ensures that the highest priority is given to the processing of the sessions to ensure no disruptions.

Version 25.05 Multicloud Defense Controller, June 5, 2025

The following features and enhancements are included in this release:

- **Secure Firewall Threat Defense Virtual Device Orchestration** – You can now orchestrate, deploy, and register a Secure Firewall Threat Defense Virtual Device (FTDv) using Multicloud Defense. This helps you retain the same firewall that you use for on premises and cloud environments, while managing policies in the same place. Multicloud Defense manages the deployment and makes it easy for you to deploy in the cloud.
- **Cloud Explorer** offers a single, unified view to visualize all your resources and their relationships. Cloud Explorer empowers you to build a robust security posture with ease. Using intuitive drag and drop functionality and simple clicks, you can form connections and use protective measures to safeguard your assets.
- Bug fixes and enhancements.

May 23, 2025 Gateway Hotfix 24.06-13-a1

This is a hotfix. The following fixes are included in this hotfix:

- Fixes an issue where a **Forwarding no SNAT Policy** could not retrieve the Service Name Indication (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 SNI, which is used by the policy to match or filter by domain. The fix ensures the Forwarding no SNAT Policy can support Client Hello sizes greater than 1415 bytes.

- Fixes an issue where a **Forwarding SNAT Policy** could not retrieve the Service Name Indication (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 SNI, which is used by the policy to match or filter by domain. The fix ensures the Forwarding SNAT Policy can support Client Hello sizes greater than 1415 bytes.
- Fixes an occasional datapath instability when processing browser-based client traffic where post-quantum cryptography is enabled. The instability would result in a datapath self-heal. The fix ensures datapath stability, resulting in no need to self-heal.

May 23, 2025 Gateway 24.06-13

The following fixes are included in this release:

- Fixes an issue where a Gateway policy change could become stuck in Updating state because the policy is incomplete due to lack of disk space. This scenario would only occur over a very long period of time when the Gateway instance is active. This fix addresses the root cause of the disk space issue so that long-running Gateway instances will successfully process policy changes.
- Fixes an issue with an Ingress Gateway where a policy with WAF protection enabled could result in a disruption in traffic during a WAF ruleset update. This only occurs when the WAF Profile name is specified in a particular way. The fix addresses the issue by ensuring the name specified by the user and permitted by the Controller/UI is properly accepted by the Gateway, ensuring no disruption during ruleset updates.
- Fixes an issue for traffic processed by an Egress Gateway where DLP protection that has detected a malicious activity marks the traffic as malicious, but the Events view for the session is missing the DLP event. This fix ensures the DLP event is represented in the session events.

May 9, 2025 Gateway Hotfix 24.06-12-a1

This is a hotfix. The following fixes are included in this hotfix:

- Fixes an issue where a **Forwarding no SNAT Policy** could not retrieve the Service Name Indication (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 SNI, which is used by the policy to match or filter by domain. The fix ensures the Forwarding no SNAT Policy can support Client Hello sizes greater than 1415 bytes.
- Fixes an issue where a **Forwarding SNAT Policy** could not retrieve the Service Name Indication (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 SNI, which is used by the policy to match or filter by domain. The fix ensures the Forwarding SNAT Policy can support Client Hello sizes greater than 1415 bytes.

- Fixes an occasional datapath instability when processing browser-based client traffic where post-quantum cryptography is enabled. The instability would result in a datapath self-heal. The fix ensures datapath stability, resulting in no need to self-heal.

May 9, 2025 Gateway 24.06-12

The following fixes are included in this release:

- Fixes an issue related to dead connections causing higher than normal CPU and memory consumption. Dead connections are connections that are left open due to the client and server disappearing without actively closing or resetting the connection. The gateway previously held onto these connections for up to 12 minutes, consuming connection pool capacity, causing an increase in CPU and memory, resulting in an unnecessary scale out to accommodate the additional capacity requirements. The fix is to introduce a tunable configuration to reduce the amount of time that dead connections are retained. If this scenario occurs, please contact Cisco Support to evaluate the scenario and adjust the setting to reduce the impact dead connections will have on the gateway capacity.
- Fixes an issue where an upgrade from a gateway version that does not support VPN to a gateway version that does support VPN could cause the new gateway instances on the new version to not become active due to an instability related to populating route prefixes into the VPN route table

May 7, 2025 Gateway Hotfix 24.06-11-a1

This is a hotfix. The following fixes are included in this hotfix:

- Fixes an issue where a **Forwarding no SNAT Policy** could not retrieve the Service Name Indication (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 SNI, which is used by the policy to match or filter by domain. The fix ensures the Forwarding no SNAT Policy can support Client Hello sizes greater than 1415 bytes.
- Fixes an issue where a **Forwarding SNAT Policy** could not retrieve the Service Name Indication (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 SNI, which is used by the policy to match or filter by domain. The fix ensures the Forwarding SNAT Policy can support Client Hello sizes greater than 1415 bytes.
- Fixes an occasional datapath instability when processing browser-based client traffic where post-quantum cryptography is enabled. The instability would result in a datapath self-heal. The fix ensures datapath stability, resulting in no need to self-heal.

April 2025 Gateway Version 24.06-11 and Controller Version 25.04

Version 24.06-11 Multicloud Defense Gateway, May 7, 2025

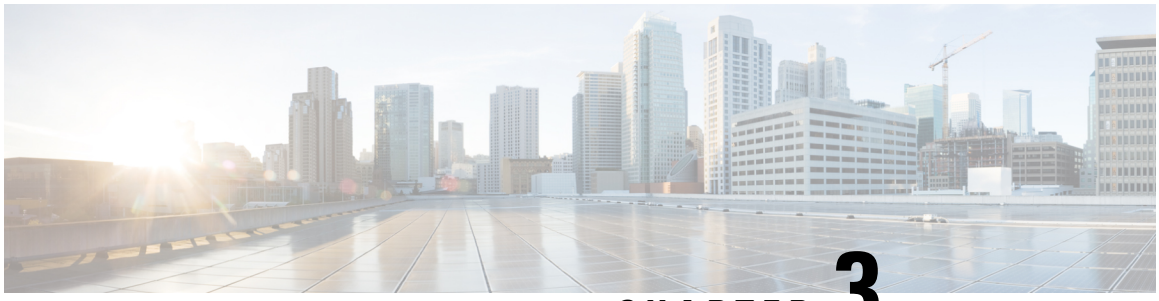
The following fixes are included in this release:

- Fixes an issue where a **Forwarding no SNAT Policy** could not retrieve the Service Name Indication (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 SNI, which is used by the policy to match or filter by domain. The fix ensures the Forwarding no SNAT Policy can support Client Hello sizes greater than 1415 bytes.
- Fixes an issue where a **Forwarding SNAT Policy** could not retrieve the Service Name Indication (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 SNI, which is used by the policy to match or filter by domain. The fix ensures the Forwarding SNAT Policy can support Client Hello sizes greater than 1415 bytes.
- Fixes an occasional datapath instability when processing browser-based client traffic where post-quantum cryptography is enabled. The instability would result in a datapath self-heal. The fix ensures datapath stability, resulting in no need to self heal.

Version 25.04 Multicloud Defense Controller, April 30, 2025

The following features and enhancements are included in this release:

- **M7i Support** - Multicloud Defense offers support for the M7i instance type for AWS accounts.
- **Metric Forwarding Logs Now Support AmazonS3 and Splunk** - You can now configure metric forwarding logs for S3/Splunk in the Multicloud Defense Controller. S3/Splunk refers to the integration between Amazon S3, a cloud object storage service, and Splunk, a data analytics platform.
- **Security Cloud Control Support** - Ongoing integration support for Security Cloud Control includes general dashboard and compatibility updates.
- **Improved Report Summaries** - Both the "Discovery" and "Threat Indicator Snapshot" reports now include an AI-generated summary that provides a synopsis of what is happening in your cloud network environment. Note that the Discovery report is only generated if you have discovery enabled; likewise, the Threat Indicator Snapshot report is only applicable if you have an actively deployed gateway.
- **New "Test" Button to Validate Log Forwarding Destination** - You can now validate the destination of a log forwarding profile before you finalize the configuration. Simply enter a test message in the text field when prompted and click **Validate** to send the message. once you confirm the message has successfully sent, you can complete the log forwarding profile.



CHAPTER 3

Multicloud Defense Controller Features and Enhancements (Archives)

- Version 25.03 March 28, 2025, on page 33
- Version 25.02 February 28, 2025, on page 33
- Version 25.01 January 6, 2025, on page 34
- Version 24.12 December 2, 2024, on page 34

Version 25.03 March 28, 2025

Features

The following features are included in this release:

Security Cloud Control Support

Multicloud Defense is now integrated with Security Cloud Control; Security Cloud Control (formerly Cisco Defense Orchestrator) is a cloud-based multi-device manager that facilitates management of security policies in highly distributed environments to achieve consistent policy implementation. You must log into Security Cloud Control and select the Multicloud Defense tab in the navigation pane to launch your Multicloud Defense environment. For more information about Security Cloud Control and what this support means for you, see "About Security Cloud Control".

Gateway Version Notification

The **Infrastructure** > **Gateways** page of the Multicloud Defense Controller now displays whether your deployed gateways are up to date with the recommended gateway version or if they are running a different version. We strongly recommend maintaining your gateways with the recommended version to take advantage of the most recent, stabilized features, enhancements, and fixes.

Version 25.02 February 28, 2025

Features

The following features are included in this release:

AI Defense

Secure your AI assets including the associated activity, types of connections, and number of identities accessing unsanctioned models by enabling AI Defense and integrating the service with your Multicloud Defense tenant.

Resource Tagging

Utilize dynamic objects in your policy rulesets and avoid relying on IP Addresses by tagging your objects as a resource. Either create new objects or select one or more existing objects in your Inventory and click "**Add Tags**"; you can use any key value to tag these resources. Once these tagged objects are attached to a ruleset, Mutlicoud Defense automatically discovers and applies them to incoming traffic.

UDP Fragmentation for Azure Environments

UDP fragmentation refers to the process of breaking down a large UDP (User Datagram Protocol) packet into smaller pieces, called fragments, so that it can be transmitted over a network that has a smaller maximum transmission unit (MTU) than the size of the packet. While fragmentation is not recommended in most scenarios, Mutlicloud Defense Gateways now support UDP fragmentation for Azure environments. Contact Cisco Support to enable this feature on your tenant.

Enhancements

The following enhancements are included in this release:

- Improves the look and feel of the UI.
- Improves general performance.

Version 25.01 January 6, 2025

Enhancements

The following enhancements are included in this release:

- Improves the look and feel of the UI.
- Improves general performance.

Version 24.12 December 2, 2024

Features

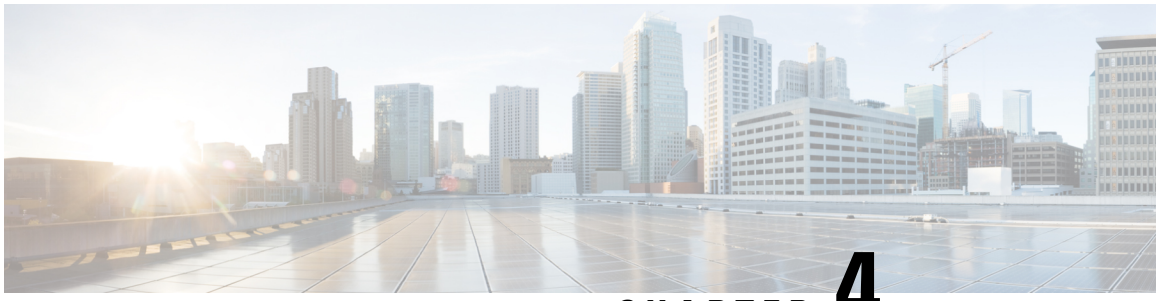
The following features are included in this release:

Improved Traffic Summary for Active and Periodic sessions

Previously, an event was only available if a connection session closed or was terminated. Now the traffic summary now posts an event for every five minutes a session is active; this ca help you examine how many ongoing sessions there are at a single time. Merely select the "All Events" checkbox in the summary page to expand the list of open connections, and uncheck it to display only closed sessions.

AI Defense (Private Preview)

Multicloud Defense now supports the private preview of AI Defense to discover and protect your Generative AI application. For more information, contact Cisco.



CHAPTER 4

Multicloud Defense Gateway Fixes and Enhancements (Archives)

- Version 24.06, on page 35
- Version 24.04, on page 43
- Version 24.02, on page 44
- Version 23.08, on page 46

Version 24.06

Version 24.06-10-a1 March 31, 2025

This is a hotfix.

Fixes

The following fixes are inculded in this hotfix:

- Fixes an occasional datapath instability when processing browser-based client traffic where post-quantum cryptography is enabled. The instability would result in a datapath self-heal. The fix ensures datapath stability, resulting in no need to self heal.
- Fixes an issue where a forwarding policy could not retrieve the Service Name Indication (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 SNI, which is used by the policy to match or filter by domain. The fix ensures the forwarding policy can support Client Hello sizes greater than 1415 bytes.

Version 24.06-10 March 31, 2025

Fixes

The following fixes are included in this release:

- Fixes an issue where the CPU would be higher than expected for traffic that is processed by a policy with action set to deny.
- Fixes an issue where a Multicloud Defense Gateway datapath could enter a stuck state when processing SMB traffic. When this occurs, the datapath will self heal. The fix addresses the issue such that the datapath does not enter the state and successfully processes SMB traffic.
- Fixes an issue with an Ingress Gateway Reverse Proxy Policy where a build-up of CPU could occur for a particular type of session behavior. If a successful end-to-end session is established and the client and server communicate and then each disappear without closing their respective sessions, the proxy will eventually close the sessions, but will not fully clean up the session allocation. This results in a build-up of CPU over time. If the session behavior occurs at a greater volume, the CPU could build-up more rapidly. This fix addresses the session cleanup to ensure the CPU does not build up over time and remains stable.
- Fixes an issue with establishing a full end-to-end session for legacy applications when using a TCP Forward Proxy Policy. Examples of legacy applications could include SSHv1 and database management traffic (Oracle). For these types of applications, after the TCP connection is established, the next packet will arrive from the server, not the client. In a TCP Forward Proxy Policy, the Multicloud Defense Gateway first establishes the frontend TCP connection (client-to-gateway) and expects the next packet to arrive from the client, not the server. Since no packet ever arrives, the backend TCP connection (gateway-to-server) is never established. This results in no end-to-end session and the application communication will fail.

  This fix addresses the issue in the following two ways: (1) enabling a gateway setting and (2) evaluating the policy rule that is processing the traffic to determine if a domain evaluation (FQDN Match, FQDN Filtering) is configured. If both (1) and (2) are configured, the Multicloud Defense Gateway will assume the traffic will be TLS encrypted and the next packet to arrive will be the TLS Hello from the client. If just (1) is configured, the gateway will assume the traffic is not TLS encrypted, therefore it will not expect the next packet to arrive from the client, and will immediately establish the backend connection. The next packet to arrive, whether from the client or server, will have a full end-to-end session to process and send the packet to its intended destination.

  In the scenario where (1) is not configured, when the traffic is TLS encrypted and a domain is obtained from the TLS Hello SNI, the gateway does a domain resolution and use one of the resolved IPs as the destination for the backend connection. In the scenario where (1) is configured, or a scenario where traffic is not TLS encrypted, the frontend TCP connection destination IP will be used as the backend TCP connection destination IP since no domain can be obtained and no domain resolution is possible.

  In order to employ this fix, a gateway setting is required. If you feel you're running into this issue, please contact Cisco Support to evaluate and obtain information on how this setting can be enabled. In a future release, this behavior will be configurable on a per-rule basis, such that a rule can be created to segment this type of traffic, where the change described above can apply only to specific traffic.

Version 24.06-09-a1 February 14, 2025

This is a hotfix.

Fixes

The following fixes are included in this hotfix:

- Fixes an occasional datapath instability when processing browser-based client traffic where post-quantum cryptography is enabled. The instability would result in a datapath self-heal. The fix ensures datapath stability, resulting in no need to self heal.
- Fixes an issue where a forwarding policy could not retrieve the Service Name Indication (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 SNI, which is used by the policy to match or filter by domain. The fix ensures the forwarding policy can support Client Hello sizes greater than 1415 bytes.

Version 24.06-09 February 14, 2025

Fixes

The following fix is included in this release:

- Fixes a downstream issue related obtaining the SNI when a browser-based client has post-quantum cryptography enabled. The post-quantum cryptography scenario causes the TLS hello to be fragmented into multiple packets. If the first packet arrives, but the second packet does not, the gateway would never release the session-allocated CPU upon session cleanup. This fix ensures that the CPU is released and does not build up over time.

Version 24.06-08-a1 January 16, 2025

This is a hotfix.

Fixes

The following fix is included in this hotfix:

- Fixes an issue where a forwarding policy could not retrieve the Service Name Indication (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 SNI, which is used by the policy to match or filter by domain. The fix ensures the forwarding policy can support Client Hello sizes greater than 1415 bytes.

Version 24.06-08 January 16, 2024

Enhancements

The following enhancements are included in this release:

- Includes additional Cipher Suites that can be configured as part of a decryption profile and used in a forward proxy or reverse proxy policy for TLS negotiation.
- Provides an advanced troubleshooting setting that can turn on and off Nginx tracing. In prior releases, Nginx tracing could only be enabled through an advanced debugging setting, which captured much more than the Nginx traces. With this setting, only the Nginx tracing is collected when enabled. The setting

can only be enabled by Cisco Support or Cisco engineering and is intended to be enabled when required for proxy troubleshooting. Once the traces are collected, they will be sent to the Multicloud Defense Controller in a Diagnostic Bundle.

Fixes

The following fix is included in this release:

- Fixes an issue with a group address object exclusion list where the IPs/CIDRs specified in the excluded address objects were not properly applied to the Multicloud Defense Gateway policy. This ensures that both the included and excluded address objects are applied for proper traffic matching.

Version 24.06-07-a1 December 18, 2024

This release is a hotfix.

Fixes

The following fix is included in this hotfix:

- Fixes an issue where a forwarding policy could not retrieve the Service Name Indication (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 SNI, which is used by the policy to match or filter by domain. The fix ensures the forwarding policy can support Client Hello sizes greater than 1415 bytes

Version 24.06-07 December 18, 2024

Fixes

The following fixes are included in this release:

- Fixes an issue related to new Talos rulesets where a ruleset change could cause issues with applying the new rulesets to the gateway. The gateway will become stuck in policy ruleset Status "`Updating...`" state. This issue was caught prior to new Talos rulesets being published. The issue has is resolved with this update such that new Talos rulesets can be successfully applied.
- Fixes an issue where the datapath could become momentarily stuck, causing issues processing traffic, including heathchecks. When this occurs, the gateway will bounce between healthy and unhealthy, which is evident in a series of system log messages. The stuckness usually does not last long enough for the controller to mark the instance for replacement.
- Fixes an issue related to a UDP connection pool leak caused by specific UDP session behavior that could eventually result in a datapath restart. When the datapath restart occurs, the instance will be unhealthy for the duration of the restart. If that unhealthy period is long enough, the controller will mark the instance for replacement.

Version 24.06-06-a1 November 28, 2024

This release is a hotfix.

Fixes

The following fix is included in this hotfix:

- Fixes an issue where a forwarding policy could not retrieve the Service Name Indication (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 SNI, which is used by the policy to match or filter by domain. The fix ensures the forwarding policy can support Client Hello sizes greater than 1415 bytes.

Version 24.06-06 November 26, 2024

Fixes

The following fix is included in this release:

- Fixes an issue where an Azure ingress gateway could crash when a new gateway instance is becoming active.

Version 24.06-05 November 22, 2024

Enhancements

The following enhancement is included in this release:

- Integrates the FIPs Teleport agent into the Gateway to accommodate both FIPS (FedRAMP) and non-FIPS (commercial) environments. Teleport is disabled by default. It can only be enabled by the customer when working in conjunction with Cisco Support for advanced troubleshooting.

Fixes

The following fixes are included in this release:

- Fixes an issue where traffic processing on an Ingress Gateway could cause high CPU resulting in an unnecessary auto-scale. The high CPU is a result of moving from a policy that initially processes a connection using an unencrypted HTTP proxy and then moving to an encrypted TCP proxy due to an HTTP redirection.
- Fixes an issue where an Egress Gateway Forward Proxy policy could get stuck in attempting to match traffic to the proper Policy Rule.
- Fixes an issue where some long-lived active connections would not be properly actively reset (send a TCP RST).
- Fixes a Gateway crash that is caused by detection of malware in an Ingress Gateway reverse proxy policy.

- Fixes the recording of Stats related to Active Connections and Connection Rate where UDP sessions were not being properly counted.

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 a proxy policy 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 policy can support Client Hello sizes greater than 1415 bytes.
- 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 a decryption profile that is configured differently than the default configuration would not properly apply to the gateway, resulting in TLS negotiation failures due to cipher suite mismatches between the client and the gateway.
- 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 suite.
- Fixes various stability issues.

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 are allowed, and all other domains that are not matched are 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 and scale-in 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.
- 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 not 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 23.08

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

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:

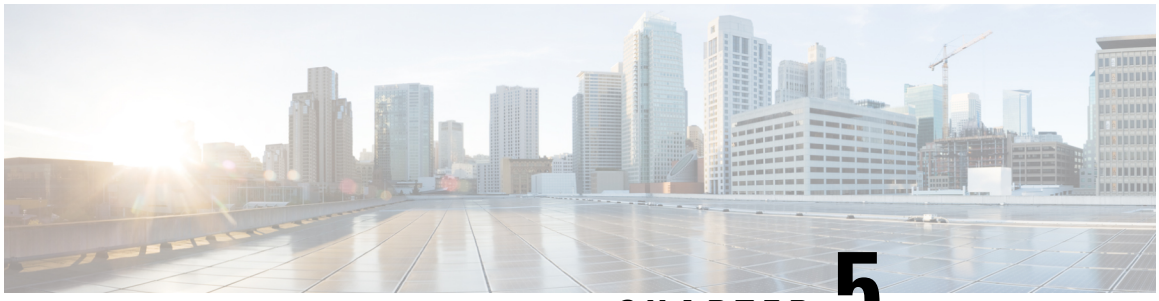
- Enhances the datapath to generate a session summary event when the gateway connection and proxy timers are exceeded. This enhancement will help in troubleshooting when a session is closed by the gateway due to timer settings.
- Enhances the gorward proxy service object to accommodate L4 (TCP) and L5 (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 5

Multicloud Defense Terraform Provider Enhancements

- Multicloud Defense Terraform Provider Version 25.8.1 September 16, 2025 (Recommended), on page 57
- Multicloud Defense Terraform Provider Version 0.3.3 June 20, 2025, on page 58
- Multicloud Defense Terraform Provider Version 0.3.2 June 20, 2025, on page 58
- Multicloud Defense Terraform Provider Version 0.3.1 May 7, 2025, on page 58
- Multicloud Defense Terraform Provider Version 0.3.0 March 3, 2025, on page 59
- Multicloud Defense Terraform Provider Version 0.2.9 November 15, 2024, on page 59
- Multicloud Defense Terraform Provider Version 0.2.8 November 7, 2024, on page 59
- Multicloud Defense Terraform Provider Version 0.2.7 August 21, 2024 , on page 60
- Multicloud Defense Terraform Provider Version 0.2.6 March 1, 2024, on page 60
- Multicloud Defense Terraform Provider Version 0.2.5 November 6, 2023, on page 61
- Multicloud Defense Terraform Provider Version 0.2.4 August 22, 2023, on page 62

Multicloud Defense Terraform Provider Version 25.8.1 September 16, 2025 (Recommended)

Enhancement

The following enhancement is included in this release:

- Adds Terraform support for integrating a Service VNet (`ciscomcd_service_vpc`) resource with Azure VWAN vHub. This capability establishes the peering between the Service VNet and the VWAN vHub and propagates the spoke VNet CIDRs into the vHub route tables.

Fixes

The following fixes are included in this release:

- Upgrades Terraform SDK to v2. The Terraform provider now requires Terraform binary version 0.12 or later.
- Fixes an issue with a Service Object (`ciscomcd_service_object`) resource where the provider would allow creating the resource where the `transport_mode` argument configuration contains multiple `port`

blocks with overlapping ports. This configuration is not supported; and the fix detects this misconfiguration and inhibits creating the resource.

Multicloud Defense Terraform Provider Version 0.3.3 June 20, 2025

The following fix is included in this release:

- Fixes to documentation formatting.

Multicloud Defense Terraform Provider Version 0.3.2 June 20, 2025

Enhancements

The following enhancement is included in this release:

- Provides Terraform support for creating and managing Firewall Threat Defense Virtual (FTDv) Gateway (`ciscomcd_ftdv_gateway`) resources. This also includes an FTDv Gateway data source and resource import support.

Fixes

The following fixes are included in this release:

- Fixes an issue when creating a Network Intrusion Profile (`ciscomcd_profile_network_intrusion`) resource with certain configuration would fail with an `Error: category app-detect is not valid` error.
- Fixes an issue where creating or modifying a Log Forwarding Profile `(ciscomcd_profile_log_forwarding)` resource would generate an error when using dynamic values.

Multicloud Defense Terraform Provider Version 0.3.1 May 7, 2025

Enhancements

The following enhancement is included in this release:

- Adds support for M7i (2-core, 4-core, 8-core) instance type when deploying a gateway (`ciscomcd_gateway`) resource in AWS. This enhancement accommodates gateway deployments into recently introduced regions that require the latest M-class family.

Multicloud Defense Terraform Provider Version 0.3.0 March 3, 2025

Fixes

The following fixes are included in this release:

- Adds Terraform support for WebHook destination for a Log Forwarding (`ciscomcd_profile_log_forwarding`) resource.
- Fixes an issue with the round trip of a Spoke VPC/VNet (`ciscomd_spoke_vpc`) resource. Attempting import of the resource(s) exported from the UI will produce an error: "Cannot import non-existent remote object". Once the import is achieved, a downstream issue occurs where the imported resource state in Terraform does not match the true resource state observed by the Multicloud Defense Controller. This state mismatch is related to the spoke VPC subnets, which are part of the orchestration for AWS spoke VPC attachments. This fix ensures that the export is formatted properly and the important functions as expected.

Multicloud Defense Terraform Provider Version 0.2.9 November 15, 2024

Fixes

The following fixes are included in this release:

- Fixes an issue where an address object (`ciscomcd_address_object`) resource with `type = DYNAMIC_SECURITY_GROUP` would be created, but the sub-objects would not be dynamically populated.
- Fixes an issue where the settings block of a gateway (`ciscomcd_gateway`) resource would change order when comparing against the current state, which would result in Terraform seeing this as an infrastructure change when no change was made. Settings order is not relevant for gateway behavior, but it is relevant when running a Terraform plan or apply to validate whether any changes need to be applied. This fix ensures that the settings order will remain consistent, unless the order is changed by the user.

Multicloud Defense Terraform Provider Version 0.2.8 November 7, 2024

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 (`ciscomcd_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 (`ciscomcd_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 (`ciscomcd_address_object`) resource would not result in a change to the name.
- Fixes an issue where attaching an ICMP rule to a policy rule (`ciscomcd_policy_rules`) resource will result in a feature compliant error message.
- Fixes an issue where a forwarding profile (`ciscomcd_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 (`ciscomcd_profile_bgp`) cannot be created without BGP neighbor blocks being specified.
- Fixes an issue where the CIDR argument for a service VPC (`ciscomcd_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 (`ciscomcd_address_object`) resource and a policy rule (`ciscomcd_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.

Multicloud Defense Terraform Provider Version 0.2.7 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.

Multicloud Defense Terraform Provider Version 0.2.6 March 1, 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.

Multicloud Defense Terraform Provider Version 0.2.5 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.

Multicloud Defense Terraform Provider Version 0.2.4 August 22, 2023

Enhancements

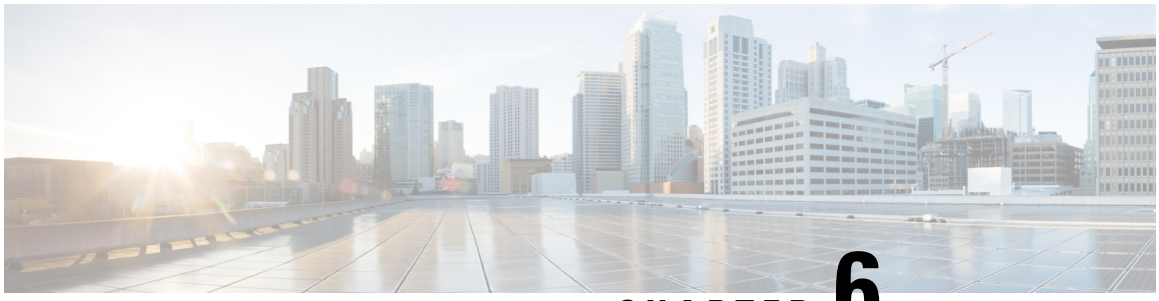
The following enhancements are included in this release:

- 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 6

Legacy Versions

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

- Legacy Multicloud Defense Gateway Versions, on page 63
- Legacy Multicloud Defense Terraform Provider Versions, on page 78

Legacy Multicloud Defense Gateway Versions

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 23.06

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

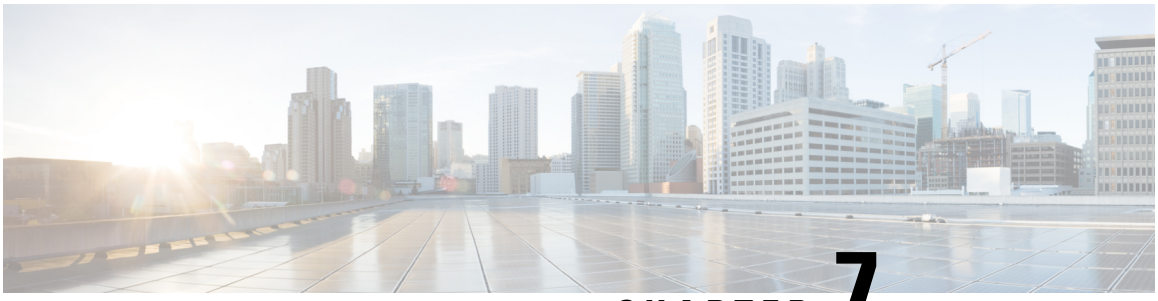
The following enhancements is included in this release:

- 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 7

Release and Service Policies

- Release Versioning and Schedule, on page 83
- Release Life and Support, on page 84

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)