

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 2
- Version 26.08 Multicloud Defense Controller, September 11, 2026, on page 2
- Version 26.08 Multicloud Defense Controller, September 8, 2026, on page 2
- Version 26.08 Multicloud Defense Controller, September 1, 2026, on page 3
- Version 26.07 Multicloud Defense Controller, August 21, 2026, on page 3
- Version 26.07 Multicloud Defense Controller, August 7, 2026, on page 4
- July 26, 2026 Gateway 25.02-10 (Recommended), on page 4
- Version 26.06 Multicloud Defense Controller, July 8, 2026, on page 4
- June 17, 2026 Gateway 25.02-09, on page 5
- June 3, 2026 Gateway 25.02-08, on page 5
- Version 26.05 Multicloud Defense Controller, May 19, 2026, on page 5
- May 7, 2026 Gateway 24.06-21, on page 6
- May 1, 2026 Gateway 25.02-07, on page 6
- May 1, 2026 Gateway 25.02-07-a1, on page 7
- Version 26.04 Multicloud Defense Controller, April 21, 2026, on page 7
- April 21, 2026 Gateway 26.03, on page 8
- Version 26.03 Multicloud Defense Controller, April 1, 2026, on page 8
- March 24, 2026 Gateway 25.02-06-a1, on page 8
- March 24, 2026 Gateway 25.02-06, on page 8
- Version 26.03 Multicloud Defense Controller, March 18, 2026, on page 9
- February 21, 2026, Gateway 25.02-05, on page 9
- Version 26.02 Multicloud Defense Controller, on page 10
- February 13, 2026 Gateway 24.06-20, on page 11
- December 12, 2025 Gateway 24.06-19, on page 11
- Version 25.12 Multicloud Defense Controller, December 12, 2025, on page 11
- November 18, 2025 Gateway 24.06-18, on page 11
- Version 25.10 Multicloud Defense Controller, November 5, 2025, on page 12

• October 15, 2025 Gateway 25.02-03, on page 13
• Version 25.09 Multicloud Defense Controller, October 7, 2025, on page 15
• October 3, 2025 Gateway Hotfix 24.06-17-a1, on page 15
• September 24, 2025 Gateway 24.06-17, on page 15
• August 22, 2025 Gateway Hotfix 24.06-16-a1, on page 16
• August 2025 Gateway Version 24.06-16 and Controller Version 25.08, on page 16
• Version 25.07 Multicloud Defense Controller, July 31, 2025, on page 17
• July 17, 2025 Gateway Hotfix 24.06-15-a1, on page 17
• June 2025 Gateway Version 24.06-15 and Controller Version 25.06, on page 18
• July 3, 2025 Gateway Hotfix 24.06-14-b1, on page 19
• July 3, 2025 Gateway 25.02-02, on page 19
• February 28, 2025 Gateway 25.02-01, on page 22
• June 5, 2025 Gateway Hotfix 24.06-14-a1, on page 26
• May 2025 Gateway Version 24.06-14 and Controller Version 25.05, on page 27
• May 23, 2025 Gateway Hotfix 24.06-13-a1, on page 27
• May 23, 2025 Gateway 24.06-13, on page 28
• May 9, 2025 Gateway Hotfix 24.06-12-a1, on page 28
• May 9, 2025 Gateway 24.06-12, on page 29
• May 7, 2025 Gateway Hotfix 24.06-11-a1, on page 29
• April 2025 Gateway Version 24.06-11 and Controller Version 25.04, on page 30

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.