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 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 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 via 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 Forward 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 processing 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 that 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 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.

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.