Multicloud Defense Gateway Fixes and Enhancements (Archives)

- Version 24.06, on page 1
- Version 24.04, on page 9
- Version 24.02, on page 10
- Version 23.08, on page 12

Version 24.06

Version 24.06-10-a1 March 31, 2025

This is a hotfix.

Fixes

The following fixes are inculded in this hotfix:

- Fixes an occasional datapath instability when processing browser-based client traffic where post-quantum cryptography is enabled. The instability would result in a datapath self-heal. The fix ensures datapath stability, resulting in no need to self heal.
- Fixes an issue where a forwarding policy could not retrieve the Service Name Indication (SNI) from a TLS Client Hello message causing the gateway to close the connection with a TCP RST. This is caused by a change made in Chrome in April 2024 to shift to Post-Quantum Cryptography. With this change, the Client Hello is larger than 1415 bytes, which can result in an inability to retrieve the SNI, which is used by the policy to match or filter by domain. The fix ensures the forwarding policy can support Client Hello sizes greater than 1415 bytes.

Version 24.06-10 March 31, 2025

Fixes

The following fixes are included in this release:

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

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

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

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

Version 24.06-09-a1 February 14, 2025

This is a hotfix.

Fixes

The following fixes are included in this hotfix:

- Fixes an occasional datapath instability when processing browser-based client traffic where post-quantum cryptography is enabled. The instability would result in a datapath self-heal. The fix ensures datapath stability, resulting in no need to self heal.
- Fixes an issue where a forwarding policy could not retrieve the Service Name Indication (SNI) from a TLS Client Hello message causing the gateway to close the connection with a TCP RST. This is caused by a change made in Chrome in April 2024 to shift to Post-Quantum Cryptography. With this change, the Client Hello is larger than 1415 bytes, which can result in an inability to retrieve the SNI, which is used by the policy to match or filter by domain. The fix ensures the forwarding policy can support Client Hello sizes greater than 1415 bytes.

Version 24.06-09 February 14, 2025

Fixes

The following fix is included in this release:

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

Version 24.06-08-a1 January 16, 2025

This is a hotfix.

Fixes

The following fix is included in this hotfix:

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

Version 24.06-08 January 16, 2024

Enhancements

The following enhancements are included in this release:

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

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

Fixes

The following fix is included in this release:

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

Version 24.06-07-a1 December 18, 2024

This release is a hotfix.

Fixes

The following fix is included in this hotfix:

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

Version 24.06-07 December 18, 2024

Fixes

The following fixes are included in this release:

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

Version 24.06-06-a1 November 28, 2024

This release is a hotfix.

Fixes

The following fix is included in this hotfix:

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

Version 24.06-06 November 26, 2024

Fixes

The following fix is included in this release:

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

Version 24.06-05 November 22, 2024

Enhancements

The following enhancement is included in this release:

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

Fixes

The following fixes are included in this release:

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

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

Version 24.06-04 October 25, 2024

Fixes

The following fix is included in this release:

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

Version 24.06-03 October 20, 2024

Enhancements

The following enhancements are inlcuded in this release:

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

Fixes

The following fixes are inlcuded in this release:

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

- Fixes an issue where a decryption profile that is configured differently than the default configuration would not properly apply to the gateway, resulting in TLS negotiation failures due to cipher suite mismatches between the client and the gateway.
- Fixes an issue where the gateway-side cipher suites used in a gateway SSH session were potentially flagged as weaker cipher suites. The fix accommodates only the most secure GCM-based cipher suite.
- Fixes various stability issues.

Version 24.06-02-a2 October 2, 2024

This release is a hotfix.

Fixes

The following fixes are included in this hotfix:

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

Version 24.06-02 September 18, 2024

Enhancements

The following enhancement is included in this release:

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

Fixes

The following fixes are included in this release:

- Fixes and issue where the gateway will self-heal if an empty FQDN/URL Filtering profile is assigned to the policy rule set.
- Fixes a deny rule action issue related to the use of domains as a 6-tuple match. If the first rule match is a 6-tuple match (includes an assigned FQDN Match Profile) and the policy action is set to **Deny**, the deny action will be based on the 5-tuple match and will not include the domain for match consideration. This fix ensures that all 6-tuples are considered when evaluating the rule and its action. If the traffic does not match the rule based on the 6-tuple match, then it will refine its match to a subsequent rule and take action based on the matched rule's configuration.
- Fixes an issue where an Azure ingress gateway will get stuck in `Health Checking Pending` state after a policy update is applied. This issue also includes new gateway deployments .
- Fixes an allow rule match issue related to the use of domains as a 6-tuple match. If the first rule match is a 6-tuple match (includes an assigned FQDN Match profile), the policy action is set to **Allow** and there are no subsequent rules that are consistent with the 5-tuple match of the first rule, then all domains will be allowed and domains will be denied. This fix ensures that only the domains that are matched in the rule are allowed, and all other domains that are not matched are denied.

- Fixes an issue where a egress policy rule set that uses an decryption-based forward proxy (TLS, HTTPS, WebsocketS) is initially matching on 5-tuple and retrieving the domain from the SNI, but not performing a match refinement based on the 6th tuple resulting in a TLS error. The fix ensures that 6-tuple match refinement occurs such that the traffic can be successfully processed by the proper decryption rule.
- Fixes an issue where sessions with TLS negotiation errors where not recording the SNI as a **Traffic Summary** > **Event**.
- Fixes an issue where multiple SNI events were being recorded for each forward proxy full decrypted session.
- Fixes an issue where the address group size could be exceeded, causing all IPs/CIDRs in excess of the size to not be included in the address group. The address group size has been increased to 20k IPs/CIDRs.
- Adds a System Log message if the GeoIP limitations of the gateway are exceeded.
- Fixes an issue where the wrong action would be taken for URL filtering category matching if a timeout occurs when attempting to retrieve the URL filtering category if the URL is not found in the cache.
- Ensures that an user with administrator access to configure a URL Filtering profile cannot use the custom URL response to inject Javascript. The fix enforces HTML encoding in the custom URL response.

Version 24.06-01 July 10, 2024

-

Enhancements

The following enhancements are included in this release:

- Adds support for inspecting content within a GRE tunnel that passes through the gateway. The gateway will decapsulate the traffic, perform inspection on the encapsulated traffic to apply proper policy and protection, then re-encapsulate that traffic back into the GRE tunnel.
- Adds support for active connection resets during gateway upgrade and scale-in scenarios. When these scenarios occur and the gateway is processing long running connections that are not closed by the client or server, the gateway will take action by sending a TCP RST to active close the connection when reaping the old instance.
- Support ability to specify a custom banner when logging into a gateway instance through Teleport (SSH access). This is a requirement for gateways deployed into FedRamp environments where any method of SSH access requires a customer-defined banner to be displayed.

Fixes

The following fixes are included in this release:

- Fixes an issue where specifying an Validate Certificate action other than "Default" in a Decryption profile will cause the gateway to become unhealthy.
- Fixes an issue for user-generate diagnostic bundles where the gateway would fail to generate the diagnostic bundle and send to the Multicloud Defense Controller.
- Fixes an issue related to the use of GeoIP. Countries with many providers have a very large number of advertised prefixes. When those country codes are used in a GeoIP address group, the address group will

contain a large number of CIDR blocks. The GeoIP address group was restricted to 64k CIDRs where exceeding this limit would result in a partial set of CIDRs applied to the policy. This fix relaxes the limit to ensure the full set of CIDRs will be applied to the policy. It is recommended to use an 8-core instance type due to the additional memory requirements imposed by GeoIP.

- Fixes an issue where the gateway could issue the wrong certificate when a Chrome browser is connecting to the gateway using TLS 1.3. This is caused by a change made in Chrome in April 2024 to shift to Post-Quantum Cryptography. With this change, the Client Hello is larger than 1415 bytes, which can result in an inability to retrieve the Server Name Indication (SNI), which is used by the proxy to determine what certificate to issue. The fix ensures the proxy can support Client Hello sizes greater than 1415 bytes.
- Fixes an issue where the gateway was not producing the correct statistics for display in the**Investigate** > **Network Analytics** > **Stats** page.
- Fixes various stability issues.
- Fixes an issue related to blue/green policy change. When the policy change occurs and the new datapath becomes active, the gateway begins draining current sessions off the old datapath. If the datapath cannot properly drain the sessions, it treats the datapath as unhealthy and will employ a datapath restart. This will terminate both old and new datapaths, which could cause disruption to old and new sessions. The fix ensures that the session draining completes properly and eliminates the situation where the datapath is seen as unhealthy.
- Fixes an issue where a VPN tunnel state transition was not generating a System Log message to provide troubleshooting and debugging information on the tunnel setup and negotiation.
- Fixes a slow memory leak for an ingress gateway that eventually results in a datapath self heal. The memory leak is related to traffic that contains files that are gzip compressed.
- Fixes an issue where an ingress gateway could drop a connection when back-to-back POST commands contain a payload greater than 160k.

Version 24.04

Version 24.04-01 May 16, 2024

Enhancements

The following enhancement is included in this release:

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

Fixes

The following fixes are included in this release:

- Ensures the gateway limits address objects to no more than 63 characters.
- Fixes an issue where the datapath could restart due to a policy change taking too long to apply.

- Fixes an issue that results in increased CPU usage during a blue/green policy update where two datapaths would be running at the same time. Each datapath would consume CPU in a way that assumes it is the only datapath running. When the second datapath is instantiated to accommodate the new policy, the CPU would not be shared properly and the CPU metrics would not be recorded properly.
- Fixes an issue related to a memory leak for that would result in a preemptive datapath self-heal.
- Fixes an issue where the gateway policy update status could be stuck in updating.
- Fixes various issues that improve the stability of the gateway.

Version 24.02

Version 24.02-02 April 18, 2024

Fixes

The following fix is included in this release:

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

Version 24.02-01 February 28, 2024

Enhancements

The following enhancements are included in this release:

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

Fixes

The following fixes are included in this release:

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

- Fixes an issue where a policy change that results in a datapath hitless restart could cause high latencies that impact traffic processing, including load balancer health checks, under light or moderate load.
- Fixes an issue addressed in version 23.08-12 that still impacted 4-core instance types. The issue addresses high CPU utilization caused by debug I/O activity. The previous fix now addresses all instance types across all cloud service providers.
- Fixes an issue related to high CPU utilization that was caused by I/O related debug activity.
- Fixes an issue related to intermittent load balancer healthcheck failures. The fix enhances the gateway by prioritizing heathchecks to ensure the load balancer does not incorrectly mark instances as unhealthy.
- Fixes an egress gateway memory leak that would be automatically corrected by triggering a self-healing preemptive datapath restart.
- Fixes an issue where a generated gateway diagnostic bundle would be larger than what would be permitted to send to the Multicloud Defense Controller resulting in the inability to analyze gateway logs. This fix addresses the restrictive limit so generated diagnostic bundles will be successfully sent to the Multicloud Defense Controller.
- Fixes an issue where more than one SNI event was being recorded for each session processed by forward proxy rule.
- Improvements to the stability of the Multicloud Defense Gateway.
- Fixes a traffic processing issue where traffic would stop being processed after TCP and TLS due to a race condition related to DNS-based FQDN caching.
- Fixes an issue where the Multicloud Defense Gateway might not successfully build the IP cache when either an active or inactive rule has DNS-based FQDN caching configured. When the cache is not properly built, policy could fail to match traffic. This fix ensures the IP cache is properly built in order for the policy match and process traffic properly.
- Changes the timeout for waiting for a SYN ACK after receiving a SYN. The original timeout was 120 seconds. In certain scenarios (e.g., port scanning) where a SYN ACK is never returned, a long timeout will consume an entry in the session pull long that desired. For scenarios where many sessions do not respond with a SYN ACK, the session pool could be exhausted. This is often referred to as a SYN flood. By reducing the timeout, the session will be released sooner in order to free up the session pool for use in processing valid sessions. The timeout has been reduced to 30s and is configurable via a Multicloud Defense Gateway setting.
- Fixes an issue related with DNS-based FQDN Address Object resources where enabling DNS caching could result in a race condition between policy change and the DNS resolution interval that would result in the cache for a domain to be reset to a value of 0 (no cache). When this situation occurs, the domain resolution will never be cached and any existing cache values will be flushed as their TTL expire. The end result is the Multicloud Defense Gateway will eventually not match traffic for that domain. This fix addresses the race condition such that the cache will operate as expected.
- Fixes an issue where the DPI (IDS/IPS) Security Event sent to a syslog server did not have the **Action** field present. The **Action** field was present, but the values were not consistent with the Action values present in the UI or the event information sent to other SIEMs. The fix addresses this universally across all security events to ensure the **Action** field has values of `ALLOW` or `DENY`.
- Fixes an issue where a change to a security profile auto-update to manual where the ruleset version is not changed would result in an unnecessary datapath restart. The fix ensures that the change is applied without requiring a datapath restart.

- Improvements to the stability of the Multicloud Defense Gateway.
- Improvements to the performance of the Multicloud Defense Gateway.
- Fixes an issue with the SNI Security Event where the domain that is obtained from the SNI field of a TLS hello message would populate the text field for the event rather than the FQDN field. The change to populate the FQDN field provides consistency across logs and events when viewing and filtering by domain using the FQDN field.
- Fixes an issue with the datapath process that could result in a session pool leak. When this situation occurs, the datapath will evaluate the session pool consumption and self heal before the leak becomes operationally impactful. This fix corrects the leak to avoid the datapath needing to self-heal.
- Improves performance of the Multicloud Defense Gateway by optimizing API calls to the Multicloud Defense Controller to retrieve gateway profile information.
- Fixes an issue where setting the policy rule set action to a `No Log` value would still generate a log message.

Version 23.08

Version 23.08-17-b1 September 27, 2024

This is a hotfix.

Fixes

The following fix is included in this hotfix:

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

Version 23.08-17-a1 September 4, 2024

This is a hotfix.

Fix

The following fix is included in this hotfix:

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

Version 23.08-17 September 4, 2024

Fixes

The following fixes are included in this release:

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

Version 23.08-16-a1 August 6, 2024

This is a hotfix.

Fixes

The following fix is included in this hotfix:

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

Version 23.08-16 June 25, 2024

Fixes

The following fixes are included in this release:

- Fixes an issue where the Multicloud Defense Gateway could issue the wrong certificate when a Chrome browser is connecting to the Gateway using TLS 1.3. This is caused by a change made in Chrome in April 2024 to shift to Post-Quantum Cryptography. With this change, the Client Hello is larger than 1415 bytes, which can result in an inability to retrieve the Server Name Indication (SNI), which is used by the proxy to determine what certificate to issue. The fix ensures the proxy can support Client Hello sizes greater than 1415 bytes.
- Fixes an issue where sending a TCP RST by the datapath to close a session could cause the datapath to self heal.
- Fixes an issue related to receive buffer exhaustion that could impact the ability of the Multicloud Defense Gateway to process traffic. For the Gateway to accommodate resetting connections (TCP RST), information from the last packet received must be retained (receive buffer). If the active session volume is high, there is a risk that the receive buffer can become exhausted, causing the Multicloud Defense Gateway to not receive new packets. This scenario can occur more commonly from half-opened connections related to SYN floods (intentional or unintentional). This fix extracts the necessary information from the last packet

of each active session and stores this information in a buffer that is large enough to accommodate the Gateway active session limits, eliminating the possibility of buffer exhaustion.

- Fixes an issue related to blue/green policy change. When the policy change occurs and the new datapath becomes active, the Multicloud Defense Gateway begins draining current sessions off the old datapath. If the datapath cannot properly drain the sessions, it treats the datapath as unhealthy and will employ a datapath restart. This will terminate both old and new datapaths, which could cause disruption to old and new sessions. The fix ensures that the session draining completes properly and eliminates the situation where the datapath is seen as unhealthy.
- Fixes an issue with log rotation for Multicloud Defense Gateway in OCI. The fix ensures that the logs are properly rotated to not consume unnecessary disk space.
- Fixes an issue related to active connection reset where the TCP RST was being sent with the wrong sequence number and not actively resetting the connection.
- Fixes a slow memory leak for an ingress gateway that eventually results in a datapath self heal. The memory leak is related to traffic that contains files that are gzip compressed.

Version 23.08-15-a3 June 22, 2024

This is a hotfix.

Fixes

The following fix is included in this hotfix:

- Fixes an issue related to the use of GeoIP. Countries with many providers have a very large number of advertised prefixes. When those country codes are used in a GeoIP address group, theaddress group will contain a large number of CIDR blocks. The GeoIP address group was restricted to 64k CIDRs where exceeding this limit would result in a partial set of CIDRs applied to the policy. This fix relaxes the limit to ensure the full set of CIDRs will be applied to the policy. It is recommended to use an 8-core instance type due to the additional memory requirements imposed by GeoIP.

Version 23.08-14-c3 June 8, 2024

This is a hotfix.

Fixes

The following fixes are included in this hotfix:

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

Version 23.08-15-c1 May 9, 2024

This is a hotfix

Fixes

The following fixes are included in this hotfix:

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

Version 23.08-15-a2 May 1, 2024

This is a hotfix.

Fixes

The following fix is included in this hotfix:

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

Version 23.08-15-b1 April 12, 2024

This is a hotfix.

Fixes

The following fix is included in this hotfix:

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

Version 23.08-15-a1 April 11, 2024

This is a hotfix.

Fixes

The following fix is included in this hotfix:

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

Version 23.08-15 March 27, 2024

Fixes

The following fixes are included in this release:

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

Version 23.08-14-e1 March 28, 2024

This is a hotfix.

Fixes

The following fixes are included in this hotfix:

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

Version 23.08-14-a2 March 20, 2024

This is a hotfix.

Fixes

The following fixes are included in this hotfix:

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

Version 23.08-14-d1 March 13, 2024

This is a hotfix.

Fixes

The following fixes are included in this hotfix:

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

Version 23.08-14-c1 February 20, 2024

This is a hotfix.

Fixes

The following fix is included in this hotfix:

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

Version 23.08-14-b1 February 21, 2024

This is a hotfix.

Fixes

The following fixes are included in this hotfix:

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

Version 23.08-14-a1 February 17, 2024

This is a hotfix.

Fixes

The following fixes are included in this hotfix:

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

Version 23.08-14 January 25, 2024

Fixes

The following fixes are inluded in this release:

- Fixes an issue addressed in 23.08-12 that still impacted 4-core instance types. The issue addresses high CPU utilization caused by debug I/O activity. The previous fix now addresses all instance types across all cloud service providers.
- Fixes an issue where a policy change that results in a datapath hitless restart could cause high latencies that impact traffic processing, including load balancer health checks, under light or moderate load.

Version 23.08-12 January 18, 2024

Fixes

The following fixes are included in this release:

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

Version 23.08-11 January 11, 2024

Enhancements

The following enhancement is included in this release:

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

Version 23.08-10 December 18, 2023

Fixes

The following fixes are included in this release:

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

Version 23.08-09 November 16, 2023

Fixes

This following fix is included in the upgrade:

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

Version 23.08-08 November 8, 2023

Fixes

The following fix is included in the upgrade:

- Improves gateway stability for all use-cases.

Version 23.08-07 October 18, 2023

Fixes

The following fix is included in this upgrade:

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

Version 23.08-06 October 7, 2023

Fixes

The following fix is included in this update:

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

Version 23.08-05 October 3, 2023

Fixes

The following fix is included in this update:

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

Version 23.08-04 September 19, 2023

Fixes

The following fix is included in this upgrade:

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

Version 23.08-03 September 10, 2023

Fixes

The following fixes are included in this upgrade:

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

Version 23.08-02 September 3, 2023

Fixes

The following fixes are included in this upgrade:

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

Version 23.08-01 August 25, 2023

Enhancements

The following enhancements are included in this upgrade:

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

- Enhances the gateway datapath process to generate a TCP reset to actively close the connections during a datapath restart.

Fixes

The following fixes are included in this upgade:

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