Multicloud Defense Gateway Fixes and Enhancements

Version 24.06

Version 24.06-02-a2 October 2, 2024

This release is a 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 24.04

Version 24.04-01 May 16, 2024

Enhancements

The following enhancement is included in this release:

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

Fixes

The following fixes are included in this release:

- Ensures the gateway limits address objects to no more than 63 characters.
- Fixes an issue where the datapath could restart due to a policy change taking too long to apply.
- Fixes an issue that results in increased CPU usage during a blue/green policy update where two datapaths would be running at the same time. Each datapath would consume CPU in a way that assumes it is the only datapath running. When the second datapath is instantiated to accommodate the new policy, the CPU would not be shared properly and the CPU metrics would not be recorded properly.
- Fixes an issue related to a memory leak for that would result in a preemptive datapath self-heal.
- Fixes an issue where the gateway policy update status could be stuck in updating.
- Fixes various issues that improve the stability of the gateway.

Version 24.02

Version 24.02-02 April 18, 2024

Fixes

The following fix is included in this release:

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

Version 24.02-01 February 28, 2024

Enhancements

The following enhancements are included in this release:

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

Fixes

The following fixes are included in this release:

- Addresses the CVE-2023-4863 vulnerability related to libwebp version 1.2.0-3.el9.
- Fixes an issue where a policy change that results in a datapath hitless restart could cause high latencies that impact traffic processing, including load balancer health checks, under light or moderate load.
- Fixes an issue addressed in version 23.08-12 that still impacted 4-core instance types. The issue addresses high CPU utilization caused by debug I/O activity. The previous fix now addresses all instance types across all cloud service providers.
- Fixes an issue related to high CPU utilization that was caused by I/O related debug activity.
- Fixes an issue related to intermittent load balancer healthcheck failures. The fix enhances the gateway by prioritizing heathchecks to ensure the load balancer does not incorrectly mark instances as unhealthy.
- Fixes an egress gateway memory leak that would be automatically corrected by triggering a self-healing preemptive datapath restart.
- Fixes an issue where a generated gateway diagnostic bundle would be larger than what would be permitted to send to the Multicloud Defense Controller resulting in the inability to analyze gateway logs. This fix addresses the restrictive limit so generated diagnostic bundles will be successfully sent to the Multicloud Defense Controller.
- Fixes an issue where more than one SNI event was being recorded for each session processed by forward proxy rule.
- Improvements to the stability of the Multicloud Defense Gateway.
- Fixes a traffic processing issue where traffic would stop being processed after TCP and TLS due to a race condition related to DNS-based FQDN caching.
- Fixes an issue where the Multicloud Defense Gateway might not successfully build the IP cache when either an active or inactive rule has DNS-based FQDN caching configured. When the cache is not properly built, policy could fail to match traffic. This fix ensures the IP cache is properly built in order for the policy match and process traffic properly.
- Changes the timeout for waiting for a SYN ACK after receiving a SYN. The original timeout was 120 seconds. In certain scenarios (e.g., port scanning) where a SYN ACK is never returned, a long timeout will consume an entry in the session pull long that desired. For scenarios where many sessions do not respond with a SYN ACK, the session pool could be exhausted. This is often referred to as a SYN flood. By reducing the timeout, the session will be released sooner in order to free up the session pool for use in processing valid sessions. The timeout has been reduced to 30s and is configurable via a Multicloud Defense Gateway setting.
- Fixes an issue related with DNS-based FQDN Address Object resources where enabling DNS caching could result in a race condition between policy change and the DNS resolution interval that would result in the cache for a domain to be reset to a value of 0 (no cache). When this situation occurs, the domain resolution will never be cached and any existing cache values will be flushed as their TTL expire. The end result is the Multicloud Defense Gateway will eventually not match traffic for that domain. This fix addresses the race condition such that the cache will operate as expected.
- Fixes an issue where the DPI (IDS/IPS) Security Event sent to a syslog server did not have the **Action** field present. The **Action** field was present, but the values were not consistent with the Action values

present in the UI or the event information sent to other SIEMs. The fix addresses this universally across all security events to ensure the **Action** field has values of `ALLOW` or `DENY`.

- Fixes an issue where a change to a security profile auto-update to manual where the ruleset version is not changed would result in an unnecessary datapath restart. The fix ensures that the change is applied without requiring a datapath restart.
- Improvements to the stability of the Multicloud Defense Gateway.
- Improvements to the performance of the Multicloud Defense Gateway.
- Fixes an issue with the SNI Security Event where the domain that is obtained from the SNI field of a TLS hello message would populate the text field for the event rather than the FQDN field. The change to populate the FQDN field provides consistency across logs and events when viewing and filtering by domain using the FQDN field.
- Fixes an issue with the datapath process that could result in a session pool leak. When this situation occurs, the datapath will evaluate the session pool consumption and self heal before the leak becomes operationally impactful. This fix corrects the leak to avoid the datapath needing to self-heal.
- Improves performance of the Multicloud Defense Gateway by optimizing API calls to the Multicloud Defense Controller to retrieve gateway profile information.
- Fixes an issue where setting the policy rule set action to a `No Log` value would still generate a log message.

Version 23.10

Version 23.10-03 January 11, 2024

Fixes

The following fixes are included in this release:

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

Version 23.10-02 November 16, 2023

Fixes

The following fix is included in the upgrade:

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

Version 23.10-01 November 3, 2023

Enhancements

The following enhancements are included in this upgrade:

- Moves the policy type mismatch message generated for each session that is processed by two rules that have mismatched policy type (forwarding and forward proxy) to an event related to each session. This eliminates many system log messages when this scenario occurs and generates error as an event associated with each session. When this scenario occurs, the session will be denied and the event will report the reason. The deny will also be represented in the traffic summary log.
- Enhances the forward proxy policy to validate the server certificate when negotiating the backend TLS session. The certificate validation is disabled by default, but can be configured in a decryption profile for all TLS sessions and in an FQDN match object on a per-domain (or set of domains) basis.
- Integrates with teleport to accommodate reverse SSH making it easier to SSH to the gateway instance management interface especially when the gateway is orchestrated without public IPs. The requirements to SSH is rare and only necessary for advanced troubleshooting purposes. Inbound communication is inhibited by default using cloud service provider restrictions (security groups, network security groups, firewall rules).

Fixes

The following fixes are included in this upgrade:

- Fixes an issue related to a forward proxy rule that uses an FQDN match object for decryption exception could result in traffic processing issues.
- Fixes an issue where traffic would be incorrectly denied by a forward proxy rule configured with an FQDN match profile due to delays in certificate validation. The deny will be seen as an `FQDNFILTER` security eent even though an FQDN filtering profile is not applied.
- Fixes an issue where a rule that uses an FQDN match object would incorrectly process traffic for an uncategorized domain.
- Fixes an issue related to dynamic address objects where a large number of IPs and a large number of changes to those IPs could result in the datapath not accepting changes, causing matching issues resulting in traffic being processed incorrectly.

- Fixes an issue with DNS-based FQDN caching where setting the DNS resolution interval would not change the frequency of DNS resolution.
- Fixes an issue with packet collection that could cause the gateway to become unhealthy.
- Fixes an issue where certain logs from the gateway could contain private key information.
- Fixes various gateway stability issues.
- Fixes a gateway memory leak that could also cause a CPU issue resulting in traffic processing issues.
- Fixes an issue where the URI information is not shown in traffic summary log.
- Fixes an issue where L7DOS event does not properly show the URI.

Version 23.08

Version 23.08-17-a1 September 4, 2024

This is a hotfix.

Fix

The following fix is included in this hotfix:

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

Version 23.08-17 September 4, 2024 (Recommended)

Fixes

The following fixes are included in this release:

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

Version 23.08-16-a1 August 6, 2024

This is a hotfix.

Fixes

The following fix is included in this hotfix:

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

Version 23.08-16 June 25, 2024

Fixes

The following fixes are included in this release:

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

Version 23.08-15-a3 June 22, 2024

This is a hotfix.

Fixes

The following fix is included in this hotfix:

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

Version 23.08-14-c3 June 8, 2024

This is a hotfix.

Fixes

The following fixes are included in this hotfix:

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

Version 23.08-15-c1 May 9, 2024

This is a hotfix

Fixes

The following fixes are included in this hotfix:

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

Version 23.08-15-a2 May 1, 2024

This is a hotfix.

Fixes

The following fix is included in this hotfix:

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

Version 23.08-15-b1 April 12, 2024

This is a hotfix.

Fixes

The following fix is included in this hotfix:

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

Version 23.08-15-a1 April 11, 2024

This is a hotfix.

Fixes

The following fix is included in this hotfix:

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

Version 23.08-15 March 27, 2024

Fixes

The following fixes are included in this release:

- Fixes an issue where HTTP traffic passing through an ingress gateway was not using the proper domain specified in the reverse proxy target associated with the matched policy rule set.
- Fixes an issue where HTTP traffic passing through an ingress gateway was not properly matching the proper policy rule set.
- Fixes an issue related to forwarding and how the datapath protocol stack handles timings with TCP FINs and RSTs. A FIN from the server and a RST from the client could occur in a sequence such that the protocol stack would inhibit accepting (and forwarding) the RST after it has already seen a FIN. The change relaxes the protocol stacks acceptance of the RST so it can be forwarded to the server and not dropped by the protocol stack. The RST drop occurs due to a mismatch in the expected sequence number since the protocol stack has already received a FIN from the server.

- Fixes an issue where the datapath could restart due to a policy change taking too long to apply.
- Fixes an issue that results in increased CPU usage during a blue/green policy update where two datapaths would be running at the same time. Each datapath would consume CPU in a way that assumes it is the only datapath running. When the second datapath is instantiated to accommodate the new policy, the CPU would not be shared properly and the CPU metrics would not be recorded properly.
- Fixes an issue related to a memory leak for that would result in a preemptive datapath self-heal.
- Addresses the CVE-2023-4863 vulnerability related to libwebp version 1.2.0-3.el9.
- Fixes an issue related to a lost write event after a write operation to the backend server returns EAGAIN. This lost event causes the gateway to think it has sent the request body to the backend server and is awaiting a response that will never arrive. This is a timing issue related to the speed of the gateway vs. the speed of the backend server.
- Fixes an issue with generating diagnostic bundles for gateways deployed in OCI.
- Fixes an issue related to active connection reset where the TCP RST was being sent with the wrong sequence number and not actively resetting the connection.
- Fixes a traffic processing issue during a policy change where traffic passing through the datapath running the old policy would be unnecessarily delayed.
- Fixes an issue with large request body traffic where the WAF component would consume the client request body. This causes thevgateway to keep expecting the request body from the client, while the client is expecting a response from the gateway, leading to a client timeout.

Version 23.08-14-e1 March 28, 2024

This is a hotfix.

Fixes

The following fixes are included in this hotfix:

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

Version 23.08-14-a2 March 20, 2024

This is a hotfix.

Fixes

The following fixes are included in this hotfix:

- Fixes an issue related to forwarding and how the datapath protocol stack handles timings with TCP FINs and RSTs. A FIN from the server and a RST from the client could occur in a sequence such that the protocol stack would inhibit accepting (and forwarding) the RST after it has already seen a FIN. The change relaxes the protocol stacks acceptance of the RST so it can be forwarded to the server and not

dropped by the protocol stack. The RST drop occurs due to a mismatch in the expected sequence number since the protocol stack has already received a FIN from the server.

- Fixes an issue that results in increased CPU usage during a blue/green policy update where two datapaths would be running at the same time. Each datapath would consume CPU in a way that assumes it is the only datapath running. When the second datapath is instantiated to accommodate the new policy, the CPU would not be shared properly and the CPU metrics would not be recorded properly.

Version 23.08-14-d1 March 13, 2024

This is a hotfix.

Fixes

The following fixes are included in this hotfix:

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

Version 23.08-14-c1 February 20, 2024

This is a hotfix.

Fixes

The following fix is included in this hotfix:

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

Version 23.08-14-b1 February 21, 2024

This is a hotfix.

Fixes

The following fixes are included in this hotfix:

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

Version 23.08-14-a1 February 17, 2024

This is a hotfix.

Fixes

The following fixes are included in this hotfix:

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

Version 23.08-14 January 25, 2024

Fixes

The following fixes are inluded in this release:

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

Version 23.08-12 January 18, 2024

Fixes

The following fixes are included in this release:

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

Version 23.08-11 January 11, 2024

Enhancements

The following enhancement is included in this release:

- Moves the policy type mismatch message generated for each session that is processed by two rules that have mismatched policy type (gorwarding and gorward proxy) to a security event log related to each session. This eliminates a large volume of per-session system log messages without eliminating the

per-session log. When this scenario occurs, the session will be denied and the event associated with the session will report the reason. The deny will also be represented in the traffic summary log.

Version 23.08-10 December 18, 2023

Fixes

The following fixes are included in this release:

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

Version 23.08-09 November 16, 2023

Fixes

This following fix is included in the upgrade:

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

Version 23.08-08 November 8, 2023

Fixes

The following fix is included in the upgrade:

- Improves gateway stability for all use-cases.

Version 23.08-07 October 18, 2023

Fixes

The following fix is included in this upgrade:

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

Version 23.08-06 October 7, 2023

Fixes

The following fix is included in this update:

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

Version 23.08-05 October 3, 2023

Fixes

The following fix is included in this update:

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

Version 23.08-04 September 19, 2023

Fixes

The following fix is included in this upgrade:

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

Version 23.08-03 September 10, 2023

Fixes

The following fixes are included in this upgrade:

- Fixes an issue related to dynamic address objects where a large number of IPs and a large number of changes to those IPs could result in the datapath not accepting changes, causing matching issues resulting in traffic being processed incorrectly.

- Fixes a slow session pool leak related to UDP traffic that would result in the DP detecting the leak and restarting the datapath.

Version 23.08-02 September 3, 2023

Fixes

The following fixes are included in this upgrade:

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

Version 23.08-01 August 25, 2023

Enhancements

The following enhancements are included in this upgrade:

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

Fixes

The following fixes are included in this upgade:

- Fixes an issue where URL encoded characters of [`and`] in an HTTP object name where decoded by the gateway, but not re-encoded before sending the request to the server. This results in the server not being able to properly locate the object, returning a 400 response code. This fix properly re-encodes the characters prior to sending the request to the server.
- Fixes an issue where the presence of underscores in an SNI would cause the proxy to not pass traffic. This change enables the proxy configuration to accommodate the use of underscores in domain names.
- Fixes an issue where traffic is matched to a correct policy, but an incorrect certificate is issued.
- Fixes an issue where traffic is matched to a correct policy, but an incorrect certificate is issued.
- Fixes an issue with large file transfers related to HTTP commands (e.g., Github repository cloning) where a proxy timeout would result in a 408 status code.
- Fixes an issue where URL Filtering category query timeout expires causing the traffic to be denied.

- Fixes a stability issue with the ingress gateway where the datapath could self heal due to an issue with the upstream proxy.
- Fixes an issue where the gateway could introduce additional latency when processing certain types of traffic.
- Fixes an unnecessary datapath restart that is triggered when enabling memory profiling.
- Fixes an issue where the gateway could intermittently generate a 502 due to a datapath restart triggered by a policy change.
- Fixes an issue with CPU-based auto-scale could result in an unnecessary scale out.
- Fixes a proxy connection leak.
- Improvements to the stability of the Multicloud Defense Gateway.