

Legacy Versions

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

- Legacy Multicloud Defense Gateway Versions, on page 1
- Legacy Multicloud Defense Terraform Provider Versions, on page 16

Legacy Multicloud Defense Gateway Versions

Version 23.10

Version 23.10-03 January 11, 2024

Fixes

The following fixes are included in this release:

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

Version 23.10-02 November 16, 2023

Fixes

The following fix is included in the upgrade:

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

Version 23.10-01 November 3, 2023

Enhancements

The following enhancements are included in this upgrade:

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

Fixes

The following fixes are included in this upgrade:

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

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

Version 23.06

Version 23.06-14 November 12, 2023

Fixes

The following fix is included in this upgrade:

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

Version 23.06-13 October 18, 2023

Fixes

The following fix is included in this upgrade:

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

Version 23.06-12 October 6, 2023

Fixes

The following fix is included in this update:

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

Version 23.06-11 September 27, 2023

Fixes

The following fix is included in this update:

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

Version 23.06-10 September 19, 2023

Fixes

The following fix is included in this upgrade:

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

Version 23.06-09 September 10, 2023

Fixes

The following fixes are included in this upgrade:

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

Version 23.06-08 September 3, 2023

Fixes

The following fix is included in this upgrade:

- Fixes an issue where a DNS-based address object that contains static IPs would fail to properly match.

Version 23.06-07 August 29, 2023

Fixes

The following fix is inlcuded in this upgrade:

- Fixes an issue with Forward Proxy where sending a HTTP POST with a payload greater than 200KB would cause the traffic to be dropped.

Version 23.06-06 August 23, 2023

Fixes

The following fixes are included in this upgrade:

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

Version 23.06-05 August 4, 2023

Fixes

The following fixes are included in this upgrade:

- Fixes an issue where HTTP headers that use underscores would not be passed by a proxy Rule. This change enables the proxy configuration to accommodate headers with underscores.
- Fixes an issue with large file transfers related to HTTP commands (e.g., Github repository cloning) where a proxy timeout would result in a 408 status code.
- Fixes an issue where HTTP traffic processed initially by a Forward Proxy Rule, then subsequently processed by a Forwarding Rule due to refined matching, would be allowed when it should be denied.

Version 23.06-04 July 27, 2023

Fixes

The following fix is included in this upgrade:

- Fixes an issue where certain types of traffic processed by the anti-malware engine could result in high CPU causing delays in traffic processing.

Version 23.06-03 July 21, 2023

Fixes

The following fix is included in this upgrade:

- Fixes an issue where a new Gateway deployment could result in a bring-up failure if a Policy Rule Set contains Address Objects that utilize a mix of IP/CIDR inclusion and exclusion.

Version 23.06-02 July 19, 2023

Fixes

The following fixes are included in this upgrade:

- Fixes an issue where an update to a CIDR-based Address Object is not properly applied to the datapath workers, resulting in incorrect Rule matching.
- Fixes an issue with a DNS-based FQDN Address Object where a DNS cache is properly established, but not properly applied to the datapath workers, resulting in incorrect Rule matching.
- Fixes a datapath processing behavior where a Forward Proxy Rule preceded by a Forwarding Rule for the same L3/L4 (IP/port/protocol) matching criteria, but distinct L5 (SNI) matching would result in traffic processed as Forwarding even though proper Rule matching occurs. A similar behavior would be seen if the Forwarding and Forward Proxy Rules order were reversed. The reason this behavior occurs is that in order to accommodate L5 (SNI) matching, the TCP handshake must be fully established to receive the TLS hello message to obtain the SNI. Once the TCP handshake has completed, the traffic has already been processed by the Rule type of the first Rule. Once the session has been established, it is not possible to change the traffic processing from Forwarding to Forward Proxy (or vice versa). If a Policy Rule Set has been configured with this conflict, the datapath will detect the conflict and generate a System Log message. The traffic will be denied as it cannot successfully be processed by the conflicting Rule.
- Fixes a stability issue with the Ingress Gateway where the datapath could self heal due to an issue with the upstream proxy.
- Fixes an issue where a datapath restart would result in a spike in CPU that could cause an unnecessary auto-scale.

Version 23.06-01 July 6, 2023

Fixes

The following fixes are included in this upgrade:

- Fixes an issue where a GCP Gateway could not generate support-related diagnostic bundles.
- Fixes an issue where an NTP Profile was repeatedly applied to a Gateway even though no Profile change was introduced.
- Fixes an issue where an empty Address Object applied to a Gateway would result in a traffic processing issue.
- Fixes an issue where an unnecessary datapath self-heal would occur when simultaneously applying both an NTP Profile and Log Forwarding Profile to a Gateway. This issue would only surface if the Profiles are applied using orchestration since the operations are independent, would occur sequentially and all within a very short separation in time.
- Fixes an issue where an Ingress Gateway could issue an incorrect certificate when a Rule has been configured with a domain that contains more than 3 levels.

- Fixes an issue where frequent changes to an Address Object could result in the datapath not accepting further changes.
- Fixes an issue where a Reset on Deny (TCP Reset) would not be issued when traffic is processed by a Ruleset that uses FQDN Match.
- Fixes an issue where an L4_FW event was not consistently produced when for traffic processed by the Gateway.
- Fixes an issue where changing the WAF action from "Allow Log" to "Rule Default" could cause the datapath to restart multiple times.
- Fixes an issue where HTTP traffic with chunked Transfer-Encoding could cause large memory consumption in WAF that would trigger a datapath self heal Fix: Fixes a slow memory leak that results in a silent datapath restart that could disrupt traffic.
- Fixes a memory issue that could result in a datapath self heal.

Version 23.04

Version 23.04-18 September 3, 2023

Fixes

The following fixes are included in this upgrade:

- Fixes an issue with reverse proxy where sending a HTTP POST with a payload greater than 200KB would cause the traffic to be dropped.
- Fixes an issue where a DNS-based address object that contains static IPs would fail to properly match.

Version 23.04-17 August 23, 2023

Fixes

The following fix is included in this upgrade:

- Fixes an issue where URL encoded characters of [and] in an HTTP object name where decoded by the Gateway, but not re-encoded before sending the request to the server. This results in the server not being able to properly locate the object, returning a 400 response code. This fix properly re-encodes the characters prior to sending the request to the server.

Version 23.04-16 August 22, 2023

Fixes

The following enhancements are included in this upgrade:

- Fixes an issue where the presence of underscores in an SNI would cause the proxy to not pass traffic. This change enables the proxy configuration to accommodate the use of underscores in domain names.
- Fixes an additional issue with large file transfers related to HTTP commands (e.g., Github repository cloning) where a proxy timeout would result in a 408 status code.

- Fixes an issue where traffic is matched to a correct policy, but an incorrect certificate is issued.
- Fixes an issue where URL Filtering category query timeout expires causing the traffic to be denied.
- Fixes a proxy connection leak.
- Improvements to the stability of the Gateway.

Version 23.04-14 July 27, 2023

Fixes

The following fix is included in this upgrade:

- Fixes an issue where certain types of traffic processed by the anti-malware engine could result in high CPU causing delays in traffic processing.

Version 23.04-13 July 27, 2023

Fixes

The following fix is included in this upgrade:

- Fixes an issue where certain types of traffic processed by the anti-malware engine could result in high CPU causing delays in traffic processing.

Version 23.04-12 July 19, 2023

Fixes

The following fixes are included in this upgrade:

- Fixes an issue where an update to a CIDR-based Address Object is not properly applied to the datapath workers, resulting in incorrect Rule matching.
- Fixes an issue with a DNS-based FQDN Address Object where a DNS cache is properly established, but not properly applied to the datapath workers, resulting in incorrect Rule matching.
- Fixes a datapath processing behavior where a Forward Proxy Rule preceded by a Forwarding Rule for the same L3/L4 (IP/port/protocol) matching criteria, but distinct L5 (SNI) matching would result in traffic processed as Forwarding even though proper Rule matching occurs. A similar behavior would be seen if the Forwarding and Forward Proxy Rules order were reversed. The reason this behavior occurs is that in order to accommodate L5 (SNI) matching, the TCP handshake must be fully established to receive the TLS hello message to obtain the SNI. Once the TCP handshake has completed, the traffic has already been processed by the Rule type of the first Rule. Once the session has been established, it is not possible to change the traffic processing from Forwarding to Forward Proxy (or vice versa). If a Policy Rule Set has been configured with this conflict, the datapath will detect the conflict and generate a System Log message. The traffic will be denied as it cannot successfully be processed by the conflicting Rule.
- Fixes a stability issue with the Ingress Gateway where the datapath could self heal due to an issue with the upstream proxy.
- Fixes an issue where a datapath restart would result in a spike in CPU that could cause an unnecessary auto-scale.

Version 23.04-11 July 10, 2023

Fixes

The following fixes are included in this upgrade:

- Fixes a stability issue in the Snort engine that could cause the Gateway to self heal.
- Fixes an issue where Ingress traffic containing a long header will cause the Reverse Proxy to generate a 400 response code.
- Fixes an issue where traffic is not processed properly by a Forward Proxy Rule when the Rule uses a FQDN Match Profile with multiple rows containing a mixture of Decryption Exception settings.

Version 23.04-10 June 28, 2023

Fixes

The following fix is included in this upgrade:

- Fixes an issue where applying a DNS-based cache setting to a Gateway will cause the Gateway instance to become unhealthy.

Version 23.04-09 June 25, 2023

Fixes

The following fixes are included in this upgrade:

- Removes 15-day periodic Gateway datapath self-heal that was in place to help ensure consistent Gateway health. This was incorporated more than 2 years ago to address an issue that was challenging to catch and fix. That issue has since been addressed, but the periodic self-heal was never removed. It is no longer needed and has now been removed.
- Fixes an issue where a GCP Gateway could not generate support-related diagnostic bundles.
- Fixes an issue where an NTP Profile was repeatedly applied to a Gateway even though no Profile change was introduced.
- Fixes an issue where a Policy Rule Set could be in a persistent "Updating" state when an FQDN Filtering Profile is applied.
- Fixes an issue where an empty Address Object applied to a Gateway would result in a traffic processing issue.
- Fixes an issue where an unnecessary datapath self-heal would occur when simultaneously applying both an NTP Profile and Log Forwarding Profile to a Gateway. This issue would only surface if the Profiles are applied using orchestration since the operations are independent, would occur sequentially and all within a very short separation in time.

Version 23.04-07 June 14, 2023

Fixes

The following fixes are included in this upgrade:

- Fixes an issue where changing the WAF action from "Allow Log" to "Rule Default" could cause the datapath to restart multiple times.
- Provides an update to revert a change that was made in 23.04-05 related to a slow session pool leak addressed by a preemptive datapath self-heal. The previous update has the potential to cause datapath self-heals that cannot be preempted. This release ensures stability while the initial issue is fully addressed.

Version 23.04-06 June 8, 2023

Fixes

The following fixes are included in this upgrade:

- Fixes an issue where an L4_FW event was not consistently produced when for traffic processed by the Gateway.
- Fixes an issue where HTTP traffic with chunked Transfer-Encoding could cause large memory consumption in WAF that would trigger a datapath self heal.

Version 23.04-05 June 1, 2023

Fixes

The following enhancements are included in this upgrade:

- Fixes a slow memory leak that results in a silent datapath restart that could disrupt traffic.
- Fixes a very slow session pool leak that would result in a preemptive datapath self-heal.
- Fixes an issue where a Reset on Deny (TCP Reset) would not be issued when traffic is processed by a Ruleset that uses FQDN Match.
- Fixes an issue where an Ingress Gateway could issue an incorrect certificate when a Rule has been configured with a domain that contains more than 3 levels.
- Fixes an issue where frequent changes to an Address Object could result in the datapath not accepting further changes.
- Fixes various Gateway stability issues that would result in a datapath self-heal.

Version 23.04-04 May 19, 2023

Fixes

The following fix is included in this upgrade:

- Fixes an issue with traffic processing for a Policy Ruleset Rule that uses FQDN Match. Sessions containing a TLS SNI that would match the FQDN would initially be denied, but subsequent sessions would be incorrectly allowed.

Version 23.04-03 May 16, 2023

Fixes

The following fix is included in this upgrade:

- Provides an enhanced memory profiling mode enabled as a Gateway setting. This is useful for advanced troubleshooting to understand memory consumption.

Version 23.04-02 May 2, 2023

Fixes

The following fixes are included in this upgrade:

- Fixes an issue where establishing an SSH session to an OCI Gateway management interface would fail with a permission denied due to invalid user account.
- Fixes an issue where a user-defined NTP Profile associated with a Gateway would not properly configure the NTP settings when applied to the Gateway.

Version 23.04-01 April 20, 2023

Enhancements

The following enhancements are included in this upgrade:

- Enhances the error message reporting by the Gateway when a TLS session cannot be negotiated due to no shared cipher suite. The error message for Security Events of type "TLS_ERROR" have been enhanced to be more descriptive.
- Enhances the hardening of the Centos base image used in the Valtix Gateway. The base image has now been moved to Centos9 and is hardened to accommodate environments that have strict compliance requirements.
- Provides support for configuring the NTP settings of a Gateway. The Gateway NTP settings can be configured using an NTP Profile that can be assigned to the Gateway.
- Support for Azure GWLB-based architectures for Ingress protection.

Fixes

The following fixes are included in this upgrade:

- Fixes an issue with FQDN Match Object where the traffic would be processed by an incorrect Rule when no SNI is present in the traffic.
- Fixes an issue where DLP and IDS/IPS Profiles that were created prior to IDS/IPS and WAF Custom Rule support might not operate as expected unless the Profile was modified and saved.

- Fixes an Ingress Gateway issue related to large-volume bursty TLS traffic where the Gateway could issue an incorrect certificate to the client. This scenario is rare and is a downstream issue that could occur in Gateway releases 22.12-04 and earlier. This fix addresses the downstream issue by ensuring it is never reached and is a safeguard to ensure the issue never occurs.
- Fixes an issue where the same certificate could be issued when the policy is specified with two or more unique listener ports, with each sharing the same SNI and backend configuration.
- Fixes an issue where the datapath engine would not start after failing to load an updated package. This issue has been addressed with the new CentOS 9 base image where package updates are handled by Valtix and not by the Linux kernel itself.
- Fixes an issue where FQDNFILTER Events where showing a reversed source and destination IP/Port information.
- Fixes an issue related to URL Filter Profile where the a Profile created using an older Controller version would not properly deny URLs when the action is configured as deny.
- Fixes a traffic processing issue related to L7DOS Profile configuration. When the Profile is configured with a Request Rate or Burst Size of 1, the datapath would not limit the traffic properly.
- Fixes a traffic processing issue related to L7DOS Profile configuration. When the Profile is configured with Request Rate or Burst Size values of 0, the datapath should inhibit any traffic related to the specified URL/URI. Even though the L7DOS Profile can be used to block URLs/URIs by using this method, the recommended method is to create a URL Filter Profile and apply the Profile to the Policy Ruleset Rules that are processing traffic related to the URL.
- Fixes an issue with Traffic Summary Logs and Events that are sent directly from the Gateway to CSP storage systems (S3 Bucket, GCP Logging) where the friendly name to field values were represented by an integer. This would require a documented integer to friendly name translation by the user. The Logs and Events will now contain the friendly name and not the integer value.
- Fixes a stability issue in an Egress Gateway related to various traffic patterns.
- Fixes an issue related to Websockets Proxy where a duplicate host header would be added to the backend connection. In general, this is not an issue as the RFC states that multiple (and duplicate) host headers are allowed. But there are some application frameworks that do not accept multiple host headers. Ngnix as an application server is one of those systems. When Nginx receives HTTP traffic with multiple host headers, it will reject the session and respond back with a 400 Bad Request.
- Fixes OS vulnerabilities related to Gateway Management Centos Linux container that would result in information notices in vulnerability scanners.
- Fixes an issue with MLX4 DPDK driver for Azure Gateway that could cause an infrequent datapath self-heal.
- Changes the auto-scaling CPU threshold from 75% to 95% to reduce the CPU-based auto-scaling sensitivity.

Version 23.02

Version 23.02-10 June 28, 2023

Fixes

The following fix is included in this upgrade:

- Fixes an issue where applying a DNS-based cache setting to a Gateway will cause the Gateway instance to become unhealthy.

Version 23.02-09 June 25, 2023

Fixes

The following fixes are included in this upgrade:

- Removes 15-day periodic Gateway datapath self-heal that was in place to help ensure consistent Gateway health. This was incorporated more than 2 years ago to address an issue that was challenging to catch and fix. That issue has since been addressed, but the periodic self-heal was never removed. It is no longer needed and has now been removed.
- Fixes an issue where a GCP Gateway could not generate support-related diagnostic bundles.
- Fixes an issue where an NTP Profile was repeatedly applied to a Gateway even though no Profile change was introduced.
- Fixes an issue where a Policy Rule Set could be in a persistent "Updating" state when an FQDN Filtering Profile is applied.
- Fixes an issue where an empty Address Object applied to a Gateway would result in a traffic processing issue.
- Fixes an issue where an unnecessary datapath self-heal would occur when simultaneously applying both an NTP Profile and Log Forwarding Profile to a Gateway. This issue would only surface if the Profiles are applied using orchestration since the operations are independent, would occur sequentially and all within a very short separation in time.

Version 23.02-08 June 15, 2023

Fixes

The following fixes are included in this upgrade:

- Fixes an issue where changing the WAF action from "Allow Log" to "Rule Default" could cause the datapath to restart multiple times.
- Provides an update to revert a change that was made in 23.04-05 related to a slow session pool leak addressed by a preemptive datapath self-heal. The previous update has the potential to cause datapath self-heals that cannot be preempted. This release ensures stability while the initial issue is fully addressed.

Version 23.02-07 June 8, 2023

Fixes

The following fixes are included in this upgrade:

- Fixes an issue where an L4_FW event was not consistently produced when for traffic processed by the Gateway.
- Fixes an issue where HTTP traffic with chunked Transfer-Encoding could cause large memory consumption in WAF that would trigger a datapath self heal

Version 23.02-06 June 2, 2023

Fixes

The following fixes are included in this upgrade:

- Fixes a slow memory leak that results in a silent datapath restart that could disrupt traffic.
- Fixes a very slow session pool leak that would result in a preemptive datapath self-heal.
- Fixes an issue where a Reset on Deny (TCP Reset) would not be issued when traffic is processed by a Ruleset that uses FQDN Match.
- Fixes an issue where an Ingress Gateway could issue an incorrect certificate when a Rule has been configured with a domain that contains more than 3 levels.
- Fixes an issue where frequent changes to an Address Object could result in the datapath not accepting further changes.
- Fixes various Gateway stability issues that would result in a datapath self-heal.

Version 23.02-05 May 22, 2023

Enhancements

The following enhancement is included in this upgrade:

- Provides an enhanced memory profiling mode enabled as a Gateway setting. This is useful for advanced troubleshooting to understand memory consumption.

Fixes

The following fix is included in this upgrade:

- Fixes an issue with traffic processing for a Policy Ruleset Rule that uses FQDN Match. Sessions containing a TLS SNI that would match the FQDN would initially be denied, but subsequent sessions would be incorrectly allowed.

Version 23.02-04 April 14, 2023

Fixes

The following fixes are included in this upgrade:

- Fixes an issue related to Websockets Proxy where a duplicate host header would be added to the backend connection. In general, this is not an issue as the RFC states that multiple (and duplicate) host headers are allowed. But there are some application frameworks that do not accept multiple host headers. Ngnix as an application server is one of those systems. When Nginx receives HTTP traffic with multiple host headers, it will reject the session and respond back with a 400 Bad Request.
- Moved the TLS renegotiation configuration to a configurable setting. Changed the renegotiation back to a default state of enabled due to potential issues with older clients that rely on renegotiation.
- Changes the auto-scaling CPU threshold from 75% to 95% to reduce the CPU-based auto-scaling sensitivity.

Version 23.02-03 March 7, 2023

Fixes

The following fix is included in this upgrade:

- Fixes an issue where DLP and IDS/IPS Profiles that were created prior to IDS/IPS and WAF Custom Rule support might not operate as expected unless the Profile was modified and saved.

Version 23.02-02 February 20, 2023

Fixes

The following fixes are included in this upgrade:

- Fixes an Ingress Gateway issue related to large-volume bursty TLS traffic where the Gateway could issue an incorrect certificate to the client. This scenario is rare and is a downstream issue that could occur in Gateway release 23.02-01. This fix addresses the downstream issue by ensuring it is never reached and is a safeguard to ensure the issue never occurs.
- Disabled TLS renegotiation to address vulnerability related to CVE-2009-3555.
- Fixes an issue where the FQDN Filtering Events would show reversed source/destination IP/Port information.

Version 23.02-01 February 15, 2023

Enhancements

The following enhancements are included in this upgrade:

- Enhances the DNS-based FQDN Address Object to accommodate IP Address caching. The enhancement provides a configurable set of Gateway settings related to DNS resolution frequency (update interval), IP Address TTL (entry TTL) and IP Address cache size (cache). These settings can be applied using

Terraform only. When not applied, default values are: 60 (seconds) for DNS resolution frequency, 0 (seconds) for IP Address TTL (no caching), and 0 (address count) for IP Address cache size (no caching).

- Enhances the Egress/East-West Policy Ruleset Rule matching criteria to introduce a new variation of an FQDN Profile called an FQDN Match Profile. The FQDN Profile variant is a set of PCRE-defined FQDNs that can be applied to TLS encrypted traffic such that the policy can match on SNI. This enhances the segmentation policy with added flexibility for policies that need to have finer-grained control based on FQDNs.

Fixes

The following fixes are included in this upgrade:

- Fixes an Ingress Gateway issue related to the session upstream connection where the connection being null could result in a datapath self heal.
- Fixes a stability issue in WAF related to large POST commands with chunked encoding enabled.
- Fixes an Ingress Gateway session pool exhaustion issue related to HTTP Keepalives where frontend (Client to Gateway) has KA enabled and backend (Gateway to Server) has KA disabled.
- Fixes an issue related to a dynamic policy that leverages a GCP service where the service does not exist resulting in a policy that contains an empty IP/CIDR. The configuration is valid requiring the Gateway to handle cases where a policy might contain an empty IP/CIDR.
- Fixes an issue related to Rule matching that could result in a datapath self-heal.
- Removes an Azure-generated message that is presented as a System Log message related to Gateway provisioning where Azure assigns a different interface type than requested and posts a warning message suggesting potential performance degradation. The message is seen as `TYPE_AZURE_DEGRADED_PERFORMANCE`. There is no performance impact related to the assigned interface type.
- Enhances Gateway stability for all use cases to eliminate any potential session pool exhaustion.

Legacy Multicloud Defense Terraform Provider Versions

Version 23.7

Version 23.7.2 July 27, 2023

Fixes

The following fix is included in this version:

- Fixes an issue where an FQDN profile (`valtix_fqdn_profile`) resource with `mode=MATCH` argument without a policy argument would result in traffic that matches to be denied. The policy argument does not need to be specified and is not listed as an argument in the Terraform Provider documentation.

Version 23.7.1 July 24, 2023

Fixes

The following fixes are included in this release:

- Fixes an issue when creating a Dynamic VPC address object (`valix_address_object`) resource for an Azure VNet would result in a "'region' parameter is not supported" error.
- Fixes an issue where an FQDN Profile (`valtix_fqdn_profile`) resource with `mode=MATCH` argument incorrectly requires 'policy' argument.

Version 23.6

Version 23.6.1 July 17, 2023

Enhancements

The following enhancements are included in this release:

- Enhanced the Alert profile (`valtix_alert_profile`) resource to support sending alerts (System Logs, Audit Logs) to Webex Teams.
- Adds support for including a Subnet resource as a scope in a Dynamic User Defined Tag address object (`valtix_address_object`) resource.

Fixes

The following fix is included in this release:

- Fixes an issue when creating a Dynamic VPC Address object (`valix_address_object`) resource for an Azure VNet would result in a "'region' parameter is not supported" error.
- Fixes an issue when deploying a gateway (`valtix_gateway`) resource in Azure would throw an error when attempting to deploy in south central/US region.

Version 23.5

Version 23.5.1 June 12, 2023

Enhancements

The following enhancement is included in this release:

- Published a Multicloud Defense Terraform Provider that mirrors the Valtix Terraform Provider. The new Provider is called `ciscomcd` and will be available publicly in the near future. The providers will be updated simultaneously and will represent mirrors of each other unless announced otherwise. In the near future, the Valtix provider will be deprecated and fully replaced by the Cisco provider.

Fixes

The following fixes are included in this release:

- Fixes an issue where deploying a gateway (`valtix_gateway`) resource into Azure zone 1 south central/US region would result in an error.
- Enhances the attributes of a gateway (`valtix_gateway`) resource to output the Azure gateway load balancer frontend resource ID when deploying the ingress gateway in an Azure gateway load balancer-based architecture. The output is specified as part of the gateway endpoint (`gateway_gwlb_endpoints`) attribute.
- Fixes the example in the policy rule set (`valtix_policy_rule_set`) group resource to reference the appropriate member resource argument.

Verison 23.4

Version 23.4.3 May 23, 2023

Fixes

The following fix is included in this release:

- Enhances the attributes of a gateway (`valtix_gateway`) resource to output the Azure gateway load balancer frontend resource ID when deploying the ingress gateway in an Azure gateway load balancer-based architecture. The output is specified as part of the gateway endpoint (gateway_gwlb_endpoints) attribute.

Version 23.4.2 May 11, 2023

Fixes

The following fixes are included in this section:

- Fixes an issue with the NTP profile (`valtix_ntp_profile`) data source where attempting to access the resource would generate an invalid data source error.
- Updates to the Terraform documentation to include the NTP profile (`valtix_ntp_profile`) resource and data source information.

Version 23.4.1 April 20, 2023

Enhancements

The following enhancements is included in this release:

- Changes the policy rule set (`valtix_policy_rule_set`) resource to include `group_member_ids` argument replacing `child_rule_set_ids` argument that is now deprecated.

Fixes

The following fixes are included in this release:

- Fixes an issue with Terraform **Import** operation related to the gateway resource (`valtix_gateway`).
- Fixes an issue in the gateway resource (') where specifying an SSH Key Pair (`ssh_key_pair)` for an Azure gateway would result in an error stating the argument is not supported.
- Fixes an issue related to suppression of WAF rule IDs 949110 and 959100. These rule IDs are informational and define security events stating the WAF anomaly scores (request and response, respectively) have been exceeded along with the action taken based on the WAF profile resource (`valtix_profile_application_threat`) configuration. When these rule IDs are suppressed, the information Events will not be generated. The fix prohibits the ability to suppress these rule IDs resulting in the informational events will always be generated.
- Fixes an issue with Terraform Import operation related to the policy rules resource (`valtix_policy_rules`).