Multicloud Defense Terraform Provider Enhancements

- Version 0.2.9 November 15, 2024 (Recommended), on page 1
- Version 0.2.8 November 7, 2024, on page 1
- Version 0.2.7 August 21, 2024 , on page 2
- Version 0.2.6 February 31, 2024, on page 2
- Version 0.2.5 November 6, 2023, on page 3
- Version 0.2.4 August 22, 2023, on page 4

Version 0.2.9 November 15, 2024 (Recommended)

Fixes

The following fixes are included in this release:

- Fixes an issue where an address object (`ciscomd_address_object`) resource with `type = DYNAMIC_SECURITY_GROUP` would be created, but the sub-objects would not be dynamically populated.
- Fixes an issue where the settings block of a gateway (`ciscomd_gateway`) resource would change order when comparing against the current state, which would result in Terraform seeing this as an infrastructure change when no change was made. Settings order is not relevant for gateway behavior, but it is relevant when running a Terraform plan or apply to validate whether any changes need to be applied. This fix ensures that the settings order will remain consistent, unless the order is changed by the user.

Version 0.2.8 November 7, 2024

Enhancements

The following enhancement is included in this release:

- Changes the default value for the argument `aws_gateway_lb` from false to true of a gateway (`ciscomd_gateway`) resource with `security_type` argument set to **EGRESS**.

Fixes

The following fixes are included in this release:

- Fixes an issue where changing the name argument of a policy rule set (`ciscomd_policy_rule_set`) resource would not result in a change to the name.
- Fixes an issue where changing the name argument of an address object (`ciscomd_address_object`) resource would not result in a change to the name.
- Fixes an issue where attaching an ICMP rule to a policy rule (`ciscomd_policy_rules`) resource will result in a feature compliant error message.
- Fixes an issue where a forwarding profile (`ciscomd_profile_log_forwarding`) resource that is configured with a reference to a dynamic IP address value would throw an error requiring an IP address to be specified.
- Fixes an issue where a BGP Profile (`ciscomd_profile_bgp`) cannot be created without BGP neighbor blocks being specified.
- Fixes an issue where the CIDR argument for a service VPC (`valtix_service_vpc`) resource was not being validated properly, allowing CIDRs that are not applicable when creating a service VPC.
- Fixes an issue where both an address object (`ciscomd_address_object`) resource and a policy rule (`ciscomd_policy_rules`) resource are created in the same apply operation where the rule references the address object, but throws an error due to the address object ID being **0**. The creation of the address object is not returning the ID and thus the ID is 0 when applying to the rule. This fixes the issue such that the address object and rule can both be created and referenced in the same apply.

Version 0.2.7 August 21, 2024

Fixes

The following fix is included in this release:

- Fixes an issue related to ordering of the `instance_details` blocks for a Gateway (`ciscodmcd_gateway`) resource deployed in Edge mode. The block order in a multi-zone deployment could be random, causing the Terraform apply to incorrectly detect an infrastructure change. This fix ensures a consistent order based on the user specified Terraform code such that no infrastructure change is detected if there is no change to the order in the code.

Version 0.2.6 February 31, 2024

Enhancements

The following enhancements are included in this release:

- Adds arm64 support for Windows, Linux and MacOS.
- Enhances the Multicloud Defense Gateway `ciscomcd_gateway` resource creation in GCP to allow a user-provided IP resource to be used as the load balancer frontend IP.

- Adds support for cross-subscription Spoke VNet peering orchestration in Azure `ciscomcd_spoke_vpc`. This ensures feature parity across cloud service providers.
- Adds support for account (Tenant/Compartment) onboarding `ciscomcd_account` and Multicloud Defense Gateway deployment `ciscomcd_gateway` resources for orchestration in OCI.

Fixes

The following fixes are included in this release:

- Fixes an issue where attempting to create an FQDN filtering `ciscomcd_profile_fqdn` resource would result in an error message: `"unknown action Inherit from decryption profile for profile type FQDN_FILTER"`.
- Fixes an issue where a change to a decryption profile `ciscomcd_profile_decryption` resource would not recognize the change producing the message: `"No changes. Your infrastructure matches the configuration"`.
- Fixes an issue with deleting a spoke VPC `ciscomcd_spoke_vpc` peering in GCP where the spoke VPC peering would not be deleted. This issue occurred only when the VPC ID was used instead of the self-link.

Version 0.2.5 November 6, 2023

Enhancements

The following enhancements are included in this release:

- Adds support in a cloud service provider account `ciscomcd_cloud_account` resource for onboarding GCP folder hierarchies to accommodate asset and traffic discovery of all projects that are contained within a Folder hierarchical structure. Onboarding GCP folders permits asset and traffic discovery, but does not permit full orchestration. Discovery is beneficial and necessary for creating a dynamic policy that adapts in real time to changes made within the GCP projects. In order to orchestrate within a project, each project where orchestration is required should be onboarded individually.
- Adds support for sending Multicloud Defense Gateway metrics to 3rd-party SIEMs. This introduces a new metrics forwarding profile `ciscomcd_profile_metrics_forwarding` resource that can be configured and assigned to Multicloud Defense Gateway `ciscomcd_gateway` resources in order for gateway metrics to be sent to the SIEM. The first implementation supports Datadog as a SIEM. Support for other SIEMs will follow in future releases.
- Changes the Multicloud Defense Gateway `ciscomcd_gateway` resource `aws_gateway_lb` argument default value from false to true. When deploying an AWS egress gateway, the supported transit architecture is an AWS gateway load balancer (GWLB) architecture. This argument is optional and if not specified should default to the appropriate value.
- Adds support for sending audit and system logs to Splunk. This introduces an update to the alert profile `ciscomcd_alert_profile` resource by adding Splunk as a new value for the type argument.
- Adds support for sending audit and system logs to Microsoft Teams. This introduces an update to the alert profile `ciscomcd_alert_profile` resource by adding Microsoft Teams as a new value for the type argument.

- 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 `ciscomcd_profile_decryption` resource for all TLS sessions and in an FQDN match object `ciscomcd_profile_fqdn` resource on a per-domain (or set of domains) basis.
- Adds support for creating an Azure Resource Group (RG) as part of the service VNet `ciscomcd_service_vpc` resource. The RG is required such that all resources orchestrated by the Multicloud Defense Controller will be associated within the specified (or newly created) RG.

Fixes

The following fix is included in this release:

- Fixes an issue where validation was not being performed when configuring a forward or reverse proxy service object `ciscomcd_service_object` resource to require a decryption profile `ciscomcd_profile_decryption` to be assigned to the tls_profile argument when using a secure proxy (TLS, HTTPS, WEBSOCKETS) value assigned to the `transport_mode` argument. If a secure proxy is configured, it must have a decryption profile assigned otherwise the proxy will not operate as a secure proxy and TLS encrypted traffic will be denied.

Version 0.2.4 August 22, 2023

Enhancements

The following enhancements are included in this release:

- Enhances the forward proxy service object `ciscomcd_service_object` resource 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 Multicloud Defense Gateway `ciscomcd_gateway` resource to perform a blue/green gateway replacement when a change to assign_public_ip setting is made.

Fixes

The following fixes are included in this release:

- Fixes an issue where an FQDN Profile `ciscomcd_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.
- Fixes an issue where an update to the policy rules `ciscomcd_policy_rule_set` resource could take a longtime and generate an RPC error.