Multicloud Defense Controller Features and Enhancements

Version 24.10 October 29, 2024

The following features and enhancements are included in this release:

Features

AWS CloudWAN

Multicloud Defense now provides the option to utlize AWS CloudWAN in tandem with service VPCs and network segments. AWS CloudWAN simplifies the process of building, managing, and monitoring a global network that connects your data centers, branch offices, and cloud resources. See Create a Service VPC or VNet for more information.

Log Forwarding Profile with Webhooks

You can now create a log forwarding profile with a generic webhook as the destination. Webhooks can enable real-time data transfer, are ideal for an event-driven architecture or centralized logging, as well as support automation and integration with other third-party services. See Webhook for more information.

Enhancements

Integration with Cisco Talos Intelligence

Multicloud Defense now uses Cisco Talos Intelligence for FQDN and URL lookups. Cisco Talos is one of the most trusted threat intelligence research teams on the globe, comprised of world-class researchers, analysts, incident responders, and engineers. See Intelligence Categories for more information.

Dashboard and Navigation Display

Starting with Version 24.10, the Multicloud Defense Controller is updating and improving the general look and feel of the dashboard appearance as well as the navigation to certain functions with Magnetic. This helps unify the dashboard with other Cisco products and creates a universally streamlined display. This is an ongoing effort.

Version 24.09 September 30, 2024

The following features and enhancements are included in this release:

Feature

Beta: AWS CLoudWAN Support

Enhancements

Network Visibility Report

The network visibility report now includes a summary of activity.

GCP Load-Balancer

GCP now uses a single load-balancer for both TCP and UDP traffic. By streamlining the the work to a single load balancer, configuration and maintenance tasks are simplified which reduces the complexity of your network infrastructure and improved resource utilization.

Version 24.08 September 3, 2024

Fixes

The following fixes are included in this release:

- Improves FQDN object matching functionality.
- Improves general performance.

Version 24.07 August 17, 2024

Features

The following feature is included in this release:

- Support for OCI real-time discovery events.

Fixes

The following fixes are included in this release:

- Improved report generation in event batching to support up to 250K for pagination.

- Fixes an issue where session summary events configured for **No Log Action** continued to generate a logged event. With this fix there is no event logged when this configuration is selected.
- Fixes an issue where syslog forwarding did not include all logging types.
- Updated the list of permissions required for connecting to an OCI account.

Version 24.06 June 26, 2024

Features

The following features are included in this release:

Site-to-Site VPN Tunnel Connections

You can now create site-to-site VPN tunnel connections with the following cloud service providers and platforms:

- Amazon Web Services (AWS)
- Microsoft Azure
- Google Cloud Platform (GCP)
- Cisco ASA managed by , formerly known as "Cisco Defense Orchestrator"

  Multicloud Defense Gateways
- Extranet devices

Use a Multicloud Defense Gateway as either endpoint, or create an environment where Multicloud Defense Gateway acts as both endpoints. Secure your gateways with either a BGP or IPSec profile to finetune the configuration for your specific environmnent. See Site-to-Site VPN Tunnel Connection for more information.

Dynamic Object Sharing

You can now share, create and deploy, and modify objects that are shared with different platforms and immediately have any changes identifed and updated. See Shared Objects for more informaiton.

Azure NAT Gateways

You can now create a service VPC with the intention of attaching it to a Network Address Translation (NAT) gateway in an egress Azure deployment. See Egress Gateways for more information.

Use an Azure Load Balancer in Your Gateway

You can now opt to use a load balancer created in the Azure dashboard instead of the the load balancer that Multicloud Defense provides when you create a gateway. See Advanced Gateway Configuration: Use Your Own Load Balancer for more information.

Miscellaneous

- Performance improvements.
- Operational improvements.
- Bug fixes and stability improvements.

Version 24.02 February 26, 2024

Features

The following features are included in this release:

Hybrid Cloud

- (Private Preview) Site-to-site VPN (requires Multicloud Defense Gateway version 24.02 or later).

Orchestration

- Cross-Subscription Spoke VNet protection (Azure).
- Route table creation for Spoke VPC/VNet protection.
- LB Health Check Security Group orchestration.

Gateway

- Reduced disk size for all Gateway instance types.
- Enable/Disable Gateway SSH access.
- Upgrade Gateway from Details page.
- Cancel Gateway upgrade.
- Instance level actions (terminate protect, replace instance, restart datapath).

Integrations

- Dynamically track changes to cloud service provider-certificates.
- User management with Azure Active Directory.

Miscellaneous

- Performance improvements.
- Operational improvements.
- Bug fixes and stability improvements.

Enhancements

The following enhancements are included in this release:

- (Private Preview) Added support for site-to-site VPN. This includes VPN tunnel configuration, including IPSec and BGP. The VPN is terminated directly on the gateway to process and protect traffic flowing across the VPN. This enhancement requires Multicloud Defense Gateway version 24.02 or later.
- Adds support for orchestrating route tables in spoke VPCs and VNets to ensure traffic originating or returning from the spoke VNet/VPC and route to the service VPC/VNet containing the Multicloud Defense Gateway. This enhancement includes a workflow for create route tables and route entries, and associating the route tables with subnets.

- Adds support for cross-subscription spoke VNet protection by orchestrating spoke VNet peering to route traffic from the spoke VNet to the services VNet containing Multicloud Defense. This ensures the orchestration in Azure is parity with similar orchestrations in AWS and GCP.
- Adds support for orchestrating the security group, network security group, and firewall rules CIDRs related to health checks from the cloud service provider load balancer (Azure, GCP, OCI) or heath check service (GCP).
- Adds support for enabling and disabling SSH from the **Gateway Details** page to accommodate reverse SSH using Teleport. Requires Multicloud Defense Gateway version 23.10 or later, which supports Teleport integration.
- Adds support for upgrading the Multicloud Defense Gateway from the **Gateway Details** page.
- Adds the ability to cancel (abort) a Multicloud Defense Gateway upgrade.
- Adds gateway instance-level actions (terminate protect, replace instance, restart datapath).
- Reduces the disk size for all instances in all cloud service providers from 256GB to 128GB.
- 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 controller instructs 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 will be generated.
- When selecting a region for gateway deployment, a region friendly name should be displayed for all regions along with the true region name (lowercase name). This enhancement ensures that all regions are displayed with both the friendly and true region names.
- Adds support for configuring the Multicloud Defense Controller to integrate with Azure Active Directory for authentication.
- Improves performance of various resource view pages to reduce number of API calls and improve overall load times.
- Adds pagination support for **Traffic Summary** page to improve performance.
- Adds pagination support for **Stats** page to improve performance.

Fixes

The following fixes are included in this release:

- Fixes an issue where the Inventory and Discovery views would not display asset information if the region does not include a gateway deployment.
- Fixes an issue where deployment of an ingress gateway Azure would not be successful if the ingress policy rule set is empty.
- Fixes an issue where log forwarding to an S3 bucket would not work if the log forward profile is used in a group log forwarding profile.
- Fixes an issue where deleting the gateway from the UI does not fully delete the gateway on the backend inhibiting deploying a replacement gateway with the same name.
- Fixes an issue where disabling assign public IP addresses for a gateway deployed in Azure performs a blue/green gateway replacement, but does still assigns public IPs.

- Fixes an issue where the first category and FQDN Row of an FQDN filter profile could not be deleted.
- Fixes an issue to ensure the gateway names in the gateway filter are sorted alphabetically.
- Fixes an issue with export to Terraform for account and gateway resources where the resulting exported Terraform was empty.
- Fixes an issue where the policy rule set Status would show as **Updating** even though the gateway policy Status is shown as **Updated**.
- Fixes an issue where a scale out would be unsuccessful due to a health check failure even though the instance is healthy.
- Changes the health check unhealthy time period to 120 seconds. When a new gateway is deployed, the load balancer heath check or health check service will be orchestrated to evaluate an instance health over a 2 minute (120 second) period. The previous orchestration would evaluate over a 20 second period.
- Fixes an issue to ensure the time zone select defaults to **Local** rather than **UTC**.
- Fixes an issue in the **Stats** page where CPU metric was always showing an order of magnitude less than what should be shown.
- Fixes an issue with deleting a spoke VPC peering in GCP where the spoke VPC would not be deleted. This issue occurs only when the VPC ID was used instead of the self-link.
- Fixes consistency issues with the display of **Last Modified** information across resources.
- Fixes various UI-related resource links where the link would not redirect to the linked resource.
- Fixes various UI-related issues related to advanced search.
- Fixes various UI workflows to ensure proper behavior

Version 23.12 December 14, 2023

Features

The following features are included in this release:

Orchestration

- User-supplied NLB IP for gateway creation in GCP.
- GCP health check CIDRs in datapath firewall rule.

Policy

- Apply ICMP policy to gateways across cloud service providers.

Integrations

- Multiple Syslog Servers in log forwarding group.

Usability

- Additional fields for filtering and advanced search.

- SNAT configuration display in policy rule set.

Miscellaneous

- Performance improvements.
- Operational improvements.
- Bug fixes and stability improvements.

Enhancements

The following enhancements are included in this release:

- Adds fields to Advanced Search that were initially not available.
- Enhances the gateway creation in GCP to allow a user-provided IP resource to be used as the load balancer frontend IP. This can only be supplied when using Terraform.
- Adds display of the service object SNAT setting in the policy rule set view.
- Relaxes the hard requirement for a cloud service provider to support ICMP to apply an ICMP policy to a gateway that is deployed in that cloud service provider. A policy rule set that contains an ICMP policy can now be applied to any gateway that resides in any cloud service provider, whether or not the cloud service provider supports ICMP.
- Adds support for more than one Syslog Server configuration in a log forwarding group.
- Adds GCP health check CIDRs when orchestrating datapath firewall rule.

Fixes

The following fixes are included in this release:

- Fixes an issue where the log forwarding profile for Splunk was showing unreachable even though the Splunk endpoint was reachable.
- Fixes an issue where de-orchestrating an AWS Service VPC would not fully clean up all VPC resources, including the VPC itself.
- Fixes an issue where all address objects would be displayed when a user is creating or editing a reverse proxy service object. Only reverse proxy service objects are now being displayed.
- Fixes an issue where the controller was using an incorrect Project ID when orchestrating a gateway into a GCP shared VPC scenario.
- Fixes an issue where the list of address objects was not showing in the drop down when creating or modifying a group address object.
- Fixes the typeahead search for cloud service provider account in the create gateway workflow.
- Fixes an issue when adding a rule within the policy rule set to improve the performance and ensure the operation is quick.
- Fixes an issue where adding an AWS account through the page, formerly known as "Cisco Defense Orchestrator", could result in a timeout.

- Fixes the count issue for FQDN match and FQDN filtering objects. The counts were representing both types of objects in each view.
- Fixes various advanced search and filter issues.
- Fixes an issue where deploying a gateway into Azure when Azure has no available capacity would fail deployment and not clean up the created resources. When Azure has no capacity, it does not inhibit creating a virtual machine and its associated resources. It creates the VM, but brings up the VM in a failed state with an error message. This scenario needed to be handled in a specific way to ensure that it is recognized, the proper action is taken to clean up the resources and the user is made aware of the cloud service provider issue through a system log message.
- Fixes an issue where the cloud service provider resource and capacity information is not displayed when deploying a gateway in Azure.
- Improves the performance of displaying the list of rules in a policy rule set.
- Fixes an issue where deleting the GCP-based account would not delete all of the inventory objects related to inventory discovery.
- Addresses an issue with gateway instance per-zone rows that would inhibit a user from removing the first row. This only applies to scenarios where the gateway is deployed into a user-managed VPC or VNet.
- Fixes an issue where deploying a gateway into GCP would not orchestrate the egress route into the orchestrated service VPC.
- Fixes an issue where orchestrating spoke VPC protection could fail.
- Corrects an issue where the SNI and L7 DOS profiles would not be displayed when editing a reverse proxy service object.
- Fixes an issue where a UI change operation to the assign public IPs settings could trigger an unnecessary blue/green gateway replacement.
- Fixes an issue where orchestrating a gateway into multiple GCP regions could result in a race condition that would inhibit the gateway from becoming active.
- Fixes an issue where a new gateway deployment would become immediately inactive due to an internal error.
- Fixes an issue where a forwarding or forward proxy policy rule set that was created by Terraform would be displayed in the UI as a reverse proxy rule.
- Fixes an issue where rules could not be reordered when editing a policy rule set.
- Fixes an issue where a service object that contained more than 20 rows would be accepted and pushed to the gateway resulting in a gateway crash. The service object is now limited to 20 rows. This limit validation is performed by both the controller and gateway.
- Fixes an issue to ensure the Gateway Details page displays the date modified and data created times.
- Fixes an issue with proper sorting for views containing objects and profiles that span multiple pages.
- Improves performance of various object creation pages.
- Improves the user experience through fixes and enhancements throughout the UI.

- Ensures the user-specified time setting of local or UTC is honored across views and persists across portal invocations. The persistence across portal invocations is achieved by storing this setting in the browser cache.
- Fixes a UI issue where the tooltip information was missing for custom managed Encryption Key gateway configuration.
- Ensures the controller generates System Log messages when the gateway fails to become active due to cloud service provider errors.