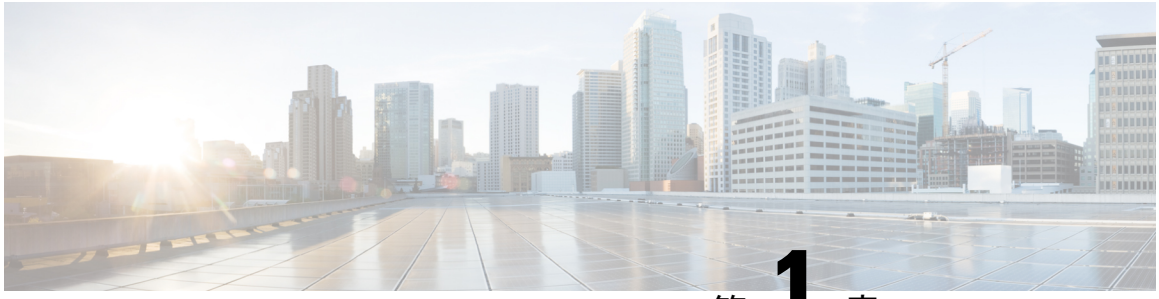
Cisco Multicloud Defense リリースノート

最終更新：2025 年 3 月 20 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

目 次



第 1 章

ようこそ

Multicloud Defense について

Multicloud Defense（MCD）は、Multicloud Defense Controller と Multicloud Defense Gateway の 2 つの主要コンポーネントで構成される包括的なセキュリティソリューションです。これらのコンポーネントが連携してセキュアなマルチクラウド環境を確立します。

Multicloud Defense は現在、Amazon Web Services（AWS）、Azure、Google Cloud Platform（GCP）、および Oracle OCI クラウドアカウントをサポートしています。これらのプラットフォームのサポート範囲はさまざまです。

本質的に、Multicloud Defense は高機能の合理化されたセキュリティフレームワークを提供し、コントローラのオーケストレーション、ゲートウェイ通信、および最適化されたデータパス処理を調和させ、堅牢で効率的なマルチクラウド保護メカニズムを実現します。

このドキュメントは、パブリック クラウド ネットワーキングとセキュリティの概念の基本を理解するために準備されており、以下を含むさまざまな職務チームに参加する実務者を対象としています。

- 開発（DevOps および DevSecOps）
- セキュリティ オペレーション センター（SOC）
- セキュリティアーキテクト情報
- セキュリティ アーキテクト クラウド アーキテクト

Multicloud Defense に関するその他の資料

Multicloud Defense の詳細については、次のドキュメントを参照してください。

- Multicloud Defense Release Notes

推奨バージョン

各 Multicloud Defense コンポーネントには、次のリリースを使用することを強くお勧めします。

Multicloud Defense Gateway

バージョン 24.06-08（2025 年 1 月 16 日）

Multicloud Defense Terraform Provider

バージョン 0.2.9（2024 年 11 月 15 日）

付加的なリソースと支援

オンラインリソース

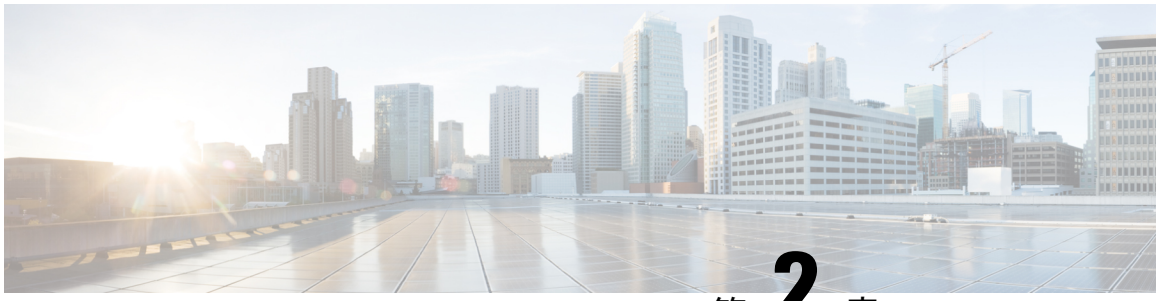
シスコは、次の追加資料を用意しています。

- Cisco Multicloud Defense User Guide [英語]
- Cisco Multicloud Defense に関する FAQ

シスコへのお問い合わせ

上記のオンライン リソースでは問題を解決できない場合は、Cisco TAC にお問い合わせください。

- Cisco TAC の電子メール アドレス：tac@cisco.com
- Cisco TAC の電話番号（北米）：1.408.526.7209 または 1.800.553.2447
- Cisco TAC の連絡先（世界全域）：Cisco Worldwide Support の連絡先



第 2 章

Multicloud Defense Controller の機能および機能拡張

バージョン 25.01（2025 年 1 月 6 日）

拡張機能

このリリースには、次の機能拡張が含まれています。

- UI のルックアンドフィールが向上します。
- 全体的なパフォーマンスが向上します。

バージョン 24.12（2024 年 12 月 2 日）

機能

このリリースには、次の機能が含まれています。

アクティブセッションと定期セッションのトラフィック概要の改善

以前は、イベントは接続セッションが閉じられたか、終了された場合にのみ利用可能でした。トラフィックの概要で、セッションがアクティブな5分ごとにイベントを投稿するようになりました。この機能は、一度にいくつのセッションが進行中であるかを調べるのに役立ちます。概要ページの [すべてのイベント（All Events）] チェックボックスを選択して、開いている接続のリストを展開し、チェックボックスをオフにすると、閉じているセッションだけが表示されます。

AI Defense（プライベートプレビュー）

Multicloud Defense は、生成 AI アプリケーションを検出して保護するための AI Defense のプライベートプレビューをサポートするようになりました。詳細については、シスコまでお問い合わせください。

バージョン 24.10（2024 年 10 月 29 日）

このリリースには、次の機能と機能拡張が含まれています。

機能

AWS CloudWAN

Multicloud Defense で、サービス VPC とネットワークセグメントと組み合わせて AWS CloudWAN を使用するオプションが提供されるようになりました。AWS CloudWAN は、お客様のデータセンター、分散拠点、クラウドリソースを接続するグローバルネットワークを構築、管理、監視するプロセスを簡素化します。詳細については、「Create a Service VPC or VNet」を参照してください。

ウェブフックを使用したログ転送プロファイル

汎用ウェブフックを宛先として使用してログ転送プロファイルを作成できるようになりました。ウェブフックは、リアルタイムのデータ転送を可能にし、イベント駆動型アーキテクチャまたは集中型ロギングに最適であるだけでなく、自動化や他のサードパーティサービスとの統合もサポートします。詳細については、「Webhook」を参照してください。

拡張機能

Cisco Talos インテリジェンスとの統合

Multicloud Defense では、FQDN および URL のルックアップに Cisco Talos インテリジェンスを使用するようになりました。Cisco Talos は、世界中で最も信頼できる脅威インテリジェンス調査チームの 1 つであり、世界クラスの研究者、アナリスト、インシデント対応者、およびエンジニアで構成されています。詳細については、「Intelligence Categories」を参照してください。

ダッシュボードとナビゲーションの表示

バージョン 24.10 以降、Multicloud Defense Controller が更新され、ダッシュボードの外観の一般的なルックアンドフィールと、Magnetic を使用した特定の機能へのナビゲーションが改善されています。これにより、ダッシュボードを他のシスコ製品と統合し、全体的に合理化された表示を作成できます。これは継続的な取り組みです。

バージョン 24.09（2024 年 9 月 30 日）

このリリースには、次の機能と機能拡張が含まれています。

機能

ベータ版：AWS CloudWAN のサポート

拡張機能

ネットワークの可視性レポート

ネットワークの可視性レポートに、アクティビティの概要が含まれるようになりました。

GCP ロードバランサ

GCP では、TCP トラフィックと UDP トラフィックの両方に単一のロードバランサが使用されるようになりました。作業を単一のロードバランサに合理化することで、構成およびメンテナンスタスクが簡素化され、ネットワークインフラストラクチャの複雑さが軽減され、リソース使用率が向上します。

バージョン 24.08（2024 年 9 月 3 日）

修正

このリリースには、次の修正が含まれています。

- FQDN オブジェクトの照合機能が改善されます。
- 全体的なパフォーマンスが向上します。

バージョン 24.07（2024 年 8 月 17 日）

機能

このリリースには、次の機能が含まれています。

- OCI リアルタイム検出イベントのサポート。

修正

このリリースには、次の修正が含まれています。

- ページネーションで最大 250K をサポートするためのイベントバッチ処理でのレポート生成が改善されました。

- **ログなしアクション**に設定されたセッションサマリーイベントが、ログ記録ありのイベントを生成し続ける問題を修正します。この修正により、この設定が選択されている場合、イベントはログに記録されません。
- syslog 転送にすべてのロギングタイプが含まれていない問題を修正します。
- OCI アカウントに接続するために必要な権限のリストを更新しました。

バージョン 24.06（2024 年 6 月 26 日）

機能

このリリースには、次の機能が含まれています。

サイト間 VPN トンネル接続

次のクラウドサービスプロバイダーとプラットフォームを使用してサイト間 VPN トンネル接続を作成できるようになりました。

- Amazon Web Services（AWS）
- Microsoft Azure
- Google Cloud Platform（GCP）
- （旧 Cisco Defense Orchestrator）により管理される Cisco ASA

  Multicloud Defense Gatewayについて
- エクストラネットデバイス

Multicloud Defense Gateway をいずれかのエンドポイントとして使用するか、Multicloud Defense Gateway が両方のエンドポイントとして機能する環境を作成します。BGP または IPSec プロファイルのいずれかでゲートウェイを保護し、特定の環境に合わせて構成を微調整します。詳細については、「Site-to-Site VPN Tunnel Connection」を参照してください。

ダイナミックオブジェクト共有

異なるプラットフォームで共有されるオブジェクトを共有、作成、展開、および変更し、すぐに変更が識別されて更新されるようになりました。詳細については、「Shared Objects」を参照してください。

Azure NAT ゲートウェイ

出力 Azure 展開のネットワークアドレス変換（NAT）ゲートウェイに接続することを目的として、サービス VPC を作成できるようになりました。詳細については、「Egress Gateways」を参照してください。

ゲートウェイでの Azure ロードバランサの使用

ゲートウェイを作成するときにMulticloud Defenseが提供するロードバランサの代わりに、Azureダッシュボードで作成されたロードバランサの使用を選択できるようになりました。詳細については、「Advanced Gateway Configuration: Use Your Own Load Balancer」を参照してください。

その他

- パフォーマンスの向上.
- 運用の改善。
- バグ修正と安定性の改善。

バージョン 24.02（2024 年 2 月 26 日）

機能

このリリースには、次の機能が含まれています。

ハイブリッド クラウド

- （プライベートプレビュー）サイト間 VPN（Multicloud Defense Gateway バージョン 24.02 以降が必要）。

オーケストレーション

- クロスサブスクリプション スポーク VNet 保護（Azure）。
- スポーク VPC/VNet 保護のためのルートテーブルの作成。
- LB ヘルス チェック セキュリティ グループのオーケストレーション。

ゲートウェイ（Gateway）

- すべてのゲートウェイ インスタンス タイプのディスクサイズが削減されました。
- ゲートウェイ SSH アクセスを有効または無効にします。
- [詳細（Details）] ページからゲートウェイをアップグレードします。
- ゲートウェイのアップグレードをキャンセルします。
- インスタンスレベルのアクション（保護の終了、インスタンスの置換、データパスの再起動）。

統合

- クラウド サービス プロバイダー証明書の変更を動的に追跡します。
- Azure Active Directory によるユーザー管理。

その他

- パフォーマンスの向上.
- 運用の改善。
- バグ修正と安定性の改善。

拡張機能

このリリースには、次の機能拡張が含まれています。

- （プライベートプレビュー）サイト間 VPN のサポートを追加しました。これには、IPSec および BGP を含む VPN トンネルの設定が含まれます。VPN は、VPN を通過するトラフィックを処理および保護するために、ゲートウェイで直接終端されます。この機能拡張には、Multicloud Defense Gateway バージョン 24.02 以降が必要です。
- スポーク VPC および VNet でルートテーブルを調整するためのサポートが追加され、トラフィックがスポーク VNet/VPC から送受信され、Multicloud Defense Gateway を含むサービス VPC/VNet にルーティングされるようにします。この機能拡張には、ルートテーブルとルートエントリを作成するワークフロー、およびルートテーブルとサブネットの関連付けが含まれています。
- スポーク VNet ピアリングをオーケストレーションして、スポーク VNet から Multicloud Defense を含むサービス VNet にトラフィックをルーティングすることにより、クロスサブスクリプション スポーク VNet 保護のサポートが追加されます。これにより、Azure のオーケストレーションが AWS および GCP の同様のオーケストレーションと同等になります。
- クラウド サービス プロバイダーのロードバランサ（Azure、GCP、OCI）またはヘルスチェックサービス（GCP）からのヘルスチェックに関連するセキュリティグループ、ネットワーク セキュリティ グループ、およびファイアウォールルール CIDR をオーケストレーションするためのサポートを追加します。
- テレポートを使用したリバース SSH に対応するために、[ゲートウェイの詳細（Gateway Details）]ページから SSH を有効または無効にするためのサポートを追加します。テレポート統合をサポートする Multicloud Defense Gateway バージョン 23.10 以降が必要です。
- [ゲートウェイの詳細（Gateway Details）] ページから Multicloud Defense Gateway をアップグレードするためのサポートを追加します。
- Multicloud Defense Gateway のアップグレードをキャンセル（中止）する機能を追加します。
- ゲートウェイのインスタンスレベルのアクション（保護の終了、インスタンスの置換、データパスの再起動）を追加します。
- すべてのクラウド サービス プロバイダーのすべてのインスタンスのディスクサイズを 256GB から 128GB に削減します。
- 秘密キーがクラウドサービス プロバイダーに保存されて Multicloud Defense Gateway によって取得される、証明書オブジェクトへの変更を動的に追跡するためのサポートが追加されます。クラウドサービスプロバイダーのリソースに変更があった場合、コントローラは、ゲートウェイに対して、クラウド サービス プロバイダーのリソースの秘密キーを再読み

取りして、アクセス可能であること、および更新されたコンテンツが使用されることを確認するように指示します。証明書へのアクセスで問題が発生した場合は、システムログメッセージが生成されます。

- ゲートウェイ展開用のリージョンを選択する場合、すべてのリージョンのリージョンフレンドリ名を実際のリージョン名（小文字の名前）とともに表示する必要があります。この機能拡張により、すべてのリージョンがリージョンフレンドリ名と実際のリージョン名の両方で表示されるようになります。
- 認証のために Azure Active Directory と統合するように Multicloud Defense Controller を設定するためのサポートが追加されます。
- さまざまなリソースビューページのパフォーマンスを向上させ、API コールの数を減らし、全体的な読み込み時間を改善します。
- パフォーマンスを向上させるために、[トラフィックの概要（Traffic Summary）] ページにページネーションのサポートを追加します。
- パフォーマンスを向上させるために、[統計（Stats）] ページにページネーションのサポートを追加します。

修正

このリリースには、次の修正が含まれています。

- リージョンにゲートウェイの展開が含まれていない場合、インベントリビューと検出ビューにアセット情報が表示されない問題を修正します。
- 入力ポリシー規則セットが空の場合、イングレスゲートウェイ Azure の展開が成功しない問題を修正します。
- ログ転送プロファイルがグループのログ転送プロファイルで使用されている場合、S3 バケットへのログ転送が機能しない問題を修正します。
- UI からゲートウェイを削除しても、バックエンドのゲートウェイが完全に削除されず、同じ名前の置換ゲートウェイの展開を妨げる問題を修正します。
- Azure に展開されたゲートウェイに対するパブリック IP アドレスの割り当てを無効にすると、青色/緑色ゲートウェイの置換が実行されても、引き続きパブリック IP が割り当てられる問題を修正します。
- FQDN フィルタプロファイルの最初のカテゴリと FQDN 行を削除できなかった問題を修正します。
- ゲートウェイフィルタ内のゲートウェイ名がアルファベット順にソートされるように問題を修正します。
- アカウントおよびゲートウェイリソースの Terraform へのエクスポートで、エクスポートされた Terraform が空になる問題を修正します。

- ゲートウェイポリシーの [ステータス（Status）] が [更新（Updated）] と表示されているにもかかわらず、ポリシー規則セットの [ステータス（Status）] が [更新中（Updating）] と表示される問題を修正します。
- インスタンスが正常であっても、ヘルスチェックが失敗したためにスケールアウトが失敗する問題を修正します。
- ヘルスチェックが異常とする期間を 120 秒に変更します。新しいゲートウェイが展開されると、ロードバランサのヘルスチェックまたはヘルスチェックサービスがオーケストレーションされ、2 分（120 秒）の期間でインスタンスの正常性が評価されます。以前のオーケストレーションは 20 秒の期間で評価されました。
- タイムゾーンの選択がデフォルトで [UTC] ではなく [ローカル（Local）] になるように問題を修正します。
- CPU メトリックが表示されるはずの値よりも常に小さい値で表示される [統計（Stats）] ページの問題を修正します。
- スポーク VPC が削除されない、GCP でのスポーク VPC ピアリングの削除に関する問題を修正します。この問題は、セルフリンクの代わりに VPC ID が使用された場合にのみ発生します。
- リソース全体での [最終変更日（Last Modified）] 情報の表示に関する一貫性の問題を修正します。
- リンクがリンク先のリソースにリダイレクトされない、さまざまな UI 関連のリソースリンクを修正します。
- 詳細検索に関するさまざまな UI 関連の問題を修正します。
- さまざまな UI ワークフローを適切に動作するように修正します

バージョン 23.12（2023 年 12 月 14 日）

機能

このリリースには、次の機能が含まれています。

オーケストレーション

- GCP でのゲートウェイ作成用にユーザーが指定した NLB IP。
- データパスファイアウォール規則の GCP ヘルスチェック CIDR。

ポリシー

- クラウド サービス プロバイダー全体のゲートウェイに ICMP ポリシーを適用します。

統合

- ログ転送グループ内の複数の Syslog サーバー。

ユーザビリティ

- フィルタリングおよび詳細検索用の追加フィールド。
- ポリシー規則セットの SNAT 設定の表示。

その他

- パフォーマンスの向上.
- 運用の改善。
- バグ修正と安定性の改善。

拡張機能

このリリースには、次の機能拡張が含まれています。

- 最初は使用できなかったフィールドを詳細検索に追加します。
- GCP でのゲートウェイの作成を強化し、ユーザーが提供する IP リソースをロードバランサのフロントエンド IP として使用できるようにします。Terraform を使用している場合にのみ指定できます。
- ポリシー規則セットビューにサービスオブジェクト SNAT 設定の表示を追加します。
- クラウド サービス プロバイダーに展開されるゲートウェイに ICMP ポリシーを適用するには、そのクラウド サービス プロバイダーが ICMP をサポートする必要があるという厳しい要件を緩和します。ICMP ポリシーを含むポリシー規則セットは、クラウド サービス プロバイダーが ICMP をサポートしているかどうかに関係なく、任意のクラウドサービス プロバイダーに存在するすべてのゲートウェイに適用できるようになりました。
- ログ転送グループで複数の Syslog サーバー設定のサポートを追加します。
- データパスファイアウォール規則をオーケストレーションするときに、GCP ヘルスチェック CIDR を追加します。

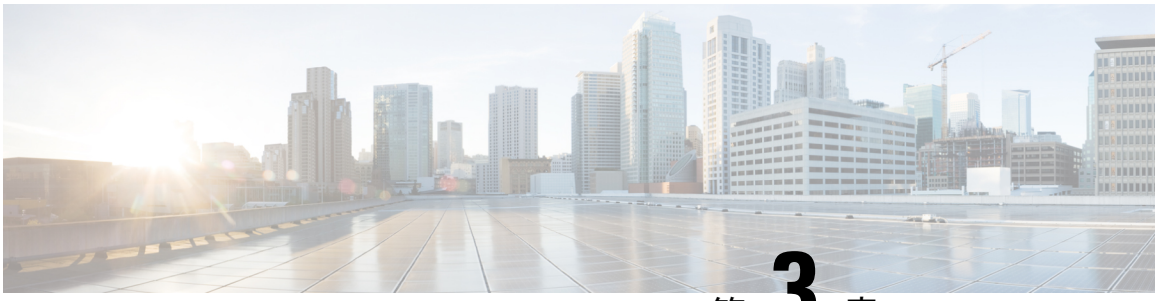
修正

このリリースには、次の修正が含まれています。

- Splunk エンドポイントが到達可能であるにもかかわらず、Splunk のログ転送プロファイルが到達不能と表示されていた問題を修正します。
- AWS サービス VPC のオーケストレーションを解除しても、VPC 自体を含むすべての VPC リソースが完全にクリーンアップされない問題を修正します。
- ユーザーがリバース プロキシ サービス オブジェクトを作成または編集しているときに、すべてのアドレスオブジェクトが表示される問題を修正します。リバース プロキシ サービス オブジェクトだけが表示されるようになりました。

- ゲートウェイを GCP 共有 VPC シナリオにオーケストレーションするときに、コントローラが誤ったプロジェクト ID を使用していた問題を修正します。
- グループ アドレス オブジェクトを作成または変更するときに、アドレスオブジェクトのリストがドロップダウンに表示されない問題を修正します。
- ゲートウェイ作成ワークフローでのクラウド サービス プロバイダー アカウントの先行入力検索を修正します。
- ポリシー規則セット内で規則を追加する際の問題を修正して、パフォーマンスを向上させ、操作を迅速に行えるようにします。
- [Security Cloud Control] ページ（旧 Cisco Defense Orchestrator）から AWS アカウントを追加すると、タイムアウトが発生する可能性がある問題を修正します。
- FQDN一致およびFQDNフィルタリングオブジェクトのカウントの問題を修正します。カウントは、各ビューの両方のタイプのオブジェクトを表していました。
- さまざまな高度な検索とフィルタの問題を修正します。
- Azure に利用可能なキャパシティがない場合に Azure にゲートウェイを展開すると、展開が失敗し、作成されたリソースがクリーンアップされない問題を修正します。Azureにキャパシティがなくても、仮想マシンとその関連リソースの作成が妨げられることはありません。VM は作成されますが、エラーメッセージを表示して障害状態で VM が起動されます。このシナリオが認識され、リソースをクリーンアップするための適切なアクションが実行されて、システムログメッセージを通じてクラウド サービス プロバイダーの問題がユーザーに通知されるようにするには、特定の方法で処理する必要がありました。
- Azure にゲートウェイを展開するときに、クラウド サービス プロバイダーのリソースとキャパシティの情報が表示されない問題を修正します。
- ポリシー規則セット内の規則のリストを表示するパフォーマンスが向上します。
- GCPベースのアカウントを削除しても、インベントリ検出に関連するすべてのインベントリオブジェクトが削除されない問題を修正します。
- ゲートウェイインスタンスのゾーンごとの行で、ユーザーが最初の行を削除できない問題に対処します。これは、ゲートウェイがユーザー管理の VPC または VNet に展開されるシナリオにのみ適用されます。
- ゲートウェイを GCP に展開しても、オーケストレーションされたサービス VPC への出力ルートがオーケストレーションされない問題を修正します。
- スポーク VPC 保護のオーケストレーションが失敗する可能性がある問題を修正します。
- リバース プロキシ サービス オブジェクトの編集時に SNI および L7 DOS プロファイルが表示されない問題を修正します。
- パブリック IP の割り当て設定の UI 変更操作により、不要な青色/緑色ゲートウェイの置換がトリガーされる可能性がある問題を修正します。

- 複数の GCP リージョンへのゲートウェイのオーケストレーションにより競合状態が発生し、ゲートウェイがアクティブになるのを妨げる可能性がある問題を修正します。
- 内部エラーが原因で新しいゲートウェイの展開がすぐに非アクティブになる問題を修正します。
- Terraform によって作成された転送または転送プロキシポリシー規則セットがリバースプロキシ規則として UI に表示される問題を修正します。
- ポリシー規則セットの編集時にルールの順序を変更できない問題を修正します。
- 20 を超える行を含むサービスオブジェクトが受け入れられてゲートウェイにプッシュされると、ゲートウェイがクラッシュする問題を修正します。サービスオブジェクトは 20 行に制限されました。この制限の検証は、コントローラとゲートウェイの両方で実行されます。
- [ゲートウェイの詳細（Gateway Details）] ページにデータの作成時刻と変更日が表示されるように問題を修正します。
- 複数のページにまたがるオブジェクトとプロファイルを含むビューの適切なソートに関する問題を修正します。
- さまざまなオブジェクト作成ページのパフォーマンスが向上します。
- UI 全体の修正と機能拡張により、ユーザー体験が向上します。
- ユーザー指定のローカルまたは UTC の時間設定がビュー全体で適用され、ポータルの呼び出し全体で保持されるようにします。ポータルの呼び出し全体での永続性は、この設定をブラウザのキャッシュに保存することによって実現されます。
- カスタム管理対象の暗号キーゲートウェイ設定のツールチップ情報が欠落していた UI の問題を修正します。
- クラウド サービス プロバイダーのエラーが原因でゲートウェイがアクティブになることができなかった場合に、コントローラがシステムログメッセージを生成するようにします。



第 3 章

Multicloud Defense Gateway の修正および機能拡張

バージョン 24.06

バージョン 24.06-08-a1（2025 年 1 月 16 日）

これはホットフィックスです。

修正

このホットフィックスには、次の修正が含まれています。

- 転送ポリシーが TLS Client Hello メッセージからサービス名指定（SNI）を取得できず、ゲートウェイが TCP RST との接続を閉じる原因となる問題を修正します。これは、2024 年 4 月に Chrome でポスト量子暗号に移行する変更が行われたことが原因です。この変更により、Client Hello は 1415 バイトより大きくなり、ドメインで照合またはフィルタリングするためにポリシーで使用される SNI を取得できなくなる可能性があります。この修正により、転送ポリシーが 1415 バイトを超える Client Hello サイズをサポートできるようになります。

バージョン 24.06-08（2024 年 1 月 16 日）（推奨）

拡張機能

このリリースには、次の機能拡張が含まれています。

- 追加の暗号スイートが含まれ、これは復号プロファイルの一部として設定でき、TLS ネゴシエーションの転送プロキシまたはリバースプロキシポリシーで使用できます。
- Nginx トレースをオンまたはオフにできる高度なトラブルシューティング設定を提供します。以前のリリースでは、Nginx トレースは、高度なデバッグ設定を介してのみ有効になり、Nginx トレースよりもはるかに多くキャプチャされていました。この設定では、有効にすると Nginx トレースのみが収集されます。この設定は、シスコサポートまたはシスコエンジニアリングによってのみ有効にでき、プロキシのトラブルシューティングで必要な場合に有効にするように意図されています。トレースが収集されると、診断バンドルの Multicloud Defense Controller に送信されます。

修正

このリリースには、次の修正が含まれています。

- 除外されたアドレスオブジェクトで指定された IP/CIDR が Multicloud Defense Gateway ポリシーに適切に適用されなかったグループ アドレス オブジェクトの除外リストの問題を修正します。これにより、包含されたアドレスオブジェクトと除外されたアドレスオブジェクトの両方が適切なトラフィック照合に適用されるようになります。

バージョン 24.06-07-a1（2024 年 12 月 18 日）

このリリースはホットフィックスです。

修正

このホットフィックスには、次の修正が含まれています。

- 転送ポリシーが TLS Client Hello メッセージからサービス名指定（SNI）を取得できず、ゲートウェイが TCP RST との接続を閉じる原因となる問題を修正します。これは、2024 年 4 月に Chrome でポスト量子暗号に移行する変更が行われたことが原因です。この変更により、Client Hello は 1415 バイトより大きくなり、ドメインで照合またはフィルタリングするためにポリシーで使用される SNI を取得できなくなる可能性があります。この修正により、転送ポリシーが 1415 バイトを超える Client Hello サイズをサポートできるようになります

バージョン 24.06-07（2024 年 12 月 18 日）

修正

このリリースには、次の修正が含まれています。

- ルールセットの変更によって、新しいルールセットのゲートウェイへの適用で問題が発生する可能性がある、新しい Talos ルールセットに関連する問題を修正します。ゲートウェイは、ポリシールールセットのステータスが「`Updating...`」の状態でスタックします。この問題は、新しい Talos ルールセットが公開される前に検出されました。この更新で問題が解決され、新しい Talos ルールセットを正常に適用できるようになりました。
- データパスが一時的にスタックし、healthcheck を含むトラフィック処理の問題を引き起こす可能性がある問題を修正します。これが発生すると、ゲートウェイは正常と異常の間で切り替わります。これは一連のシステムログメッセージで確認できます。通常、スタック状態は、コントローラがインスタンスを置換対象としてマークするほど長くは続きません。
- 最終的にデータパスの再起動を引き起こす可能性のある特定の UDP セッションの動作が原因で発生する UDP 接続プールのリークに関連する問題を修正します。データパスの再起動が発生すると、再起動中、インスタンスは異常な状態になります。その異常な期間が十分に長い場合、コントローラはインスタンスを置換対象としてマークします。

バージョン 24.06-06-a1（2024 年 11 月 28 日）

このリリースはホットフィックスです。

修正

このホットフィックスには、次の修正が含まれています。

- 転送ポリシーが TLS Client Hello メッセージからサービス名指定（SNI）を取得できず、ゲートウェイが TCP RST との接続を閉じる原因となる問題を修正します。これは、2024 年 4 月に Chrome でポスト量子暗号に移行する変更が行われたことが原因です。この変更により、Client Hello は 1415 バイトより大きくなり、ドメインで照合またはフィルタリングするためにポリシーで使用される SNI を取得できなくなる可能性があります。この修正により、転送ポリシーが 1415 バイトを超える Client Hello サイズをサポートできるようになります。

バージョン 24.06-06（2024 年 11 月 26 日）

修正

このリリースには、次の修正が含まれています。

- 新しいゲートウェイインスタンスがアクティブになったときに Azure イングレスゲートウェイがクラッシュする可能性がある問題を修正します。

バージョン 24.06-05（2024 年 11 月 22 日）

拡張機能

このリリースには、次の機能拡張が含まれています。

- FIPS テレポートエージェントをゲートウェイに統合して、FIPS（FedRAMP）環境と非 FIPS（商用）環境の両方に対応します。テレポートはデフォルトでは無効になっています。このオプションは、お客様がシスコサポートと連携して高度なトラブルシューティングを行う場合にのみ有効にできます。

修正

このリリースには、次の修正が含まれています。

- イングレスゲートウェイでのトラフィック処理により CPU 使用率が高くなり、不要な自動スケーリングが発生する可能性がある問題を修正します。CPU 使用率が高くなるのは、最初に暗号化されていない HTTP プロキシを使用して接続を処理するポリシーから、HTTP リダイレクションのために暗号化された TCP プロキシに移動した結果です。
- 出力ゲートウェイ転送プロキシポリシーが、トラフィックを適切なポリシー規則に一致させようとして、スタックする可能性がある問題を修正します。
- 長時間のアクティブな接続の一部が適切にアクティブにリセット（TCP RST を送信）されない問題を修正します。
- イングレスゲートウェイのリバースプロキシポリシーでのマルウェアの検出に起因するゲートウェイのクラッシュを修正します。
- UDP セッションが適切にカウントされていなかったアクティブ接続と接続レートに関連する統計の記録を修正します。

バージョン 24.06-04（2024 年 10 月 25 日）

修正

このリリースには、次の修正が含まれています。

- バックエンド接続が応答せず、トラフィックの処理で遅延が発生するプロキシシナリオで、ゲートウェイが不必要に CPU を消費する可能性がある問題を修正します。

バージョン 24.06-03（2024 年 10 月 20 日）

拡張機能

このリリースには、次の機能拡張が含まれています。

- FedRamp 環境に展開されたゲートウェイで使用するために必要な BoringCrypto をサポートする拡張ゲートウェイイメージを提供します。これは Multicloud Defense の FedRamp 準拠に向けた継続的な取り組みです。
- テレポートを介してゲートウェイへの SSH セッションが確立された場合に表示されるカスタムバナーのサポートが追加されます。

修正

このリリースには、次の修正が含まれています。

- Kyber 暗号スイートを含む TLS セッションにより、CPU 使用率が増加し、トラフィックを処理できなくなる可能性がある問題を修正します。
- ゲートウェイインスタンスが置換されたときに、接続ドレイン時間が適用されなかった問題を修正します。
- ポリシーの変更またはゲートウェイインスタンスの置換中にプロキシセッションがアクティブに終了したときに、ゲートウェイのデータパスが自己修復する可能性がある、安定性の問題を修正します。
- 診断バンドルの生成が失敗する可能性がある問題を修正します。
- プロキシポリシーが TLS Client Hello メッセージから SNI を取得できず、ゲートウェイが TCP RST との接続を閉じる原因となる問題を修正します。これは、2024 年 4 月に Chrome でポスト量子暗号に移行する変更が行われたことが原因です。この変更により、Client Hello は 1415 バイトより大きくなり、発行する証明書を決定するためにプロキシで使用されるサーバー名指定（SNI）を取得できなくなる可能性があります。この修正により、プロキシポリシーが 1415 バイトを超える Client Hello サイズをサポートできるようになります。
- FQDN ベースのアドレスオブジェクトで使用されるドメインの DNS への変更がゲートウェイ データパス エージェントによって受信されるが、データパスワーカーに適用されない問題を修正します。これにより、DNS の変更がアドレスオブジェクトの動的性質に適用されず、適切なトラフィック処理に影響を及ぼします。
- デフォルト設定と異なる設定の復号プロファイルがゲートウェイに正しく適用されず、クライアントとゲートウェイ間の暗号スイートの不一致が原因で TLS ネゴシエーションが失敗する問題を修正します。
- ゲートウェイ SSH セッションで使用されるゲートウェイ側の暗号スイートが、脆弱な暗号スイートとしてフラグ付けされている可能性がある問題を修正します。この修正は、最も安全な GCM ベースの暗号スイートにのみ対応します。

- さまざまな安定性の問題を修正します。

バージョン 24.06-02-a2（2024 年 10 月 2 日）

このリリースはホットフィックスです。

修正

このホットフィックスには、次の修正が含まれています。

- 新しいゲートウェイイメージが展開されたときに Multicloud Defense Gateway が一時的にクラッシュする問題を修正します。
- Multicloud Defense Gateway は、ゲートウェイインスタンスを終了するときに、Multicloud Defense Controller で設定されたドレイン時間値を適用するようになりました。

バージョン 24.06-02（2024 年 9 月 18 日）

拡張機能

このリリースには、次の機能拡張が含まれています。

- FedRAMP CIS レベル 2 の強化に対応するために、ゲートウェイの機能拡張を継続しています。

修正

このリリースには、次の修正が含まれています。

- 空の FQDN/URL フィルタリングプロファイルがポリシー規則セットに割り当てられている場合に、ゲートウェイが自己修復する問題を修正します。
- 6 タプル一致としてのドメインの使用に関連する拒否ルールアクションの問題を修正します。最初のルール一致が 6 タプル一致（割り当てられた FQDN 一致プロファイルを含む）で、ポリシーアクションが**拒否**に設定されている場合、拒否アクションは 5 タプル一致に基づいて設定され、一致対象にドメインは含まれません。この修正により、ルールとそのアクションを評価するときに、6 つのタプルすべてが適用されるようになります。トラフィックが 6 タプル一致に基づくルールでは一致しない場合、トラフィックは後続のルールまで一致するようにして、一致したルールの設定に基づいてアクションを実行します。
- ポリシーの更新が適用された後、Azure イングレスゲートウェイがヘルスチェックの保留状態でスタックする問題を修正します。この問題には、新しいゲートウェイの展開も含まれます。
- 6 タプル一致としてのドメインの使用に関連する許可ルール一致の問題を修正します。最初のルール一致が 6 タプル一致（割り当てられた FQDN 一致プロファイルを含む）で、ポリシーアクションが**許可**に設定され、最初のルールの 5 タプル一致と整合性のある後続の

ルールがない場合、すべてのドメインは許可され、ドメインは拒否されます。この修正により、ルールに一致するドメインのみが許可され、他のすべてのドメインは拒否されるようになります

- 復号ベースの転送プロキシ（TLS、HTTPS、WebsocketS）を使用するイーグレスポリシーのルールセットが最初に 5 タプルで一致し、SNI からドメインを取得しても、6 番目のタプルに基づいて一致の絞り込みを実行せず、TLS エラーが発生する問題を修正します。この修正により、6 タプル一致の絞り込みが実行され、トラフィックが適切な復号ルールによって正常に処理されるようになります。
- **[トラフィックの概要（Traffic Summary）]** > **[イベント（Event）]** で SNI が記録されない、TLS ネゴシエーションエラーのあるセッションの問題を修正します。
- 転送プロキシのフル復号化セッションごとに複数の SNI イベントが記録されていた問題を修正します。
- アドレスグループのサイズを超えると、サイズを超えるすべての IP/CIDR がアドレスグループに含まれなくなる可能性がある問題を修正します。アドレスグループのサイズが 20k の IP/CIDR に増加しました。
- ゲートウェイの GeoIP 制限を超えた場合にシステムログメッセージを追加します。
- URL がキャッシュで見つからず、URL フィルタリングカテゴリを取得しようとしたときにタイムアウトが発生した場合、URL フィルタリングカテゴリの一致に対して誤ったアクションが実行される問題を修正します。
- URL フィルタリングプロファイルを設定する管理者アクセス権を持つユーザーが、カスタム URL 応答を使用して Javascript を挿入できないようにします。この修正により、カスタム URL 応答に HTML エンコーディングが適用されます。

バージョン 24.06-01（2024 年 7 月 10 日）

-

拡張機能

このリリースには、次の機能拡張が含まれています。

- ゲートウェイを通過する GRE トンネル内でコンテンツを検査するためのサポートが追加されます。ゲートウェイはトラフィックのカプセル化を解除し、適切なポリシーと保護を適用するためにカプセル化されたトラフィックに対する検査を実行してから、そのトラフィックを再カプセル化して GRE トンネルに戻します。
- ゲートウェイのアップグレードおよびスケールインのシナリオ中に、アクティブな接続をリセットするためのサポートを追加します。これらのシナリオが発生し、ゲートウェイがクライアントまたはサーバーによって閉じられていない長時間接続を処理している場合、ゲートウェイは TCP RST を送信することで、古いインスタンスを獲得するときに接続をアクティブに閉じるようアクションを実行します。

- テレポート（SSHアクセス）を介してゲートウェイインスタンスにログインするときに、カスタムバナーを指定する機能をサポートします。これは、SSHアクセスのいずれかの方法で顧客定義のバナーを表示する必要がある FedRamp 環境に展開されたゲートウェイの要件です。

修正

このリリースには、次の修正が含まれています。

- 復号プロファイルで「デフォルト」以外の証明書の検証アクションを指定すると、ゲートウェイが異常になる問題を修正します。
- ゲートウェイが診断バンドルの生成と Multicloud Defense Controller への送信に失敗する、ユーザー生成の診断バンドルの問題を修正します。
- GeoIP の使用に関する問題を修正します。多くのプロバイダーが存在する国では、アドバタイズされるプレフィックスの数が非常に多くなります。これらの国コードがGeoIPアドレスグループで使用されている場合、アドレスグループには多数の CIDR ブロックが含まれます。GeoIP アドレスグループは 64k CIDR に制限されており、この制限を超えると、部分的な CIDR セットがポリシーに適用されることになります。この修正により、CIDR の完全なセットがポリシーに適用されるように制限が緩和されます。GeoIP によって課される追加のメモリ要件があるため、8 コアインスタンスタイプを使用することをお勧めします。
- Chrome ブラウザが TLS 1.3 を使用してゲートウェイに接続しているときに、ゲートウェイが誤った証明書を発行する可能性がある問題を修正します。これは、2024 年 4 月に Chrome でポスト量子暗号に移行する変更が行われたことが原因です。この変更により、Client Hello は 1415 バイトより大きくなり、発行する証明書を決定するためにプロキシで使用されるサーバー名指定（SNI）を取得できなくなる可能性があります。この修正により、プロキシが 1415 バイトを超える Client Hello サイズをサポートできるようになります。
- ゲートウェイが**[調査（Investigate）] > [ネットワーク分析（Network Analytics）] > [統計（Stats）]**ページに表示する正しい統計を生成していた問題を修正します。
- さまざまな安定性の問題を修正します。
- 青色/緑色ポリシーの変更に関連する問題を修正します。ポリシーの変更が発生し、新しいデータパスがアクティブになると、ゲートウェイは古いデータパスから現在のセッションのドレインを開始します。データパスがセッションを適切にドレインできない場合、データパスは異常として扱われ、データパスの再起動が行われます。これにより、古いデータパスと新しいデータパスの両方が終了し、古いセッションと新しいセッションの中断が発生する可能性があります。この修正により、セッションドレインが適切に完了し、データパスが異常と見なされる状況がなくなります。
- トンネルの設定とネゴシエーションに関するトラブルシューティングとデバッグ情報を提供するシステムログメッセージが VPN トンネルの状態遷移で生成されなかった問題を修正します。

- 最終的にデータパスの自己修復を引き起こす、イングレスゲートウェイの低速メモリリークを修正します。メモリリークは、gzip圧縮されたファイルを含むトラフィックに関連しています。
- バックツーバック POST コマンドに 160k を超えるペイロードが含まれている場合に、イングレスゲートウェイが接続をドロップする可能性がある問題を修正します。

バージョン 24.04

バージョン 24.04-01（2024 年 5 月 16 日）

拡張機能

このリリースには、次の機能拡張が含まれています。

- AWS、Azure、GCP で実行されているゲートウェイのサイト間 VPN のサポートを追加します。これには、IPSec および BGP プロファイルを含む VPN トンネルの設定が含まれます。VPN は、VPN を通過するトラフィックを処理および保護するために、ゲートウェイで直接終端されます。この機能拡張には、ゲートウェイバージョン24.04以降が必要です。

修正

このリリースには、次の修正が含まれています。

- ゲートウェイでアドレスオブジェクトが 63 文字以下に制限されるようにします。
- ポリシーの変更の適用に時間がかかりすぎるためにデータパスが再起動する可能性がある問題を修正します。
- 2 つのデータパスが同時に実行される青色/緑色ポリシーの更新中に CPU 使用率が増加する問題を修正します。各データパスは、それが実行中の唯一のデータパスであると想定して、CPUを消費します。新しいポリシーに対応するために2番目のデータパスがインスタンス化されると、CPU は正しく共有されず、CPU メトリックは正しく記録されません。
- プリエンプティブなデータパスの自己修復を引き起こすメモリリークに関連する問題を修正します。
- ゲートウェイポリシーの更新ステータスが更新中にスタックする可能性がある問題を修正します。
- ゲートウェイの安定性を向上させるようにさまざまな問題を修正します。

バージョン 24.02

バージョン 24.02-02（2024 年 4 月 18 日）

修正

このリリースには、次の修正が含まれています。

- 新しいゲートウェイインスタンスがアクティブになるのを妨げる、ゲートウェイ初期化中のメモリバッファアクセスに関連した問題を修正します。

バージョン 24.02-01（2024 年 2 月 28 日）

拡張機能

このリリースには、次の機能拡張が含まれています。

- （プライベートプレビュー）サイト間 VPN のサポートを追加します。これには、IPSec および BGP を含む VPN トンネルの設定が含まれます。VPN は、VPN を通過するトラフィックを処理および保護するために、Multicloud Defense Gateway で直接終端されます。この機能拡張には、Multicloud Defense Gateway バージョン 24.02 以降が必要です。
- 秘密キーがクラウドサービスプロバイダーに保存されて Multicloud Defense Gateway によって取得される、証明書オブジェクトへの変更を動的に追跡するためのサポートが追加されます。クラウドサービスプロバイダーのリソースに変更があった場合、Multicloud Defense Controller は、ゲートウェイに対して、クラウドサービスプロバイダーのリソースの秘密キーを再読み取りして、アクセス可能であること、および更新されたコンテンツが使用されることを確認するように指示します。証明書へのアクセスで問題が発生した場合は、システムログメッセージが生成されます。
- SSH 経由でログインするときに管理 Linux シェルにメッセージを追加します。このメッセージは、デバイスがシスコの管理対象デバイス（Multicloud Defense Controller で管理されているデバイスなど）であることを強調します。
- ログ転送グループで複数の syslog サーバー設定のサポートを追加します。

修正

このリリースには、次の修正が含まれています。

- libwebp バージョン 1.2.0-3.el9 に関連する CVE-2023-4863 脆弱性に対処します。
- データパスのヒットレス再起動を引き起こすポリシー変更により、軽負荷または中程度の負荷の下で、ロードバランサのヘルスチェックを含むトラフィック処理に影響を与える大きい遅延が発生する可能性がある問題を修正します。

- バージョン 23.08-12 で対処されたが、依然として 4 コアインスタンスタイプに影響を与えている問題を修正します。この問題は、デバッグ I/O アクティビティによって引き起こされる高い CPU 使用率に対処します。以前の修正により、すべてのクラウド サービス プロバイダーのすべてのインスタンスタイプに対処するようになりました。
- I/O 関連のデバッグアクティビティによって引き起こされた高い CPU 使用率に関連する問題を修正します。
- 断続的なロードバランサのヘルスチェックエラーに関連する問題を修正します。この修正により、ヘルスチェックに優先順位を付け、ロードバランサがインスタンスを誤って異常としてマークしないようにすることで、ゲートウェイが強化されます。
- 自己修復プリエンプティブデータパスの再起動をトリガーすることによって自動的に修正される出力ゲートウェイのメモリリークを修正します。
- 生成されたゲートウェイ診断バンドルが、Multicloud Defense Controller への送信が許可されないほどに大きくなり、ゲートウェイログを分析できなくなる問題を修正します。この修正により、生成された診断バンドルが Multicloud Defense Controller に正常に送信されるように制限が追加されます。
- 転送プロキシルールによって処理される各セッションで複数の SNI イベントが記録される問題を修正します。
- Multicloud Defense Gateway の安定性が向上します。
- DNS ベースの FQDN キャッシングに関連した競合状態が原因で、TCP および TLS の後にトラフィックの処理が停止するトラフィック処理の問題を修正します。
- アクティブまたは非アクティブのルールに DNS ベースの FQDN キャッシングが設定されている場合に、Multicloud Defense Gateway が IP キャッシュを正常に構築しない可能性がある問題を修正します。キャッシュが適切に構築されていない場合、ポリシーはトラフィックの照合に失敗する可能性があります。この修正により、ポリシーが一致し、トラフィックが適切に処理されるように、IP キャッシュが適切に構築されます。
- SYN の受信後に SYN ACK を待機するタイムアウトを変更します。元のタイムアウトは 120 秒でした。SYN ACK が返されることのない特定のシナリオ（ポートスキャンなど）では、長いタイムアウトにより、セッションプルのエントリが必要以上に消費されます。多くのセッションが SYN ACK で応答しないシナリオでは、セッションプールが使い果たされる可能性があります。これは多くの場合、SYN フラッドと呼ばれます。タイムアウトを短縮することで、有効なセッションの処理に使えるようにセッションプールを解放するために、セッションがより早くリリースされます。タイムアウトは 30 秒に短縮され、Multicloud Defense Gateway 設定を介して設定できます。
- DNS キャッシングを有効にすると、ポリシーの変更と DNS 解決の間隔の間で競合状態が発生し、ドメインのキャッシュが値 0（キャッシュなし）にリセットされる、DNS ベースの FQDN アドレス オブジェクト リソースに関連する問題を修正します。この状況が発生すると、ドメイン解決はキャッシュされず、既存のキャッシュ値は TTL の期限が切れるとフラッシュされます。最終的に、Multicloud Defense Gateway はそのドメインのトラフィックと一致しなくなります。この修正により、キャッシュが期待どおりに動作するように競合状態が解決されます。

- syslog サーバーに送信された DPI（IDS/IPS）セキュリティイベントに[アクション（Action）] フィールドが存在しなかった問題を修正します。[アクション（Action）] フィールドは存在していましたが、その値は、UI に表示されるアクション値または他の SIEM に送信されたイベント情報と一致しませんでした。修正では、すべてのセキュリティイベントにわたって広くこの問題に対処し、[アクション（Action）] フィールドの値が ALLOW または DENY であるようにします。
- ルールセットバージョンが変更されていないセキュリティプロファイルの自動更新が手動に変更されると、データパスの不要な再起動が発生する問題を修正します。この修正により、データパスの再起動を必要とせずに変更が適用されます。
- Multicloud Defense Gateway の安定性が向上します。
- Multicloud Defense Gateway のパフォーマンスが向上します。
- TLS hello メッセージの SNI フィールドから取得したドメインが FQDN フィールドではなくイベントのテキストフィールドに入力される SNI セキュリティイベントの問題を修正します。FQDN フィールドへの入力が変更されることにより、FQDN フィールドを使用してドメインを表示およびフィルタリングするときに、ログとイベント全体で一貫性が提供されます。
- セッションプールのリークを引き起こす可能性のあるデータパスプロセスの問題を修正します。この状況が発生すると、データパスは、リークが運用に影響を与える前に、セッションプールの消費と自己修復を評価します。これにより、データパスの自己修復が必要なくなるようにリークが修正されます。
- Multicloud Defense Controller への API コールを最適化してゲートウェイプロファイル情報を取得することで、Multicloud Defense Gateway のパフォーマンスを向上します。
- ポリシー規則セットアクションを[ログなし（No Log）]の値に設定してもログメッセージが生成される問題を修正します。

バージョン 23.10

バージョン 23.10-03（2024 年 1 月 11 日）

修正

このリリースには、次の修正が含まれています。

- 生成されたゲートウェイ診断バンドルが、コントローラへの送信が許可されないほどに大きくなり、ゲートウェイログを分析できなくなる問題を修正します。この修正により、生成された診断バンドルがコントローラに正常に送信されるように制限が追加されます。
- アクティブまたは非アクティブのルールに DNS ベースの FQDN キャッシングが設定されている場合に、ゲートウェイが IP キャッシュを正常に構築しない可能性がある問題を修正します。キャッシュが適切に構築されていない場合、ポリシーはトラフィックの照合に

失敗する可能性があります。この修正により、ポリシーが一致し、トラフィックが適切に処理されるように、IP キャッシュが適切に構築されます。

- SYN の受信後に SYN ACK を待機するタイムアウトを変更します。元のタイムアウトは 120 秒でした。SYN ACK が返されることのない特定のシナリオ（ポートスキャンなど）では、長いタイムアウトにより、セッションプルのエントリが必要以上に消費されます。多くのセッションが SYN ACK で応答しないシナリオでは、セッションプールが使い果たされる可能性があります。これは多くの場合、SYN フラッドと呼ばれます。タイムアウトを短縮することで、有効なセッションの処理に使えるようにセッションプールを解放するために、セッションがより早くリリースされます。タイムアウトは30秒に短縮され、ゲートウェイ設定を介して設定できます。
- ゲートウェイの安定性を向上させます。

バージョン 23.10-02（2023 年 11 月 16 日）

修正

このアップグレードには、次の修正が含まれています。

- DNS キャッシングを有効にすると、ポリシーの変更と DNS 解決の間隔の間で競合状態が発生し、ドメインのキャッシュが値 0（キャッシュなし）にリセットされる、DNS ベースの FQDN アドレス オブジェクト リソースに関連する問題を修正します。この状況が発生すると、ドメイン解決はキャッシュされず、既存のキャッシュ値は TTL の期限が切れるとフラッシュされます。最終的に、ゲートウェイはそのドメインのトラフィックと一致しなくなります。この修正により、キャッシュが期待どおりに動作するように競合状態が解決されます。

バージョン 23.10-01（2023 年 11 月 3 日）

拡張機能

このアップグレードには、次の機能拡張が含まれています。

- ポリシータイプ（転送および転送プロキシ）が一致しない 2 つのルールによって処理される各セッションに対して生成されるポリシータイプの不一致メッセージを、各セッションに関連するイベントに移動します。これにより、このシナリオが発生した場合に多くのシステムログメッセージが排除され、各セッションに関連付けられたイベントとしてエラーが生成されます。このシナリオが発生すると、セッションは拒否され、イベントによって理由が報告されます。拒否は、トラフィックサマリーログにも表示されます。
- バックエンド TLS セッションをネゴシエートするときにサーバー証明書を検証するように転送プロキシポリシーを拡張します。証明書の検証はデフォルトでは無効になっていますが、すべての TLS セッションの復号プロファイルで、およびドメイン（またはドメインのセット）ごとに FQDN 一致オブジェクトで設定できます。

- リバース SSH に対応するためのテレポートとの統合により、特にゲートウェイがパブリック IP なしでオーケストレーションされている場合に、ゲートウェイインスタンス管理インターフェイスへの SSH を容易にします。SSH に対する要件はまれであり、高度なトラブルシューティングを目的とする場合のみ必要です。インバウンド通信は、クラウドサービスプロバイダーの制限（セキュリティグループ、ネットワークセキュリティグループ、ファイアウォールルール）を使用してデフォルトで禁止されます。

修正

このアップグレードには、次の修正が含まれています。

- 復号例外に FQDN 一致オブジェクトを使用してトラフィック処理の問題を引き起こす可能性のある、転送プロキシルールに関連する問題を修正します。
- 証明書検証の遅延が原因で、FQDN 一致プロファイルで設定された転送プロキシルールによって、トラフィックが誤って拒否される問題を修正します。FQDN フィルタリングプロファイルが適用されていなくても、拒否は `FQDNFILTER` セキュリティイベントと見なされます。
- FQDN 一致オブジェクトを使用するルールが、未分類のドメインのトラフィックを誤って処理する問題を修正します。
- IP が多数存在し、それらの IP に対する変更が多数あるためにデータパスが変更を受け入れないことが原因で一致の問題が発生し、トラフィックが正しく処理されない可能性がある、ダイナミック アドレス オブジェクトに関連した問題を修正します。
- DNS 解決の間隔を設定しても DNS 解決の頻度が変更されない DNS ベースの FQDN キャッシングの問題を修正します。
- ゲートウェイが異常になる可能性があるパケット収集の問題を修正します。
- ゲートウェイからの特定のログに秘密キー情報が含まれる可能性がある問題を修正します。
- さまざまなゲートウェイの安定性の問題を修正します。
- トラフィック処理の問題の原因となる CPU の問題も引き起こす可能性があるゲートウェイのメモリリークを修正します。
- URI 情報がトラフィックサマリーログに表示されない問題を修正します。
- L7DOS イベントが URI を正しく表示しない問題を修正します。

バージョン 23.08

バージョン 23.08-17-b1（2024 年 9 月 27 日）

これはホットフィックスです。

修正

このホットフィックスには、次の修正が含まれています。

- ゲートウェイが TLS Client Hello メッセージから SNI を取得できず、ゲートウェイが TCP RST との接続を閉じる原因となる問題を修正します。これは、2024 年 4 月に Chrome でポスト量子暗号に移行する変更が行われたことが原因です。この変更により、Client Hello は 1415 バイトより大きくなり、発行する証明書を決定するためにプロキシで使用されるサーバー名指定（SNI）を取得できなくなる可能性があります。この修正により、プロキシが 1415 バイトを超える Client Hello サイズをサポートできるようになります。

バージョン 23.08-17-a1（2024 年 9 月 4 日）

これはホットフィックスです。

修正

このホットフィックスには、次の修正が含まれています。

- DNS ベースの FQDN キャッシュを使用するポリシー規則が破損し、Multicloud Defense Gateway がトラフィックを適切に処理しなくなる可能性がある問題を修正します。

バージョン 23.08-17（2024 年 9 月 4 日）

修正

このリリースには、次の修正が含まれています。

- GeoIP の使用に関する問題を修正します。多くのプロバイダーが存在する国では、アドバタイズされるプレフィックスの数が非常に多くなります。これらの国コードが GeoIP アドレスグループで使用されている場合、アドレスグループには多数の CIDR ブロックが含まれます。GeoIP アドレスグループは 64k CIDR に制限されており、この制限を超えると、部分的な CIDR セットがポリシーに適用されることになります。この修正により、CIDR の完全なセットがポリシーに適用されるように制限が緩和されます。GeoIP によって課される追加のメモリ要件があるため、8 コアインスタンスタイプを使用することをお勧めします。
- TCP 確立タイムアウトが 240 秒を超える値に変更された場合でも、出力ゲートウェイが 240 秒でサイレントに TCP 接続を閉じる問題を修正します。
- URL フィルタリングプロファイルを使用してトラフィックをフィルタリングするときに、出力ゲートウェイのデータパスが自己修復する可能性がある問題を修正します。

バージョン 23.08-16-a1（2024 年 8 月 6 日）

これはホットフィックスです。

修正

このホットフィックスには、次の修正が含まれています。

- DNS ベースの FQDN キャッシュを使用するポリシー規則が破損し、ゲートウェイがトラフィックを適切に処理しなくなる可能性がある問題を修正します。

バージョン 23.08-16（2024 年 6 月 25 日）

修正

このリリースには、次の修正が含まれています。

- Chrome ブラウザが TLS 1.3 を使用してゲートウェイに接続しているときに、Multicloud Defense Gateway が誤った証明書を発行する可能性がある問題を修正します。これは、2024 年 4 月に Chrome でポスト量子暗号に移行する変更が行われたことが原因です。この変更により、Client Hello は 1415 バイトより大きくなり、発行する証明書を決定するためにプロキシで使用されるサーバー名指定（SNI）を取得できなくなる可能性があります。この修正により、プロキシが 1415 バイトを超える Client Hello サイズをサポートできるようになります。

- データパスによって TCP RST を送信してセッションを閉じると、データパスの自己修復が発生する可能性がある問題を修正します。

- Multicloud Defense Gateway がトラフィックを処理する能力に影響を与える可能性のある、受信バッファの枯渇に関連する問題を修正します。ゲートウェイが接続のリセット（TCP RST）に対応するためには、受信した最後のパケットからの情報を保持（受信バッファ）する必要があります。アクティブセッションのボリュームが多い場合、受信バッファが枯渇し、Multicloud Defense Gateway が新しいパケットを受信しなくなる可能性があります。このシナリオは、（意図的または意図せずに）SYN フラッドに関連するハーフオープン接続からより多く発生する可能性があります。この修正は、各アクティブセッションの最終パケットから必要な情報を抽出し、この情報をゲートウェイのアクティブセッション制限に対応するのに十分な大きさのバッファに保存し、バッファの枯渇の可能性を排除します。

- 青色/緑色ポリシーの変更に関連する問題を修正します。ポリシーの変更が発生し、新しいデータパスがアクティブになると、Multicloud Defense Gateway は古いデータパスから現在のセッションのドレインを開始します。データパスがセッションを適切にドレインできない場合、データパスは異常として扱われ、データパスの再起動が行われます。これにより、古いデータパスと新しいデータパスの両方が終了し、古いセッションと新しいセッションの中断が発生する可能性があります。この修正により、セッションドレインが適切に完了し、データパスが異常と見なされる状況がなくなります。

- OCI の Multicloud Defense Gateway のログローテーションの問題を修正します。この修正により、ログが適切にローテーションされ、不要なディスク領域が消費されなくなります。

- TCP RST が誤ったシーケンス番号で送信されて、接続をアクティブにリセットしない、アクティブな接続のリセットに関連する問題を修正します。

- 最終的にデータパスの自己修復を引き起こす、イングレスゲートウェイの低速メモリリークを修正します。メモリリークは、gzip圧縮されたファイルを含むトラフィックに関連しています。

バージョン 23.08-15-a3（2024 年 6 月 22 日）

これはホットフィックスです。

修正

このホットフィックスには、次の修正が含まれています。

- GeoIP の使用に関する問題を修正します。多くのプロバイダーが存在する国では、アドバタイズされるプレフィックスの数が非常に多くなります。これらの国コードがGeoIPアドレスグループで使用されている場合、アドレスグループには多数の CIDR ブロックが含まれます。GeoIP アドレスグループは 64k CIDR に制限されており、この制限を超えると、部分的な CIDR セットがポリシーに適用されることになります。この修正により、CIDR の完全なセットがポリシーに適用されるように制限が緩和されます。GeoIP によって課される追加のメモリ要件があるため、8 コアインスタンスタイプを使用することをお勧めします。

バージョン 23.08-14-c3（2024 年 6 月 8 日）

これはホットフィックスです。

修正

このホットフィックスには、次の修正が含まれています。

- Chrome ブラウザが TLS 1.3 を使用してゲートウェイに接続しているときに、ゲートウェイが誤った証明書を発行する可能性がある問題を修正します。これは、2024 年 4 月に Chrome でポスト量子暗号に移行する変更が行われたことが原因です。この変更により、Client Hello は 1415 バイトより大きくなり、発行する証明書を決定するためにプロキシで使用されるサーバー名指定（SNI）を取得できなくなる可能性があります。この修正により、プロキシが 1415 バイトを超える Client Hello サイズをサポートできるようになります。
- 最終的にデータパスの自己修復を引き起こす、イングレスゲートウェイの低速メモリリークを修正します。メモリリークは、gzip圧縮されたファイルを含むトラフィックに関連しています。

バージョン 23.08-15-c1（2024 年 5 月 9 日）

これはホットフィックスです

修正

このホットフィックスには、次の修正が含まれています。

- ゲートウェイがトラフィックを処理する能力に影響を与える可能性のある、受信バッファの枯渇に関連する問題を修正します。ゲートウェイが接続のリセット（TCP RST）に対応するためには、受信した最後のパケットからの情報を保持（受信バッファ）する必要があります。アクティブセッションのボリュームが多い場合、受信バッファが枯渇し、ゲートウェイが新しいパケットを受信しなくなる可能性があります。このシナリオは、（意図的または意図せずに）SYN フラッドに関連するハーフオープン接続からより多く発生する可能性があります。この修正は、各アクティブセッションの最終パケットから必要な情報を抽出し、この情報をゲートウェイのアクティブセッション制限に対応するのに十分な大きさのバッファに保存し、バッファの枯渇の可能性を排除します。

バージョン 23.08-15-a2（2024 年 5 月 1 日）

これはホットフィックスです。

修正

このホットフィックスには、次の修正が含まれています。

- データパスによって TCP RST を送信してセッションを閉じると、データパスの自己修復が発生する可能性がある問題を修正します。

バージョン 23.08-15-b1（2024 年 4 月 12 日）

これはホットフィックスです。

修正

このホットフィックスには、次の修正が含まれています。

- OCI のゲートウェイのログローテーションの問題を修正します。この修正により、ログが適切にローテーションされ、不要なディスク領域が消費されなくなります。

バージョン 23.08-15-a1（2024 年 4 月 11 日）

これはホットフィックスです。

修正

このホットフィックスには、次の修正が含まれています。

- 青色/緑色ポリシーの変更に関連する問題を修正します。ポリシーの変更が発生し、新しいデータパスがアクティブになると、ゲートウェイは古いデータパスから現在のセッションのドレインを開始します。データパスがセッションを適切にドレインできない場合、

データパスは異常として扱われ、データパスの再起動が行われます。これにより、古いデータパスと新しいデータパスの両方が終了し、古いセッションと新しいセッションの中断が発生する可能性があります。この修正により、セッションドレインが適切に完了し、データパスが異常と見なされる状況がなくなります。

バージョン 23.08-15（2024 年 3 月 27 日）

修正

このリリースには、次の修正が含まれています。

- イングレスゲートウェイを通過する HTTP トラフィックが、一致したポリシー規則セットに関連付けられているリバースプロキシターゲットで指定された適切なドメインを使用していないという問題を修正します。
- イングレスゲートウェイを通過する HTTP トラフィックが、適切なポリシー規則セットと適切に一致していないという問題を修正します。
- 転送と、データパス プロトコル スタックが TCP FIN と RST のタイミングを処理する方法に関連する問題を修正します。サーバーからの FIN とクライアントからの RST は、プロトコルスタックがすでに FIN を検出した後、RST の受け入れ（および転送）を禁止するような順番で発生する可能性があります。この変更により、プロトコルスタックによる RST の受け入れが緩和されて、サーバーに転送できるようになり、プロトコルスタックによってドロップされなくなります。RST のドロップは、プロトコルスタックがサーバーからすでに FIN を受信しているため、予想されるシーケンス番号の不一致が原因で発生します。
- ポリシーの変更の適用に時間がかかりすぎるためにデータパスが再起動する可能性がある問題を修正します。
- 2 つのデータパスが同時に実行される青色/緑色ポリシーの更新中に CPU 使用率が増加する問題を修正します。各データパスは、それが実行中の唯一のデータパスであると想定して、CPU を消費します。新しいポリシーに対応するために 2 番目のデータパスがインスタンス化されると、CPU は正しく共有されず、CPU メトリックは正しく記録されません。
- プリエンプティブなデータパスの自己修復を引き起こすメモリリークに関連する問題を修正します。
- libwebp バージョン 1.2.0-3.el9 に関連する CVE-2023-4863 脆弱性に対処します。
- バックエンドサーバーへの書き込み操作が EAGAIN を返した後の損失書き込みイベントに関連する問題を修正します。この損失イベントにより、ゲートウェイは、要求本文がバックエンドサーバーに送信されたと考え、着信することのない応答を待っています。これは、ゲートウェイの速度とバックエンドサーバーの速度に関連するタイミングの問題です。
- OCI に展開されたゲートウェイの診断バンドルの生成に関する問題を修正します。
- TCP RST が誤ったシーケンス番号で送信されて、接続をアクティブにリセットしない、アクティブな接続のリセットに関連する問題を修正します。

- 古いポリシーを実行しているデータパスを通過するトラフィックが不必要に遅延する、ポリシー変更中のトラフィック処理の問題を修正します。
- WAF コンポーネントがクライアント要求本文を消費する、大量の要求本文のトラフィックの問題を修正します。これにより、ゲートウェイはクライアントからの要求本文を予期し続けますが、クライアントはゲートウェイからの応答を予期していて、クライアントタイムアウトにつながります。

バージョン 23.08-14-e1（2024 年 3 月 28 日）

これはホットフィックスです。

修正

このホットフィックスには、次の修正が含まれています。

- DNS ベースの FQDN キャッシュを使用するポリシー規則が破損し、ゲートウェイがトラフィックを適切に処理しなくなる可能性がある問題を修正します。
- libwebp バージョン 1.2.0-3.el9 に関連する CVE-2023-4863 脆弱性に対処します。

バージョン 23.08-14-a2（2024 年 3 月 20 日）

これはホットフィックスです。

修正

このホットフィックスには、次の修正が含まれています。

- 転送と、データパス プロトコル スタックが TCP FIN と RST のタイミングを処理する方法に関連する問題を修正します。サーバーからの FIN とクライアントからの RST は、プロトコルスタックがすでにFINを検出した後、RSTの受け入れ（および転送）を禁止するような順番で発生する可能性があります。この変更により、プロトコルスタックによるRSTの受け入れが緩和されて、サーバーに転送できるようになり、プロトコルスタックによってドロップされなくなります。RSTのドロップは、プロトコルスタックがサーバーからすでにFINを受信しているため、予想されるシーケンス番号の不一致が原因で発生します。
- 2 つのデータパスが同時に実行される青色/緑色ポリシーの更新中に CPU 使用率が増加する問題を修正します。各データパスは、それが実行中の唯一のデータパスであると想定して、CPUを消費します。新しいポリシーに対応するために2番目のデータパスがインスタンス化されると、CPU は正しく共有されず、CPU メトリックは正しく記録されません。

バージョン 23.08-14-d1（2024 年 3 月 13 日）

これはホットフィックスです。

修正

このホットフィックスには、次の修正が含まれています。

- イングレスゲートウェイを通過する HTTP トラフィックが、一致したポリシー規則セットに関連付けられているリバースプロキシターゲットで指定された適切なドメインを使用していないという問題を修正します。
- イングレスゲートウェイを通過する HTTP トラフィックが、適切なポリシー規則セットと一致していないという問題を修正します。

バージョン 23.08-14-c1（2024 年 2 月 20 日）

これはホットフィックスです。

修正

このホットフィックスには、次の修正が含まれています。

- libwebp バージョン 1.2.0-3.el9 に関連する CVE-2023-4863 脆弱性に対処します。

バージョン 23.08-14-b1（2024 年 2 月 21 日）

これはホットフィックスです。

修正

このホットフィックスには、次の修正が含まれています。

- バックエンドサーバーへの書き込み操作が EAGAIN を返した後の損失書き込みイベントに関連する問題を修正します。この損失イベントにより、Multicloud Defense Gateway は、要求本文がバックエンドサーバーに送信されたと考え、着信することのない応答を待っています。これは、ゲートウェイの速度とバックエンドサーバーの速度に関連するタイミングの問題です。
- OCI に展開されたゲートウェイの診断バンドルの生成に関する問題を修正します。
- WAF コンポーネントがクライアント要求本文を消費する、大量の要求本文のトラフィックの問題を修正します。これにより、Multicloud Defense Gateway はクライアントからの要求本文を予期し続けますが、クライアントは Multicloud Defense Gateway からの応答を予期していて、クライアントタイムアウトにつながります。

バージョン 23.08-14-a1（2024 年 2 月 17 日）

これはホットフィックスです。

修正

このホットフィックスには、次の修正が含まれています。

- TCP RST が誤ったシーケンス番号で送信されて、接続をアクティブにリセットしない、アクティブな接続のリセットに関連する問題を修正します。
- 古いポリシーを実行しているデータパスを通過するトラフィックが不必要に遅延する、ポリシー変更中のトラフィック処理の問題を修正します。

バージョン 23.08-14（2024 年 1 月 25 日）

修正

このリリースには、次の修正が含まれています。

- 23.08-12 で対処されたが、依然として 4 コアインスタンスタイプに影響を与えている問題を修正します。この問題は、デバッグ I/O アクティビティによって引き起こされる高い CPU 使用率に対処します。以前の修正により、すべてのクラウド サービス プロバイダーのすべてのインスタンスタイプに対処するようになりました。
- データパスのヒットレス再起動を引き起こすポリシー変更により、軽負荷または中程度の負荷の下で、ロードバランサのヘルスチェックを含むトラフィック処理に影響を与える大きい遅延が発生する可能性がある問題を修正します。

バージョン 23.08-12（2024 年 1 月 18 日）

修正

このリリースには、次の修正が含まれています。

- I/O 関連のデバッグアクティビティによって引き起こされた高い CPU 使用率に関連する問題を修正します。
- 断続的なロードバランサのヘルスチェックエラーに関連する問題を修正します。この修正により、ヘルスチェックに優先順位を付け、ロードバランサがインスタンスを誤って異常としてマークしないようにすることで、ゲートウェイが強化されます。
- コントローラへの API コールを最適化してゲートウェイプロファイル情報を取得することで、ゲートウェイのパフォーマンスを向上します。

バージョン 23.08-11（2024 年 1 月 11 日）

拡張機能

このリリースには、次の機能拡張が含まれています。

- ポリシータイプ（転送および転送プロキシ）が一致しない2つのルールによって処理される各セッションに対して生成されるポリシータイプの不一致メッセージを、各セッションに関連するセキュリティイベントログに移動します。これにより、セッションごとのログを削除することなく、セッションごとの大量のシステムログメッセージが削除されます。このシナリオが発生すると、セッションは拒否され、セッションに関連するイベントによって理由が報告されます。拒否は、トラフィックサマリーログにも表示されます。

バージョン 23.08-10（2023 年 12 月 18 日）

修正

このリリースには、次の修正が含まれています。

- SYN の受信後に SYN ACK を待機するタイムアウトを変更します。元のタイムアウトは 120 秒でした。SYN ACK が返されることのない特定のシナリオ（ポートスキャンなど）では、長いタイムアウトにより、セッションプルのエントリが必要以上に消費されます。多くのセッションが SYN ACK で応答しないシナリオでは、セッションプールが使い果たされる可能性があります。これは多くの場合、SYN フラッドと呼ばれます。タイムアウトを短縮することで、有効なセッションの処理に使えるようにセッションプールを解放するために、セッションがより早くリリースされます。タイムアウトは30秒に短縮され、ゲートウェイ設定を介して設定できます。
- アクティブまたは非アクティブのルールに DNS ベースの FQDN キャッシングが設定されている場合に、ゲートウェイが IP キャッシュを正常に構築しない可能性がある問題を修正します。キャッシュが適切に構築されていない場合、ポリシーはトラフィックの照合に失敗する可能性があります。この修正により、ポリシーが一致し、トラフィックが適切に処理されるように、IP キャッシュが適切に構築されます。
- 生成されたゲートウェイ診断バンドルが、コントローラへの送信が許可されないほどに大きくなり、ゲートウェイログを分析できなくなる問題を修正します。この修正により、生成された診断バンドルがコントローラに正常に送信されるように制限が追加されます。
- ゲートウェイの安定性を向上させます。

バージョン 23.08-09（2023 年 11 月 16 日）

修正

このアップグレードには、次の修正が含まれています。

- DNS キャッシングを有効にすると、ポリシーの変更と DNS 解決の間隔の間で競合状態が発生し、ドメインのキャッシュが値0（キャッシュなし）にリセットされる、DNS ベースの FQDN アドレス オブジェクト リソースに関連する問題を修正します。この状況が発生すると、ドメイン解決はキャッシュされず、既存のキャッシュ値は TTL の期限が切れるとフラッシュされます。最終的に、ゲートウェイはそのドメインのトラフィックと一致し

なくなります。この修正により、キャッシュが期待どおりに動作するように競合状態が解決されます。

バージョン 23.08-08（2023 年 11 月 8 日）

修正

このアップグレードには、次の修正が含まれています。

- すべてのユースケースでゲートウェイの安定性が向上します。

バージョン 23.08-07（2023 年 10 月 18 日）

修正

このアップグレードには、次の修正が含まれています。

- GCP ロギングへのログ転送が JSON エンコード文字列ではなく JSON 構造としてログを送信するように問題を修正します。

バージョン 23.08-06（2023 年 10 月 7 日）

修正

この更新には、次の修正が含まれています。

- 復号例外にFQDN一致オブジェクトを使用してトラフィック処理の問題を引き起こす可能性のある、転送プロキシルールに関連する問題を修正します。

バージョン 23.08-05（2023 年 10 月 3 日）

修正

この更新には、次の修正が含まれています。

- 証明書検証の遅延が原因で、FQDN一致プロファイルで設定された転送プロキシルールによって、トラフィックが誤って拒否される問題を修正します。FQDNフィルタリングプロファイルが適用されていなくても、拒否はFQDNFILTERセキュリティイベントと見なされます。

バージョン 23.08-04（2023 年 9 月 19 日）

修正

このアップグレードには、次の修正が含まれています。

- FQDN一致オブジェクトを使用するルールが、未分類のドメインのトラフィックを誤って処理する問題を修正します。

バージョン 23.08-03（2023 年 9 月 10 日）

修正

このアップグレードには、次の修正が含まれています。

- IP が多数存在し、それらの IP に対する変更が多数あるためにデータパスが変更を受け入れないことが原因で一致の問題が発生し、トラフィックが正しく処理されない可能性がある、ダイナミック アドレス オブジェクトに関連した問題を修正します。
- DP がリークを検出してデータパスを再起動する、UDP トラフィックに関連した低速セッションプールリークを修正します。

バージョン 23.08-02（2023 年 9 月 3 日）

修正

このアップグレードには、次の修正が含まれています。

- 200KB を超えるペイロードで HTTP POST を送信するとトラフィックがドロップされるリバースプロキシの問題を修正します。
- 静的 IP を含む DNS ベースのアドレスオブジェクトが適正に一致しない問題を修正します。
- TCP 転送プロキシの SNI またはホストヘッダーへの依存関係を削除します。

バージョン 23.08-01（2023 年 8 月 25 日）

拡張機能

このアップグレードには、次の機能拡張が含まれています。

- ゲートウェイ接続とプロキシのタイマーが超過した場合に、セッションサマリーイベントを生成するようにデータパスを拡張します。この機能拡張は、タイマー設定が原因でセッションがゲートウェイによって閉じられた場合のトラブルシューティングに役立ちます。

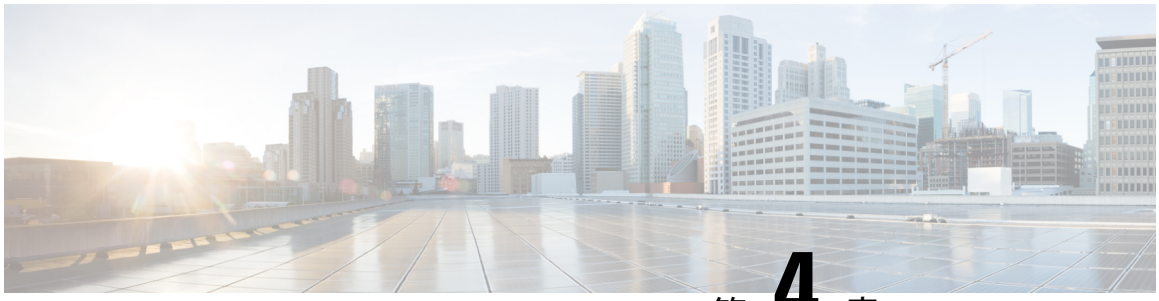
- L4（TCP）および L5（TLS）プロキシに対応するように転送プロキシ サービス オブジェクトを拡張します。この拡張は、`transport_mode` 引数の有効な値として TCP または TLS を指定することにより達成されます。
- セッションのパフォーマンスを追跡するようにゲートウェイのデータパスを拡張します。
- TCP リセットを生成するゲートウェイ データパス プロセスを拡張し、データパスの再起動中に接続を意図的に閉じるようにします。

修正

このアップグレードには、次の修正が含まれています。

- HTTP オブジェクト名の URL エンコード文字 [`and`] がゲートウェイによって復号化された後、サーバーに要求を送信する前に再エンコードされない問題を修正します。この問題より、サーバーはオブジェクトを正しく捕捉することができず、400 応答コードを返します。この修正により、サーバーに要求を送信する前に、文字が適切に再エンコードされるようになります。
- SNI に下線が存在すると、プロキシによってトラフィックが渡されない問題を修正します。この変更により、プロキシ設定でドメイン名での下線の使用に対応できるようになります。
- トラフィックが正しいポリシーと一致するのに、間違った証明書が発行される問題を修正します。
- トラフィックが正しいポリシーと一致するのに、間違った証明書が発行される問題を修正します。
- プロキシタイムアウトによって 408 ステータスコードが発生する HTTP コマンド（GitHub リポジトリの複製など）に関連した大規模ファイル転送の問題を修正します。
- URL フィルタリングカテゴリのクエリタイムアウトが期限切れになり、トラフィックが拒否される問題を修正します。
- アップストリームプロキシの問題が原因でデータパスが自己修復される可能性がある、イングレスゲートウェイの安定性の問題を修正します。
- ゲートウェイが特定のタイプのトラフィックを処理するときに、遅延が長引く可能性がある問題を修正します。
- メモリプロファイリングを有効にするときにトリガーされる、データパスの不要な再起動を修正します。
- ポリシーの変更によってトリガーされたデータパスの再起動が原因で、ゲートウェイが断続的に 502 を生成する可能性がある問題を修正します。
- CPU ベースの自動スケーリングで不要なスケールアウトが発生する可能性がある問題を修正します。
- プロキシ接続リークを修正します。

• Multicloud Defense Gateway の安定性が向上します。



第 4 章

Multicloud Defense Terraform Providerの機能拡張

バージョン 0.2.9（2024 年 11 月 15 日）（推奨）

修正

このリリースには、次の修正が含まれています。

- `type = DYNAMIC_SECURITY_GROUP` のアドレスオブジェクト（`ciscomd_address_object`）リソースが作成されるが、サブオブジェクトが動的に入力されない問題を修正します。
- 現在の状態と比較して、ゲートウェイ（`ciscomd_gateway`）リソースのブロックの設定順序が変わった場合、変更が行われていなくても Terraform がこれをインフラストラクチャの変更と見なす問題を修正します。設定の順序はゲートウェイの動作には関係ありませんが、Terraform プランを実行するか、変更を適用する必要があるかどうかを検証するために適用する場合は関係します。この修正により、順序がユーザーによって変更されない限り、設定の順序は一貫して変わりません。

バージョン 0.2.8（2024 年 11 月 7 日）

拡張機能

このリリースには、次の機能拡張が含まれています。

- security_type 引数を **EGRESS** に設定してゲートウェイ（ciscomd_gateway）リソースの引数 aws_gateway_lb のデフォルト値を false から true に変更します。

修正

このリリースには、次の修正が含まれています。

- ポリシー規則セット（ciscomd_policy_rule_set）リソースの name 引数を変更しても、名前が変更されない問題を修正します。
- アドレスオブジェクト（ciscomd_address_object）リソースの name 引数を変更しても、名前が変更されない問題を修正します。
- ICMP ルールをポリシー規則（ciscomd_policy_rules）リソースに添付すると、機能準拠のエラーメッセージが表示される問題を修正します。
- ダイナミック IP アドレス値への参照を使用して設定された転送プロファイル（ciscomd_profile_log_forwarding）リソースで、IP アドレスの指定を求めるエラーがスローされる問題を修正します。
- BGP ネイバーブロックが指定されていないと BGP プロファイル（ciscomd_profile_bgp）を作成できない問題を修正します。
- サービス VPC（valtix_service_vpc）リソースの CIDR 引数が適切に検証されず、サービス VPC の作成時に適用されない CIDR を許可する問題を修正します。
- アドレスオブジェクト（ciscomd_address_object）リソースとポリシー規則（ciscomd_policy_rules）リソースの両方が同じ適用操作で作成され、規則がアドレスオブジェクトを参照すると、アドレスオブジェクト ID が **0** であるためにエラーがスローされる問題を修正します。アドレスオブジェクトの作成は ID を返さないため、規則に適用されるときの ID は 0 になります。これにより、アドレスオブジェクトと規則を同じ適用で作成および参照できるように、問題が修正されます。

バージョン 0.2.7（2024 年 8 月 21 日）

修正

このリリースには、次の修正が含まれています。

- エッジモードで展開されたゲートウェイ（ciscodmcd_gateway）リソースの instance_details ブロックの順序に関連する問題を修正します。マルチゾーン展開でのブロックの順序がランダムになる可能性があり、Terraform が適用してインフラストラクチャの変更が誤って検出されることになります。この修正により、コードで順序に変更がない場合、インフラストラクチャの変更が検出されないように、ユーザー指定の Terraform コードに基づいて一貫した順序が保証されます。

バージョン 0.2.6（2024 年 2 月 31 日）

拡張機能

このリリースには、次の機能拡張が含まれています。

- Windows、Linux、および MacOS の arm64 サポートを追加します。
- GCP での Multicloud Defense Gateway `ciscomcd_gateway` リソースの作成を強化し、ユーザーが提供する IP リソースをロードバランサのフロントエンド IP として使用できるようにします。
- Azure `ciscomcd_spoke_vpc` でのクロスサブスクリプション スポーク VNet ピアリング オーケストレーションのサポートを追加します。これにより、クラウドサービスプロバイダー間での機能の同等性が保証されます。
- OCI でのオーケストレーションのためのアカウント（テナント/コンパートメント）のオンボーディング `ciscomcd_account` および Multicloud Defense Gateway 展開 `ciscomcd_gateway` リソースのサポートを追加します。

修正

このリリースには、次の修正が含まれています。

- FQDN フィルタリング `ciscomcd_profile_fqdn` リソースを作成しようとすると、「プロファイルタイプ FQDN_FILTER の復号プロファイルから不明なアクションが継承されます（unknown action Inherit from decryption profile for profile type FQDN_FILTER）」というエラーメッセージが表示される問題を修正します。
- 復号プロファイル `ciscomcd_profile_decryption` リソースへの変更が、変更を認識せず、「変更なし。インフラストラクチャは設定と一致しています。（No changes. Your infrastructure matches the configuration）」というメッセージが生じる問題を修正します。
- スポーク VPC ピアリングが削除されない、GCP でのスポーク VPC `ciscomcd_spoke_vpc` ピアリングの削除に関する問題を修正します。この問題は、セルフリンクの代わりに VPC ID が使用された場合にのみ発生していました。

バージョン 0.2.5（2023 年 11 月 6 日）

拡張機能

このリリースには、次の機能拡張が含まれています。

- フォルダ階層構造内に含まれるすべてのプロジェクトのアセットとトラフィックの検出に対応するために、GCP フォルダ階層のオンボーディングに対する、クラウド サービス プロバイダー アカウント `ciscomcd_cloud_account` リソースのサポートを追加します。GCP

フォルダのオンボーディングにより、アセットとトラフィックの検出は許可されますが、完全なオーケストレーションは許可されません。検出は、GCPプロジェクト内で行われた変更にリアルタイムで適応する動的ポリシーを作成するために有益であり、必要です。プロジェクト内でオーケストレーションを行うには、オーケストレーションが必要な各プロジェクトを個別にオンボーディングする必要があります。

- サードパーティ製SIEMへのMulticloud Defense Gatewayメトリックの送信のサポートを追加します。これにより、ゲートウェイメトリックをSIEMに送信するために、設定しMulticloud Defense Gateway `ciscomcd_gateway` リソースに割り当てることができる新しいメトリック転送プロファイル `ciscomcd_profile_metrics_forwarding` リソースが導入されます。最初の導入では、DatadogをSIEMとしてサポートします。他のSIEMのサポートは、今後のリリースで予定されています。
- Multicloud Defense Gateway `ciscomcd_gateway` リソース `aws_gateway_lb` 引数のデフォルト値をfalseからtrueに変更します。AWS出力ゲートウェイを展開する場合、サポートされるトランジットアーキテクチャはAWSゲートウェイロードバランサ（GWLB）アーキテクチャです。この引数はオプションであり、指定しない場合、デフォルトで適切な値になります。
- 監査ログとシステムログをSplunkに送信するためのサポートを追加します。これにより、type引数の新しい値としてSplunkを追加することで、アラートプロファイル `ciscomcd_alert_profile` リソースが更新されます。
- 監査ログとシステムログをMicrosoft Teamsに送信するためのサポートを追加します。これにより、type引数の新しい値としてMicrosoft Teamsを追加することで、アラートプロファイル `ciscomcd_alert_profile` リソースが更新されます。
- バックエンドTLSセッションをネゴシエートするときにサーバー証明書を検証するように転送プロキシポリシーを拡張します。証明書の検証はデフォルトでは無効になっていますが、すべてのTLSセッションの復号プロファイル `ciscomcd_profile_decryption` リソースで、およびドメイン（またはドメインのセット）ごとにFQDN一致オブジェクト `ciscomcd_profile_fqdn` リソースで設定できます。
- サービスVNet `ciscomcd_service_vpc` リソースの一部としてAzureリソースグループ（RG）を作成するためのサポートを追加します。RGは、Multicloud Defense Controllerによってオーケストレーションされるすべてのリソースを指定した（または新しく作成した）RG内で関連付けるために必要です。

修正

このリリースには、次の修正が含まれています。

- `transport_mode` 引数に割り当てられたセキュアプロキシ（TLS、HTTPS、WEBSOCKETS）値を使用するときに、復号プロファイル `ciscomcd_profile_decryption` をtls_profile引数に割り当てる必要がある転送プロキシ サービス オブジェクトまたはリバース プロキシ サービス オブジェクト `ciscomcd_service_object` リソースを設定するときに、検証が実行されなかった問題を修正します。セキュアなプロキシが設定されている場合は、復号プロファ

イルを割り当てる必要があります。割り当てなかった場合、プロキシはセキュアなプロキシとして動作せず、TLS 暗号化トラフィックは拒否されます。

バージョン 0.2.4（2023 年 8 月 22 日）

拡張機能

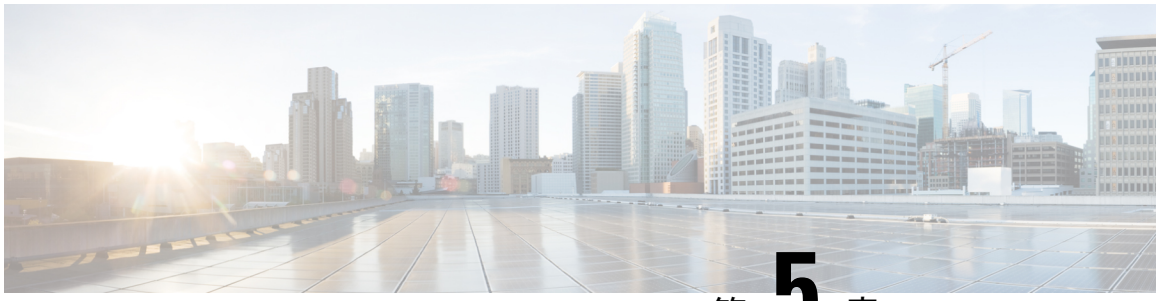
このリリースには、次の機能拡張が含まれています。

- L4（TCP）および L5（TLS）プロキシに対応するように転送プロキシ サービス オブジェクト `ciscomcd_service_object` リソースを拡張します。この拡張は、`transport_mode` 引数の有効な値として TCP または TLS を指定することにより達成されます。
- assign_public_ip 設定への変更が行われた場合に、青色/緑色ゲートウェイの置換を実行するように Multicloud Defense Gateway `ciscomcd_gateway` リソースを拡張します。

修正

このリリースには、次の修正が含まれています。

- policy 引数のない `mode=MATCH` 引数を持つ FQDN プロファイル `ciscomcd_fqdn_profile` リソースにより、一致するトラフィックが拒否される問題を修正します。policy 引数を指定する必要はなく、Terraform プロバイダーのドキュメントには引数としてリストされていません。
- ポリシー規則 `ciscomcd_policy_rule_set` リソースの更新に時間がかかり、RPC エラーが生成される可能性がある問題を修正します。



第 5 章

レガシーバージョン

次のレガシーバージョンは推奨されませんが、引き続きサポートされています。

Multicloud Defense Gateway のレガシーバージョン

バージョン 23.06

バージョン 23.06-14（2023 年 11 月 12 日）

修正

このアップグレードには、次の修正が含まれています。

- DNS キャッシングを有効にすると、ポリシーの変更と DNS 解決の間隔の間で競合状態が発生し、ドメインのキャッシュが値 0（キャッシュなし）にリセットされる、DNS ベースの FQDN アドレス オブジェクト リソースに関連する問題を修正します。この状況が発生すると、ドメイン解決はキャッシュされず、既存のキャッシュ値は TTL の期限が切れるとフラッシュされます。最終的に、ゲートウェイはそのドメインのトラフィックと一致しなくなります。この修正により、キャッシュが期待どおりに動作するように競合状態が解決されます。

バージョン 23.06-13（2023 年 10 月 18 日）

修正

このアップグレードには、次の修正が含まれています。

- GCP ロギングへのログ転送が JSON エンコード文字列ではなく JSON 構造としてログを送信するように問題を修正します。

バージョン 23.06-12（2023 年 10 月 6 日）

修正

この更新には、次の修正が含まれています。

- 復号例外にFQDN一致オブジェクトを使用してトラフィック処理の問題を引き起こす可能性のある、転送プロキシルールに関連する問題を修正します。

バージョン 23.06-11（2023 年 9 月 27 日）

修正

この更新には、次の修正が含まれています。

- 証明書検証の遅延が原因で、FQDN一致プロファイルで設定された転送プロキシルールによって、トラフィックが誤って拒否される問題を修正します。FQDNフィルタリングプロファイルが適用されていなくても、拒否はFQDNFILTERセキュリティイベントと見なされます。

バージョン 23.06-10（2023 年 9 月 19 日）

修正

このアップグレードには、次の修正が含まれています。

- FQDN一致オブジェクトを使用するルールが、未分類のドメインのトラフィックを誤って処理する問題を修正します。

バージョン 23.06-09（2023 年 9 月 10 日）

修正

このアップグレードには、次の修正が含まれています。

- IP が多数存在し、それらの IP に対する変更が多数あるためにデータパスが変更を受け入れないことが原因で一致の問題が発生し、トラフィックが正しく処理されない可能性がある、ダイナミック アドレス オブジェクトに関連した問題を修正します。
- DP がリークを検出してデータパスを再起動する、UDP トラフィックに関連した低速セッションプールリークを修正します。

バージョン 23.06-08（2023 年 9 月 3 日）

修正

このアップグレードには、次の修正が含まれています。

- 静的 IP を含む DNS ベースのアドレスオブジェクトが適正に一致しない問題を修正します。

バージョン 23.06-07（2023 年 8 月 29 日）

修正

このアップグレードには、次の修正が含まれています。

- 200KB を超えるペイロードで HTTP POST を送信するとトラフィックがドロップされる転送プロキシの問題を修正します。

バージョン 23.06-06（2023 年 8 月 23 日）

修正

このアップグレードには、次の修正が含まれています。

- SNI に下線が存在すると、プロキシによってトラフィックが渡されない問題を修正します。この変更により、プロキシ設定でドメイン名での下線の使用に対応できるようになります。
- ゲートウェイの安定性を向上させます。
- プロキシタイムアウトによって 408 ステータスコードが発生する HTTP コマンド（GitHub リポジトリの複製など）に関連した大規模ファイル転送の付加的な問題を修正します。
- トラフィックが正しいポリシーと一致するのに、間違った証明書が発行される問題を修正します。
- URL フィルタリングカテゴリのクエリタイムアウトが期限切れになり、トラフィックが拒否される問題を修正します。
- プロキシ接続リークを修正しました。修正：HTTP オブジェクト名の URL エンコード文字 [および] がゲートウェイによって復号化された後、サーバーに要求を送信する前に再エンコードされない問題を修正します。この問題より、サーバーはオブジェクトを正しく捕捉することができず、400 応答コードを返します。この修正により、サーバーに要求を送信する前に、文字が適切に再エンコードされるようになります。

バージョン 23.06-05（2023 年 8 月 4 日）

修正

このアップグレードには、次の修正が含まれています。

- 下線を使用している HTTP ヘッダーがプロキシルールによって渡されない問題を修正します。この変更により、プロキシ設定で下線付きのヘッダーに対応できるようになります。

- プロキシタイムアウトによって 408 ステータスコードが発生する HTTP コマンド（GitHub リポジトリの複製など）に関連した大規模ファイル転送の問題を修正します。
- HTTP トラフィックがまず転送プロキシルールによって処理され、次いでさらに詳細な照合のために転送ルールによって処理された後、拒否する必要があるときに許可される問題を修正します。

バージョン 23.06-04（2023 年 7 月 27 日）

修正

このアップグレードには、次の修正が含まれています。

- マルウェア対策エンジンによって特定のタイプのトラフィックが処理されると、CPU の使用率が高くなり、トラフィック処理の遅延が発生する可能性がある問題を修正します。

バージョン 23.06-03（2023 年 7 月 21 日）

修正

このアップグレードには、次の修正が含まれています。

- ポリシー規則セットに、IP/CIDR の包含と除外の組み合わせを使用するアドレスオブジェクトが含まれている場合、新しいゲートウェイの展開により起動エラーが発生する可能性がある問題を修正します。

バージョン 23.06-02（2023 年 7 月 19 日）

修正

このアップグレードには、次の修正が含まれています。

- CIDR ベースのアドレスオブジェクトへの更新がデータパスワーカーに適切に適用されず、誤ったルール照合が発生する問題を修正します。
- DNS キャッシュが適切に確立されているものの、データパスワーカーに適切に適用されないために誤ったルール照合が発生する、DNS ベース FQDN アドレスオブジェクトの問題を修正します。
- 同じ L3/L4（IP/ポート/プロトコル）照合基準の転送ルールが転送プロキシルールに先行するものの、別個の L5（SNI）照合により、適切なルール照合が発生してもトラフィックが転送として処理されるデータパス処理動作を修正します。転送ルールと転送プロキシルールの順序を逆にした場合も、同様の動作が発生する場合があります。この動作が発生する理由は、L5（SNI）照合に対応するために、TCP ハンドシェイクを完全に確立して、TLS hello メッセージを受信し、SNI を取得する必要があるためです。TCP ハンドシェイクが完了すると、トラフィックは最初のルールのルールタイプによってすでに処理されています。セッションが一旦確立されると、トラフィック処理を転送から転送プロキシに（またはその逆に）変更することはできません。ポリシー規則セットにこの競合が設定されてい

る場合、データパスは競合を検出し、システムログメッセージを生成します。競合するルールではトラフィックを正常に処理できないため、トラフィックは拒否されます。

- アップストリームプロキシの問題が原因でデータパスが自己修復される可能性がある、イングレスゲートウェイの安定性の問題を修正します。
- データパスの再起動によって CPU のスパイクが発生し、不要な自動スケーリングが発生する可能性がある問題を修正します。

バージョン 23.06-01（2023 年 7 月 6 日）

修正

このアップグレードには、次の修正が含まれています。

- GCP ゲートウェイがサポート関連の診断バンドルを生成できない問題を修正します。
- プロファイルの変更が導入されていないにもかかわらず、NTP プロファイルがゲートウェイに繰り返し適用される問題を修正します。
- 空のアドレスオブジェクトがゲートウェイに適用されると、トラフィック処理の問題が発生する問題を修正します。
- NTP プロファイルとログ転送プロファイルの両方をゲートウェイに同時に適用すると、データパスの不要な自己修復が発生する問題を修正します。この問題は、それぞれの操作が独立しているため、オーケストレーションを使用してプロファイルが適用された場合にのみ発生します。順次、非常に短い期間内に発生します。
- 3 つを超えるレベルを含むドメインでルールが設定されている場合に、イングレスゲートウェイが誤った証明書を発行する可能性がある問題を修正します。
- アドレスオブジェクトを頻繁に変更すると、データパスがそれ以上の変更を受け入れなくなる可能性がある問題を修正します。
- FQDN 一致を使用するルールセットによってトラフィックが処理されるときに、拒否時のリセット（TCP リセット）が実行されない問題を修正します。
- ゲートウェイによって処理されるトラフィックに対して L4_FW イベントが一貫して生成されない問題を修正します。
- WAF アクションを [ログの許可（Allow Log）] から [ルールデフォルト（Rule Default）] に変更すると、データパスが複数回再起動する可能性がある問題を修正します。
- チャンクされた転送エンコーディングを含む HTTP トラフィックにより、WAF で大量のメモリが消費され、データパスの自己修復がトリガーされる可能性がある問題を修正します。修正：低速メモリリークによってデータパスのサイレント再起動が生じ、トラフィックが中断する可能性がある問題を修正します。
- データパスの自己修復を引き起こす可能性のあるメモリの問題を修正します。

バージョン 23.04

バージョン 23.04-18（2023 年 9 月 3 日）

修正

このアップグレードには、次の修正が含まれています。

- 200KB を超えるペイロードで HTTP POST を送信するとトラフィックがドロップされるリバースプロキシの問題を修正します。
- 静的 IP を含む DNS ベースのアドレスオブジェクトが適正に一致しない問題を修正します。

バージョン 23.04-17（2023 年 8 月 23 日）

修正

このアップグレードには、次の修正が含まれています。

- HTTP オブジェクト名の URL エンコード文字 [および] がゲートウェイによって復号化された後、サーバーに要求を送信する前に再エンコードされない問題を修正します。この問題より、サーバーはオブジェクトを正しく捕捉することができず、400 応答コードを返します。この修正により、サーバーに要求を送信する前に、文字が適切に再エンコードされるようになります。

バージョン 23.04-16（2023 年 8 月 22 日）

修正

このアップグレードには、次の機能拡張が含まれています。

- SNI に下線が存在すると、プロキシによってトラフィックが渡されない問題を修正します。この変更により、プロキシ設定でドメイン名での下線の使用に対応できるようになります。
- プロキシタイムアウトによって 408 ステータスコードが発生する HTTP コマンド（GitHub リポジトリの複製など）に関連した大規模ファイル転送の付加的な問題を修正します。
- トラフィックが正しいポリシーと一致するのに、間違った証明書が発行される問題を修正します。
- URL フィルタリングカテゴリのクエリタイムアウトが期限切れになり、トラフィックが拒否される問題を修正します。
- プロキシ接続リークを修正します。
- ゲートウェイの安定性を向上させます。

バージョン 23.04-14（2023 年 7 月 27 日）

修正

このアップグレードには、次の修正が含まれています。

- マルウェア対策エンジンによって特定のタイプのトラフィックが処理されると、CPUの使用率が高くなり、トラフィック処理の遅延が発生する可能性がある問題を修正します。

バージョン 23.04-13（2023 年 7 月 27 日）

修正

このアップグレードには、次の修正が含まれています。

- マルウェア対策エンジンによって特定のタイプのトラフィックが処理されると、CPUの使用率が高くなり、トラフィック処理の遅延が発生する可能性がある問題を修正します。

バージョン 23.04-12（2023 年 7 月 19 日）

修正

このアップグレードには、次の修正が含まれています。

- CIDRベースのアドレスオブジェクトへの更新がデータパスワーカーに適切に適用されず、誤ったルール照合が発生する問題を修正します。
- DNSキャッシュが適切に確立されているものの、データパスワーカーに適切に適用されないために誤ったルール照合が発生する、DNS ベース FQDN アドレスオブジェクトの問題を修正します。
- 同じL3/L4（IP/ポート/プロトコル）照合基準の転送ルールが転送プロキシルールに先行するものの、別個のL5（SNI）照合により、適切なルール照合が発生してもトラフィックが転送として処理されるデータパス処理動作を修正します。転送ルールと転送プロキシルールの順序を逆にした場合も、同様の動作が発生する場合があります。この動作が発生する理由は、L5（SNI）照合に対応するために、TCP ハンドシェイクを完全に確立して、TLS helloメッセージを受信し、SNIを取得する必要があるためです。TCPハンドシェイクが完了すると、トラフィックは最初のルールのルールタイプによってすでに処理されています。セッションが一旦確立されると、トラフィック処理を転送から転送プロキシに（またはその逆に）変更することはできません。ポリシー規則セットにこの競合が設定されている場合、データパスは競合を検出し、システムログメッセージを生成します。競合するルールではトラフィックを正常に処理できないため、トラフィックは拒否されます。
- アップストリームプロキシの問題が原因でデータパスが自己修復される可能性がある、イングレスゲートウェイの安定性の問題を修正します。
- データパスの再起動によって CPU のスパイクが発生し、不要な自動スケーリングが発生する可能性がある問題を修正します。

バージョン 23.04-11（2023 年 7 月 10 日）

修正

このアップグレードには、次の修正が含まれています。

- ゲートウェイの自己修復を引き起こす可能性がある、Snort エンジンの安定性の問題を修正します。
- 長いヘッダーを含む入力トラフィックにより、リバースプロキシが 400 応答コードを生成する問題を修正します。
- ルールが FQDN 一致プロファイルを使用しており、プロファイルの複数の行に復号例外設定が混在している場合に、転送プロキシルールによってトラフィックが適切に処理されない問題を修正します。

バージョン 23.04-10（2023 年 6 月 28 日）

修正

このアップグレードには、次の修正が含まれています。

- DNS ベースのキャッシュ設定をゲートウェイに適用すると、ゲートウェイインスタンスに異常が発生する問題を修正します。

バージョン 23.04-09（2023 年 6 月 25 日）

修正

このアップグレードには、次の修正が含まれています。

- 一貫したゲートウェイの正常性を確保するために設定されていた 15 日間の定期的なゲートウェイデータパスの自己修復を削除します。この機能は、把握と修正が困難なある問題に対処するために 2 年以上前に組み込まれました。問題はその後解決しましたが、定期的な自己修復は削除されませんでした。この機能は不要になり、現在は削除されています。
- GCP ゲートウェイがサポート関連の診断バンドルを生成できない問題を修正します。
- プロファイルの変更が導入されていないにもかかわらず、NTP プロファイルがゲートウェイに繰り返し適用される問題を修正します。
- FQDN フィルタリングプロファイルが適用されているときに、ポリシールールセットが持続的な「更新中」状態になる可能性がある問題を修正します。
- 空のアドレスオブジェクトがゲートウェイに適用されると、トラフィック処理の問題が発生する問題を修正します。
- NTP プロファイルとログ転送プロファイルの両方をゲートウェイに同時に適用すると、データパスの不要な自己修復が発生する問題を修正します。この問題は、それぞれの操作

が独立しているため、オーケストレーションを使用してプロファイルが適用された場合にのみ発生します。順次、非常に短い期間内に発生します。

バージョン 23.04-07（2023 年 6 月 14 日）

修正

このアップグレードには、次の修正が含まれています。

- WAF アクションを [ログの許可（Allow Log）] から [ルールデフォルト（Rule Default）] に変更すると、データパスが複数回再起動する可能性がある問題を修正します。
- プリエンプティブデータパスの自己修復によって対処される、低速セッションプールリークに関連した 23.04-05 で行われた変更を元に戻すための更新を提供します。以前の更新では、プリエンプトできないデータパスの自己修復が発生する可能性があります。このリリースでは、最初の問題が完全に解決されるまでの間、安定性が確保されます。

バージョン 23.04-06（2023 年 6 月 8 日）

修正

このアップグレードには、次の修正が含まれています。

- ゲートウェイによって処理されるトラフィックに対して L4_FW イベントが一貫して生成されない問題を修正します。
- チャンクされた転送エンコーディングを含む HTTP トラフィックにより、WAF で大量のメモリが消費され、データパスの自己修復がトリガーされる可能性がある問題を修正します。

バージョン 23.04-05（2023 年 6 月 1 日）

修正

このアップグレードには、次の機能拡張が含まれています。

- トラフィックを中断させる可能性のあるサイレントデータパスの再起動を引き起こす低速メモリリークを修正します。
- プリエンプティブなデータパスの自己修復を引き起こす可能性のある、超低速セッションプールリークを修正します。
- FQDN一致を使用するルールセットによってトラフィックが処理されるときに、拒否時のリセット（TCP リセット）が実行されない問題を修正します。
- 3 つを超えるレベルを含むドメインでルールが設定されている場合に、イングレスゲートウェイが誤った証明書を発行する可能性がある問題を修正します。

- アドレスオブジェクトを頻繁に変更すると、データパスがそれ以上の変更を受け入れなくなる可能性がある問題を修正します。
- データパスの自己修復を引き起こす、ゲートウェイの安定性のさまざまな問題を修正します。

バージョン 23.04-04（2023 年 5 月 19 日）

修正

このアップグレードには、次の修正が含まれています。

- FQDN一致を使用するポリシー規則セットルールのトラフィック処理に関する問題を修正します。FQDN と一致する TLS SNI を含むセッションが最初は拒否されますが、後続のセッションが誤って許可されます。

バージョン 23.04-03（2023 年 5 月 16 日）

修正

このアップグレードには、次の修正が含まれています。

- ゲートウェイ設定として有効になっている拡張メモリ プロファイリング モードを使用可能にします。このモードは、メモリ消費を把握する高度なトラブルシューティングに役立ちます。

バージョン 23.04-02（2023 年 5 月 2 日）

修正

このアップグレードには、次の修正が含まれています。

- OCI ゲートウェイ管理インターフェイスへの SSH セッションを確立するときに、無効なユーザーアカウントが原因で権限が拒否されて失敗する問題を修正します。
- ゲートウェイに関連付けられたユーザー定義の NTP プロファイルがゲートウェイに適用されたときに、NTP 設定が適切に構成されない問題を修正します。

バージョン 23.04-01（2023 年 4 月 20 日）

拡張機能

このアップグレードには、次の機能拡張が含まれています。

- 共有暗号スイートがないために TLS セッションをネゴシエートできない場合に、ゲートウェイによって報告されるエラーメッセージが改善されます。「TLS_ERROR」タイプのセキュリティイベントのエラーメッセージが改善され、わかりやすくなりました。

- Valtix ゲートウェイで使用される Centos ベースイメージの強化を促進します。ベースイメージは Centos9 に移動され、厳格なコンプライアンス要件が設定された環境に対応するように強化されています。
- ゲートウェイの NTP 設定をサポートします。ゲートウェイの NTP 設定は、ゲートウェイに割り当てることが可能な NTP プロファイルを使用して設定できます。
- 入力保護のための Azure GWLB ベースのアーキテクチャをサポートします。

修正

このアップグレードには、次の修正が含まれています。

- トラフィックに SNI が存在しない場合にトラフィックが誤ったルールによって処理される FQDN 一致オブジェクトの問題を修正します。
- IDS/IPS および WAF カスタムルールのサポートより前に作成された DLP および IDS/IPS プロファイルが、プロファイルが変更されて保存されない限り、想定どおりに動作しない可能性がある問題を修正します。
- ゲートウェイがクライアントに誤った証明書を発行する可能性がある、大量のバースト TLS トラフィックに関連したイングレスゲートウェイの問題を修正します。このシナリオの発生はまれであり、ゲートウェイリリース 22.12-04 以前で発生する可能性があるダウンストリームの問題です。この修正は、ダウンストリームの問題にまで発展しないようにすることでこの問題に対処し、問題の発生を防ぎます。
- ポリシーが 2 つ以上の一意のリスナーポートで指定され、それぞれが同じ SNI とバックエンド設定を共有している場合に、同じ証明書が発行される可能性がある問題を修正します。
- 更新済みパッケージのロードに失敗した後に、データパスエンジンが起動しない問題を修正します。この問題は、パッケージの更新が Linux カーネル自体ではなく Valtix によって処理される、新しい CentOS 9 ベースイメージを使用して対処されています。
- FQDNFILTER イベントで、送信元および宛先 IP/ポート情報が逆に表示される問題を修正します。
- アクションが拒否に設定されているときに、古い Controller バージョンを使用して作成されたプロファイルが URL を正常に拒否しない、URL フィルタプロファイルに関連した問題を修正します。
- L7DOS プロファイル設定に関連したトラフィック処理の問題を修正します。プロファイルの要求レートまたはバーストサイズが 1 に設定されている場合、データパスによってトラフィックが適正に制限されません。
- L7DOS プロファイル設定に関連したトラフィック処理の問題を修正します。プロファイルの要求レートまたはバーストサイズが 0 に設定されている場合、データパスは指定された URL/URI に関連したトラフィックを抑制します。この方法を使用して L7DOS プロファイルで URL/URI をブロックすることもできますが、推奨される方法は、URL フィルタプ

ロファイルを作成し、URLに関連したトラフィックを処理するポリシー規則セットルールにそのプロファイルを適用することです。

- ゲートウェイからCSPストレージシステム（S3バケット、GCPロギング）に直接送信されるトラフィックサマリーログとイベントのフィールド値のフレンドリ名が整数で表される問題を修正します。この修正には、ユーザーによる文書化された整数からフレンドリ名への変換が必要です。ログとイベントには、整数値ではなくフレンドリ名が含まれるようになります。
- さまざまなトラフィックパターンに関連したイーグレスゲートウェイの安定性の問題を修正します。
- 重複するホストヘッダーがバックエンド接続に追加される、Websocketプロキシに関連した問題を修正します。一般に、RFCでは複数の（および重複する）ホストヘッダーが許可されているため、これは問題ではありません。ただし、複数のホストヘッダーを受け入れないアプリケーション フレームワークもあります。アプリケーションサーバーとしてのNgnixは、そのようなシステムの1つです。Nginxは、複数のホストヘッダーを持つHTTPトラフィックを受信すると、セッションを拒否して400 Bad Requestを返します。
- 脆弱性スキャナに情報通知が表示される可能性がある、ゲートウェイ管理CentOS Linuxコンテナに関連したOSの脆弱性を修正します。
- まれにデータパスの自己修復を引き起こす場合がある、AzureゲートウェイのMLX4 DPDKドライバの問題を修正します。
- 自動スケーリングCPUのしきい値を75%から95%に変更して、CPUベースの自動スケーリングの感度を下げます。

バージョン 23.02

バージョン 23.02-10（2023 年 6 月 28 日）

修正

このアップグレードには、次の修正が含まれています。

- DNSベースのキャッシュ設定をゲートウェイに適用すると、ゲートウェイインスタンスに異常が発生する問題を修正します。

バージョン 23.02-09（2023 年 6 月 25 日）

修正

このアップグレードには、次の修正が含まれています。

- 一貫したゲートウェイの正常性を確保するために設定されていた15日間の定期的なゲートウェイデータパスの自己修復を削除します。この機能は、把握と修正が困難なある問題

に対処するために2年以上前に組み込まれました。問題はその後解決しましたが、定期的な自己修復は削除されませんでした。この機能は不要になり、現在は削除されています。

- GCP ゲートウェイがサポート関連の診断バンドルを生成できない問題を修正します。
- プロファイルの変更が導入されていないにもかかわらず、NTPプロファイルがゲートウェイに繰り返し適用される問題を修正します。
- FQDNフィルタリングプロファイルが適用されているときに、ポリシールールセットが持続的な「更新中」状態になる可能性がある問題を修正します。
- 空のアドレスオブジェクトがゲートウェイに適用されると、トラフィック処理の問題が発生する問題を修正します。
- NTP プロファイルとログ転送プロファイルの両方をゲートウェイに同時に適用すると、データパスの不要な自己修復が発生する問題を修正します。この問題は、それぞれの操作が独立しているため、オーケストレーションを使用してプロファイルが適用された場合にのみ発生します。順次、非常に短い期間内に発生します。

バージョン 23.02-08（2023 年 6 月 15 日）

修正

このアップグレードには、次の修正が含まれています。

- WAF アクションを [ログの許可（Allow Log）] から [ルールデフォルト（Rule Default）] に変更すると、データパスが複数回再起動する可能性がある問題を修正します。
- プリエンプティブデータパスの自己修復によって対処される、低速セッションプールリークに関連した23.04-05で行われた変更を元に戻すための更新を提供します。以前の更新では、プリエンプトできないデータパスの自己修復が発生する可能性があります。このリリースでは、最初の問題が完全に解決されるまでの間、安定性が確保されます。

バージョン 23.02-07（2023 年 6 月 8 日）

修正

このアップグレードには、次の修正が含まれています。

- ゲートウェイによって処理されるトラフィックに対して L4_FW イベントが一貫して生成されない問題を修正します。
- チャンクされた転送エンコーディングを含む HTTP トラフィックにより、WAF で大量のメモリが消費され、データパスの自己修復がトリガーされる可能性がある問題を修正します

バージョン 23.02-06（2023 年 6 月 2 日）

修正

このアップグレードには、次の修正が含まれています。

- トラフィックを中断させる可能性のあるサイレントデータパスの再起動を引き起こす低速メモリリークを修正します。
- プリエンプティブなデータパスの自己修復を引き起こす可能性のある、超低速セッションプールリークを修正します。
- FQDN一致を使用するルールセットによってトラフィックが処理されるときに、拒否時のリセット（TCP リセット）が実行されない問題を修正します。
- 3 つを超えるレベルを含むドメインでルールが設定されている場合に、イングレスゲートウェイが誤った証明書を発行する可能性がある問題を修正します。
- アドレスオブジェクトを頻繁に変更すると、データパスがそれ以上の変更を受け入れなくなる可能性がある問題を修正します。
- データパスの自己修復を引き起こす、ゲートウェイの安定性のさまざまな問題を修正します。

バージョン 23.02-05（2023 年 5 月 22 日）

拡張機能

このアップグレードには、次の機能拡張が含まれています。

- ゲートウェイ設定として有効になっている拡張メモリ プロファイリング モードを使用可能にします。このモードは、メモリ消費を把握する高度なトラブルシューティングに役立ちます。

修正

このアップグレードには、次の修正が含まれています。

- FQDN一致を使用するポリシー規則セットルールのトラフィック処理に関する問題を修正します。FQDN と一致する TLS SNI を含むセッションが最初は拒否されますが、後続のセッションが誤って許可されます。

バージョン 23.02-04（2023 年 4 月 14 日）

修正

このアップグレードには、次の修正が含まれています。

- 重複するホストヘッダーがバックエンド接続に追加される、Websocket プロキシに関連した問題を修正します。一般に、RFC では複数の（および重複する）ホストヘッダーが許可されているため、これは問題ではありません。ただし、複数のホストヘッダーを受け入れないアプリケーション フレームワークもあります。アプリケーションサーバーとしての Ngnix は、そのようなシステムの 1 つです。Nginx は、複数のホストヘッダーを持つ HTTP トラフィックを受信すると、セッションを拒否して 400 Bad Request を返します。
- TLS 再ネゴシエーション設定を設定可能な設定に移動しました。再ネゴシエーションに依存する古いクライアントに関する潜在的な問題のため、再ネゴシエーションのデフォルト状態を有効に戻しました。
- 自動スケーリング CPU のしきい値を 75% から 95% に変更して、CPU ベースの自動スケーリングの感度を下げます。

バージョン 23.02-03（2023 年 3 月 7 日）

修正

このアップグレードには、次の修正が含まれています。

- IDS/IPS および WAF カスタムルールのサポートより前に作成された DLP および IDS/IPS プロファイルが、プロファイルが変更されて保存されない限り、想定どおりに動作しない可能性がある問題を修正します。

バージョン 23.02-02（2023 年 2 月 20 日）

修正

このアップグレードには、次の修正が含まれています。

- ゲートウェイがクライアントに誤った証明書を発行する可能性がある、大量のバースト TLS トラフィックに関連したイングレスゲートウェイの問題を修正します。このシナリオの発生はまれであり、ゲートウェイリリース 23.02-01 で発生する可能性があるダウンストリームの問題です。この修正は、ダウンストリームの問題にまで発展しないようにすることでこの問題に対処し、問題の発生を防ぎます。
- CVE-2009-3555 に関連する脆弱性に対処するための TLS 再ネゴシエーションを無効にしました。
- FQDN フィルタリングイベントで、送信元および宛先 IP/ポート情報が逆に表示される問題を修正します。

バージョン 23.02-01（2023 年 2 月 15 日）

拡張機能

このアップグレードには、次の機能拡張が含まれています。

- IP アドレスキャッシングに対応するように DNS ベースの FQDN アドレスオブジェクトを拡張します。この機能拡張により、DNS 解決頻度（更新間隔）、IP アドレス TTL（エントリ TTL）、IP アドレスキャッシュサイズ（キャッシュ）に関連するゲートウェイ設定の構成可能なセットが提供されます。これらの設定は、Terraform を使用してのみ適用できます。適用されない場合、デフォルト値は、DNS 解決頻度が 60（秒）、IP アドレス TTL（キャッシングなし）が 0（秒）、IP アドレスキャッシュサイズ（キャッシングなし）が 0（アドレス数）です。
- Egress/East-West ポリシールールセットのルール一致基準を強化し、FQDN 一致プロファイルと呼ばれる FQDN プロファイルの新しいバリエーションを導入します。FQDN プロファイルバリアントは、ポリシーが SNI で一致できるように TLS 暗号化トラフィックに適用できる PCRE 定義の FQDN のセットです。これにより、セグメンテーションポリシーが強化され、FQDN に基づいてより細かく制御する必要があるポリシーの柔軟性が高まります。

修正

このアップグレードには、次の修正が含まれています。

- 接続が null になるとデータパスの自己修復を引き起こす可能性がある、セッションのアップストリーム接続に関連するイングレスゲートウェイの問題を修正します。
- チャンクエンコーディングが有効になっている大規模な POST コマンドに関連する WAF の安定性の問題を修正します。
- フロントエンド（クライアントからゲートウェイ）で KA が有効になっており、バックエンド（ゲートウェイからサーバーへ）で KA が無効になっている、HTTP キープアライブに関連するイングレス ゲートウェイ セッション プールの枯渇の問題を修正します。
- サービスが存在しない GCP サービスを利用して、空の IP/CIDR を含むポリシーが生成される、動的ポリシーに関連する問題を修正します。設定が有効であり、ポリシーに空の IP/CIDR が含まれている可能性があるケースをゲートウェイが処理する必要があります。
- データパスの自己修復を引き起こす可能性のある、ルール一致に関連する問題を修正します。
- Azure が要求されたものとは異なるインターフェイスタイプを割り当て、パフォーマンスの低下の可能性を示す警告メッセージを投稿するゲートウェイ プロビジョニングに関連するシステムログメッセージとして表示される、Azure で生成されたメッセージを削除します。メッセージは「`TYPE_AZURE_DEGRADED_PERFORMANCE`」と表示されます。割り当てられたインターフェイスタイプに関連するパフォーマンスへの影響はありません。
- すべてのユースケースでゲートウェイの安定性を強化し、セッションプールが枯渇する可能性を排除します。

Multicloud Defense Terraform Provider のレガシーバージョン

バージョン 23.7

バージョン 23.7.2（2023 年 7 月 27 日）

修正

このバージョンには、次の修正が含まれています。

- policy 引数のない `mode=MATCH` 引数を持つ FQDN プロファイル（`valtix_fqdn_profile`）リソースにより、一致するトラフィックが拒否される問題を修正します。policy 引数を指定する必要はなく、Terraform プロバイダーのドキュメントには引数としてリストされていません。

バージョン 23.7.1（2023 年 7 月 24 日）

修正

このリリースには、次の修正が含まれています。

- Azure VNet のダイナミック VPC アドレスオブジェクト（`valix_address_object`）リソースを作成すると、「'region' パラメータがサポートされていません（'region' parameter is not supported）」というエラーが発生する問題を修正します。
- `mode=MATCH` 引数を持つ FQDN プロファイル（`valtix_fqdn_profile`）リソースが「policy」引数を誤って必要とする問題を修正します。

バージョン 23.6

バージョン 23.6.1（2023 年 7 月 17 日）

拡張機能

このリリースには、次の機能拡張が含まれています。

- アラートプロファイル（`valtix_alert_profile`）リソースを強化して、アラート（システムログ、監査ログ）の Webex Teams への送信をサポートするようになりました。
- 動的ユーザー定義タグのアドレスオブジェクト（`valtix_address_object`）リソースにスコープとしてサブネットリソースを含めることに対するサポートを追加します。

修正

このリリースには、次の修正が含まれています。

- Azure VNet のダイナミック VPC アドレスオブジェクト（`valix_address_object`）リソースを作成すると、「'region' パラメータがサポートされていません（'region' parameter is not supported）」というエラーが発生する問題を修正します。
- Azure でのゲートウェイ（`valtix_gateway`）リソースの展開で、中南部/米国リージョンに展開しようとするとエラーが表示される問題を修正します。

バージョン 23.5

バージョン 23.5.1（2023 年 6 月 12 日）

拡張機能

このリリースには、次の機能拡張が含まれています。

- Valtix Terraform プロバイダーをミラーリングする Multicloud Defense Terraform Provider を公開しました。新しいプロバイダーは `ciscomcd` と呼ばれ、近い将来に公開される予定です。プロバイダーは同時に更新され、特に明記されていない限り、相互にミラーになります。近い将来、Valtix プロバイダーは廃止され、シスコプロバイダーに完全に置き換えられます。

修正

このリリースには、次の修正が含まれています。

- ゲートウェイ（`valtix_gateway`）リソースを Azure ゾーン 1 中南部/米国リージョンに展開するとエラーが発生する問題を修正します。
- Azure ゲートウェイ ロードバランサベースのアーキテクチャにイングレスゲートウェイを展開するときに、Azure ゲートウェイロードバランサのフロントエンドリソース ID を出力するように、ゲートウェイ（`valtix_gateway`）リソースの属性を強化します。出力は、ゲートウェイエンドポイント（`gateway_gwlb_endpoints`）属性の一部として指定されます。
- 適切なメンバーリソース引数を参照するように、ポリシー規則セット（`valtix_policy_rule_set`）グループリソースの例を修正します。

バージョン 23.4

バージョン 23.4.3（2023 年 5 月 23 日）

修正

このリリースには、次の修正が含まれています。

- Azure ゲートウェイ ロードバランサベースのアーキテクチャにイングレスゲートウェイを展開するときに、Azure ゲートウェイロードバランサのフロントエンドリソース ID を出力するように、ゲートウェイ（valtix_gateway）リソースの属性を強化します。出力は、ゲートウェイエンドポイント（gateway_gwlb_endpoints）属性の一部として指定されます。

バージョン 23.4.2（2023 年 5 月 11 日）

修正

このセクションには、次の修正が含まれています。

- リソースにアクセスしようとすると、無効なデータソースエラーが生成される、NTP プロファイル（valtix_ntp_profile）データソースの問題を修正します。
- Terraform ドキュメントを更新して、NTP プロファイル（valtix_ntp_profile）リソースとデータソースの情報を追加します。

バージョン 23.4.1（2023 年 4 月 20 日）

拡張機能

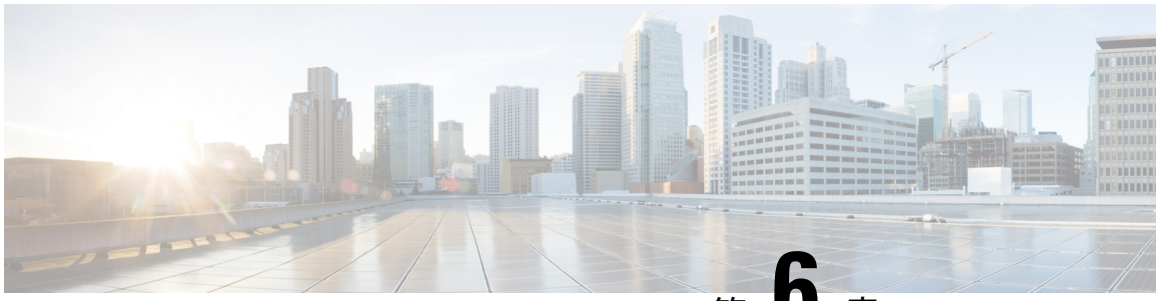
このリリースには、次の機能拡張が含まれています。

- ポリシー規則セット（valtix_policy_rule_set）リソースを変更して、現在は廃止されている child_rule_set_ids 引数に代わる group_member_ids 引数を含めます。

修正

このリリースには、次の修正が含まれています。

- ゲートウェイリソース（valtix_gateway）に関連する Terraform の**インポート**操作の問題を修正します。
- Azure ゲートウェイに SSH キーペア（ssh_key_pair）を指定すると、引数がサポートされていないことを示すエラーが発生するゲートウェイリソース（'）の問題を修正します。
- WAF 規則 ID 949110 および 959100 の抑制に関連する問題を修正します。これらの規則 ID は情報提供であり、WAF プロファイルリソース（valtix_profile_application_threat）設定に基づいて実行されたアクションとともに、WAF 異常スコア（要求と応答それぞれ）を超えたことを示すセキュリティイベントを定義します。これらの規則 ID が抑制されると、情報イベントは生成されません。この修正により、これらの規則 ID を抑制する機能が抑制され、情報イベントが常に生成されるようになります。
- ポリシー規則リソース（valtix_policy_rules）に関連する Terraform のインポート操作の問題を修正します。



第 6 章

リリースおよびサービスポリシー

リリースのバージョン管理とスケジュール

リリースのバージョン管理

Multicloud Defense リリースのバージョン管理は、X.Y-Z または X.Y.Z として定義されます。X はメジャーリリース（暦年で示される）、Y はマイナーリリース（暦月で示される）、Z はメンテナンスリリース（値 1 から始まる整数で示される）を示します。

メジャー リリース

メジャーバージョンは Multicloud Defense によるリリースであり、メジャーな機能拡張、安定性の向上、およびバグ修正が含まれています。

マイナー リリース

マイナーバージョンは Multicloud Defense によるリリースであり、マイナーな機能拡張、安定性の向上、およびバグ修正が含まれています。

メンテナンス リリース

メンテナンスバージョンは Multicloud Defense による頻繁な更新リリースであり、安定性の向上とバグ修正、および時折（まれに）機能拡張が含まれています。

ホットフィックスリリース

ホットフィックスリリースは、少数の展開（通常は単一の展開）に影響を与える運用上の問題に対処するバグ修正を含む優先リリースです。

ホットフィックスは、対応するメジャー、マイナー、およびメンテナンスリリースの機能拡張です。各ホットフィックスリリースには、文字で示されるホットフィックスリリース全体の累積的な機能拡張が含まれていません（たとえば、ホットフィックス B にはホットフィックス

Aからの機能拡張が含まれていません）。ただし、番号で示される、ホットフィックスリリース文字内の各ホットフィックスリリースには、累積的な機能拡張が含まれています（たとえば、ホットフィックス A2 にはホットフィックス A1 からの機能拡張が含まれています）。

各ホットフィックスリリースのリリースノートには、メジャー、マイナー、およびメンテナンスリリースの機能拡張以外の特定の機能拡張に関する情報が含まれています。

ホットフィックスリリースの機能拡張は、最終的にメンテナンスリリースに展開されます。ホットフィックスリリースへのアップグレードは、シスコサポートの指示があった場合にのみ行ってください。

リリースのスケジュール

Multicloud Defense は、3 ヵ月ごとにメジャーリリースまたはマイナーリリースの公表を試みます。メンテナンスリリースは、サポート終了およびライフサイクル終了ポリシーに従って、メジャーリリースまたはマイナーリリースごとに定期的に行われます。

リリースの有効期間とサポート

リリース日からサポート終了を経てライフサイクル終了に至るまでのリリースの有効期間を告知および適用するための定義とプロセス。

ライフサイクル終了/サポートポリシー

リリース日からサポート終了を経てライフサイクル終了に至るまでのリリースの有効期間を告知および適用するための定義とプロセス。

サポート終了（EoS）

すべてのメンテナンスリリースを含むメジャーまたはマイナーリリースが、問題のトラブルシュートまたは修正のためにサポートされる最後の日。この日以降はサポートされなくなります。新しいメンテナンスリリースは発行されません。Multicloud Defense は、推奨されるメジャーまたはマイナー、およびメンテナンスリリースへのアップグレードを支援し、問題がまだ存在するかどうかを判断し、修正または回避策の提供に取り組みます。

メジャーリリースまたはマイナーリリースは、リリース日から 6 ヵ月後にサポート終了としてマークされます。

通知

- 1 ヵ月前
- 1 週間前
- 当日

ライフサイクル終了（EOL）

メジャーリリースまたはマイナーリリース（関連メンテナンスリリースを含む）をインストールできる最後の日。この日以降はインストールできなくなります。Multicloud Defenseは、推奨されるメジャーまたはマイナー、およびメンテナンスリリースへのアップグレードを支援し、問題がまだ存在するかどうかを判断し、修正または回避策の提供に取り組みます。

メジャーまたはマイナーリリース（およびすべてのメンテナンスリリース）は、メジャーまたはマイナーリリースがサポート終了としてマークされてから2ヵ月後にライフサイクル終了としてマークされます。

通知

- 1ヵ月前
- 1週間前
- 当日

繰り上げられたEoS/EoL

Multicloud Defenseは、メジャーリリースまたはマイナーリリース（およびすべての関連メンテナンスリリース）のサポート終了および/またはライフサイクル終了を早める権利を留保します。Multicloud Defenseはお客様に通知し、推奨リリースへのアップグレードを支援します。

通知

- ケースバイケースで定義

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。