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。

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。