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。

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。