Cisco Multicloud Defense に関する FAQ

初版：2023 年 5 月 17 日

Cisco Multicloud Defense に関する FAQ

エッジ、ハブ、入力、出力とは何を意味しますか。

入力：アプリケーションは、VPC で実行されています。トラフィックは、外部（インターネット）から VPC に入ります。外部ユーザーからアプリケーションを保護するために、入力ゲートウェイが展開されます。

出力：外部（インターネット）との通信を必要とするクライアント/EC2 インスタンス/アプリケーション。インターネットへの出力トラフィックから、これらのクライアントを保護/制御するには、特定の Web サイト（決済ゲートウェイなど）や承認されたソースコードリポジトリとの通信のみに制限する必要があります。出力ゲートウェイは、発信トラフィックを制御するために展開されます。

エッジ：ゲートウェイ（出力および入力）は、エッジモードまたはハブモードで展開できます。エッジモードでは、ゲートウェイはアプリケーションと同じ VPC に展開されます。アプリケーションを実行している VPC が 5 つある場合は、5 つのゲートウェイが展開されます。これは、VPC の数が少ない場合に最適です。

ハブ：Multicloud Defense は、新しい VPC（サービス VPC と呼ばれる）を作成し、このサービス VPC 内にゲートウェイを展開します。アプリケーションを実行するすべての VPC と、ゲートウェイを内包するサービス VPC は、AWS Transit Gateway を介して接続されます。Multicloud Defense は Transit Gateway、VPC 接続、およびルーティングのオーケストレーションを自動的に管理します。ユーザーは、VPC ルートテーブルを編集して、Transit Gateway をデフォルトルートの宛先にする必要があります。Transit Gateway は、新規または既存の場合があります。

Multicloud Defense では、入力および出力での使用に応じて個別にゲートウェイを展開する必要があります。単一のゲートウェイを使用して入力トラフィックと出力トラフィックを保護することはできません。

フォワードプロキシとリバースプロキシとは何ですか。

転送プロキシのルールとサービスは、出力ゲートウェイによって使用されます。ゲートウェイは、入力モードと出力モードの両方でプロキシサーバーとして機能します。入力の場合、ユーザーは Multicloud Defense Gateway によって提供されるプロキシエンドポイントにアクセスします。出力シナリオでは、プロキシは透過的です。VPC 内のクライアントは、Multicloud Defense Gateway を介したルーティングによって外部サイト（インターネット）にアクセスします。ゲートウェイは、クライアントに応答します。ゲートウェイが外部サイトの証明書に署名する

ために使用するルート証明書を指定するように求められます。クライアントには、このルート証明書が信頼できるソースとしてインストールされている必要があります。

リバースプロキシのルールとサービスは、入力ゲートウェイによって使用されます。サービス定義は、プロキシがリッスンするポート番号と、トラフィックを転送するターゲットのアプリケーション/ホストを定義します。

URL フィルタリングとは何ですか。

URL フィルタリングは、出力ゲートウェイでのみ使用されます。URL プロファイルとは、URL のリストと、各 URL のアクションです。URL プロファイルを作成すると、ポリシー規則に関連付けられます。トラフィックが URL プロファイルを持つルールに一致すると、URL フィルタリング処理が開始されます。リストは順番に渡され、トラフィックの URL に一致するリスト内の最初の項目のアクションが実行されます。デフォルトポリシーは、許可された URL に一致する URL がない場合に使用されます。プロファイルには、暗黙のアクション（デフォルトの ALLOW）があります。URL は、文字列または正規表現として指定できます。リスト内に DENY の正規表現一致がない限り、通常は ALLOW ルールは必要ありません。たとえば、https://website.com/news を許可し、同じ Web サイトの他のすべてを拒否する場合は、プロファイルで次の 2 つの項目を定義します。

https://www.website.com/news ALLOW

https://www.website.com/.* DENY

URL がドロップされると、Multicloud Defense Controller の **[調査（Investigate）]** > **[URL フィルタリング（URL Filtering）]** メニューの URL フィルタリングイベントにイベントのログが記録されます。

URL フィルタリングで正規表現を使用できますか。

はい。

URL フィルタリングのデフォルトアクションが許可である場合、なぜ ALLOW アクションが必要なのでしょうか。一致がない場合の URL フィルタリングのデフォルトアクションは、ALLOW です。リスト内で非常に広い範囲を対象とする DENY が下にある場合、特定のアクションを ALLOW にすると便利です。デフォルトアクションを DENY にするには、次のルールを追加します。

.* DENY 502

これにより、すべての URL がドロップされます。許可された特定の URL を開くには、この上にルールを追加して ALLOW を設定します。たとえば、google.com へのすべてのトラフィックを許可し、残りをすべて拒否する場合は、次のようにします。

https://www.google.com ALLOW .* DENY 502

これは、Web サイト上の広範なページを制限し、特定のページを許可するためにも使用できます。

https://www.website.com/news ALLOW

https://www.website.com/.* DENY

URL プロファイルに URL をどのように記述しますか。

URL リストの URL は、http または https を含む完全な文字列である必要があります。.*（ドットスター）などの正規表現を使用して、.google.com. などの汎用スキームを定義できます。これは、http または https、および google.com の前にあるプレフィックスと google.com の後にあるサフィックスに一致します。

L7 DOS とは何ですか。

L7 DOS は、入力ゲートウェイでのみ使用されます。ゲートウェイがバックエンド アプリケーションをターゲットとする入力プロキシとして機能する場合、URL のレート制限を適用できます。この制限は、HTTP アクション（GET、POST など）ごとに URL レベルで設定できます。レート制限は、ゲートウェイクラスタレベル全体ではなく、ファイアウォール インスタンス レベルで設定されます。そのため、レート制限が 1000 要求/秒に設定され、ゲートウェイに 3 つのファイアウォール インスタンスがある場合、アプリケーションは秒あたり 3000 要求を受信する場合があります。

ハブモードのゲートウェイを作成して VPC を保護するにはどうすればよいですか。

ハブモードのゲートウェイは、クラウド環境の一元的なセキュリティ管理に役立ちます。複数のスポーク VPC がアプリケーションを実行している場合、すべての VPC を保護する方法としてハブモードが推奨されます。セキュリティ管理は、サービス VPC で実行されます。ゲートウェイをホストするサービス VPC は、Multicloud Defense Controller によって管理されます。すべての VPC には、Transit Gateway に接続する前に、重複しない CIDR が必要です。ゲートウェイの作成時に、[入力（Ingress）] または [出力（Egress）] を選択し（プロセスは同じ）、[ハブモード（Hub mode）] オプションを選択します。既存の Transit Gateway を使用するか、新しい Transit Gateway を作成するかを選択します。すでにサービス VPC を作成している場合はサービス VPC を選択するか、または新しいサービス VPC を作成します。新しいサービス VPC を作成するときは、保護する予定のスポーク VPC のいずれとも重複しない CIDR を指定します。ゲートウェイの作成プロセスを続行します。他のサブネットまたはセキュリティグループ情報を入力する必要はありません。これらは、Multicloud Defense によって管理されます。アカウントの導入準備の一環として作成されたキーペアとファイアウォールロールを指定します。

ゲートウェイが作成されたら、ゲートウェイを編集して、保護するスポーク VPC を追加します。[ゲートウェイの編集（Edit Gateway）] オプションで、[VPCの保護（Protect VPCs）] まで下にスクロールし、保護する VPC をすべて選択します。Multicloud Defense は、選択したすべての VPC に Transit Gateway 接続を作成します。これにより、VPC からサブネットをランダムに選択して、接続を行います。VPC が接続されたら、アプリケーションサブネットにアタッチされている VPC ルートテーブルを変更し、Transit Gateway へのデフォルトルートを追加また

は設定します。入力ハブモードのゲートウェイの場合、デフォルトルートの代わりにサービス VPC CIDR へのルートを設定できます。出力ゲートウェイの場合、デフォルトルートが優先オプションですが、SSH/管理タスクでは、インターネットゲートウェイを使用するための特定のルートを設定できます。

自分の AWS アカウントを Valtix コントローラに追加するにはどうすればよいですか。

Multicloud Defense Controller には、ゲートウェイを作成するために AWS アカウントへのアクセス権が必要で、そのアカウントのインベントリおよび他のタスクへのアクセス権も必要です。Multicloud Defense Controller で使用するクロスアカウント IAM ロールを作成する CloudFormation テンプレート（CFT）は、Multicloud Defense によって提供されます。導入準備プロセスの一環として Multicloud Defense アカウント番号が提供されます。IAM ロールによって、このアカウントに権限が付与されます。このロールに割り当てられている権限については、IAM ロールのドキュメントを参照してください。

ゲートウェイとファイアウォールとは何ですか。

ゲートウェイとファイアウォールという用語は、ソリューションとドキュメント全体で同じ意味で使用されることがあります。ゲートウェイは、単一のエンティティとして管理されるファイアウォール インスタンスのクラスタです。ネットワークロードバランサ（NLB）は、このロードバランサのターゲットとしてすべてのファイアウォール VM インスタンスを持つゲートウェイ展開の一部として作成されます。ユーザーがインスタンスとゲートウェイを個別に管理することはありません。すべてコントローラによって管理されます。NLB は、セッショントラフィックが同じファイアウォール インスタンスに到達するようにします。ファイアウォール インスタンスは、セキュリティエンフォーサです。

Valtix ゲートウェイは HA、自動スケーリングをサポートしていますか。

Multicloud Defense セキュリティ プラットフォームは、クラウドに特化しています。HA と自動スケーリングは、最初からシステムに組み込まれています。ゲートウェイの作成中に、複数のゾーン（AZ）でアプリケーションを実行するのと同様に、複数のゾーンでインスタンスを作成するオプションが表示されます。少なくとも 2 つのゾーンでゲートウェイインスタンスを実行することをお勧めします。また、実行するゲートウェイインスタンスの数を選択することもできます。最小インスタンス数と最大インスタンス数を選択できます。自動スケーリングの詳細については、次の質問を確認してください。

自動スケーリングとは何ですか。Valtixはトラフィックに応じてどのようにスケーリングしますか。

ゲートウェイの作成中に、実行するファイアウォールインスタンスの数を選択するオプションが表示されます。最小数は常に 1 です。最大値は 10 です。これは可用性ゾーン（AZ）ごとに設定します。インスタンス数を 2 から開始し、2 つの AZ がある場合、アカウントで合計 4 つのインスタンスが実行されます。コントローラはインスタンスの使用状況をトラッキングし、ファイアウォールがビジーになると、最大数に達するまで新しいインスタンスを自動的に作成します。トラフィックが低下すると、インスタンスは自動的に削除されます。オンデマンドでリソースを作成し、使用するまたは必要な場合にのみ料金が発生します。インスタンスが必要ない場合、インスタンスは削除され、料金は発生しません。

Valtix の使用を開始するために AWS 環境を準備するにはどうすればよいですか。

Multicloud Defense セキュリティサービスは、ハブモードまたはエッジモードで動作します。ハブモードは、保護する VPC が複数ある場合に使用されます。AWS Transit Gateway は、すべての VPC の接続に使用されます。このモードでは、Multicloud Defense がゲートウェイを展開する新しいサービス VPC を作成できるように、重複しない CIDR を指定する必要があります。サービス VPC は、Multicloud Defense Controller によって完全に管理されます。

エッジモードの展開では、ゲートウェイはアプリケーションと同じ VPC にインストールされます。この展開では、Multicloud Defense に 2 つのパブリックサブネット（管理およびデータパス）と 2 つのセキュリティグループ（管理およびデータパス）が必要です。両方のセキュリティグループに、アウトバウンドトラフィックを許可するルールが必要です。データパス セキュリティグループですべてのトラフィックを許可するか、Multicloud Defense Controller でサービスに設定した特定のポートを自分で有効にできます。

どちらの展開モードでも、Multicloud Defense に次の複数の IAM ロールが必要です。AWS アカウントにアクセスするコントローラのクロスアカウント IAM ロール、KMS にアクセスするゲートウェイインスタンスに割り当てられた IAM ロール、PCAP ファイルを書き込む Secrets Manager および S3。

Multicloud Defense は、IAM ロールの作成を支援し、権限に関する詳細を含む CloudFormation テンプレートを提供します。これについては、ユーザーガイドの IAM ロールのドキュメントを参照してください。

Valtix の使用を開始するために Azure 環境を準備するにはどうすればよいですか。

Multicloud Defense ソリューションは、ハブモードまたはエッジモードで動作します。ハブモードは、保護する VNet が複数ある場合に使用されます。Azure UDR は、この目的で使用されます。

エッジモードの展開では、ゲートウェイはアプリケーションと同じ VNet にインストールされます。この展開では、Multicloud Defense に 2 つのパブリックサブネット（管理およびデータパス）と 2 つのネットワークセキュリティグループ（管理およびデータパス）が必要です。両方のセキュリティグループに、アウトバウンドトラフィックを許可するルールが必要です。データパスセキュリティグループですべてのトラフィックを許可するか、Multicloud Defense Controller でサービスに設定した特定のポートを自分で有効にできます。

どちらの展開モードでも、Multicloud Defense には Azure Active Directory ID（テナント ID）、サブスクリプション ID、クライアントキーとシークレットを指定した Active Directory（AD）のアプリケーション、そのアプリケーションに割り当てられた、リソース作成や Vault へのアクセスなどの権限があるカスタムロールが必要です。

詳細については、ユーザーガイドのドキュメントを参照してください。

フローログの Sessionid とは何ですか。

Multicloud Defense Gateway は、入力と出力の両方のプロキシとして機能します。入力シナリオでは、インターネットからの外部ユーザーがゲートウェイエンドポイントにアクセスし、ゲートウェイがバックエンド（ターゲット）への新しいセッションを開始します。これらは、2 つの異なるトラフィックフローです。Sessionid は、これら 2 つのフローを関連付け、フローログに表示するために結び付けます。

プロキシ経由のアプリケーションに証明書を指定するにはどうすればよいですか。

TLS 復号化プロファイルは、自己署名証明書を生成するオプションや、すでに生成された証明書の内容をインポートするオプションがある場合に定義する必要があります。

TLS 復号化プロファイルは、バックエンドでプロキシされるアプリケーションのリバースプロキシのリスナー復号化プロファイルとして設定できます。

TLS 復号化プロファイルは、転送プロキシのルート CA 復号化プロファイルとして設定できます。ルート CA の証明書と秘密キーは、クライアント（転送プロキシ経由でインターネットに送信される）にインストールされています。

Valtixコントローラに渡さずに秘密キーを保護するにはどうすればよいですか。

TLS 復号化プロファイルの定義では、秘密キーをインポートする方法が複数あります。

- 内容を平文形式でインポート。
- AWS KMS で暗号化された秘密キー。
- AWS Secrets Manager のシークレット名。
- 指定されたクレデンシャルストアの Credstash キー名。
- 指定された Key Vault の Azure キー名。

秘密キーを Multicloud Defense Controller に残したくない場合は（b）、（c）、（d）、（e）を選択することをお勧めします。

リバースプロキシサービスに表示される、さまざまなプロトコルオプションには何がありますか。

表 *1:* リバースプロキシサービスに表示される、さまざまなプロトコルオプションには何がありますか。

プロキシ タイプ（Proxy Type）	復号化プロファイル	フロントエンドプロトコル	バックエンドプロトコル
TCP-TCP	非対応	TCP	TCP
TLS-TLS	対応	TCP	TCP
HTTP-HTTP	非対応	TCP	HTTP
HTTPS-HTTPS	対応	TCP	HTTPS
HTTPS-HTTP	対応	TCP	HTTP
WEBSOCKET-WEBSOCKET	非対応	TCP	WEBSOCKET
WEBSOCKETS - WEBSOCKETS	対応	TCP	WEBSOCKET_S

SSH アプリケーションのリバースプロキシを設定するにはどうすればよいですか。

プロキシタイプ TCP-TCP を使用します。

リバースプロキシターゲットの HTTPS と TLS の違いは何ですか。

TLS プロキシでは、クライアントまたはサーバーから受信した TCP ペイロードは、復号化と再暗号化の間、バイト単位で保持されます。TCP ペイロードバイトの保存が必須である NTLM に依存する RDP などのアプリケーションがあります。

HTTPS プロキシでは、プロキシは HTTP 接続を終了し、HTTP ペイロードをプロキシの 1 つのレッグから別のレッグに移動し、HTTP PDU にプロキシヘッダーを付加します。HTTPS プロキシを使用すると、ディープ パケット セキュリティ関連のアクションに対して HTTP レベルで応答を送信できます。また、URL レベルでレート制限を指定することもできます。

複数のゲートウェイに同じポリシー規則を適用するにはどうすればよいですか。

ポリシー規則は、常にポリシー規則セットのコンテキストで定義されます。ポリシー規則セットでは、一連のルールが定義されます。このポリシー規則セットは、複数のゲートウェイに関連付けることができます。各ゲートウェイに設定できるポリシー規則セットは 1 つだけです。

ターゲットアプリケーションの IP はリージョンごとに異なるか、または変更する可能性があります。サービスでバックエンドターゲットを設定するにはどうすればよいですか。

アプリケーションが実行されているインスタンスに関連付けられているユーザー定義タグを定義します。このタグを使用して、バックエンドアドレス オブジェクトを定義します。このバックエンド アドレス オブジェクトをサービスのターゲットとして関連付けます。コントローラは、そのタグを持つインスタンスの IP セットのメンバーシップを自動的に維持します。メンバーシップの変更は、そのユーザー定義タグを持つインスタンスが起動および停止した場合、またはそのユーザー定義タグを持つインスタンスの IP アドレスが変更された場合にも、コントローラによって自動的に処理されます。

サービスオブジェクトの SNI とは何ですか。

SNI は Server Name Indication の略です。サーバーの FQDN を含む server_name と呼ばれる TLS クライアント hello 拡張があります。これをサービスオブジェクトの定義で使用し、適切なバックエンドにトラフィックをルーティングできます。サービスオブジェクトで定義された SNI のセットを使用して、クライアントからそれらのサービスへのアクセスのみを許可することもできます。

サービスオブジェクトの定義における SNI の例：service1.enterprise.com

これは、バックエンドサービスと、関連するFQDNが明確に定義されているリバースプロキシでのみ意味があります。

バックエンド/ターゲットが複数の Web サイトをホストしています。Valtix ゲートウェイを使用して、これらを同じポートでプロキシ経由にする必要があります。これを実現するにはどうすればよいですか。

Web サイトごとにサービスオブジェクトを定義します。各サービスオブジェクトで同じリスナーポートを使用し、Web サイトの SNI と FQDN を同じにします。

ゲートウェイによってプロキシされる必要がある複数の Web バックエンド/ターゲットがあります。これを設定するにはどうすればよいですか。

同じリスナーポートを使用するWebバックエンドごとに、以下の設定をしたサービスオブジェクトを定義します。

- SNI = Web バックエンド FQDN および
- target = Web バックエンドをフロントエンド化するバックエンド FDQN または ALB FQDN

復号化プロファイルと証明書の関係とは何ですか。

復号化プロファイルは、証明書と 1 対 1 です。この復号化プロファイルは、ポリシー規則の一部として使用されるサービスオブジェクトに関連付けることができます。このレベルの間接化によって、この証明書に依存するポリシー規則/サービスのすべてを更新することなく、復号化プロファイルのみを更新して、期限切れの証明書の更新または定期的な証明書のローテーションを行う証明書管理が容易になります。

バックエンドごとに異なる IPS 保護ルールが必要です。どのようにすればよいですか。

各ゲートウェイに設定できる IPS プロファイルは 1 つだけです。これはルールレベルで設定されますが、ゲートウェイごとに設定されます。そのため、同じゲートウェイを使用して複数の IPS プロファイルを持つことはできません。複数のゲートウェイを作成する必要があります。

IPSルールはどこにあり、どのくらいの頻度で更新されますか。更新はゲートウェイに自動的にプッシュされますか。

Cisco TALOS ルールは、隔週で定期的にポーリングされます。重大なルール更新通知の場合は、これより短い期間でポーリングされます。これらの更新は、コントローラで自動的に利用可能になります。対象となるユーザーには、適切なルールセットバージョンを選択してゲートウェイにプッシュするオプションがあります。

IPSプロファイルには多くの設定オプションがあります。説明してください。

IPS プロファイルを使用すると、ユーザーは SNORT ポリシー、カテゴリ、またはクラスタイプに基づいてルールセットからルールのセットを選択できます。

また、脅威ベースの PCAP ファイルの作成を有効にするオプションもあります。

ルールの抑制は、信頼できる送信元 CIDR に基づく誤検出に対して適用されます。

ルールレベルのイベントフィルタは、通信量の多さに関するルールまたはすべてのルールにわたるグローバル プロファイル レベルのイベントフィルタに対して有効にできます。

すべての攻撃のPCAP（パケットキャプチャ）ファイルを取得したいのですが、可能ですか。

はい。ネットワーク侵入プロファイルまたは Web 保護プロファイルの [脅威ベースのPCAP（Threat Based PCAP）] チェックボックスをオンにします。

独自のログ分析インフラストラクチャがあります。ログを転送できますか。

はい。Syslog、Splunk、および DataDog がサポートされています。詳細については、ユーザーガイドのドキュメントを参照してください。

バックエンドアプリケーションへのリバースプロキシを設定しました。他に何をする必要がありますか。

1. Multicloud Defense Gateway の FDQN を指すように DNS レコードを変更します。

2. 既存のアプリケーションロードバランサをプライベートに変更して、直接パブリックアクセスをしないようにします。

DNS のプロファイルとレコードとは何ですか。それを使用する理由は何ですか。

AWS の Web ベースのアプリケーションは、通常、ロードバランサの作成時に動的に生成される内部 FQDN によって参照されます。Multicloud Defense をアプリケーションの入力パスに配置してインスペクションを行う場合、Multicloud Defense Gateway を参照するアプリケーションの DNS レコードを更新することをお勧めします。

たとえば、app.xyz.com の DNS レコードは、内部アプリケーション ロード バランサの CNAME を指します。Multicloud Defense Gateway をこのアプリケーションの入力パスに配置する場合、Multicloud Defense Gateway エンドポイントの CNAME を指すように DNS レコードを更新します。Multicloud Defense DNS プロファイルを使用すると、アプリケーションに関連付けられた Route53 ドメイン名を指定できます。これにより、このアプリケーションのレコードを設定し、ゲートウェイのリストから適切な Multicloud Defense 入力ゲートウェイを選択できます。

【注意】シスコ製品をご使用になる前に、安全上の注意（ **www.cisco.com/jp/go/safety_warning/** ）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

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。