サービス オブジェクト

リバース プロキシ サービス オブジェクト（入力）

入力サービスオブジェクトは、入力/リバースプロキシルールで使用されます。このオブジェクトは、Multicloud Defense ゲートウェイが受信したトラフィックをリッスンし、ターゲット/バックエンドアドレスに転送するリスナーポートを定義します。リスナーポートは、TLS 証明書が設定された復号プロファイルを使用して設定できます。トラフィックがリスナーポートに到達すると、Multicloud Defense Gateway は設定された TLS 証明書を返します。次の設定可能なオプションを検討してください。

- このポートで SNI を設定できます。これにより、単一のリスナーポート（443 など）を SNI に基づいて複数のバックエンドターゲットにプロキシできます。
- L7 DoS（L7 サービス妨害）をサービスで設定して、URI や HTTP メソッドのレート制限を設定できます。
- ターゲットは、トラフィックを転送するバックエンド アドレス オブジェクトとポートを定義します。プロキシされたトラフィックは、HTTP、HTTPS、TCP、または TLS として転送できます。

リバース プロキシ サービス オブジェクトを作成して追加するには、次の手順を実行します。

手順

ステップ 1 **[管理（Manage）] > [セキュリティポリシー（Security Policies）] > [サービス（Services）]**に移動します。

ステップ 2 [作成（Create）] をクリックします。

ステップ 3 [リバースプロキシ（Reverse Proxy）] をクリックします。

ステップ 4 [名前（Name）] と [説明（Description）] に入力します。

ステップ 5 以下の定義に従ってプロキシパラメータを設定します。

オプション	説明
復号プロファイル	プロキシサービスに使用する復号プロファイル（サーバー証明書も含まれる）を割り当てます。
Dst Port	宛て先ポートを割り当てます。ほとんどの Web ベースのサービスでは、宛て先ポートは 443 になります。これは、Multicloud Defense Gateway が着信トラフィックをリッスンするポートです。
プロトコル	デフォルトは TCP です。
SNI	SNI のリストを入力します。
L7 DoS	このプロキシサービスに割り当てるレイヤ 7 DoS プロファイルを入力します。
ターゲット バックエンド ポート	ターゲット/バックエンド アプリケーションのポート番号を入力します。
プロトコル	バックエンドプロトコルを選択します。
アドレス（Address）	バックエンド IP アドレスを選択します。ほとんどの場合、IP アドレスは内部ロードバランサのフロントエンド IP になります。

（注）
プロキシサービスを複数のポートで実行する必要がある場合は、エントリを追加できます。ただし、すべてのポートは同じ証明書を提供し、同じバックエンド宛先アドレスオブジェクトにプロキシされます。

転送サービスオブジェクト（出力/East-West）

転送プロキシサービスは、特に HTTP ベースのトラフィックに使用されます。オブジェクトは、Multicloud Defense Gateway が受信するトラフィックをリッスンし、 TLS SNI 拡張ヘッダーまたは HTTP ホストヘッダーで使用可能なアドレス/ホストに転送するリスナーポートを定義します。

（注） これは、出力/East-West トラフィックに使用することを推奨します。

転送プロキシサービスを作成して追加するには、次の手順を実行します。

手順

ステップ 1 **[管理（Manage）]** > **[セキュリティポリシー（Security Policies）]** > **[サービス（Services）]**に移動します。

ステップ 2 [作成（Create）] をクリックします。

ステップ 3 [転送プロキシ（Forward Proxy）] をクリックします。

ステップ 4 名前と説明を入力します。

ステップ 5 必要に応じて、照合するアプリケーション ID を選択します。

ステップ 6 以下の定義に従ってプロキシパラメータを設定します。

オプション	description
復号プロファイル	復号プロファイル（証明書も含まれる）を割り当てます。Multicloud Defense は、このプロファイルで提供される証明書で署名することにより、外部証明書を装います。ルート証明書がすべてのクライアントアプリケーションインスタンスにインストールされていることを前提とします。
Dst Port	宛て先ポートを割り当てます。ほとんどの Web ベースのサービスでは、宛て先ポートは 443 になります。
プロトコル	HTTP または HTTPS。

（注）

- Multicloud Defense は [宛て先ポート（Dst Port）] でリッスンし、HTTP ホストヘッダーまたは TLS SNI ヘッダーパケットを待機します。Multicloud Defense は、このパケットを受信すると、プロトコルを使用してホストに接続します。プロトコルが HTTPS の場合、外部ホストから受信した証明書データは、復号プロファイル内の証明書によって署名され、クライアントに送信されます。証明書エラーを回避するには、ルート証明書をクライアントアプリケーションインスタンスにインストールする**必要があります**。
- 特定の宛て先ポートに対して、すべてのサービスオブジェクトのポリシールールセットに存在できる復号プロファイル（ルート CA 証明書）のアソシエーションは 1 つだけです。
- 転送プロキシセッション中に、Multicloud Defense Gateway は接続先で DNS ルックアップを実行します。このとき、DNS リクエストタイムアウトは 30 秒、キャッシュエージアウトは TTL 秒です。

転送サービスオブジェクト（出力/East-West）

転送サービスオブジェクトは、転送ルールで使用されます。このタイプのルール/サービスに一致するトラフィックはプロキシされず、そのまま転送されます。つまり、暗号化されたトラフィックにはディープ パケット インスペクションもアプリケーション ID もありません。

（注） これは、East-West トラフィックに使用することを**強く**推奨します。

転送サービスオブジェクトを作成して追加するには、次の手順を実行します。

手順

ステップ 1 **[管理（Manage）] > [セキュリティポリシー（Security Policies）] > [サービス（Services）]**に移動します。

ステップ 2 [作成（Create）] をクリックします。

ステップ 3 [転送（Forwarding）] をクリックします。

ステップ 4 名前と説明を入力します。

ステップ 5 Multicloud Defense は、サービスレベルごとに送信元 NAT をサポートします。送信元 IP の保持が必要なトラフィック（East-West トラフィックなど）では、SNAT を無効化にします。

出力トラフィックでは、SNAT を常に有効にする**必要があります**。

ステップ 6 以下の定義に従ってポートパラメータを設定します。

オプション	説明
Dst Port	宛て先ポートまたは宛て先ポートの範囲を `start-end` として割り当てます。
プロトコル	TCP、UDP、ICMP

（注）
転送ポリシーでは、ディープ パケット インスペクション操作は、暗号化されていないトラフィックで**のみ**発生します。

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。