ルールとルールセット

ルール

ルールは一般に、ユーザー、グループ、ロール、または組織がドメイン内の指定されたタイプおよび状態のオブジェクトにアクセスするための権限を指定するものです。Multicloud Defense はさまざまなクラウド サービス プロバイダーをサポートしており、これらの環境にはそれぞれ独自の要件やルールのメソッドがあります。クラウドアカウントで作成されたルールは、Multicloud Defense Controller で作成されたルールとは異なる方法で処理される場合があります。一部のルールはデフォルトでゲートウェイとインスタンスに適用されるため、最適なパフォーマンスとカバレッジのためにルールとポリシーを追加および変更し続けても、環境には基本的なレベルの保護が提供されます。

ルールの**タイプ**は、対処するゲートウェイ環境のタイプを検討する際に重要です。すべてのルールまたはルールタイプがすべてのゲートウェイ環境に完全に対応しているわけではありません。Multicloud Defense Controller でサポートされているゲートウェイタイプは、イングレス、エグレス、および East-West です。

ルールとルールセットの詳細、またはポリシーとグループ向けにルールやルールセットを作成または変更する方法については、この章の残りの部分を参照してください。

ポリシー管理

ポリシーは、Multicloud Defense ダッシュボードで、または Multicloud Defense Terraform プロバイダーを使用したオーケストレーションによって作成されます。ポリシーは、Multicloud Defense Controller データベースの一部として保存および保持されます。ゲートウェイは定期的なハートビートを介してポリシーまたはポリシーの変更を取得します。ここでゲートウェイはコントローラに正常性とテレメトリ情報を提供すると同時に、適用する必要があるポリシー変更がある場合は要求します。ゲートウェイからコントローラへの通信は完全に暗号化され、相互 TLS

セッションを介して確立されます。ハートビートは5秒ごとに発生し、ゲートウェイ上のポリシーがユーザーによって作成または変更されたポリシーと確実に同期されるようにします。

ポリシールールセットのゲートウェイと管理

ポリシールールの管理

ゲートウェイに割り当てられたポリシールールセットは、別のポリシールールセットに動的に変更することができます。アクティブなゲートウェイで別のポリシールールセットに切り替える必要がある場合、この操作は影響のない方法で開始できます。新しいポリシールールセットの割り当ては、ゲートウェイの更新/アップグレードプロセスと同様に動作します。新しいゲートウェイインスタンスは、新しいポリシールールセットでインスタンス化されます。新しいトラフィックセッションがアクティブで正常な状態になると、新しいゲートウェイインスタンスにリダイレクトされます。古いトラフィックセッションは、古いゲートウェイインスタンスからフラッシュされます。古いゲートウェイインスタンスが削除されます。操作は数分で完了します。この変更は、ゲートウェイ構成設定の一部として開始されます。**[管理（Manage）]**>**[ゲートウェイ（Gateways）]**>**[ゲートウェイ（Gateways）]**に移動します。変更は、Multicloud Defense ポータルまたは Multicloud Defense Terraform Provider を使用して開始できます。

ポリシールールセットのゲートウェイステータス

ポリシールールとそれが関連付けられているゲートウェイ間の接続のステータスは、次の2つのオプションのいずれかになります。

- [更新済み（Updated）]：ポリシーはゲートウェイでアクティブであり、コントローラと同期されています。
- [更新中（Updating）]：ゲートウェイはポリシーの変更をアクティブに処理しています。ポリシーの変更はゲートウェイに認識されていますが、まだアクティブではありません。ゲートウェイは引き続き現在のポリシーを使用してトラフィックを処理します。

ルールセットとルールセットグループ

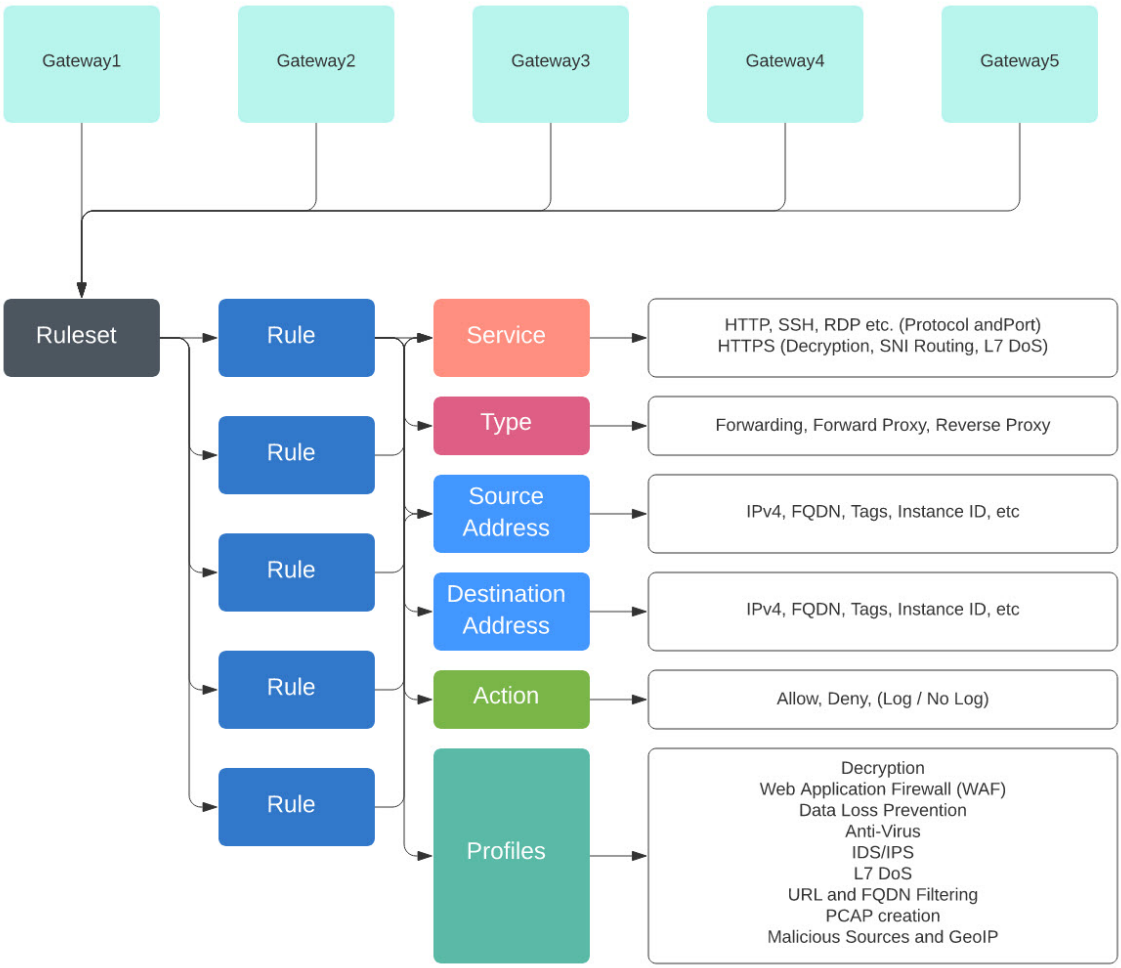
ルールセット

ルールセットは、アプリケーションとワークロードの保護に対応するために1つ以上のゲートウェイのセットに適用される、セグメンテーションと高度なセキュリティポリシーを定義する一連のルールで構成されます。ルールは優先順位リストとして整理されます。トラフィックは一致したルールによって処理され、許可または拒否の一般的なアクションが実行され、高度なセキュリティによってさらなる検査にも対応します。

ルールセットは、少なくとも 1 つの Multicloud Defense Gateway に関連付ける必要があります。次の制限は、すべてのルールセットに適用されます。

- ルールセットはクラウドに依存せず、複数のクラウド環境にまたがる 1 つ以上のゲートウェイ操作に適用できます。

- ゲートウェイは単一のルールセットにのみ関連付けることができますが、ルールセットのグループを使用して複数のルールセットを適用できます。
- ルールセット内のルールは、検出されたクラウドアセット情報を使用して、ダイナミックポリシー、または変更にリアルタイムで適応するポリシーを形成できます。
- ルールセットには、特定のクラウドアカウントやクラウドリージョンにのみ適用されるルールを含めることができますが、ルールセットはクラウド環境をまたぐゲートウェイに適用されます。次に例を示します。
  - ダイナミックなタグベースのアドレスオブジェクトを、2 つのクラウドにまたがる 2 つのゲートウェイに適用されるルールセット内のルールで使用して、片方のクラウド内のゲートウェイに関連付けられている IP アドレスのセットに解決できると同時に、別のクラウド内のゲートウェイに関連付けられている別の IP アドレスのセットに解決できます。
- ルールセットは、**[管理（Manage）]** > **[セキュリティポリシー（Security Policies）]** > **[ルールセット（Rule Sets）]**ページから、またはゲートウェイ作成ワークフロー内から作成できます。次の図は、複数のゲートウェイに適用される単一のルールセットを示しています。



サポートされているもう1つのユースケースは、複数のゲートウェイに関連付けられた複数のルールセットです。

ポリシー ルールセット グループ

ポリシー ルールセット グループは、スタンドアロンルールセットの集合です。ユーザーは、複数のスタンドアロンルールセットをポリシー ルールセット グループに結合し、そのグループを1つ以上のMulticloud Defense Gatewayに関連付けることができます。ポリシー ルールセット グループを使用すると、組織は、ポリシーを整然と区分けし、それらを包括的なポリシーに結合できます。

（注）

- ポリシー ルールセット グループは、ルールセットメンバーのみを構成要素とすることができます。
- ポリシー ルールセット グループに関連付けられているすべてのルールセットに競合するルールがないことを確認します。
- ポリシー ルールセット グループには、最大 100 のルールセットメンバーを含めることができます。

ポリシールールセットの作成

ポリシールールセットを作成するには、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）]** > **[ルールセット（Rule Sets）]**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 ポリシールールセットの名前と説明を追加します。

ステップ 4 [保存（Save）] をクリックします。

次のタスク

ポリシールールセットが作成されたら、ルールセットでの転送プロキシルールの追加または編集をルールセットに追加します。

ルールセットでのルールの作成

-

ルールセットでの転送ルールの追加または編集

ポリシールールセットに既存のルールを追加したり、ポリシールールセットにすでに含まれているルールを編集したりするには、次の手順を実行します。

始める前に

Multicloud Defense Gateway 内で新しいルールを作成できます。ルールセットにルールを追加または編集する前に、次の制限事項に注意してください。

- 1 つのポリシールールセットには、最大 2047 個のルールを含めることができます。

- 1つのポリシールールセットグループには、最大2047個のルールの組み合わせを含めることができます。

手順

ステップ1 **[管理（Manage）]** > **[セキュリティポリシー（Security Policies）]** > **[ルールセット（Rule Sets）]**に移動します。

ステップ2 ポリシールールセット名をクリックすると、ポリシールールセットが表示されます。

ステップ3 [ルールの追加（Add Rule）] をクリックして、新しいルールを作成するか、または既存のルールを追加します。これにより、プロンプトが生成されます。

ステップ4 次のプロパティを入力します。

- [名前（Name）]：ルールを参照するために使用される一意の名前。
- （任意）[説明（Description）]：ルールの簡単な説明。
- [タイプ（Type）]：[転送（Forwarding）] を選択します。

ステップ5 次のオブジェクト情報を入力します。

- [サービス（Service）]：ルールが適用されるプロトコルとポートを決定するために使用されるサービスオブジェクト。
- [送信元（Source）]：ルールが適用されるリソースを決定するために使用されるアドレスオブジェクト。
- [接続先（Destination）]：ルールが適用される接続先リソースを決定するために使用されるアドレスオブジェクト。[リバースプロキシ（ReverseProxy）]ルールタイプの場合、接続先は常にMulticloud Defense Gatewayです。[転送プロキシ（Forward Proxy）] ルールタイプの場合、接続先は常に [any] です。
- [FQDN]：ドロップダウンメニューを使用して、SNIの照合に使用される一連のFQDNを選択します。これは [転送（Forwarding）] ルールタイプにのみ適用されることに注意してください。

ステップ6 次の詳細情報を入力します。

- [アクション（Action）]：アクションは、トラフィックを許可または拒否するか、およびトラフィックをイベントに記録するかどうかを定義します。トラフィックは、アクションが [ログ（Log）] または [ログなし（No Log）] に設定されているかどうかに関係なく、常にトラフィックの概要に記録されます。ルールによって許可されるトラフィックでは、高度なセキュリティプロファイルが評価されます。高度なセキュリティプロファイルそれぞれに、このアクションを使用またはオーバーライドする独自のアクションがあることに注意してください。
- [拒否時にリセット（Reset On Deny）]：有効にすると、Multicloud Defense Gatewayは、このポリシーに一致し、ゲートウェイによってドロップされたセッションのTCPリセットパケットを送信します。これは [転送（Forwarding）] ルールタイプにのみ適用されることに注意してください。

ステップ7 次のプロファイル情報を入力します。

- （任意）[ネットワーク侵入（Network Intrusion）]：高度なセキュリティに使用されるネットワーク侵入（IPS）プロファイル。
- （任意）[マルウェア対策（Anti-malware）]：高度なセキュリティに使用されるマルウェア対策プロファイル。マルウェア対策プロファイルをまだ作成していない場合は、[+マルウェア対策プロファイルの作成（+ Create Anti Malware）] をクリックします。
- （任意）[データ損失防止（Data Loss Prevention）]：高度なセキュリティに使用されるデータ損失防止（DLP）プロファイル。これは [転送プロキシ（ForwardProxy）] ルールタイプにのみ適用されることに注意してください。
- （任意）[FQDNフィルタリング（FQDN Filtering）]：高度なセキュリティに使用される FQDN フィルタリング（FQDN）プロファイル。
- （任意）[悪意のあるIP（Malicious IPs）]：高度なセキュリティに使用される悪意のある IP（MIP）プロファイル。
- （任意）[PCAP]：有効にするには、このチェックボックスをオンにします。ルールでパケットキャプチャを有効にするか無効にするかを指定します。PCAP が有効になっているルールにトラフィックが一致するたびに、セッショントラフィックのパケットキャプチャが発生し、PCAP は PCAP プロファイルで指定された場所に保存されます。PCAP プロファイルは Multicloud Defense Gateway で設定されます。

ステップ 8 ルールの設定を指定したら、[保存（Save）] をクリックします。

ステップ 9 さらにルールを追加します。必要なルールをすべて追加したら、[変更を保存（Save Changes）] をクリックします。ルールセットに加えられたすべての変更の適用前と適用後のビューが表示されます。変更に問題がなければ、[保存（Save）] をクリックします。さらに変更を加える必要がある場合は、[キャンセル（Cancel）] をクリックしてルールセットの編集に戻ります。

ルールセットでのリバースプロキシルールの追加または編集

ポリシールールセットに既存のルールを追加したり、ポリシールールセットにすでに含まれているルールを編集したりするには、次の手順を実行します。

始める前に

Multicloud Defense Gateway 内で新しいルールを作成できます。ルールセットにルールを追加または編集する前に、次の制限事項に注意してください。

- 1 つのポリシールールセットには、最大 2047 個のルールを含めることができます。
- 1 つのポリシールールセットグループには、最大 2047 個のルールの組み合わせを含めることができます。

手順

ステップ 1 **[管理（Manage）]** > **[セキュリティポリシー（Security Policies）]** > **[ルールセット（Rule Sets）]**に移動します。

ステップ 2 ポリシールールセット名をクリックすると、ポリシールールセットが表示されます。

ステップ 3 [ルールの追加（Add Rule）] をクリックして、新しいルールを作成するか、または既存のルールを追加します。これにより、プロンプトが生成されます。

ステップ 4 次のプロパティを入力します。

- [名前（Name）]：ルールを参照するために使用される一意の名前。
- （任意）[説明（Description）]：ルールの簡単な説明。
- [タイプ（Type）]：[リバースプロキシ（ReverseProxy）] を選択します。

ステップ 5 次のオブジェクト情報を入力します。

- [サービス（Service）]：ルールが適用されるプロトコルとポートを決定するために使用されるサービスオブジェクト。
- [送信元（Source）]：ルールが適用されるリソースを決定するために使用されるアドレスオブジェクト。
- [接続先（Destination）]：ルールが適用される接続先リソースを決定するために使用されるアドレスオブジェクト。[リバースプロキシ（ReverseProxy）]ルールタイプの場合、接続先は常にMulticloud Defense Gateway です。
- [ターゲット（Target）]：Multicloud Defense Gateway がゲートウェイからサーバーへの接続を確立する接続先を指定するために使用されるアドレスオブジェクト。

ステップ 6 優先ルールの [アクション（Action）] を選択します。これは、トラフィックを許可または拒否するか、およびトラフィックをイベントに記録するかどうかを定義します。トラフィックは、アクションが [ログ（Log）] または [ログなし（No Log）] に設定されているかどうかに関係なく、常にトラフィックの概要に記録されます。ルールによって許可されるトラフィックでは、高度なセキュリティプロファイルが評価されます。高度なセキュリティプロファイルそれぞれに、このアクションを使用またはオーバーライドする独自のアクションがあることに注意してください。

ステップ 7 次のプロファイル情報を入力します。

- （任意）[ネットワーク侵入（Network Intrusion）]：高度なセキュリティに使用されるネットワーク侵入（IPS）プロファイル。
- （任意）[マルウェア対策（Anti-malware）]：高度なセキュリティに使用されるマルウェア対策プロファイル。マルウェア対策プロファイルをまだ作成していない場合は、[+マルウェア対策プロファイルの作成（+ Create Anti Malware）] をクリックします。

- （任意）[Webの保護（Web Protection）]：高度なセキュリティに使用される Web の保護（WAF）プロファイル。これは [リバースプロキシ（ReverseProxy）] ルールタイプにのみ適用されることに注意してください。
- （任意）[URLフィルタリング（URL Filtering）]：高度なセキュリティに使用される URL フィルタリング（URL）プロファイル。これは [転送プロキシ（ForwardProxy）] および[リバースプロキシ（ReverseProxy）] ルールタイプにのみ適用されることに注意してください。
- （任意）[悪意のあるIP（Malicious IPs）]：高度なセキュリティに使用される悪意のある IP（MIP）プロファイル。
- （任意）[PCAP]：有効にするには、このチェックボックスをオンにします。ルールでパケットキャプチャを有効にするか無効にするかを指定します。PCAP が有効になっているルールにトラフィックが一致するたびに、セッショントラフィックのパケットキャプチャが発生し、PCAP は PCAP プロファイルで指定された場所に保存されます。PCAP プロファイルは Multicloud Defense Gateway で設定されます。

ステップ 8 ルールの設定を指定したら、[保存（Save）] をクリックします。

ステップ 9 さらにルールを追加します。必要なルールをすべて追加したら、[変更を保存（Save Changes）] をクリックします。ルールセットに加えられたすべての変更の適用前と適用後のビューが表示されます。変更に問題がなければ、[保存（Save）] をクリックします。さらに変更を加える必要がある場合は、[キャンセル（Cancel）] をクリックしてルールセットの編集に戻ります。

ルールセットでの転送プロキシルールの追加または編集

ポリシールールセットに既存のルールを追加したり、ポリシールールセットにすでに含まれているルールを編集したりするには、次の手順を実行します。

始める前に

Multicloud Defense Gateway 内で新しいルールを作成できます。ルールセットにルールを追加または編集する前に、次の制限事項に注意してください。

- 1 つのポリシールールセットには、最大 2047 個のルールを含めることができます。
- 1 つのポリシールールセットグループには、最大 2047 個のルールの組み合わせを含めることができます。

手順

ステップ 1 **[管理（Manage）]** > **[セキュリティポリシー（Security Policies）]** > **[ルールセット（Rule Sets）]** に移動します。

ステップ 2 ポリシールールセット名をクリックすると、ポリシールールセットが表示されます。

ステップ 3 [ルールの追加（Add Rule）] をクリックして、新しいルールを作成するか、または既存のルールを追加します。これにより、プロンプトが生成されます。

ステップ 4 次のプロパティを入力します。

- [名前（Name）]：ルールを参照するために使用される一意の名前。
- （任意）[説明（Description）]：ルールの簡単な説明。
- [タイプ（Type）]：[転送プロキシ（ForwardProxy）] を選択します。

ステップ 5 次のオブジェクト情報を入力します。

- [サービス（Service）]：ルールが適用されるプロトコルとポートを決定するために使用されるサービスオブジェクト。
- [送信元（Source）]：ルールが適用されるリソースを決定するために使用されるアドレスオブジェクト。
- [接続先（Destination）]：ルールが適用される接続先リソースを決定するために使用されるアドレスオブジェクト。[転送プロキシ（Forward Proxy）] ルールタイプの場合、接続先は常に [any] です。
- [FQDN]：ドロップダウンメニューを使用して、SNI の照合に使用される一連の FQDN を選択します。これは [転送（Forwarding）] ルールタイプにのみ適用されることに注意してください。

ステップ 6 優先ルールの [アクション（Action）] を入力します。これは、トラフィックを許可または拒否するか、およびトラフィックをイベントに記録するかどうかを定義します。トラフィックは、アクションが [ログ（Log）] または [ログなし（No Log）] に設定されているかどうかに関係なく、常にトラフィックの概要に記録されます。ルールによって許可されるトラフィックでは、高度なセキュリティプロファイルが評価されます。高度なセキュリティプロファイルそれぞれに、このアクションを使用またはオーバーライドする独自のアクションがあることに注意してください。

ステップ 7 次のプロファイル情報を入力します。

- （任意）[ネットワーク侵入（Network Intrusion）]：高度なセキュリティに使用されるネットワーク侵入（IPS）プロファイル。
- （任意）[マルウェア対策（Anti-malware）]：高度なセキュリティに使用されるマルウェア対策プロファイル。マルウェア対策プロファイルをまだ作成していない場合は、[+マルウェア対策プロファイルの作成（+ Create Anti Malware）] をクリックします。
- （任意）[データ損失防止（Data Loss Prevention）]：高度なセキュリティに使用されるデータ損失防止（DLP）プロファイル。これは [転送プロキシ（ForwardProxy）] ルールタイプにのみ適用されることに注意してください。
- （任意）[URLフィルタリング（URL Filtering）]：高度なセキュリティに使用される URL フィルタリング（URL）プロファイル。これは [転送プロキシ（ForwardProxy）] および[リバースプロキシ（ReverseProxy）] ルールタイプにのみ適用されることに注意してください。
- （任意）[FQDNフィルタリング（FQDN Filtering）]：高度なセキュリティに使用される FQDN フィルタリング（FQDN）プロファイル。

- （任意）[悪意のあるIP（Malicious IPs）]：高度なセキュリティに使用される悪意のある IP（MIP）プロファイル。
- （任意）[PCAP]：有効にするには、このチェックボックスをオンにします。ルールでパケットキャプチャを有効にするか無効にするかを指定します。PCAP が有効になっているルールにトラフィックが一致するたびに、セッショントラフィックのパケットキャプチャが発生し、PCAP は PCAP プロファイルで指定された場所に保存されます。PCAP プロファイルは Multicloud Defense Gateway で設定されます。

ステップ 8 ルールの設定を指定したら、[保存（Save）] をクリックします。

ステップ 9 さらにルールを追加します。必要なルールをすべて追加したら、[変更を保存（Save Changes）] をクリックします。ルールセットに加えられたすべての変更の適用前と適用後のビューが表示されます。変更に問題がなければ、[保存（Save）] をクリックします。さらに変更を加える必要がある場合は、[キャンセル（Cancel）] をクリックしてルールセットの編集に戻ります。

ルールセットでのルールの無効化、編集、複製、または削除

ルールセットに設定されている既存のルールを編集または複製するには、次の手順を実行します。現在のポリシーまたはルールセットでアクティブにする必要がないルールについては、そのルールを無効化することもできます。ルールが不要になった場合、または今後の展開でルールが不要になる場合は、ルールを削除できます。

一度に編集または複製できるルールは1つだけであることに注意してください。複数のルールを同時に無効化または削除できます。

手順

ステップ 1 **[管理（Manage）]** > **[セキュリティポリシー（Security Policies）]** > **[ルールセット（Rule Sets）]**に移動します。

ステップ 2 無効化、編集、複製、または削除するルールを含むルールセットを探し、ルールセット名をクリックします。

ステップ 3 スタンドアロンルールのチェックボックスをオンにします。

ステップ 4 [アクション（Actions）] ボタンを展開します。

ステップ 5 アクション可能な項目を選択します。

- [無効化（Disable）]：このオプションでは、ルールはルールセット内に保持されますが、ルールおよび設定されたルールアクションがトラフィックに影響を与えないように無効化されます。
- [編集（Edit）]：このオプションを選択すると、[プロパティ（Properties）] ウィンドウが開き、ルールの設定を編集できます。[保存（Save）] をクリックして、変更を保存します。
- [複製（Clone）]：このオプションを選択すると、ルールの複製が作成されます。[プロパティ（Properties）] ウィンドウが開き、複製されたルールに名前を付けたり、ルールの設定に追加の変更を

加えたりできます。[保存（Save）] をクリックして、この設定を確定します。複製されたルールを保存すると、表示しているルールセットに自動的に追加されます。

- [削除（Delete）]：このオプションは、ルールセットからルールを完全に削除します。ルールはゲートウェイからも削除されることに注意してください。

ステップ 6 [変更を保存（Save Changes）] をクリックすると、ルールに加えた変更が確定され、間接的にルールセットが実行されます。変更を保存しない場合は、[キャンセル（Cancel）] をクリックします。ゲートウェイに加えた変更が失われても問題ないことを確認します。

ポリシー ルール セット グループの作成

ポリシー ルール セット グループを作成するには、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）] > [ルール（Rules）]**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 ポリシー ルール セット グループの名前と説明を追加します。

ステップ 4 グループとしての [タイプ（Type）] を選択します。

ステップ 5 ドロップダウンメニューを展開して、[ルールセットリスト（Rule Set List）] セクションでルールセットを追加します。ルールセットをさらに追加する場合は、[ルールセットの追加（Add Rule Sets）] をクリックして別の行を追加します。

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。