アクセス制御

ここでは、アクセス コントロール ルールについて説明します。これらのルールにより、デバイスを通過するトラフィックが制御されるとともに、侵入インスペクションなどの高度なサービスがトラフィックに適用されます。

アクセス コントロールの概要

次に、アクセス コントロール ポリシーを説明します。

アクセス コントロール ルールとデフォルト アクション

ネットワーク リソースへのアクセスを許可またはブロックするには、アクセス コントロール ポリシーを使用します。ポリシーは順序付けられた一連のルールで構成され、上から下へと評価されます。トラフィックに適用されるルールは、すべてのトラフィック条件が一致する最初のルールです。

アクセスの制御は次に基づいて行われます。

- 送信元と宛先の IP アドレス、プロトコル、ポート、インターフェイスなど従来のネットワーク特性（セキュリティ ゾーンの形式で）。
- 使用されているアプリケーション。アクセスコントロールは特定のアプリケーションに基づいて行うことも、アプリケーションのカテゴリ、特定の特性がタグ付けされたアプリケーション、アプリケーションのタイプ（クライアント、サーバ、Web）、またはアプリケーションのリスクやビジネスとの関連性の格付けを対象とするルールを作成できます。

- 汎用的なURLのカテゴリが含まれるWeb要求の宛先URL。ターゲット サイトのパブリック レピュテーションに基づいて、カテゴリの一致を絞り込むことができます。
- 要求を作成したユーザ、またはユーザが所属するユーザ グループ。

ユーザが許可する暗号化トラフィックの場合、IPS インスペクションを適用して脅威をチェックし、攻撃だと思われるトラフィックをブロックできます。また、禁止されたファイルやマルウェアをチェックするためにファイル ポリシーも使用できます。

アクセス ルールに一致しないすべてのトラフィックは、アクセス コントロールの [デフォルト アクション（Default Action）] によって処理されます。デフォルトでトラフィックを許可する場合は、侵入インスペクションをトラフィックに適用できます。ただし、デフォルト アクションで処理されるトラフィックでは、ファイルまたはマルウェアのインスペクションを実行できません。

アプリケーション フィルタリング

アクセス コントロール ルールを使用すると、接続で使用されるアプリケーションに基づいてトラフィックをフィルタリングできます。このシステムはさまざまアプリケーションを認識できるため、すべての Web アプリケーションをブロックせずに 1 つの Web アプリケーションをブロックする方法を探す必要はありません。

人気のあるアプリケーションでは、アプリケーションのさまざまな要素にフィルタ処理を行えます。たとえば、Facebook をブロックせずに、Facebook Games をブロックするルールを作成できます。

一般的なアプリケーション特性に基づいて、リスクまたはビジネスとの関連性、タイプ、タグを選択することでアプリケーション グループ全体をブロックまたは許可するルールを作成できます。**ただし、アプリケーション フィルタでカテゴリを選択するときは、目的のアプリケーション以外を含まないように一致するアプリケーションのリストをよく確認してください。**可能なグループ処理の詳細については、アプリケーション基準 （18 ページ）を参照してください。

暗号化および復号トラフィックのアプリケーション制御

アプリケーションが暗号化を使用する場合、システムはアプリケーションを識別できない場合があります。

システムは StartTLS（SMTPS、POPS、FTPS、TelnetS、IMAPSなど）で暗号化されたアプリケーション トラフィックを検出できます。さらに、TLS ClientHello メッセージの Server Name Indication、またはサーバ証明書のサブジェクト識別名の値に基づいて、特定の暗号化されたアプリケーションを識別できます。

アプリケーション フィルタのダイアログボックスを使用し、次のタグを選択することでアプリケーションに復号が必要かどうかを決定してから、アプリケーションのリストを確認します。

- [SSLプロトコル（SSL Protocol）]：SSL プロトコルとしてタグ付けされたトラフィックを解釈する必要はありません。システムはこのトラフィックを認識し、アクセス コントロー

ル操作を適用できます。リストされたアプリケーションのアクセス コントロール ルールは、想定される接続に一致する必要があります。

- [復号されたトラフィック（Decrypted Traffic）]：最初にトラフィックを復号する場合のみ、システムがこのトラフィックを特定できます。このトラフィックにSSL復号ルールを設定します。

アプリケーション フィルタリングのベスト プラクティス

アプリケーションフィルタリングのアクセス制御ルールを設計する際は、次の推奨事項を覚えておいてください。

- アドバタイズメント トラフィックなどの Web サーバによって参照されるトラフィックを処理するには、参照しているアプリケーションではなく、参照されるアプリケーションを照合します。
- アプリケーションと URL の基準を同じルールで組み合わせることは避けてください（特に暗号化されたトラフィックの場合）。
- [復号トラフィック（Decrypted Traffic）]のタグが付けられたトラフィックにルールを作成する場合、一致するトラフィックを復号するSSL復号ルールがあることを確認します。これらのアプリケーションは、復号された接続でのみ識別できます。
- システムは、Skype の複数のタイプの アプリケーション トラフィックを検出できます。Skypeトラフィックを制御するには、個々のアプリケーションを選択する代わりに、[アプリケーション フィルタ（Application Filters）] リストから [Skype] タグを選択します。これにより、システムは同じ方法でSkypeのすべてのトラフィックを検出して制御できるようになります。
- Zohoメールへのアクセスを制御するには、Zohoアプリケーションと Zoho Mailアプリケーションの両方を選択します。

URL フィルタリング

アクセス制御ルールを使用して、HTTP または HTTPS 接続に使用される URL に基づいてトラフィックをフィルタ処理できます。HTTPS は暗号化されるので、HTTP の URL フィルタリングは HTTPS の URL フィルタリングよりも簡単なものであることに注意してください。

次の手法を使用して、URL フィルタリングを実装できます。

- カテゴリおよびレピュテーション ベースのURL フィルタリング：URL フィルタリング ライセンスにより、URLの一般的な分類（カテゴリ）とリスク レベル（レピュテーション）に基づいて、Webサイトへのアクセスを制御できます。これは、不要なサイトをブロックするのに最も簡単で効果的な方法です。
- 手動 URL フィルタリング：任意のライセンスで、個々の URL および URL のグループを手動で指定し、Web トラフィックのきめ細かいカスタム制御を実現できます。手動フィルタリングの主な目的はカテゴリベースのブロック ルールに例外を作成することですが、他の目的にも手動ルールを使用できます。

ここでは、URL フィルタリングについてさらに詳しく説明します。

カテゴリ別とレピュテーション別の URL のフィルタリング

URL フィルタリング ライセンスを使用することにより、要求された URL のカテゴリおよびレピュテーションに基づいて Web サイトへのアクセスを制御できます。

- カテゴリ：URL の一般的な分類。たとえば ebay.com はオークション カテゴリ、monster.com は求職カテゴリに属します。1 つの URL は複数のカテゴリに属することができます。
- レピュテーション：この URL が、組織のセキュリティ ポリシーに違反するかもしれない目的で使用される可能性がどの程度であるか。レピュテーションは、高リスク（レベル 1）からウェルノウン（レベル 5）の範囲です。

URL カテゴリとレピュテーションによって、URL フィルタリングをすぐに設定できます。たとえば、アクセス コントロールを使用して、乱用薬物カテゴリの高リスク URL をブロックできます。

カテゴリ データおよびレピュテーション データを使用することで、ポリシーの作成と管理も簡素化されます。脅威を示すサイトや、望ましくないコンテンツを提供するサイトが現れては消えるペースが早すぎて、新しいポリシーを更新して適用するのが間に合わないこともあります。シスコが URL データベースで新しいサイト、変更された分類、変更されたレピュテーションについて更新すると、ルールは自動的に新しい情報に調整されます。新しいサイトを考慮するようにルールを編集する必要はありません。

定期的な URL データベースの更新を有効にすると、システムは最新の情報を使用して URL フィルタリングを行うことができます。また、Cisco Collective Security Intelligence（CSI）との通信を有効にすると、不明なカテゴリとレピュテーションについて URL の最新の脅威インテリジェンスを取得することもできます。詳細については、URL フィルタリングの設定を参照してください。

（注） イベントで URL カテゴリおよびレピュテーション情報を表示するには、URL 条件を使用して少なくとも 1 つのルールを作成する必要があります。

カテゴリとレピュテーションでの URL の検索

次のサイトを使用して、特定の URL のカテゴリとレピュテーションをチェックできます。この情報は、カテゴリおよびレピュテーショ ンベースの URL フィルタリング ルールの動作をチェックするために役立ちます。

https://www.brightcloud.com/tools/url-ip-lookup.php

手動 URL フィルタリング

個別の URL または URL のグループを手動でフィルタリングすることにより、カテゴリおよびレピュテーションベースの URL フィルタリングを補完または選択的にオーバーライドできます。特殊なライセンスなしでこのタイプの URL フィルタリングを実行できます。

たとえば、アクセス制御を使用して、組織にとって不適切なカテゴリの Web サイトをブロックできます。ただし、カテゴリに適切な Web サイトが含まれ、アクセスを提供したい場合、そのサイトに対して手動の許可ルールを作成し、カテゴリのブロック ルールの前に配置できます。

手動で URL フィルタリングを設定するには、対象の URL を含む URL オブジェクトを作成します。この URL を解釈する方法は、次のルールに基づきます。

- パスを含めない（つまり、URL に / の文字がない）場合、一致はサーバのホスト名のみに基づきます。ホスト名は、:// の区切り記号の後、またはホスト名のドットの後に来る場合、一致とみなされます。たとえば、ign.com は ign.com および www.ign.com と一致するが、verisign.com とは一致しません。
- 1 つ以上の / を含める場合、サーバ名、パス、およびクエリ パラメータを含む文字列の部分一致には URL 文字列全体が使用されます。ただし、サーバは再構成することができ、ページは新しいパスに移動できるため、個々の Web ページまたはサイトの一部をブロックまたは許可するのに手動の URL フィルタリングは使用しないことをお勧めします。文字列の部分一致も予期しない一致となる可能性があり、URL オブジェクトに含める文字列が意図しないサーバ上のパスやクエリ パラメータ内の文字列とも一致することがあります。
- システムは、暗号化プロトコル（HTTP と HTTPS）を無視します。つまり、ある Web サイトをブロックした場合、アプリケーション条件で特定のプロトコルを対象にしない限り、その Web サイトに向かう HTTP トラフィックと HTTPS トラフィックの両方がブロックされます。URL オブジェクトを作成する場合は、オブジェクトの作成時にプロトコルを指定する必要はありません。たとえば、http://example.com ではなく example.com を使用します。
- アクセス コントロール ルールで URL オブジェクトを使用して HTTPS トラフィックを照合することを計画している場合は、トラフィックの暗号化に使用される公開キー証明書内でサブジェクトの共通名を使用するオブジェクトを作成します。なお、システムはサブジェクトの共通名に含まれるドメインを無視するため、サブドメイン情報は含めないでください。たとえば、www.example.com ではなく、example.com を使用します。

  ただし、証明書のサブジェクト共通名が Web サイトのドメイン名とはまったく関係ない場合があることをご了承ください。たとえば、youtube.com の証明書のサブジェクト共通名は *.google.com です（当然、これは随時変更される可能性があります）。SSL 復号ポリシーを使用して HTTPS トラフィックを復号し、URL フィルタリング ルールが復号されたトラフィックで動作するようにすると、より一貫性のある結果が得られるようになります。

（注） 証明書情報を利用できないためにブラウザが TLS セッションを再開した場合、URL オブジェクトは HTTPS トラフィックと一致しません。このため、慎重に URL オブジェクトを設定した場合でも、HTTPS 接続では一貫性のない結果が得られることがあります。

HTTPS トラフィックのフィルタリング

HTTPS トラフィックは暗号化されているために、HTTPS トラフィックに対して直接URL フィルタリングを実行しても、HTTP トラフィックに対して行う場合ほどシンプルではありません。そのため、SSL 復号ポリシーを使用してフィルタリング対象のすべての HTTPS トラフィックを復号することを検討する必要があります。この方法では、URL フィルタリング アクセス コントロール ポリシーは復号されたトラフィックで機能し、通常のHTTP トラフィックの場合と同じ結果が得られます。

ただし、一部のHTTPS トラフィックが復号せずにアクセス コントロール ポリシーに渡されるようにする場合は、HTTPS トラフィックと一致するルールは HTTP トラフィックの場合と異なることを理解する必要があります。暗号化されたトラフィックをフィルタリングするには、システムはSSLハンドシェイク時に渡される情報（トラフィックを暗号化するために使用される公開キー証明書のサブジェクト共通名）に基づいて、要求された URL を決定します。URL の Web サイトのホスト名とサブジェクト共通名の間には、ほとんど、またはまったく関係がないことがあります。

HTTPSフィルタリングは、HTTPフィルタリングとは異なり、サブジェクト共通名内のサブドメインを無視します。HTTPS の URL を手動でフィルタリングする場合は、サブドメイン情報を含めないでください。たとえば、www.example.com ではなく、example.com を使用します。また、サイトによって使用される証明書の内容を確認し、サブジェクト共通名で使用されるドメインが正しいこと、この名前が他のルールと競合しないことを確認してください（たとえば、ブロックするサイトの名前が許可する名前と重複する可能性があります）。たとえば、youtube.com の証明書のサブジェクト共通名は *.google.com です（当然、これは随時変更される可能性があります）。

（注） 証明書情報を利用できないためにブラウザが TLS セッションを再開した場合、URL オブジェクトはHTTPS トラフィックと一致しません。このため、慎重にURL オブジェクトを設定した場合でも、HTTPS 接続では一貫性のない結果が得られることがあります。

暗号化プロトコルによるトラフィックの制御

システムは、URL フィルタリングの実行時に暗号化プロトコル（HTTP と HTTPS）を無視します。これは、手動およびレピュテーションベース両方の URL 条件で発生します。つまり、URL フィルタリングでは、次の Web サイトへのトラフィックが同様に処理されます。

- http://example.com
- https://example.com

両方ではなく、HTTP トラフィックのみまたは HTTPS トラフィックのみと一致するルールを設定するには、宛先の条件で TCP ポートを指定するか、アプリケーション条件をルールに追加します。たとえば、それぞれ、TCP ポートまたはアプリケーション条件と URL 条件を含む 2 つのアクセス制御ルールを作成することにより、サイトへの HTTPS アクセスを許可しながら、HTTP アクセスを禁止できます。

最初のルールは Web サイトへの HTTPS トラフィックを許可します。

アクション：許可
TCP ポートまたはアプリケーション：HTTPS（TCP ポート 443）
URL：example.com

2 番目のルールは同じ Web サイトへの HTTP アクセスをブロックします。

アクション：ブロック
TCP ポートまたはアプリケーション：HTTP（TCP ポート 80）
URL：example.com

URL フィルタリングとアプリケーション フィルタリングの比較

URL フィルタリングとアプリケーション フィルタリングには類似点があります。しかし、それらは非常に異なる目的で使用する必要があります。

- URL フィルタリングは、Web サーバ全体へのアクセスをブロックまたは許可するのに適しています。たとえば、ネットワーク上であらゆるタイプのギャンブルを許可しないようにする場合は、ギャンブル カテゴリをブロックする URL フィルタリング ルールを作成できます。このルールでは、ユーザはカテゴリ内の Web サーバ上のどのページにもアクセスできません。
- アプリケーション フィルタリングは、ホスティング サイトに関係なく特定のアプリケーションをブロックするため、またはそうしないと許容される Web サイトの特定の機能をブロックするために便利です。たとえば、Facebook のすべてをブロックすることなく Facebook のゲーム アプリケーションだけをブロックできます。

アプリケーション基準と URL の基準を組み合わせると予期しない結果につながることがあるため、URL とアプリケーションの基準では別のルールを作成するのが良いポリシーです。1 つのルールでアプリケーション基準と URL の基準を組み合わせる必要がある場合は、アプリケーションと URL のルールがより一般的なアプリケーションのみまたは URL のみのルールの例外として機能する場合を除き、単純なアプリケーションのみまたは URL のみのルールの後に配置する必要があります。URL フィルタリング ブロック ルールはアプリケーション フィルタリングよりも広範になるため、アプリケーションのみのルールの上に配置する必要があります。

アプリケーション基準と URL の基準を組み合わせる場合、より慎重にネットワークをモニタし、不要なサイトやアプリケーションへのアクセスを許可しないようにする必要があります。

効果的な URL フィルタリングのベスト プラクティス

URL フィルタリングのアクセス制御ルールを設計するときは、次の推奨事項を覚えておいてください。

- カテゴリとレピュテーションブロックは可能な限り使用します。これにより、新しいサイトはカテゴリに追加されるとともに、自動的にブロックされ、そのレピュテーションに基づくブロックは、サイトの評判が上がる（または下がる）と調整されます。
- URL カテゴリのマッチングを使用するときは、サイトのログイン ページがサイトそのものと異なるカテゴリにある場合に注意してください。たとえば、Gmail は [Webベースの電子メール（Web-based Email）] カテゴリにあり、ログイン ページは [インターネットポー

タル（Internet Portals）] カテゴリにあります。それらのカテゴリに関して異なるアクションを実行する異なるルールがある場合、意図しない結果が生じる可能性があります。

- URL オブジェクトを使用して、Web サイト全体を対象とし、カテゴリ ブロック ルールの例外を作成します。つまり、本来はカテゴリ ルールでブロックされる特定のサイトを許可します。
- （URL オブジェクトを使用して）Web サーバを手動でブロックする場合は、セキュリティ インテリジェンス ポリシーでこれを行うとより効果的です。セキュリティ インテリジェンス ポリシーはアクセス制御ルールが評価される前に接続をドロップするので、より速くより効率的にブロックできます。
- HTTPS 接続の最も効果的なフィルタリングのために、記述しているアクセス制御ルールの対象のトラフィックを復号する SSL 復号ルールを実装します。復号された HTTPS 接続はアクセス制御ポリシーの HTTP 接続としてフィルタ処理されるので、HTTPS フィルタリングの制限はすべて回避されます。
- URL のブロック ルールはアプリケーション フィルタリング ルールの前に配置します。URL フィルタリングは Web サーバ全体をブロックするのに対し、アプリケーション フィルタリングは Web サーバに関係なく、特定のアプリケーションの使用を対象とするためです。

Web サイトのブロック時にユーザに表示される内容

URL フィルタリング ルールで Web サイトをブロックした場合、ユーザに表示される内容は、サイトが暗号化されているかどうかに基づいて異なります。

- HTTP 接続：タイムアウトまたはリセットされた接続の場合、通常のブラウザ ページの代わりにシステムのデフォルトのブロック応答ページが表示されます。このページには、故意に接続がブロックされたことが明確に示されます。
- HTTPS（暗号化）接続：システムのデフォルトのブロック応答ページは表示されません。代わりに、ブラウザのセキュアな接続の障害時のデフォルト ページが表示されます。エラー メッセージには、ポリシーによってサイトがブロックされたことは示されません。代わりに、一般的な暗号化アルゴリズムがないと示される場合があります。このメッセージからは、故意に接続がブロックされたことは明らかになりません。

さらに、Web サイトは、明示的な URL フィルタリング ルールではないその他のアクセス コントロール ルールまたはデフォルトのアクションによってブロックされている場合があります。たとえば、ネットワーク全体または地理位置情報をブロックしている場合、ネットワーク上またはその地理的な位置にある Web サイトもブロックされます。これらのルールによってブロックされたユーザには、以下の制限で説明するとおり、応答ページが表示されることもあれば、表示されないこともあります。

URL フィルタリングを実装している場合、サイトが意図的にブロックされているときに表示されることがある内容と、どのタイプのサイトをブロックしているかについてエンドユーザに説明することを検討してください。そうでないと、エンドユーザがブロックされた接続のトラブルシューティングにかなりの時間を費やしてしまう場合があります。

HTTP 応答ページの制限

システムがWebトラフィックをブロックする場合に、常に、HTTP応答ページが表示されるわけではありません。

- Webトラフィックがプロモートされたアクセス コントロール ルール（単純なネットワーク条件のみの早期に適用されたブロッキング ルール）の結果としてブロックされている場合、システムは応答ページを表示しません。
- システムが要求されたURLを特定する前に、Webトラフィックがブロックされている場合、システムは応答ページを表示しません。
- アクセス コントロール ルールによってブロックされている暗号化された接続の場合、システムは応答ページを表示しません。

侵入、ファイル、マルウェアのインスペクション

侵入ポリシーとファイル ポリシーは、トラフィックが宛先に対して許可される前の最後のとりでとして連携して動作します。

- 侵入ポリシーは、システムの侵入防御機能を制御します。
- ファイル ポリシーは、システムのファイル コントロールとAMP for Firepowerの機能を制御します。

他のトラフィック処理はすべて、侵入、禁止されたファイル、およびマルウェアについて、ネットワーク トラフィックが調べられる前に実行されます。侵入ポリシーまたはファイル ポリシーをアクセス コントロール ルールに関連付けることで、アクセス コントロール ルールの条件に一致するトラフィックを通過させる前に、侵入ポリシーまたはファイル ポリシー（またはその両方）を使ってトラフィックのインスペクションを実行するよう、システムに指示できます。

トラフィックを [許可（allow）] するのみの侵入ポリシーおよびファイル ポリシーを設定できます。トラフィックを [信頼（trust）] または [ブロック（block）] するように設定されたルールではインスペクションは実行されません。さらに、アクセス コントロール ポリシーのデフォルトのアクションが [許可（allow）] の場合は、侵入ポリシーを設定できますが、ファイル ポリシーは設定できません。

アクセス コントロール ルールによって処理される単一接続の場合、ファイル インスペクションは侵入インスペクションの前に行われます。つまり、システムは侵入のためファイル ポリシーによってブロックされたファイルを検査しません。ファイル インスペクション内では、タイプによる単純なブロッキングの方が、マルウェア インスペクションおよびブロッキングよりも優先されます。ファイルがセッションで検出されてブロックされるまで、セッションからのパケットは侵入インスペクションの対象になります。

（注） デフォルトでは、暗号化されたペイロードの侵入インスペクションとファイルインスペクションは無効になっています。これにより、侵入およびファイルインスペクションが設定されたアクセス コントロール ルールに暗号化接続が一致したときの誤検出が減少し、パフォーマンスが向上します。暗号化されていないトラフィックのみのインスペクションが実行されます。

アクセス制御ルールの順序のベスト プラクティス

ルールは最初に一致したものから順に適用されるため、限定的なトラフィック一致基準を持つルールは、同じトラフィックに適用され、汎用的な基準を持つルールよりも上に置く必要があります。次の推奨事項を考慮してください。

- 固有のルールは一般的なルールの前に来る必要があります（特に特定のルールが一般的なルールの例外である場合）。
- レイヤ3/4基準（IPアドレス、セキュリティゾーン、ポート番号など）にのみ基づいてトラフィックをドロップするルールはできるだけ早く来る必要があります。レイヤ3/4基準は迅速かつ検査なしで評価することができるので、アプリケーションやURL基準などの検査を必要とするルールの前に来ることをお勧めします。もちろん、これらのルールの例外はこれらより上位に配置されなければなりません。
- 可能な限り、固有のドロップルールはポリシーの最上位近くに配置します。これにより、望ましくないトラフィックへの可能な限り早期の決定が保証されます。
- アプリケーションとURLの基準の両方を含むルールは、より一般的なアプリケーションのみまたはURLのみのルールの例外として機能している場合を除き、単純なアプリケーションのみまたはURLのみのルールの後に来る必要があります。アプリケーションとURLの基準を組み合わせることで、予期しない結果が生じることがある（特に暗号化されたトラフィックの場合）ため、可能な限り、URLとアプリケーションのフィルタリング用に個別のルールを作成することをお勧めします。

NAT とアクセス ルール

アクセス ルールは、NAT を設定している場合でも、アクセス ルールの一致を決定する際に常に実際の IP アドレスを使用します。たとえば、内部サーバ 10.1.1.5 用の NAT を設定して、パブリックにルーティング可能な外部の IP アドレス 209.165.201.5 をこのサーバに付与する場合は、この内部サーバへのアクセスを外部トラフィックに許可するアクセス ルールの中で、サーバのマッピング アドレス（209.165.201.5）ではなく実際のアドレス（10.1.1.5）を参照する必要があります。

その他のセキュリティ ポリシーがアクセス制御に影響する仕組み

その他のセキュリティ ポリシーは、アクセス制御ルールが機能し接続と一致する方法に影響を与えます。アクセス ルールを設定するときは、次の点に注意してください。

- [SSL復号] ポリシー：SSL 復号ルールはアクセス制御の前に評価されます。したがって、暗号化された接続が、復号化のいくつかのタイプを適用する SSL 復号ルールと一致する場合、それはアクセス コントロール ポリシーによって評価されるプレーン テキスト（復号化）接続です。アクセス ルールは、暗号化されたバージョンの接続を参照しません。また、トラフィックをドロップする SSL 復号ルールと一致するすべての接続はアクセス コントロールポリシーによって参照されることがありません。最後に、復号しないルールと一致する暗号化された接続は、その暗号化された状態で評価されます。
- [アイデンティティ] ポリシー：送信元 IP アドレスのユーザ マッピングがある場合にのみ接続はユーザ（およびユーザ グループ）と一致します。ユーザまたはグループ メンバーシップを重視するアクセス ルールは、ユーザ アイデンティティがアイデンティティ ポリシーによって正常に収集された接続のみと一致できます。
- [セキュリティインテリジェンス] ポリシー：アクセス コントロール ポリシーではブラックリストに登録されてドロップされた接続が参照されることはありません。
- [VPN]（サイト間またはリモート アクセス）：VPN トラフィックは常にアクセス コントロール ポリシーに対して評価され、一致するルールに基づいて接続は許可またはドロップされます。ただし、VPN トンネル自体はアクセス コントロール ポリシーが評価される前に復号化されます。アクセス コントロール ポリシーは、トンネル自体ではなく VPN トンネル内に組み込まれている接続を評価します。

アクセス制御のためのライセンス要件

アクセス制御ポリシーを使用するのに特別なライセンスは必要ありません。

ただし、アクセス制御ポリシー内の特定の機能には、次のライセンスが必要です。ライセンスの設定については、オプション ライセンスの有効化と無効化を参照してください。

- [URLフィルタリング] ライセンス：URL カテゴリおよびレピュテーションを一致基準として使用するルールを作成するため。
- [脅威] ライセンス：アクセス ルールまたはデフォルト アクションに侵入ポリシーを設定するため。ファイル ポリシーを使用する場合もこのライセンスが必要です。
- [マルウェア] ライセンス：マルウェア制御のためのアクセス ルールにファイル ポリシーを設定するため。

アクセスコントロールポリシーに関する注意事項と制限事項

アクセス制御のためのいくつかの追加の制限事項を次に示します。ルールから期待どおりの結果を得ているかどうかを評価してこれらを検討してください。

- Firepower Device Manager はディレクトリ サーバから最大 2000 人のユーザに関する情報をダウンロードできます。ディレクトリ サーバに 2000 以上のユーザ アカウントが含まれる場合、アクセス ルールでユーザを選択するとき、またはユーザ ベースのダッシュボード情報を閲覧するときに、すべての可能な名前を確認することができません。ルールは、ダウンロードしたこれらの名前だけに書き込むことができます。

  2000 までの制限は、グループに関連付けられた名前にも適用されます。グループに 2000 を超えるメンバーが含まれている場合は、ダウンロードした 2000 個の名前だけをグループメンバーシップと照合できます。

- 脆弱性データベース（VDB）の更新によってアプリケーションが削除（廃止）される場合は、削除されたアプリケーションを使用するアクセス制御ルールまたはアプリケーション フィルタに変更を加える必要があります。これらのルールを修正するまで、変更を展開することはできません。また、問題を修正する前にシステム ソフトウェア アップデートをインストールすることはできません。[アプリケーション フィルタ（Application Filters）] オブジェクト ページ、またはルールの [アプリケーション（Application）] タブでは、これらのアプリケーション名の後に「（廃止）（Deprecated）」と表示されます。

- 実際に使用されているルールを編集する場合、その変更は、Snort によって検査されなくなった、確立されている接続には適用されません。新しいルールは、将来の接続に対する照合に使用されます。また、Snort によって接続がアクティブに検査されている場合、Snort は、変更された一致またはアクション基準を既存の接続に適用できます。現在のすべての接続に変更を確実に適用する必要がある場合は、デバイス CLI にログインし、**clear conn** コマンドを使用して、確立されている接続を終了させることができます。これは、その後に接続の送信元が接続を再確立を試み、そのために新しいルールに対して適切に照合されることを前提としています。

- 接続のアプリケーションまたは URL を識別するためにシステムは 3 ～ 5 パケットを使用します。したがって、正しいアクセス制御ルールでも特定の接続ではすぐに一致しない可能性があります。ただし、アプリケーション/URL が判明すると、接続は一致するルールに基づいて処理されます。暗号化された接続の場合、これは SSL ハンドシェイクでのサーバ証明書の交換後に発生します。

- システムは、アプリケーションが識別される接続内にペイロードがないパケットに対してデフォルト ポリシー アクションを適用します。

- 可能な場合は常に、一致基準を空のままにします（特にセキュリティ ゾーン、ネットワーク オブジェクト、およびポート オブジェクトの場合）。たとえば、すべてのインターフェイスを含むゾーンを作成するのではなく、セキュリティ ゾーンの条件を空白のままにするだけで、すべてのインターフェイスのトラフィックについて照合の効率を高めることができます。基準を複数指定すると、指定した条件の内容についてすべての組み合わせと照合する必要があります。

- メモリの制約上、一部のモデルでは、小規模でそれほど細分化されていないカテゴリとレピュテーションによってほとんどの URL フィルタリングが実行されます。たとえば、親 URL のサブサイトがそれぞれ異なる URL カテゴリとレピュテーションを持っている場合でも、一部のデバイスでは、親 URL のデータのみが保存される場合があります。これらのデバイスによって処理される Web トラフィックの場合、システムはクラウドルックアッ

プを実行して、ローカルデータベースにないサイトのカテゴリとレピュテーションを判断できます。低メモリ デバイスには、5506-X、5506H-X、5506W-X、5508-X、5512-X、5515-X、5516-X、5525-X などの ASA モデルが含まれます。

アクセス コントロール ポリシーを設定する

ネットワーク リソースへのアクセスを制御するには、アクセス コントロール ポリシーを使用します。ポリシーは順序付けられた一連のルールで構成され、上から下へと評価されます。トラフィックに適用されるルールは、すべてのトラフィック条件が一致する最初のルールです。トラフィックに一致するルールがない場合、ページ下部に表示されるデフォルトアクションが適用されます。

アクセス コントロール ポリシーを設定するには、**[ポリシー（Policies）] > [アクセスコントロール（Access Control）]** を選択します。

アクセスコントロール表には、すべてのルールが順番に表示されます。各ルールで以下を実行します。

- 左側の列にあるルール番号の隣の [>] ボタンをクリックし、ルール図を開きます。この図は、ルールがトラフィックをどのように制御するかを視覚的に示します。ボタンを再度クリックして図を閉じます。
- ほとんどのセルはインライン編集が可能です。たとえば、アクションをクリックして別のものを選択したり、送信元ネットワーク オブジェクトをクリックして送信元の条件を追加または変更したりできます。
- ルールを移動するには、[移動（move）] アイコン（  ）が表示されるまでルールにカーソルを合わせ、次にルールをクリックして新しいロケーションにドラッグし、ドロップします。また、ルールを編集して [順序（Order）] リストで新しいロケーションを選択することで、ルールを移動することもできます。希望する処理の順番にルールを配置することが重要です。具体的なルール（特に、より一般的なルールに対する例外を定義するルール）は上部近くに配置します。
- 右側の列には、ルールのアクション ボタンが含まれます。セルにマウスを当てるとボタンが表示されます。ルールを編集（  ）または削除（  ）できます。

次に、ポリシーの設定方法について説明します。

デフォルト アクションの設定

接続が特定のアクセス ルールに一致しない場合、アクセス コントロール ポリシーのデフォルト アクションによって処理されます。

手順

ステップ 1 **[ポリシー（Policies）] > [アクセスコントロール（Access Control）]** を選択します。

ステップ 2 [デフォルトアクション（Default Action）] フィールドの任意の場所をクリックします。

ステップ 3 一致するトラフィックに適用するアクションを選択します。

- [信頼性（Trust）]：いかなる種類の追加インスペクションもなしでトラフィックを許可します。
- [許可（Allow）]：侵入ポリシーの対象となるトラフィックを許可します。
- [ブロック（Block）]：トラフィックを無条件でドロップします。トラフィックのインスペクションは実行されません。

ステップ 4 アクションが [許可（Allow）] の場合、侵入ポリシーを選択します。

ポリシー オプションの説明については、侵入ポリシーの設定 （22 ページ）を参照してください。

ステップ 5 （オプション）デフォルト アクションのロギングを設定します。

デフォルトアクションに一致するトラフィックのロギングをダッシュボードのデータまたはイベントビューアに記載されるようにするには、トラフィックのロギングを有効にする必要があります。ロギングの設定 （25 ページ）を参照してください。

ステップ 6 [OK] をクリックします。

アクセス コントロール ルールの設定

アクセスコントロールルールを使用して、ネットワーク リソースへのアクセスを制御します。アクセス コントロール ポリシーのルールは、上から下に評価されます。トラフィックに適用されるルールは、すべてのトラフィック基準が一致する最初のルールです。

手順

ステップ 1 **[ポリシー（Policies）] > [アクセスコントロール（Access Control）]** を選択します。

ステップ 2 次のいずれかを実行します。

- 新しいルールを作成するには、[+] ボタンをクリックします。
- 既存のルールを編集するには、ルールの [編集（edit）] アイコン（  ）をクリックします。

不要になったルールを削除するには、ルールの [削除（delete）] アイコン（  ）をクリックします。

ステップ 3 [順序（Order）] で、ルールの番号付きリストのどこにルールを挿入するかを選択します。

ルールは最初に一致したものから順に適用されるため、限定的なトラフィック一致基準を持つルールは、同じトラフィックに適用され、汎用的な基準を持つルールよりも上に置く必要があります。

デフォルトでは、ルールはリストの最後に追加されます。ルールの順序を後で変更する場合、このオプションを編集します。

ステップ 4 [タイトル（Title）] にルールの名前を入力します。

この名前にスペースを含めることはできません。英数字と以下の特殊文字を使用できます：+ . _ -

ステップ 5 一致するトラフィックに適用するアクションを選択します。

- [信頼（Trust）]：どのような種類のインスペクションも行わずにトラフィックを許可します。
- [許可（Allow）]：ポリシーで侵入およびその他のインスペクション設定の対象となるトラフィックを許可します。
- [ブロック（Block）]：トラフィックを無条件でドロップします。トラフィックのインスペクションは実行されません。

ステップ 6 次のタブの任意の組み合わせを使用して、トラフィック一致基準を定義します。

- [送信元/宛先（Source/Destination）]：トラフィックが通過するセキュリティ ゾーン（インターフェイス）、IP アドレス、または IP アドレスの国または大陸（地理的位置）、またはトラフィックで使用されるプロトコルおよびポート。デフォルトは、すべてのゾーン、アドレス、地理的位置、プロトコル、およびポートです。送信元/宛先基準 （16 ページ）を参照してください。
- [アプリケーション（Application）]：アプリケーション、またはタイプ、カテゴリ、タグ、リスク、ビジネスとの関連性ごとにアプリケーションを定義するフィルタ。デフォルトはすべてのアプリケーションです。アプリケーション基準 （18 ページ）を参照してください。
- [URL]：Web リクエストの URL または URL カテゴリ。デフォルトはすべての URL です。「URL 基準 （20 ページ）」を参照してください。
- [ユーザ（Users）]：ユーザまたはユーザ グループ。アイデンティティ ポリシーは、ユーザとグループの情報がトラフィックの照合に使用できるかどうかを定義します。この基準を使用するには、アイデンティティ ポリシーを設定する必要があります。ユーザ基準 （21 ページ）を参照してください。

条件を変更するには、条件内の [+] ボタンをクリックし、希望するオブジェクトまたは要素を選択し、ポップアップ ダイアログボックスの [OK] をクリックします。基準にオブジェクトが必要で、そのオブジェクトが存在しない場合、[新規オブジェクトの作成（Create New Object）] をクリックします。オブジェクトまたは要素をポリシーから削除するには、そのオブジェクトまたは要素の [x] をクリックします。

条件をアクセス コントロール ルールに追加する場合は、次のヒントを参考にしてください。

- 1 つのルールにつき複数の条件を設定できます。ルールがトラフィックに適用されるには、トラフィックがそのルールのすべての条件に一致する必要があります。たとえば、特定のホストまたはネットワークの URL フィルタリングを行う単一のルールを使用できます。

- ルールの条件ごとに、最大 50 の条件を追加できます。条件の基準のいずれかに一致するトラフィックはその条件を満たします。たとえば、最大 50 のアプリケーションまたはアプリケーション フィルタにアプリケーション制御を適用する単一のルールを使用できます。したがって、単一の条件では項目間に OR 関係がありますが、条件タイプ間（たとえば、送信元/宛先とアプリケーション間）には AND 関係があります。
- 一部の機能では、適切なライセンスを有効にする必要があります。

ステップ 7 （オプション）[許可（Allow）] アクションを使用するポリシーの場合、暗号化されていないトラフィックについてさらにインスペクションを設定できます。次のいずれかのリンクをクリックします。

- [侵入ポリシー（Intrusion Policy）]：トラフィックで侵入およびエクスプロイトを検査する場合は、**[侵入ポリシー（Intrusion Policy）]** > **[オン（On）]** を選択し、侵入検査ポリシーを選択します。「侵入ポリシーの設定 （22 ページ）」を参照してください。
- [ファイルポリシー（File Policy）]：マルウェアを含むファイルやブロックすべきファイルのトラフィックのインスペクションを実行するファイルポリシーを選択します。ファイルポリシーの設定 （23 ページ）を参照してください。

ステップ 8 （オプション）ルールのロギングを設定します。

デフォルトでは、ルールに一致するトラフィックに対して接続イベントは生成されませんが、ファイル ポリシーを選択した場合、ファイル イベントはデフォルトで生成されます。この動作は変更できます。ダッシュボード データまたはイベント ビューアに含まれるポリシーに一致するトラフィックのロギングを有効にする必要があります。ロギングの設定 （25 ページ）を参照してください。

マッチング アクセス ルールのログ構成に関係なくドロップまたはアラートするように設定されている侵入ルールについては、常に侵入イベントが生成されます。

ステップ 9 [OK] をクリックします。

送信元/宛先基準

アクセス ルールの送信元/宛先基準によって、トラフィックが通過するセキュリティ ゾーン（インターフェイス）、IP アドレスや IP アドレスの国または大陸（地理的位置）、またはトラフィックで使用されるプロトコルおよびポートが定義されます。デフォルトは、すべてのゾーン、アドレス、地理的位置、プロトコル、およびポートです。

条件を変更するには、その条件内の [+] ボタンをクリックして、目的のオブジェクトまたは要素を選択し、[OK] をクリックします。基準にオブジェクトが必要で、そのオブジェクトが存在しない場合、[新規オブジェクトの作成（Create New Object）] をクリックします。オブジェクトまたは要素をポリシーから削除するには、そのオブジェクトまたは要素の [x] をクリックします。

次の基準を使用して、ルールに一致する送信元および宛先を特定できます。

送信元ゾーン、宛先ゾーン

トラフィックが通過するインターフェイスを定義するセキュリティゾーンオブジェクト。1つの基準を定義する、両方の基準を定義する、またはどちらの基準も定義しないことができます。指定しない基準は、すべてのインターフェイスのトラフィックに適用されます。

- ゾーン内のインターフェイスからデバイスを離れるトラフィックを照合するには、そのゾーンを [宛先ゾーン（Destination Zones）] に追加します。
- ゾーン内のインターフェイスからデバイスに入るトラフィックを照合するには、そのゾーンを [送信元ゾーン（Source Zones）] に追加します。
- 送信元ゾーン条件と宛先ゾーン条件の両方をルールに追加する場合、一致するトラフィックは指定された送信元ゾーンの1つから発生し、宛先ゾーンの1つを通って出力する必要があります。

トラフィックがデバイスに出入りする場所に基づいてルールを適用する必要がある場合は、この基準を使用します。たとえば、ホスト内部に向かうすべてのトラフィックが侵入検査を受けるようにする場合は、内部ゾーンを [送信先ゾーン（Destination Zones）] として選択し、送信元ゾーンは空白のままにします。侵入フィルタリングをルールに含めるには、ルールのアクションを [許可（Allow）] にし、ルールで侵入ポリシーを選択する必要があります。

送信元ネットワーク、宛先ネットワーク

トラフィックのネットワーク アドレスまたは場所を定義する、ネットワーク オブジェクトまたは地理的位置。

- IPアドレスまたは地理的位置からのトラフィックを照合するには、[送信元ネットワーク（Source Networks）] を設定します。
- IP アドレスまたは地理的位置へのトラフィックを照合するには、[宛先ネットワーク（Destination Networks）] を設定します。
- 送信元（Source）ネットワーク条件と宛先（Destination）ネットワーク条件の両方をルールに追加する場合、送信元 IP アドレスから発信されかつ宛先 IP アドレスに送信されるトラフィックの照合を行う必要があります。

この条件を追加する場合、次のタブから選択します。

- [ネットワーク（Network）]：制御するトラフィックの送信元または宛先 IP アドレスを定義するネットワーク オブジェクトまたはグループを選択します。
- [地理位置情報（Geolocation）]：位置情報機能を選択して、その送信元または宛先の国や大陸に基づいてトラフィックを制御できます。大陸を選択すると、大陸内のすべての国が選択されます。ルール内で地理的位置を直接選択する以外に、作成した地理位置オブジェクトを選択して、場所を定義することもできます。地理的位置を使用すると、そこで使用される可能性があるすべての IP アドレスを知らなくても、特定の国へのアクセスを簡単に制限できます。

（注） 最新の地理的位置データを使用してトラフィックをフィルタ処理できるように、地理位置情報データベース（GeoDB）を定期的に更新することを強くお勧めします。

送信元ポート、宛先ポート/プロトコル

トラフィックで使用されるプロトコルを定義するポート オブジェクト。TCP/UDP では、ポートを含めることができます。ICMP では、コードとタイプを含めることができます。

- プロトコルまたはポートからのトラフィックを照合するには、[送信元ポート（Source Ports）] を設定します。送信元ポートを使用できるのは、TCP/UDP のみです。
- プロトコルまたはポートへのトラフィックを照合するには、[宛先ポート（Destination Ports）]/[宛先プロトコル（Destination Protocols）] を設定します。宛先ポートだけを条件に追加する場合は、異なるトランスポートプロトコルを使用するポートを追加できます。ICMP およびその他の非 TCP/UDP 仕様は、宛先ポートでのみ許可されます。送信元ポートでは許可されません。
- 特定の TCP/UDP ポートから送信されるトラフィックと特定の TCP/UDP ポートに向かうトラフィックの両方を照合するには、両方を設定します。送信元ポートと宛先ポートの両方を条件に追加する場合、単一のトランスポート プロトコル、TCP、または UDP を共有するポートのみを追加できます。たとえば、ポート TCP/80 からポート TCP/8080 へのトラフィックをターゲットにできます。

アプリケーション基準

アクセス ルールのアプリケーション基準では、IP 接続で使用されるアプリケーション、あるいは、タイプ、カテゴリ、タグ、リスク、またはビジネスとの関連性によってアプリケーションを定義するフィルタが規定されます。デフォルトは任意のアプリケーションです。

ルールで個別のアプリケーションを指定できますが、アプリケーション フィルタを使用すれば、ポリシーの作成と管理が簡単になります。たとえば、リスクが高く、ビジネスとの関連性が低いアプリケーションをすべて認識してブロックする、アクセス コントロール ルールを作成できます。ユーザがこのようなアプリケーションのいずれかを使用しようとすると、セッションがブロックされます。

また、シスコは、システムおよび脆弱性データベース（VDB）の更新を通じて頻繁にアプリケーションディテクタを更新し追加します。そのため、ルールを手動で更新せずに、高リスクアプリケーションをブロックするルールを新しいアプリケーションに自動的に適用できます。

アプリケーションとフィルタをルールで直接指定することも、これらの特性を定義するアプリケーション フィルタ オブジェクトを作成することもできます。指示は同じですが、複雑なルールを作成する場合、オブジェクトを使用した方が 基準当たり 50 項目のシステム上限範囲を超えにくくなります。

アプリケーションとフィルタ リストを変更するには、条件内の [+] ボタンをクリックし、別のタブに表示される目的のアプリケーションまたはアプリケーション フィルタ オブジェクトを

選択してから、ポップアップ表示されるダイアログボックスで [OK] をクリックします。いずれかのタブで [詳細フィルタ（Advanced Filte）] をクリックするか、またはフィルタ条件を選択して特定のアプリケーションを検索します。ポリシーからそれを削除するアプリケーション、フィルタ、またはオブジェクトの [x] をクリックします。[フィルタとして保存（Save As Filter）] リンクをクリックして、すでにオブジェクトではない結合基準を新しいアプリケーション フィルタ オブジェクトとして保存します。

（注） 選択したアプリケーションが VDB の更新によって削除されていた場合は、アプリケーション名の後ろに「（廃止（Deprecated））」と表示されます。これらのアプリケーションはフィルタから削除する必要があります。それ以降の展開では、システムソフトウェアのアップグレードがブロックされます。

次の [詳細フィルタ（Advanced Filter）] 基準を使用すると、ルールに一致するアプリケーションまたはフィルタを特定できます。これらはアプリケーション フィルタ オブジェクトで使用されるものと同じ要素です。

（注） 1 つのフィルタ条件内での複数の選択はOR関係にあります。たとえば、リスクが「高（High）」または（OR）「非常に高い（Very High）」となります。フィルタ間の関係は「論理積（AND）」であるため、リスクが「高（High）」または（OR）「非常に高い（Very High）」であり、かつ（AND）ビジネスとの関連性が「低（Low）」または（OR）「非常に低い（Very Low）」となります。フィルタを選択すると、ディスプレイに表示されるアプリケーションが更新され、条件を満たすものだけが表示されます。これらのフィルタを使用すると、個別に追加するアプリケーションを容易に見つけたり、ルールに追加する目的のフィルタを選択していることを確認したりできます。

リスク

アプリケーションが組織のセキュリティポリシーに反する可能性がある目的のために使用される確率（「非常に低い」から「非常に高い」まで）。

ビジネスとの関連性

アプリケーションが、娯楽とは逆に、組織の事業運営の文脈内で使用される確率（「非常に低い」から「非常に高い」まで）。

タイプ

アプリケーションのタイプ：

- [アプリケーションプロトコル（Application Protocol）]：HTTP や SSH などのホスト間の通信を表すアプリケーション プロトコル。
- [クライアントプロトコル（Client Protocol）]：Web ブラウザや電子メール クライアントなどのホスト上で動作しているソフトウェアを表すクライアント。

- [Webアプリケーション（Web Application）]：HTTP トラフィックの内容または要求された URL を表す MPEG ビデオや Facebook などの Web アプリケーション。

カテゴリ

アプリケーションの最も重要な機能を説明する一般分類。

タグ

カテゴリに似た、アプリケーションに関する追加情報。

暗号化されたトラフィックの場合、システムは[SSLプロトコル（SSL Protocol）] とタグ付けされたアプリケーションだけを使用して、トラフィックを識別およびフィルタリングできます。このタグがないアプリケーションは、暗号化されていないまたは復号されたトラフィックでのみ検出できます。また、システムは、復号されたトラフィック（暗号化された、または暗号化されていないトラフィックではなく）のみで検出を行うことができるアプリケーションに [復号されたトラフィック（decrypted traffic）] タグを割り当てます。

アプリケーション リスト（ディスプレイ下部）

上記のリストのオプションからフィルタを選択するとこのリストが更新されるため、現在のフィルタに一致するアプリケーションを確認できます。ルールにフィルタ条件を追加するときに、フィルタが目的のアプリケーションを対象としていることを確認するためにこのリストを使用します。特定のアプリケーションを追加しようとしている場合、このリストからそのアプリケーションを選択します。

URL 基準

アクセス ルールの URL 基準は、Web 要求で使用される URL または要求された URL が属するカテゴリを定義します。カテゴリが一致する場合は、許可またはブロックするためのサイトの相対レピュテーションも指定できます。デフォルトでは、すべての URL が許可されます。

URL のカテゴリおよびレピュテーションにより、アクセス コントロール ルールの URL 条件をすぐに作成できます。たとえば、すべての暗号化されたギャンブル サイトをブロックしたり、リスクの高いすべてのソーシャル ネットワーキング サイトを復号できます。ユーザがそのカテゴリとレピュテーションの組み合わせで URL を閲覧しようとすると、セッションがブロックされます。

カテゴリ データおよびレピュテーション データを使用することで、ポリシーの作成と管理も簡素化されます。この方法では、システムが Web トラフィックを期待通りに確実に制御します。最後に、脅威インテリジェンスは新しい URL だけでなく、既存の URL に対する新しいカテゴリとリスクで常に更新されるため、システムは確実に最新の情報を使用して、要求された URL をフィルタします。マルウェア、スパム、ボットネット、フィッシングなど、セキュリティに対する脅威を表す悪意のあるサイトは、組織でポリシーを更新したり新規ポリシーを展開したりするペースを上回って次々と現れては消える可能性があります。

URL リストを変更するには、条件内の [+] ボタンをクリックし、次の手法のいずれかを使用して、目的のカテゴリまたは URL を選択します。ポリシーからカテゴリまたはオブジェクトを削除するには、対応する [x] をクリックします。

[URL] タブ

[+] をクリックし、URL オブジェクトまたはグループを選択して、[OK] をクリックします。必要なオブジェクトが存在しない場合は、[URLの新規作成（Create New URL）] をクリックします。

（注） 特定のサイトをターゲットにするようにURLオブジェクトを設定する前に、手動URLフィルタリングに関する情報を注意深く読みます。

[カテゴリ（Categories）] タブ

[+] をクリックし、目的のカテゴリを選択して、[OK] をクリックします。

デフォルトでは、レピュテーションに関係なく、選択した各カテゴリ内のすべての URL にルールが適用されます。レピュテーションに基づいてルールを制限するには、各カテゴリの下矢印をクリックして、[任意（Any）] チェックボックスを選択解除し、[レピュテーション（Reputation）] スライダを使用してレピュテーション レベルを選択します。レピュテーション スライダの左側は許可されるサイトを、右側はブロックされるサイトを示しています。レピュテーションがどのように使用されるかは、ルール アクションによって異なります。

- ルールによって Web アクセスをブロックまたは監視する場合は、レピュテーション レベルを選択することで、そのレベルより深刻なすべてのレピュテーションも選択されます。たとえば、**[疑わしいサイト（Suspicious sites）]**（レベル 2）をブロックまたはモニタするルールを設定した場合、**[高リスク（High risk）]**（レベル 1）サイトも自動的にブロックまたはモニタされます。
- ルールが Web アクセスを許可する場合は、レピュテーション レベルを選択すると、そのレベルより深刻でないすべてのレピュテーションも選択されます。たとえば、**[無害なサイト（Benign sites）]**（レベル 4）を許可するルールを設定した場合、**[既知（Well known）]**（レベル 5）サイトも自動的に許可されます。

ユーザ基準

アクセス ルールのユーザ基準は、IP 接続のユーザまたはユーザ グループを定義します。アクセス ルールにユーザまたはユーザ グループの基準を含めるには、アイデンティティ ポリシーと関連付けられたディレクトリ サーバを設定する必要があります。

アイデンティティ ポリシーは、特定の接続に関してユーザ アイデンティティを収集するかどうかを決定します。アイデンティティが確立されると、ホストのIPアドレスに識別されたユーザが関連付けられます。したがって、送信元 IP アドレスがユーザにマッピングされているトラフィックは、そのユーザからのものとみなされます。IP パケット自体にはユーザ アイデンティティ情報は含まれていないため、この IP アドレスとユーザ間のマッピングが使用可能な中での最良近似となります。

1つのルールに最大50のユーザまたはグループを追加できるため、通常は、グループを選択する方が個々のユーザを選択するより有意義です。たとえば、エンジニアリング グループに開発

ネットワークへのアクセスを許可するルールを作成し、それに続くルールとして、そのネットワークへの他のすべてのアクセスを拒否するルールを作成できます。その後、ルールを新しいエンジニアに適用するには、エンジニアをディレクトリ サーバのエンジニアリング グループに追加するだけです。

ユーザリストを変更するには、条件の中にある [+] ボタンをクリックし、次のいずれかの方法で必要なアイデンティティを選択します。ポリシーからアイデンティティを削除するには、該当する [x] をクリックします。

- [ユーザおよびグループ（Users and Groups）] タブ：目的のユーザまたはユーザ グループを選択します。グループは、ディレクトリ サーバにグループが設定されている場合のみ使用可能です。グループを選択すると、ルールはサブグループを含むグループのすべてのメンバーに適用されます。サブグループを別の方法で処理する場合は、サブグループ用の個別のアクセス ルールを作成し、それをアクセス コントロール ポリシー内で親グループのルールの上に配置する必要があります。
- [特別なエンティティ（Special Entities）]：次から選択します。
  - [認証失敗（Failed Authentication）]：ユーザは認証を求められましたが、最大許容試行回数内に有効なユーザ名/パスワードのペアを入力できませんでした。認証の失敗は、それ自体ではユーザのネットワークへのアクセスは妨げられませんが、これらのユーザのネットワーク アクセスを制限するためのアクセス ルールを記述できます。
  - [ゲスト（Guest）]：ゲストユーザは、これらのユーザをゲストと呼ぶようにアイデンティティ ルールが設定されている点を除き、認証失敗ユーザと同様です。ゲストユーザは認証を求められましたが、最大試行回数内に認証されることができませんでした。
  - [認証不要（No Authentication Required）]：ユーザの接続が認証なしに指定されたアイデンティティ ルールに一致したため、ユーザは認証を求められませんでした。
  - [不明（Unknown）]：IP アドレスのユーザ マッピングがなく、認証失敗の記録もありません。通常、これは、HTTP トラフィックがそのアドレスからまだ見られていないことを意味します。

侵入ポリシーの設定

Firepower システムには複数の侵入ポリシーが付属しています。これらのポリシーは Cisco Talos Intelligence Group（Talos） によって設計されており、侵入ルール、プリプロセッサ ルール状態、詳細設定が設定されています。これらのポリシーは変更できません。ただし、侵入ルールのアクションの変更で説明しているように、特定のルールに対して実行するアクションを変更することは可能です。

トラフィックを許可するアクセス コントロール ルールでは、次の侵入ポリシーのいずれかを選択して、トラフィックの侵入やエクスプロイトのインスペクションを実行できます。侵入ポリシーは、復号されたパケットの攻撃をパターンに基づいて調査し、悪意のあるトラフィックをブロックしたり、変更したりします。

侵入検査を有効化するには、**[侵入ポリシー（Intrusion Policy）]** > **[オン（On）]** を選択し、必要なポリシーを選択します。ポリシーは、安全性の低いものから高いものへの順で表示されています。

- [セキュリティよりも接続性を優先（Connectivity over Security）]：このポリシーは、ネットワーク インフラストラクチャのセキュリティよりも接続性（すべてのリソースにアクセスできること）が優先される組織のために作成されています。侵入ポリシーは、[接続性を上回るセキュリティ（Security over Connectivity）] ポリシーで有効にされるルールよりはるかに少ないルールが有効化されます。トラフィックをブロックする最も重要なルールのみが有効にされます。このポリシーは、侵入からの保護を適用する必要があるが、ネットワークのセキュリティにかなり自信がある場合に選択します。
- [バランスのとれたセキュリティと接続性（Balanced Security and Connectivity）]：このポリシーは、全体的なネットワーク パフォーマンスとネットワーク インフラストラクチャのセキュリティのバランスを取るように設計されています。このポリシーは大部分のネットワークに適しています。このポリシーは、侵入防御を適用したい大部分の状況で選択できます。
- [接続性よりもセキュリティを優先（Security over Connectivity）]：このポリシーは、ユーザの利便性よりもネットワーク インフラストラクチャのセキュリティが優先される組織のために作成されています。この侵入ポリシーは、正式なトラフィックに対して警告またはドロップする可能性のある膨大な数のネットワーク異常侵入ルールを有効にします。このポリシーは、セキュリティが特に重要であるか、トラフィックのリスクが高い場合に選択します。
- [最大検出（Maximum Detection）]：このポリシーは、[接続性よりもセキュリティを優先（Security over Connectivity）] ポリシーよりもさらに、ネットワーク インフラストラクチャのセキュリティを重視する組織のために作成されています。動作への影響がさらに高くなる可能性があります。たとえば、この侵入ポリシーでは、マルウェア、エクスプロイト キット、古い脆弱性や一般的な脆弱性、および既知の流行中のエクスプロイトを含め、多数の脅威カテゴリのルールを有効にします。このポリシーを選択する場合、正当なトラフィックが過剰にドロップされていないか慎重に評価してください。

ファイル ポリシーの設定

Advanced Malware Protection for Firepower（AMP for Firepower）を使用して悪意のあるソフトウェア、つまり、マルウェアを検出するファイル ポリシーを使用します。ファイル制御を実行するファイル ポリシーを使用して、ファイルにマルウェアが含まれているかどうかに関係なく、特定のタイプのすべてのファイルを制御することもできます。

AMP for Firepower は、ネットワーク トラフィックで検出された潜在的なマルウェアの性質を取得し、ローカル マルウェア ファイル分析と事前分類の更新を取得するために AMP クラウドを使用します。AMP クラウドにアクセスし、マルウェア ルックアップを実行するため、管理インターフェイスにはインターネットへのパスが必要です。デバイスが対象ファイルを検出すると、ファイルの SHA-256 ハッシュ値を使用してファイルの性質について AMP クラウドに問い合わせます。可能な性質を次に示します。

- マルウェア（Malware）：AMP クラウドはファイルをマルウェア クラウドとして分類しました。ファイル内のいずれかのファイルがマルウェアである場合、アーカイブ ファイル（たとえば zip ファイル）はマルウェアとしてマークされます。
- クリーン（Clean）：AMP クラウドはファイルをマルウェアが含まれないクリーンな状態であると分類しました。その中のすべてのファイルがクリーンであれば、アーカイブ ファイルはクリーンであるとマークされます。
- 不明（Unknown）：AMP クラウドがまだファイルの性質を指定していません。その中のすべてのファイルが不明であれば、アーカイブ ファイルは不明であるとマークされます。
- 利用不可（Unavailable）：システムは、ファイルの性質を判断するために AMP クラウドに問い合わせできませんでした。この性質に関するイベントが、わずかながら存在する可能性があります。これは予期された動作です。複数の「利用不可」イベントが連続して発生している場合、管理アドレスのインターネット接続が正常に機能していることを確認します。

使用可能なファイル ポリシー

次のいずれかのファイル ポリシーを選択できます。

- [なし（None）]は、送信したファイルでマルウェアの評価を行わず、特定のファイルをブロックしません。このオプションは、ファイル送信が信頼されている、またはファイル送信の可能性が低い（または不可能である）、あるいはアプリケーションを信頼している、または URL フィルタリングがネットワークを適切に保護しているルールに対して選択します。
- [マルウェアをすべてブロック（Block Malware All）] は、AMPクラウドに問い合わせてネットワークを通過するファイルにマルウェアが含まれているかどうかを判断し、脅威を示しているファイルをブロックします。
- [クラウドをすべてルックアップ（Cloud Lookup All）] は、AMPクラウドに問い合わせてネットワークを通過するファイルの傾向を取得して記録したうえでその伝送を許可します。
- [オフラインドキュメントとアップロードされたPDFをブロック、その他のマルウェアをブロック（Block Office Document and PDF Upload, Block Malware Others）] は、ユーザによる Microsoft Office のドキュメントと PDF のアップロードをブロックします。AMPクラウドに問い合わせてネットワークを通過するファイルにマルウェアが含まれているかどうかを判断し、脅威を示しているファイルをブロックします。
- [オフラインドキュメントのアップロードをブロック、その他のマルウェアをブロック（Block Office Documents Upload, Block Malware Others）] は、ユーザによる Microsoft Office のドキュメントのアップロードをブロックします。AMPクラウドに問い合わせてネットワークを通過するファイルにマルウェアが含まれているかどうかを判断し、脅威を示しているファイルをブロックします。

ロギングの設定

アクセス ルールのロギング設定は、接続イベントがルールに一致するトラフィックに対して発行されるかどうかを決定します。イベント ビューアでルールに関連するイベントを確認するには、ロギングを有効にする必要があります。また、一致するトラフィックがシステムをモニタするために使用できるさまざまなダッシュボードに反映されるようにするためにも、ロギングを有効にする必要があります。

組織のセキュリティおよびコンプライアンスの要件に従って接続をロギングしてください。生成するイベントの数を抑え、パフォーマンスを向上させることが目標である場合は、分析のために重要な接続のロギングのみを有効にします。一方、プロファイリングの目的でネットワーク トラフィックの広範な表示が必要な場合は、その他の接続のロギングを有効化します。

注意 サービス妨害（DoS）攻撃の間にブロックされた TCP 接続をロギングすると、システム パフォーマンスに影響し、複数の同様のイベントによってデータベースが過負荷になる可能性があります。ブロック ルールにロギングを有効にする前に、そのルールがインターネット側のインターフェイスまたは DoS 攻撃を受けやすい他のインターフェイスを対象としているかどうかを検討します。

次のロギング オプションを設定できます。

ログ アクションの選択

次のいずれかのアクションを選択できます。

- [接続の開始時と終了時にログを記録する（Log at Beginning and End of Connection）]：接続の開始時と終了時にイベントを発行します。接続終了イベントには接続開始イベントに含まれるすべての情報と、接続中に拾うことができるすべての情報が含まれているため、許可しようとしているトラフィックではこのオプションを選択しないことをお勧めします。両方のイベントのロギングは、システム パフォーマンスに影響する可能性があります。ただし、これはブロックされているトラフィックに許可されている唯一のオプションです。
- [接続終了時にログを記録する（Log at End of Connection）]：接続の終了時に接続ログの記録を許可する場合は、このオプションを選択します。これは許可されている、または信頼されているトラフィックに推奨されます。
- [接続のロギングなし（No Logging at Connection）]：ルールのロギングを無効にするには、このオプションを選択します。これがデフォルトです。

（注） アクセス コントロール ルールによって呼び出された侵入ポリシーが侵入を検出して侵入イベントを生成すると、システムはルールのロギング設定に関係なく、侵入が発生した接続の終了を自動的にロギングします。侵入がブロックされた接続では、接続ログ内の接続のアクションは [ブロック（Block）]、理由は [侵入ブロック（Intrusion Block）] ですが、侵入インスペクションを実行するには、許可ルールを使用する必要があります。

ファイル イベント

禁止されたファイルまたはマルウェア イベントのロギングを有効にするには、[ファイルのロギング（Log Files）] を選択します。このオプションを設定するには、ルールでファイル ポリシーを選択する必要があります。ルールにファイル ポリシーを選択している場合、このオプションはデフォルトで有効になっています。シスコは、このオプションを有効のままにすることを推奨します。

システムが禁止されたファイルを検出すると、次のタイプのイベントの1つを自動的にロギングします。

- ファイル イベント：検出またはブロックされたファイル（マルウェア ファイルを含む）を表します。
- マルウェア イベント：検出されたまたはブロックされたマルウェア ファイルのみを表します。
- レトロスペクティブ マルウェア イベント：以前に検出されたファイルでのマルウェア処理が変化した場合に生成されます。

ファイルがブロックされた接続の場合、接続ログにおける接続のアクションは [ブロック（Block）] ですが、ファイルおよびマルウェアのインスペクションを実行するには、許可ルールを使用する必要があります。接続の原因は、[ファイルモニタ（File Monitor）]（ファイル タイプまたはマルウェアが検出された）、あるいは [マルウェアブロック（Malware Block）] または [ファイルブロック（File Block）]（ファイルがブロックされた）です。

接続イベントの送信先

外部 syslog サーバにイベントのコピーを送信するには、syslog サーバを定義するサーバ オブジェクトを選択します。必要なオブジェクトがすでに存在しない場合、[Syslogサーバの新規作成（Create New Syslog Server）] をクリックして作成します（syslog サーバへのロギングを無効にするには、サーバ リストから [任意（Any）] を選択します）。

デバイスのイベント ストレージは限られているため、外部 syslog サーバへイベントを送信すると、長期的な保存が可能になり、イベント分析を強化できます。

アクセス コントロール ポリシーのモニタリング

以下のトピックでは、アクセス制御ポリシーのモニタ方法について説明します。

ダッシュボードでのアクセス制御統計情報のモニタリング

[モニタリング（Monitoring）] ダッシュボードの大半のデータは、アクセス コントロール ポリシーに直接関連しています。「トラフィックのモニタリングおよびシステム ダッシュボード」を参照してください。

- **[モニタリング（Monitoring）] > [アクセスおよびSIルール（Access And SI Rules）]** には最もヒットしたアクセス ルールと関連する統計情報が表示されます。

- 一般的な統計情報は、[ネットワーク概要（Network Overview）]、[送信先（Destinations）] および [ゾーン（Zones）] ダッシュボードで確認できます。
- URL フィルタリングの結果は [Webカテゴリ（Web Categories）]、[URLカテゴリ（URL Categories）]および [送信先（Destinations）] ダッシュボードで確認できます。[Webカテゴリ（Web Categories）]、[URLカテゴリ（URL Categories）]ダッシュボードに情報を表示するには、少なくとも 1 つの URL フィルタリング ポリシーが必要です。
- アプリケーション フィルタリングの結果は、[アプリケーション（Applications）] および [Webアプリケーション（Web Applications）] ダッシュボードで確認できます。
- [ユーザ（Users）] ダッシュボードでは、ユーザベースの統計情報を確認できます。ユーザ情報を収集するには、アイデンティティ ポリシーを実装する必要があります。
- [攻撃者（Attackers）] および [ターゲット（Targets）] ダッシュボードでは、侵入ポリシーの統計情報を確認できます。これらのダッシュボードで情報を表示するには、少なくとも 1 つのアクセス コントロール ルールに侵入ポリシーを適用する必要があります。
- ファイル ポリシーおよびマルウェア フィルタリング統計情報は、[ファイルログ（File Logs）] および [マルウェア（Malware）] ダッシュボードで確認できます。このダッシュボードに情報を表示するには、ファイル ポリシーを 1 つ以上のアクセス制御ルールに適用する必要があります。
- **[モニタリング（Monitoring）] > [イベント（Events）]** には、アクセス コントロール ルールに関連する接続とデータのイベントも表示されます。

CLI でのアクセス コントロール ポリシーのモニタリング

CLI コンソールを開くか、またはデバイスの CLI にログインして、次のコマンドを使用し、アクセス制御ポリシーと統計情報に関する詳細情報を取得することもできます。

- **show access-control-config** はアクセス制御ルールに関する概要情報とルールごとのヒット数を表示します。
- **show access-list** はアクセス制御ルールから生成されたアクセス制御リスト（ACL）を表示します。ACL は初期フィルタを提供し、できる限り迅速な決定を実現しようとするため、ドロップされる接続を調査する（および、そのために不必要にリソースを消費する）必要はありませんこの情報には、ヒット数が含まれます。
- **show snort statistics** は主要なインスペクタである Snort インスペクション エンジンに関する情報を表示します。Snort は、アプリケーション フィルタリング、URL フィルタリング、侵入からの保護、ファイルおよびマルウェア フィルタリングを実装します。
- **show conn** は現在インターフェイスを通じて確立されている接続に関する情報を表示します。
- **show traffic** は各インターフェイスを介したトラフィック フローに関する統計情報を表示します。

- **show ipv6 traffic** はデバイスを介した IPv6 トラフィック フローに関する統計情報を表示します。

アクセス制御の例

使用例の章には、アクセス制御ルールのいくつかの実装例が含まれています。次の例を参照してください。

- ネットワーク トラフィックを調べる方法。この例では、全体的な接続およびユーザ情報を収集するための基本的な考え方が示されています。
- 脅威をブロックする方法。この例では、侵入ポリシーを適用する方法が示されています。
- マルウェアをブロックする方法。この例では、ファイルポリシーを適用する方法が示されています。
- アクセプタブル ユース ポリシー（URL フィルタリング）の実装方法。この例では、URL フィルタリングを実行する方法が示されています。
- アプリケーションの使用を制御する方法。この例では、アプリケーション フィルタリングを実行する方法が示されています。
- サブネットを追加する方法。この例では、トラフィック フローを許可するために必要なアクセスルールを含め、新しいサブネットをネットワーク全体に統合する方法が示されています。