アクセス コントロール

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。これらのルールは、どのトラフィックにデバイスの通過を許可するかを制御し、侵入検知などのアドバンスド サービスをトラフィックに適用します。

- アクセス コントロールの概要，1 ページ
- アクセス コントロール ポリシーを設定する，7 ページ
- アクセス コントロール ポリシーのモニタリング，22 ページ
- アクセス コントロールの制限，23 ページ

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制御するには、アクセス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することができます。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、トラフィックに IPS インスペクションを適用できます。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, （13 ページ）を参照してください。

アプリケーションのフィルタリングについて特に注意すべき点については、アプリケーション制御の制限, （24 ページ）で言及されています。最も注意すべき制限は暗号化トラフィックについてです。

アプリケーションが HTTPS 接続などの暗号化を使用する場合、システムがアプリケーションを特定できない可能性があります。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。Firepower Device Manager を使用して SSL 復号を設定することはできないため、これらのアプリケーションのアクセス コントロール ルールは機能しません。たとえば、この書き込み時に、Dropbox にこのタグが付けられているとします。この場合、Dropbox アプリケーションのアクセス ルールは Dropbox 接続に一致しません。

URL フィルタリング

URL 条件は、ネットワークのユーザがアクセスできる Web サイトを制御します。この機能は、*URL* フィルタリングと呼ばれます。

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 ライセンスでは、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することができます。
- 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。

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。

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 ライセンスでは、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。

（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。また、Cisco Collective Security Intelligence（CSI）との通信を有効にして、最新の脅威インテリジェンスを取得する必要もあります。

レピュテーションベースの URL フィルタリングの利点

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。

カテゴリおよびレピュテーション データを使用すると、ポリシーの作成と管理がより簡単になります。この方法では、システムが Web トラフィックを期待どおりに確実に制御します。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 をフィルタ処理します。セキュリティに対する脅威を表すサイトや望ましくないコンテンツが表示されるサイトは、ユーザが新しいポリシーを更新したり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。

システムはどのように適応するのか、いくつかの例を示します。

- アクセス コントロール ルールですべてのゲーム サイトをブロックする場合、新しいドメインが登録されてゲームに分類されると、これらのサイトをシステムで自動的にブロックできます。
- アクセス コントロール ルールですべてのマルウェア サイトをブロックし、あるブログ ページがマルウェアに感染すると、システムはそのURLをブログからマルウェアに再分類して、そのサイトをブロックすることができます。
- アクセス コントロール ルールでリスクの高いソーシャル ネットワーキング サイトをブロックし、だれかがプロファイルページに悪意のあるペイロードへのリンクが含まれるリンクを掲載すると、システムはそのページのレピュテーションを無害なサイトから高リスクに変更してブロックすることができます。

手動 URL フィルタリング

アクセス コントロール ルールでは、個々の 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で、カテゴリとレピュテーション ベースの URL のフィルタリングを補足したり、選択的にオーバーライドしたりできます。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することができます。

たとえば、アクセスコントロールを使用して組織に適していないWebサイトのカテゴリをブロックできます。ただし、カテゴリに適切な Web サイトが含まれていて、そこにアクセスを提供する必要がある場合は、そのサイトに手動で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。

特定のURLを手動でフィルタリングする場合、影響を受ける可能性のある他のトラフィックについて慎重に検討してください。ネットワーク トラフィックが URL 条件に一致するかどうか判別するために、システムは単純な部分文字列マッチングを実行します。要求されたURLが文字列の一部に一致すると、 URL が一致したと見なされます。

たとえば example.com へのすべてのトラフィックを許可する場合、ユーザは次の URL を含むサイトを参照できます。

- http://example.com/
- http://example.com/newexample
- http://www.example.com/

別の例として、ign.com（ゲーム サイト）を明示的にブロックする場合を考えてください。部分文字列マッチングにより ign.com 自体だけでなく verisign.com もブロックされることになり、意図しない動作が生じる可能性があります。

HTTPS トラフィックのフィルタリング

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。

HTTP フィルタリングでは、サブドメインを含むホスト名全体を検討します。しかし、HTTPS フィルタリングではサブジェクト共通名内のサブドメインを無視するため、HTTPS URL を手動でフィルタリングする場合はにサブドメイン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。

暗号化プロトコルによるトラフィックの制御

で URL フィルタリングを実行する場合、システムは暗号化プロトコル（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 フィルタリングは、次の Web サイトへのトラフィックを同じように扱います。

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

HTTP または HTTPS トラフィックのみに一致するルールを設定するには、アプリケーション条件をルールに追加します。たとえば、あるサイトへの HTTPS アクセスを許可する一方で、HTTP アクセスを許可しないようにできます。そのためには、2 つのアクセス コントロール ルールを作成し、それぞれにアプリケーションと URL の条件を割り当てます。

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。

Action: Allow
Application: HTTPS
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。

Action: Block
Application: HTTP
URL: example.com

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、トラフィックがその宛先に許可される前の最後の防御ラインとして機能します。

- 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制御と AMP for Firepower の機能を管理します。

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。

トラフィックのみを [許可（allow）]する侵入ポリシーとファイル ポリシーをルールに設定できます。インスペクションは、[信頼（trust）]または[ブロック（block）]トラフィックに設定されているルールでは実施されません。また、アクセス コントロール ポリシーのデフォルト アクションが、[許可（allow）]の場合、侵入ポリシーは設定できますが、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のインスペクションを実行しません。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、暗号化ペイロードの侵入およびファイル インスペクションは無効化されます。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。インスペクションは暗号化トラフィックのみで機能します。

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。

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。
- 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（）したり削除（）したりできます。

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（Intrusion Policy）] の下で [ポリシーの有効化（Enable Policy）] > [オン（On）] を選択し、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, （18 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必要があります。ロギングの設定, （20 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, （10 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, （13 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, （15 ページ）を参照してください。
- [ユーザ（Users）]：ユーザとユーザ 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, （16 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、特定のホストの URL フィルタリングを実行する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）]：[侵入ポリシー（Intrusion Policy）]>[オン（On）]を選択し、トラフィックへの侵入と弱点をインスペクションのする IPS 侵入インスペクションのポリシーを選択します。侵入ポリシーの設定，（18 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，（18 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，（20 ページ）を参照してください。

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（OK）]をクリックします。基準にオブジェクトが必要で、必要なオブジェクトが存

在しない場合は、[Create New *Object*（新規オブジェクトの作成）] をクリックします。ポリシーからオブジェクトまたは要素を削除するには、それらの [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。片方または両方の基準を定義できます。両方とも定義しないことも可能です。指定されていない基準は、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を出入りする場所に基づいてルールを適用する場合は、この基準を使用します。たとえば、内部ホストに移動するすべてのトラフィックが IPS インスペクションを必ず受けるようにするには、[宛先ゾーン（Destination Zones）]として内部ゾーンを選択し、送信元ゾーンを空のままにします。ルールに IPS フィルタリングを実装するには、ルール アクションを [許可（Allow）]にして、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。

この基準を追加する場合、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）：送信元または宛先の国または大陸に基づいてトラフィックを制御する地理的位置を選択します。大陸を選択すると、その大陸にあるすべての国が選択されます。ルールで地理的位置を直接選択する以外に、場所を定義するために作成した地理位置情報オブジェクトを選択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、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は、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することができます。

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。ユーザがそれらのアプリケーションの 1 つ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。

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することができます。

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不可欠な機能を表す一般的な分類。

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 条件をすぐに作成することができます。たとえば、すべてのゲームサイトや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ブロックすることができます。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、シスコの脅威インテリジェンスは新しい URL および既存の URL に対する新たな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をフィルタ処理します。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。URL マッチングが予期したとおりに動作せず、意図せずにサイトをブロックしてしまうことがよくあります。たとえば、明示的にゲームサイト ign.com をブロックしようとすると、verisign.com や “ign.” で終わる他のサイトもブロックされてしまいます。

[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（レベル 2）をブロックまたはモニタするようルールを設定した場合、高リスク（レベル 1）の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）を許可するようルールを設定した場合、有名（Well known）（レベル 5）サイトもまた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必要があるだけです。

ユーザ 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、目的のユーザまたはユーザ グループを選択します。ポリシーからユーザまたはグループを削除するには、対応する [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。

（注） デフォルトでは、Active Directory サーバはセカンダリ グループから報告するユーザの数を制限します。この制限は、セカンダリ グループ内のすべてのユーザが報告され、ユーザ条件を含むアクセス コントロール ルールでの使用に適するようにカスタマイズする必要があります。Firepower Device Manager では、全体で2000ユーザまでに制限されています。そのため、ディレクトリに2000を超えるユーザが存在する場合は、存在するすべてのユーザ名は表示されません。

- [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 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 ルールを記述することができます。
  - [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。

侵入ポリシーの設定

シスコではFirepower Systemを使用して複数の侵入ポリシーを提供しています。これらのポリシーは、侵入ルールやプリプロセッサルールの状態や詳細設定を定めるCisco Talos Security Intelligence and Research Groupによって設計されています。これらのポリシーは変更できません。

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。

侵入インスペクションを有効にするには、[侵入ポリシー（Intrusion Policy）] > [オン（On）] を選択し、スライダを使用して目的のポリシーを選択します。ポリシーは安全性が低いものから高いものへとリストされます。

- [セキュリティよりも接続を重視（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。この侵入ポリシーは、Security over Connectivityポリシー内で有効になっているルールよりもはるかに少ないルールを有効にします。トラフィックをブロックする最も重要なルールだけが有効にされます。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。
- [セキュリティと接続のバランス型（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。
- [接続よりもセキュリティを重視（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、接続よりもセキュリティを重視（Security over Connectivity）する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。この性質を持つイベントはごくわずかであ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上およびコンプライアンス上の要件に従って接続をロギングしてください。目標が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。しかし、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、追加の接続のロギングを有効にできます。

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（FileMonitor）]（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することができます。

アクセス コントロール ポリシーのモニタリング

[モニタリング（Monitoring）]ダッシュボードのデータの大半は、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）] > [ポリシー（Policies）] には、ヒット数が最も多いアクセス コントロール ルールと関連の統計情報が表示されます。
- [ネットワークの概要（Network Overview）]、[宛先（Destinations）]、[入力ゾーン（Ingress Zones）]、および[出力ゾーン（Egress Zones）] ダッシュボードには、一般的な統計情報が表示されます。

- [Web カテゴリ（Web Categories）] および [宛先（Destinations）] ダッシュボードには、URL フィルタリングの結果が表示されます。[Web カテゴリ（Web 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（Applications）]ダッシュボードには、アプリケーション フィルタリングの結果が表示されます。
- [ユーザ（Users）]ダッシュボードには、ユーザベースの統計情報が表示されます。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）] ダッシュボードには、侵入ポリシーの統計情報が表示されます。これらの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 ログ（File Logs）] ダッシュボードには、ファイル ポリシーおよびマルウェア フィルタリングの統計情報が表示されます。このダッシュボードに情報を表示するには、少なくとも 1 つのアクセス コントロール ルールにファイル ポリシーを適用する必要があります。
- [モニタリング（Monitoring）] > [イベント（Events）] にも、接続のイベントとアクセス コントロール ルールに関連するデータが表示されます。

CLI でのアクセス コントロール ポリシーのモニタリング

デバイス CLI にログインして次のコマンドを使用すると、アクセス コントロール ポリシーと統計情報に関するより詳細な情報を取得することもできます。

- **show access-control-config** は、ルールごとのヒット数とともにアクセス コントロール ルールに関するサマリ情報を表示します。
- **show access-list** は、アクセス コントロール ルールから生成されたアクセス コントロール 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、およびファイルとマルウェアのフィルタリングを実装しています。
- **show conn** は、インターフェイスを介して現在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て移動するトラフィックに関する統計情報を表示します。
- **show ipv6 traffic** は、デバイスを介して移動する IPv6 トラフィックに関する統計情報を表示します。

アクセス コントロールの制限

次に、アクセス コントロール ポリシーの制限の一部を説明します。

アプリケーション制御の制限

アプリケーション識別の速度

システムは、次が実行されるまで、アプリケーション制御を実行できません。

- モニタ対象の接続がクライアントとサーバの間で確立され、
- システムがセッションでアプリケーションを識別する

この識別は 3 ～ 5 パケット以内で、またはトラフィックが暗号化されている場合は、SSL ハンドシェイクのサーバ証明書交換の後に行われる必要があります。

早期のトラフィックがその他のすべての基準に一致するが、アプリケーション識別が不完全な場合、システムは、パケットの受け渡しと接続の確立（または、SSL ハンドシェイクの完了）を許可します。システムは識別を完了した後、残りのセッション トラフィックに適切なアクションを適用します。

アクセス コントロールの場合、これらの受け渡されたパケットは、アクセス コントロール ポリシーのデフォルトの侵入ポリシー（デフォルト アクション侵入ポリシーでもほぼ一致するルールの侵入ポリシーでもない）によりインスペクションが実行されます。

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

システムは暗号化トラフィックと復号トラフィックを識別し、フィルタ処理することができます。

- 暗号化トラフィック：システムは、SMTPS、POPS、FTPS、TelnetS、IMAPS を含む StartTLS 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。これらのアプリケーションに `SSL Protocol` タグが付けられます。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。
- 復号トラフィック：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 `decrypted traffic` タグを割り当てます。

ペイロードのないアプリケーション トラフィック パケットの処理

アクセス コントロールを実行している場合、システムは、アプリケーションが識別された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。

参照されるアプリケーション トラフィックの処理

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。

複数のプロトコルを使用するアプリケーション トラフィックの制御（Skype）

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 の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のではなく、[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。

ユーザまたはグループ制御の制限

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 人以上のユーザ 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適用されます。グループに 2000 人以上のメンバーがいる場合、ダウンロードされた 2000 の名前のみをグループ メンバーシップと一致させることができます。

2000 人以上のユーザがいる場合、Firepower Device Manager ではなく Firepower Management Center（リモート マネージャ）の使用を検討してください。Firepower Management Center では、はるかに多くのユーザをサポートします。

URL フィルタリングの制限

URL 識別の速度

システムは以下の動作の前に URL をフィルタリングできません。

- モニタ対象の接続がクライアントとサーバの間で確立される。
- システムがセッションで HTTP または HTTPS アプリケーションを識別する
- システムが要求された URL を識別する（ClientHello メッセージまたはサーバ証明書からの暗号化されたセッションの場合）

この識別は 3 ～ 5 パケット以内で、またはトラフィックが暗号化されている場合は、SSL ハンドシェイクのサーバ証明書交換の後に行われる必要があります。

早期のトラフィックがその他のすべてのルール条件に一致するが、識別が不完全な場合、システムは、パケットの受け渡しと接続の確立（または、SSL ハンドシェイクの完了）を許可します。システムは識別を完了した後、残りのセッショントラフィックに適切なルールアクションを適用します。

アクセスコントロールの場合、これらの受け渡されたパケットは、デフォルトアクション侵入ポリシーでもほぼ一致するルールの侵入ポリシーでもなく、アクセス コントロール ポリシーのデフォルトの侵入ポリシーによりインスペクションが実行されます。

手動 URL フィルタリング

特定のURLを手動でフィルタリングする場合は、影響を受ける可能性のある他のトラフィックを慎重に考慮してください。ネットワーク トラフィックが URL 条件に一致するかどうか判別するために、システムは単純な部分文字列マッチングを実行します。要求されたURLが文字列の任意の部分に一致する場合、URL は一致するとみなされます。

暗号化された Web トラフィックの URL フィルタリング

暗号化された Web トラフィックに対して URL フィルタリングを実行すると、システムは次のように動作します。

- 暗号化プロトコルを無視します。ルールに URL 条件はあるがプロトコルを指定するアプリケーション条件がない場合、ルールは HTTPS および HTTP 両方のトラフィックを照合します。
- トラフィックを暗号化するために使用する公開キー証明書のサブジェクト共通名に基づいて HTTPS トラフィックを照合し、サブジェクト共通名に含まれるサブドメインを無視します。

URL での検索クエリ パラメータ

システムでは、URL 条件の照合に URL 内の検索クエリ パラメータを使用しません。たとえば、すべてのショッピング トラフィックをブロックする場合を考えます。amazon.com を探すために Web 検索を使用してもブロックされませんが、amazon.com を閲覧しようとするとブロックされます。

選択したデバイス モデルのメモリ制限

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 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、一部のデバイスでは、すべてのサブサイトに対して親URLのデータが使用されます。具体的な例として、システムはgoogle.comカテゴリとレピュテーションを使用して mail.google.com を評価します。影響を受けるデバイスには、次の ASA モデルが含まれます：ASA5506-X、ASA5506H-X、ASA5506W-X、ASA5508-X、ASA5512-X、ASA5515-X、ASA5516-X および ASA5525-X。