アクセス制御

ここでは、アクセス制御ルールについて説明します。これらのルールによって、デバイスを通過することが許可されるトラフィックが制御され、侵入検査などの高度なサービスがトラフィックに適用されます。

アクセス制御のベストプラクティス

アクセス制御ポリシーは、内部ネットワークを保護し、ユーザが望ましくない外部ネットワークリソース（不適切な Web サイトなど）にアクセスすることを防止するための主要なツールです。そのため、このポリシーに特に注意を払い、必要な保護と接続のレベルを得るためにポリシーを微調整することをお勧めします。

次の手順は、アクセス制御ポリシーを使用する場合に実行する必要がある基本的なことの概要を示しています。これは概要であり、各タスクを実行するための完全な手順は示していません。

アクセス制御ポリシーにアクセスするには、**[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** を選択します。

手順

ステップ 1 ポリシーのデフォルト アクションを設定します。

デフォルトアクションでは、ポリシー内の特定のルールに一致しない接続が処理されます。デフォルトでは、このアクションは [ブロック（Block）] であるため、ルールに含まれていない

ものはすべてブロックされます。そのため、必要なトラフィックを許可するアクセス制御ルールを作成するだけで済みます。これは、アクセス制御ポリシーを設定する従来の方法です。

反対に、デフォルトでトラフィックを許可して既知の望ましくないトラフィックをドロップするルールを作成することができます。この場合、許可するすべてのものに関するルールを用意する必要がなくなります。これにより、新しいサービスの使用が容易になりますが、気付かないうちに新しい望ましくないトラフィックが通過するリスクが生じます。

ステップ 2 [アクセスポリシーの設定] (⚙)ボタンをクリックし、[TLSサーバアイデンティティ検出]オプションを有効にします。

このオプションにより、TLS 1.3 接続の最初のアプリケーション検出と URL カテゴリおよびレピュテーションの識別が改善されます。このオプションを有効にしないと、TLS 1.3 トラフィックが意図したルールと一致しない可能性があります。また、このオプションを有効にすることにより、復号ルールの有効性が向上する可能性もあります。

ステップ 3 できるだけ少ないアクセス制御ルールを作成します。

従来のファイアウォールでは、IP アドレスとポートのさまざまな組み合わせに対して何万ものルールが作成される場合があります。次世代ファイアウォールでは、高度な検査を使用して、これらの詳細なルールの一部を回避できます。ルールの数が少ないほど、トラフィックが速く評価されるようになり、ルールセット内の問題を見つけて修正することも容易になります。

ステップ 4 アクセス制御ルールのロギングを有効にします。

ロギングを有効にした場合にのみ、一致するトラフィックの統計が収集されます。ロギングを有効にしないと、モニタリングダッシュボードが不正確になります。

ステップ 5 より固有性の高いルールをポリシーの上の方に配置し、固有性の高いルールも一致する接続と一致する、より一般的なルールが、それらの固有性の高いルールよりも下になっていることを確認します。

ポリシーはトップダウンで評価され、最初の一致が優先されます。そのため、特定のサブネットへのすべてのトラフィックをブロックするルールを配置し、その後にそのサブネット内の単一 IP アドレスへのアクセスを許可するルールを配置しても、最初のルールによってブロックされるため、そのアドレスへのトラフィックは許可されません。

また、入力/出力インターフェイス、送信元/宛先 IP アドレス、ポート、地理位置情報などの従来の基準のみに基づいてトラフィックを評価するルールは、ユーザ基準、URL フィルタリング、アプリケーションフィルタリングなどに適用される、詳細な検査が必要なルールの前に配置してください。前者のルールは検査を必要としないため、それらのルールを前に配置することにより、接続の一致に関するアクセス制御の決定を迅速に行うことが可能になります。

その他の推奨事項については、アクセス コントロール ルールの順序のベスト プラクティス（17 ページ）を参照してください。

ステップ 6 トラフィックのターゲットサブセットに対するブロックルールと許可ルールをペアで設定します。

たとえば、多くの HTTP/HTTPS トラフィックを許可する一方で、望ましくないサイト（ポルノサイトやギャンブルサイトなど）へのアクセスをブロックしたい場合があります。これを実

現するには、次のルールを作成し、それらをポリシー内で順番に並べます（たとえば、ルール 11 とルール 12）。

- 内部セキュリティゾーン（送信元）および外部セキュリティゾーン（宛先）と、IP アドレス、ポート、または地理位置情報に適用される、望ましくない URL カテゴリを対象とした URL フィルタリング ブロック ルール。たとえば、ボットネット、児童虐待コンテンツ、クリプトジャッキング、DNS トンネリング、電子バンキング詐欺、エクスプロイト、エクストリーム、フィルタ回避、ギャンブル、ハッキング、ヘイトスピーチ、ハイリスクのサイト/場所、違法行為、違法ダウンロード、違法薬物、悪意のあるサイト、 マルウェアサイト、モバイル脅威、P2P マルウェアノード、フィッシング、ポルノ、スパム、スパイウェア、およびアドウェアをブロックします。
- 内部セキュリティゾーン（送信元）および外部セキュリティゾーン（宛先）と、IP アドレス、ポート、または地理位置情報に適用される、HTTP および HTTPS アプリケーションのアプリケーションフィルタ処理許可ルール。この URL フィルタ処理ルールでは、望ましくない Web リソースへのアクセスをブロックした後、他のすべての HTTP/HTTPS アクセスが許可されます。

ステップ 7 高度な次世代ファイアウォール機能を使用して、IP アドレスやポートに関係なくトラフィックが評価されます。

攻撃者やその他の悪意のある人物は、IP アドレスとポートを頻繁に変更することにより、従来のアクセス制御トラフィックの一致基準を回避します。代わりに、次の次世代機能を使用してください。

- ユーザ基準：トラフィックを開始しているユーザに関する情報を取得するようにアイデンティティポリシーを設定します。理想的には、Active Directory サーバがユーザをグループに編成します。これによって、ユーザ グループ メンバーシップに基づいてトラフィックを許可またはブロックするアクセス制御ルールを作成できます。たとえば、エンジニアユーザには開発サブネットへのアクセスを許可しますが、エンジニアグループに属していないユーザは暗黙的にブロックします。個別のユーザ名ではなくグループを使用するため、ユーザがネットワークに追加されるたびにルールを更新する必要がありません。
- アプリケーション基準：アプリケーションフィルタ処理基準を使用して、アプリケーションのタイプを許可またはブロックします。これにより、ユーザが HTTP 接続のポートを変更した場合、システムは、ポート 80 に接続していなくても HTTP であることを認識できます。その他の推奨事項については、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 （7 ページ）を参照してください。
- URL カテゴリおよびレピュテーション基準：カテゴリに基づく URL フィルタ処理を使用して、サイトのタイプに基づいてサイトを動的に許可またはブロックします。サイトのタイプ（またはカテゴリ）内で、サイトのレピュテーション（正常または危険）に基づいてルールを微調整できます。URL によってサイトを手動でブロックしようとする場合には URL が変更されるたびにルールを調整する必要がありますが、カテゴリとレピュテーションを使用することにより、そのような調整が不要になります。その他の推奨事項については、効果的な URL フィルタリングのベスト プラクティス （12 ページ）を参照してください。

URLカテゴリ/レピュテーション フィルタリング ルールをDNSルックアップ要求のFQDNに適用することもできます。システムは、ブロックされたカテゴリ/レピュテーションに対するDNS応答を防止し、ユーザの接続試行を効果的にブロックできます。詳細は、URLカテゴリとレピュテーションに基づいたDNS要求のフィルタリング （15 ページ）を参照してください。

ステップ 8 すべての許可ルールに侵入検査を適用します。

次世代ファイアウォールの強力な機能の一つは、同じデバイスを使用して侵入検査とアクセス制御を適用できることです。侵入ポリシーを各許可ルールに適用してください。これにより、攻撃が通常は害のないパスを介してネットワークに侵入した場合でも、それを察知して攻撃接続をドロップできます。

デフォルトアクションが「許可」の場合は、デフォルトアクションに一致するトラフィックに侵入防御を適用することもできます。

ステップ 9 また、望ましくないIPアドレスおよびURLをブロックするようにセキュリティ インテリジェンス ポリシーを設定します。

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ポリシーの前に適用されるため、アクセス制御ルールが評価される前に望ましくない接続をブロックできます。これにより早い段階でのブロックを実現でき、アクセス制御ルールの複雑さを軽減するために役立ちます。

ステップ 10 SSL 復号ポリシーの実装を検討します。

システムは、暗号化されたトラフィックに対して詳細な検査を実行できません。SSL復号ポリシーを設定すると、アクセス制御ポリシーが復号されたバージョンのトラフィックに適用されます。そのため、詳細な検査によって攻撃を識別でき（侵入ポリシーを使用）、アプリケーションおよびURL フィルタリングをより効果的に適用できるため、ルールの照合が強化されます。アクセス制御ポリシーで許可されたトラフィックは、デバイスから送信される前に再暗号化されるため、エンドユーザが暗号化の保護を失うことはありません。

ステップ 11 オブジェクトグループ検索を有効にして、ルールの展開を簡素化します。

リリース 7.2 以降、この機能は新しい展開ではデフォルトで有効になっていますが、アップグレードされたシステムでは自動的に有効になりません。

オブジェクトグループ検索を有効にすると、ネットワークオブジェクトを含むアクセス コントロール ポリシーのメモリ要件が軽減されます。ただし、オブジェクトグループ検索では、ルールルックアップのパフォーマンスが低下して、CPU使用率が増大する可能性があることに注意してください。CPU に対する影響と、特定のアクセス コントロール ポリシーに関するメモリ要件の軽減とのバランスをとる必要があります。ほとんどの場合、オブジェクトグループ検索を有効にすると、ネット運用が改善されます。

FlexConfig を使用してこのオプションを設定するには、**object-group-search access-control** コマンドを発行します。否定テンプレートでは、このコマンドの **no** 形式を使用します。

アクセス制御の概要

以下のトピックでは、アクセス制御ポリシーについて説明します。

アクセス制御ルールおよびデフォルト 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基準が一致した最初のルールです。

アクセス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）。
- 送信元と宛先の完全修飾ドメイン名（FQDN）（ネットワーク オブジェクトの形式）。トラフィックの照合は、その名前に関して DNS ルックアップから返された IP アドレスに基づいて行われます。
- Cisco Identity Services Engine（ISE）によって送信元または宛先に割り当てられたセキュリティグループタグ（SGT）。
- 使用されているアプリケーション。特定のアプリケーションに基づいてアクセスを制御するか、アプリケーションのカテゴリ、特性タグ、タイプ（クライアント、サーバ、Web）、リスク、ビジネスとの関連性に基づいたルールを作成することができます。
- Web 要求の宛先 URL（URL の汎用カテゴリを含む）。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めます。
- DNSルックアップ要求のFQDNのURLカテゴリとレピュテーション。不要なカテゴリや低いレピュテーションに対してDNS応答をブロックして、その後の接続試行を効果的に防ぐことができます。
- 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。

暗号化されていない許可したトラフィックに対しては、IPS インスペクションを適用して、脅威をチェックし、攻撃とみられるトラフィックをブロックできます。また、ファイル ポリシーを使用して、禁止されているファイルやマルウェアをチェックできます。

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に対してファイル インスペクションやマルウェア インスペクションは実行できません。

アプリケーションのフィルタリング

アクセス制御ルールを使用して、接続に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処理できます。システムはさまざまなアプリケーションを認識できるので、すべての Web アプリケーションをブロックすることなく、特定の Web アプリケーションのみをブロックする方法を自分で試行錯誤する必要はありません。

よく使われるアプリケーションの場合、そのアプリケーションの特殊な機能に絞ってフィルタ処理できます。たとえば、Facebook をすべてブロックするのではなく、Facebook のゲームのみをブロックするルールを作成できます。

アプリケーションの一般的な特性（リスク、ビジネスとの関連性、タイプ、カテゴリ、タグ）に基づいて、そのグループ全体をブロックしたり許可したりするルールを作成することもできます。**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。**グループ化の詳細については、アプリケーション基準 （29 ページ）を参照してください。

暗号化トラフィック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。また、TLS ClientHello メッセージのサーバ ネーム インジケーション、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アプリケーションを特定できます。

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は復号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てアクセス制御アクションを適用します。リストされたアプリケーションのアクセス制御ルールは、想定される接続と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。

Common Industrial Protocol（CIP）および Modbus アプリケーション（ISA 3000）でのフィルタリング

Cisco ISA 3000 デバイスで Common Industrial Protocol（CIP） および Modbus プリプロセッサを有効にし、CIP および Modbus アプリケーションのアクセス制御ルールでフィルタを有効にすることができます。CIP アプリケーションの名前はすべて、CIP Write のように「CIP」で始まります。Modbus 用のアプリケーションは 1 つだけです。

プリプロセッサを有効にするには、CLIセッション（SSHまたはコンソール）でエキスパートモードに移行し、次のコマンドを発行して、これらの遠隔監視制御・情報取得（SCADA）アプリケーションの一方または両方を有効にする必要があります。

sudo /usr/local/sf/bin/enable_scada.sh {cip | modbus | both}

たとえば、両方のプリプロセッサを有効にするには次の手順を実行します。

```
> expert
admin@firepower:~$ sudo /usr/local/sf/bin/enable_scada.sh both
```

（注） このコマンドは、展開のたびに発行する必要があります。これらのプリプロセッサは、展開時には無効になります。

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。

- Web サーバによって参照されるトラフィック（アドバタイズメント トラフィックなど）を処理するには、参照元アプリケーションではなく、参照先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。
- TLS 1.3 では、ほとんどのハンドシェイクメッセージが暗号化されるため、証明書情報を簡単に利用できません。TLS 1.3 で暗号化されたトラフィックで、アプリケーションまたは URL フィルタリングを使用するアクセスルールに効果的に対応するには、システムがサーバーのクリアテキスト証明書を取得する必要があります。アクセス制御設定で [TLS 1.3証明書の可視性（TLS 1.3 Certificate Visibility）] を有効にすることをお勧めします。このオプションを有効にすると、システムは、クライアントの Hello パケットの IP アドレスおよび SNI（Server Name Indication）に基づいて、サイトの証明書がキャッシュに保存されているかどうかを確認します。保存されていない場合、システムは、TLS 1.2 プローブを使用して証明書を取得します。その後は、この証明書を使用して、接続を復号せずにアプリケーション/URL カテゴリおよびレピュテーションを識別することができます。
- システムでは複数の種類の Skype 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。
- 手動での URL フィルタリング：どのライセンスでも、個々の URL と URL グループを指定して、Web トラフィックに対する制御をより細かくカスタマイズできます。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。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：組織のセキュリティ ポリシーに反する目的でその URL が使用される可能性。信頼できない（レベル 1）から信頼できる（レベル 5）までのレピュテーション範囲。

URL カテゴリおよびレピュテーションにより、URL フィルタリングを素早く設定することができます。たとえば、アクセス制御を使用して、薬物乱用カテゴリの信頼できないURLをブロックできます。

カテゴリの説明については、https://www.talosintelligence.com/categoriesを参照してください。

カテゴリ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） イベントおよびアプリケーションの詳細に、URL カテゴリとレピュテーションの情報を含めるには、URL 条件を付けたルールを少なくとも 1 つ作成する必要があります。

URL のカテゴリとレピュテーションのルックアップ

特定の URL のカテゴリとレピュテーションを確認できます。アクセスコントロールルールまたはSSL復号ルールの[URL]タブに移動するか、**[デバイス]** > **[システム設定]** > **[URLフィルタリング設定]**に移動します。そこで、[確認するURL（URL to Check）] ボックスに URL を入力し、[移動（Go）] をクリックします。

ルックアップ結果を示すWebサイトが表示されます。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。

分類に同意しない場合は、Device Manager で [URLカテゴリの異議を送信する（Submit a URL Category Dispute）] をクリックして、ご意見をお聞かせください。

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。このタイプの URL フィルタリングは特別なライセンスなしで実行できます。

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、一致はサーバーのホスト名のみに基づきます。1 つ以上の / を含める場合、文字列の部分一致には URL 文字列全体が使用されます。次に、次のいずれかに該当する場合、URL は一致と見なされます。
  - 文字列が URL の先頭にある。
  - 文字列がドットの後に続く。
  - 文字列の先頭にドットが含まれている。
  - 文字列が :// 文字の後に続く。

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。

（注） サーバーは再構成でき、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（つまり / 文字を含む URL 文字列）をブロックまたは許可するために手動の URL フィルタリングは使用しないことをお勧めします。

- 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ときに、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。また、システムはサブジェクト共通名に含まれるサブドメインを無視するので、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。

  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処理するために、システムはSSLハンドシェーク中に渡された情報（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内のサブジェクト共通名）に基づいて要求された URL を特定します。URL のWebサイト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。

DNS要求フィルタリングを有効にすると、カテゴリ/レピュテーションルールのHTTPSでのマッチングを改善できます。システムは、ユーザがHTTPS接続の試行を開始する前に、DNS解決フェーズでカテゴリとレピュテーションを決定し、不要な組み合わせに対するDNS応答をブロックできます。許可されたDNS応答の場合、システムは後続のHTTPS接続で使用可能なカテゴリ/レピュテーション情報を保持します。DNS要求のフィルタリング （14 ページ）を参照してください。

HTTP フィルタリングと異なり、HTTPS フィルタリングは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、手動とレピュテーションベースの両方の URL 条件に対して行われます。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 アクセスを禁止することができます。

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 つ目のルールでは、同じ Web サイトへの HTTP アクセスがブロックされます。

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することができます。

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 カテゴリ照合を使用する場合は、サイトのログイン ページがサイト自体とは異なるカテゴリに含まれる場合があることに注意してください。たとえば、Gmail は [Webベース電子メール（Web based Email）] カテゴリに含まれますが、ログインページは [検索エンジンとポータル（Search Engines and Portals）] カテゴリに含まれます。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することができます。
- 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。
- TLS 1.3 では、ほとんどのハンドシェイクメッセージが暗号化されるため、証明書情報を簡単に利用できません。TLS 1.3 で暗号化されたトラフィックで、アプリケーションまたは URL フィルタリングを使用するアクセスルールに効果的に対応するには、システムがサーバーのクリアテキスト証明書を取得する必要があります。アクセス制御設定で [TLS 1.3証明書の可視性（TLS 1.3 Certificate Visibility）] を有効にすることをお勧めします。このオプションを有効にすると、システムは、クライアントの Hello パケットの IP アドレスおよび SNI（Server Name Indication）に基づいて、サイトの証明書がキャッシュに保存されているかどうかを確認します。保存されていない場合、システムは、TLS 1.2 プローブを使用して証明書を取得します。その後は、この証明書を使用して、接続を復号せずにアプリケーション/URL カテゴリおよびレピュテーションを識別することができます。
- 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からです。
- カテゴリが不明な高リスクサイトをブロックする場合は、[未分類（Uncategorized）] カテゴリを選択し、評価スライダを [疑わしい（Questionable）] または [信頼できない（Untrusted）] に調整します。
- DNS要求フィルタリングも有効にすることで、URLフィルタリング全般の有効性を向上させることができます。DNS要求フィルタリングを使用すると、DNSルックアップ時にFQDNのURLカテゴリとレピュテーションが決定されるため、後続のHTTP/HTTPS要求が同じ宛先に送信される際にこの情報を使用できます。さらに、カテゴリ/レピュテーションをブロックすると、試行された接続は、Webセッションの確立段階ではなく、DNS要求段階で停止します。「DNS要求のフィルタリング （14 ページ）」を参照してください。

Web サイトがブロックされた際、ユーザに対して表示される内容

URL フィルタリング ルールを使用して Web サイトをブロックする場合、ユーザに対して表示される内容は、サイトが暗号化されているかどうかによって異なります。

- HTTP接続：接続のタイムアウトまたはリセットが発生した場合の標準ブラウザページではなく、システムのデフォルトブロック応答ページが表示されます。このページにより、接続が意図的にブロックされていることを明示的に示します。
- HTTPS（暗号化）接続：システムのデフォルトブロック応答ページは表示されません。代わりに、セキュア接続が失敗したことを示すブラウザのデフォルトページが表示されます。このエラーメッセージは、ポリシーに基づいてサイトがブロックされたことは示しません。代わりに、一般的な暗号化アルゴリズムが存在しないことを示します。このメッセージでは、接続が意図的にブロックされたのかは分かりません。

また、明示的なURLフィルタリングルールではない他のアクセス制御ルールや、デフォルトのアクションによっても、Webサイトがブロックされることがあります。たとえば、ネットワーク全体または特定地域全体をブロックすると、そのネットワークまたは地域内のすべてのWebサイトがブロックされます。このようなルールによってブロックされるユーザに対しては、以下の制限により、応答ページが表示される場合と表示されない場合があります。

URLフィルタリングを導入する場合は、サイトが意図的にブロックされた際の表示で、ブロックされた理由やブロックするサイトのタイプについてエンドユーザに説明することをお勧めします。この点を説明しないと、エンドユーザはブロックされた接続のトラブルシューティングに多大な時間を費やすことになります。

HTTP応答ページの制限

システムによりWebトラフィックがブロックされる場合、HTTP応答ページが表示されないこともあります。

- プロモートされたアクセス制御ルール（単純なネットワーク条件だけが指定されている初期に適用されたブロックルール）の結果としてトラフィックがブロックされる場合には、応答ページは表示されません。
- 要求されたURLをシステムが特定する前にWebトラフィックがブロックされる場合、応答ページは表示されません。
- アクセス制御ルールによって暗号化接続がブロックされる場合、応答ページは表示されません。

DNS要求のフィルタリング

HTTP/HTTPS以外の接続試行でも、URLカテゴリとレピュテーションデータベースをDNSルックアップ要求に適用できます。

たとえば、ユーザがwww.example.comにFTP接続しようとすると、その完全修飾ドメイン名(FQDN)のDNSルックアップ要求が検出されたときに、www.example.comのカテゴリとレピュテーションを検索するようにシステムを設定できます。返されたカテゴリ/レピュテーションのDNS/URLフィルタリングルールがブロックルールの場合、システムはDNS応答をブロックします。そのため、ユーザはFQDNのIPアドレスを取得できず、接続試行に失敗します。

DNS ルックアップ要求フィルタリングを有効にすることで、URL フィルタリングルールを HTTP/HTTPS 以外のプロトコルに拡張し、FTP、TFTP、SCP、ICMP などのプロトコルが Web アクセスをブロックしているサイトへの接続を確立しないようにできます。このフィルタリングは、ユーザがFQDN名を使用しており、DNSルックアップを必要とする限り機能します。ユーザがIPアドレスを使用する場合、DNS要求は発生しないため、DNS要求のブロックはできません。

HTTP/HTTPSトラフィックの場合、DNS要求時にカテゴリ/レピュテーションルックアップを実行すると、システムパフォーマンスが向上する可能性があります。これは、Webセッションの確立を試行する前に接続される事態を妨ぐことができるためです。これは、特に暗号化されているHTTPSに対して有効です。DNS要求の段階で拒否することで、システムはHTTPS接続を認識しないため、復号ルールを評価する必要がなくなり、暗号されたセッションを適切なアクセス制御ルールに一致させるというさらに難しいタスクを実行する必要もなくなります。

DNS要求のフィルタリングのガイドライン

DNS要求のフィルタリングを設定する際は、次の点に注意してください。

- DNS要求のフィルタリングは、DNSセッションでのみ機能します。DNS応答を許可する場合(つまり、URLィルタリングルールアクションが[許可]の場合)、返されたIPアドレスを使用してユーザが確立する後続の接続は、アクセス制御ルールに対して個別に照合されます。接続が別のルールに一致するためブロックされることも、他の理由で許可されることもあります。たとえば、FTPがDNSルックアップを介してIPアドレスを取得しようとすると、FTP接続を禁止する別のアクセス制御ルールが存在するため接続が最終的にブロックされることがあります。
- URL/DNS要求のフィルタリングルールの前にあるアクセス制御ルールに一致するDNSルックアップ要求は、一致ルールに従って許可またはブロックされます。これらの接続では、カテゴリ/レピュテーションルックアップは実行されません。
- この機能では、カテゴリ/レピュテーションに基づいてURLフィルタリングを実装する必要があります。このタイプのURLフィルタリングには、URLフィルタリングライセンスが必要です。カテゴリ/レピュテーションに基づくURLフィルタリングルールがない場合、DNS要求のフィルタリングは関係ないため、有効にしないでください。
- DNSフィルタリングによって生成される接続イベントには、DNSクエリ、URLカテゴリ、およびURLレピュテーションという特に重要なフィールドが含まれます。[DNSクエリ]フィールドには、ルックアップ要求の完全修飾ドメイン名(FQDN)が表示されます。DNSフィルタリングイベントの場合、URLフィールドは空白になります。
- DNS要求のフィルタリングは、URLカテゴリとレピュテーションデータベースのみを使用します。一致するアクセス制御ルールで定義されたURLオブジェクトまたはその他の手動URLフィルタリングは無視されます。手動でDNS名のブロックを実装する場合は、セキュリティインテリジェンスDNSポリシーを使用します。

URLカテゴリとレピュテーションに基づいたDNS要求のフィルタリング

次の手順では、DNSルックアップ要求フィルタリングを実装する方法について説明します。

始める前に

まだ有効になっていない場合は、URL ライセンスを有効にする必要があります。

手順

ステップ 1 **[ポリシー]** > **[アクセス制御]**の順に選択します。

ステップ 2 必要に応じて、[アクセスポリシー設定] (⚙)ボタンをクリックし、[DNSトラフィックへのレピュテーション適用]オプションを選択して、[OK]をクリックします。

このオプションは、アクセス コントロール ポリシーのDNS要求のフィルタリングを有効にします。このオプションは、デフォルトでは有効になっています。

ステップ 3 既存のURLフィルタリングルールを評価するか、新しいルールを作成して、DNS要求にも適用されるURLカテゴリとレピュテーションに基づくフィルタリングを実装します。

URLフィルタリングは通常、HTTP/HTTPSトラフィックにのみ適用されるため、アプリケーションやポートに基づいてこれらのルールを制限する必要はありません。ただし、次の制限がある場合は、ルールがDNS要求にも適用できることを確認してください。

- [送信元/宛先]タブで、[宛先ポート]フィールドに[任意]が指定されている場合、変更は不要です。ポートを指定した場合は、[DNS over UDP]および[DNS over TCP]をリストに追加します。
- [アプリケーション]タブで、アプリケーションリストに[任意]だけが指定されてる場合、変更は不要です。アプリケーションまたはアプリケーションフィルタを指定した場合は、[DNS]アプリケーションをリストまたはフィルタに追加します。その他のDNS関連オプションは、この目的には関係ありません。

アクセス制御ルールの作成の詳細については、アクセス制御ルールの設定 （24 ページ）を参照してください。

ステップ 4 DNS要求がこれらのルールに一致しないことを確認するには、前述のルールを評価します。

カテゴリおよびレピュテーションの決定は、DNS要求がカテゴリおよびレピュテーションの仕様を持つURLフィルタリングルールと一致する場合にのみ行われます。URLフィルタリングルールよりも前のアクセス コントロール ポリシーのルールに一致するDNS要求は、DNS要求のフィルタリングをバイパスします。このようなDNS要求は、ブロックまたは許可された一致ルールに従って処理されます。

侵入、ファイル、およびマルウェア検査

侵入ポリシーとファイルポリシーは共に連携して、トラフィックの侵入に対する最後の防衛線として機能します。

- 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機能とマルウェア防御機能を管理します。

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制御ルールに関連付けることによって、アクセス制御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、そのトラフィックを検査するよう、システムに指示できます。

トラフィックを**許可する**ルールで、侵入ポリシーとファイルポリシーの設定を行えます。トラフィックを**信頼**または**ブロック**するように設定したルールで検査は行われません。さらに、アクセス制御ポリシーのデフォルト アクションが、**許可**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。

アクセス制御ルールで処理されるすべての単一接続において、侵入検査の前にファイル検査が行われます。つまり、侵入のファイルポリシーによってブロックされたファイルに対してシステムは検査を行いません。ファイル 検査では、ファイル タイプによるブロックが、マルウェア インスペクションおよびブロックよりも優先されます。セッションでファイルが検出されブロックされるまで、そのパケットは侵入検査の対象となります。

（注） デフォルトでシステムは、暗号化ペイロードの侵入検査とファイル検査を無効化します。これにより、暗号化された接続が、侵入検査とファイル検査が設定されたアクセス制御ルールに一致した際の誤検出を減らすため、パフォーマンスが向上されます。検査は暗号化されていないトラフィックにのみ機能します。

アクセス コントロール 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指定するルールを汎用的な基準を指定するルールよりも上に配置して、限定的なルールが汎用的なルールよりも先にトラフィックと一致して適用されるようにする必要があります。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）の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）ので、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）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（Security Intelligence）] ポリシー：アクセス コントロール ポリシーではドロップされた接続が参照されることはありません。ブロックリストに一致しない接続は、その後にアクセス制御ルールと照合され、最終的に、そのアクセス制御ルールによって、接続の処理方法（許可またはドロップ）が決定されます。
- **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イネーブル化とディセーブル化を参照してください。

- **URL** 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。
- **IPS** 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には、このライセンスも必要です（マルウェア防御ライセンスも必要）。
- **マルウェア防御**ライセンス：アクセスルールにファイルポリシーを設定するため。IPS ライセンスは、ファイルポリシーにも必要です。

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。

- URL データベースの更新にカテゴリの追加（新規、着信）、廃止（送信）、または削除が含まれている場合は、影響を受けるアクセス制御ルールを変更するための猶予期間があります。影響を受けるルールは情報メッセージと一緒にマークされ、メッセージにはルールに影響する問題についての説明と、カテゴリ変更に関する詳細情報がある Cisco Talos Intelligence Group（Talos） Web サイトへのリンクが記載されます。最新の URL データベースで使用可能な適切なカテゴリを使用するように、ルールを更新する必要があります。

  猶予期間に対応するため、廃止された送信カテゴリを削除せずに新しく追加された着信カテゴリを適切なルールに追加します。ルールは新旧のカテゴリの両方を含める必要があります。新しいカテゴリは、古いカテゴリが削除対象としてマークされている場合に有効になります。古いカテゴリが最終的に削除されたら、ルールを編集して削除されたカテゴリを除去し、設定を再展開する必要があります。削除されたカテゴリを使用するルールを修正するまで、設定の展開はブロックされます。注意が必要なルールをフィルタリングするには、表の上にある [問題のルールを表示（See Problem Rules）] リンクをクリックします。

- Device Manager はディレクトリサーバーから最大 50,000 人のユーザー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 50,000 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。

  50,000 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 50,000 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 50,000 個の名前だけをグループ メンバーシップに照らして照合できます。

- 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、変更は展開できません。さらに、システムソフトウェアの更新は、問題を修正するまでインストールできません。[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。

- 完全修飾ドメイン名（FQDN）ネットワーク オブジェクトを送信元または宛先の基準として使用するには、**[デバイス（Device）] > [システム設定（System Settings）] > [DNS サーバ（DNS Server）]** でデータ インターフェイスの DNS も設定する必要があります。システムでは、アクセス制御ルールで使用されているFQDNオブジェクトのルックアップを実行するために管理DNSサーバの設定は使用されません。FQDN解決のトラブルシューティングについては、DNS の一般的な問題のトラブルシューティングを参照してください。

  FQDNによるアクセスの制御はベストエフォート型のメカニズムであることに注意してください。次の点を考慮してください。

  - DNS応答はスプーフィングされる可能性があるため、完全に信頼できる内部DNSサーバのみを使用します。

  - 一部のFQDNは、特に非常に人気の高いサーバーの場合、数千とはいかなくても、数百の IP アドレスを持つことがあり、それらが頻繁に変更されることがあります。システムはキャッシュされている DNS ルックアップの結果を使用するため、ユーザーはキャッシュに存在しないアドレスを取得する可能性があり、その接続はFQDNルールに合致しません。FQDN ネットワークオブジェクトを使用するルールは、100 未満のアドレスに解決される名前に対してのみ効果的に機能します。

    100 を超えるアドレスに解決される FQDN のネットワーク オブジェクト ルールを作成しないことを推奨します。接続のアドレスが解決され、デバイスのDNSキャッシュで使用可能である可能性は低いからです。このような場合は、FQDNネットワーク オブジェクト ルールの代わりに URL ベースのルールを使用します。

  - 人気のある FQDN では、異なる DNS サーバが異なるセットの IP アドレスを返す場合があります。したがって、ユーザが設定したものとは異なる DNS サーバを使用している場合、FQDNベースのアクセス制御ルールがクライアントで使用されているサイトのすべての IP アドレスに適用されないことがあり、ルールで意図した結果が得られません。

  - 一部の FQDN DNS エントリには、非常に短い存続可能時間（TTL）値が設定されています。この結果、ルックアップテーブルで頻繁に再コンパイルが発生し、全体的なシステムパフォーマンスに影響を与える場合があります。

- 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た接続内のペイロードを持た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。
- マッチング基準はなるべく空欄にしておきます（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で）。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、システムはすべてのインターフェイスのトラフィックをより効率的に照合できます。複数の基準を指定すると、指定された条件の内容のすべての組み合わせを照合する必要があります。
- 送信元または宛先の基準にIPアドレスを指定する場合は、同じルールにIPv4アドレスとIPv6アドレスを混在させないでください。IPv4アドレスとIPv6アドレスに個別のルールを作成します。
- 動作中、Threat Defense デバイスは、アクセスルールで使用されるネットワークオブジェクトの内容に基づいて、アクセス制御ルールを複数のアクセスコントロールリストのエントリに展開します。オブジェクトグループ検索を有効にすることで、アクセスコントロールルールの検索に必要なメモリを抑えることができます。オブジェクトグループ検索を有効にした場合、システムによってネットワークオブジェクトは拡張されませんが、オブジェクトグループの定義に基づいて一致するアクセスルールが検索されます。オブジェクトグループ検索は、アクセスルールがどのように定義されるか、または Device Manager にどのように表示されるかには影響しません。アクセスコントロールルールと接続を照合するときに、デバイスがアクセスコントロールルールを解釈して処理する方法のみに影響します。

  オブジェクトグループ検索を有効にすると、ネットワークオブジェクトを含むアクセス コントロール ポリシーのメモリ要件が軽減されます。ただし、オブジェクトグループ検索では、ルールルックアップのパフォーマンスが低下して、CPU使用率が増大する可能性があることに注意してください。CPUに対する影響と、特定のアクセス コントロール ポリシーに関するメモリ要件の軽減とのバランスをとる必要があります。ほとんどの場合、オブジェクトグループ検索を有効にすると、ネット運用が改善されます。

  FlexConfig を使用してこのオプションを設定するには、**object-group-search access-control** コマンドを発行します。否定テンプレートでは、このコマンドの **no** 形式を使用します。

  リリース 7.2 以降、この機能は新しい展開ではデフォルトで有効になっていますが、アップグレードされたシステムでは自動的に有効になりません。
- 関連 RFC に違反する GRE トンネルはドロップされます。たとえば、RFC に反して GRE トンネルの予約ビットにゼロ以外の値が含まれている場合、そのトンネルはドロップされ

ます。非準拠の GRE トンネルを許可する必要がある場合は、リモートマネージャを使用して、そのセッションを信頼するプレフィルタルールを設定する必要があります。Device Manager を使用してプレフィルタルールを設定することはできません。

アクセス コントロール ポリシーの設定

ネットワーク リソースへのアクセスを制御するには、アクセス制御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基準が一致した最初のルールです。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。

アクセス制御ポリシーを設定するには、**[ポリシー（Policies）]** > **[アクセス 制御（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。各ルールに対して次を実行します。

- 一番左の列にあるルール番号の隣の [>] ボタンをクリックして、ルールの図を開きます。図は、ルールがどのようにトラフィックを制御するかを視覚的に理解するのに役立ちます。もう一度ボタンをクリックすると図が閉じます。
- ほとんどのセルではインライン編集が可能です。例えば、アクションをクリックして別のものを選択するか、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、ルールを編集してから [順番（Order）] リストで新しい場所を選択することにより、ルールを移動することもできます。処理したい順番でルールを配置することが重要です。特に、一般的なルールにおける例外など、特別なルールは上部に配置する必要があります。
- 一番右の列には、ルールのアクション ボタンがあります。セルにマウス オーバーするとボタンが表示されます。ルールを編集（）または削除（）することができます。
- [アクセスコントロールの設定（Access Control Settings）]（）ボタンをクリックして、ポリシー内の特定のルールではなく、アクセス コントロール ポリシーに適用される設定を行います。
- テーブルの上の [ヒットカウントの切り替え（Toggle Hit Counts）] アイコン（）をクリックし、テーブルの [ヒットカウント（Hit Count）] 列を追加または削除します。[ヒットカウント（Hit Count）] 列は [名前（Name）] 列の右側にあり、ルールの合計ヒット数と最新のヒットの日付と時刻が表示されます。ヒットカウント情報は、切り替えボタンをクリックしたときに取得されます。最新情報を取得するには、更新アイコン（）をクリックします。

- URL カテゴリの削除または変更などが原因で特定のルールに問題が発生した場合、これらのルールのみを表示するには、検索ボックスの横にある [See Problem Rules] リンクをクリックしてテーブルをフィルタ処理します。これらのルールを編集および修正（または削除）して、必要とするサービスが提供されるようにします。

ここでは、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）]** > **[アクセス制御（Access Control）]** の順に選択します。

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）]：どんな種類の検査も行うことなくトラフィックを許可します。
- [許可（Allow）]：侵入ポリシーに基づいて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 （34 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をダッシュボード データやイベント ビューアに含めるには、ロギングを有効にする必要があります。ロギングの設定 （35 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 ポリシーの設定

ポリシー内の特定のルールではなく、アクセス コントロール ポリシーに適用される設定を行います。

手順

ステップ 1 **[ポリシー（Policy）]** > **[アクセス制御（Access Control）]** の順に選択します。

ステップ 2 [アクセスポリシーの設定（Access Policy Settings）]（⚙）ボタンをクリックします。

ステップ 3 以下の設定項目を設定します。

- [TLSサーバーアイデンティティ検出（TLS Server Identity Discovery）]：TLS 1.3 では、ほとんどのハンドシェイクメッセージが暗号化されるため、証明書情報を簡単に利用できません。TLS 1.3 で暗号化されたトラフィックで、アプリケーションまたは URL フィルタリングを使用するアクセスルールに対応するには、システムにサーバーのクリアテキスト証明書がある必要があります。このオプションを有効にすると、システムは、クライアントの Hello パケットの IP アドレスおよび SNI（Server Name Indication）に基づいて、サイトの証明書がキャッシュに保存されているかどうかを確認します。保存されていない場合、システムは、TLS 1.2 プローブを使用して証明書を取得します。その後は、この証明書を使用して、アプリケーション/URL カテゴリおよびレピュテーションを識別することができます。暗号化された接続が適切なアクセス制御ルールに適合していることを確認するために、このオプションを有効にすることを推奨します。この設定では、証明書のみが取得されます。接続は暗号化されたままになります。TLS 1.3 証明書を取得するには、このオプションを有効にするだけで十分です。対応する SSL 復号ルールを作成する必要はありません。ただし、キャッシュされた証明書は、アクセス制御処理に加えて、より効果的な復号ルール処理にも使用されます。

- [DNSトラフィックへのレピュテーション適用]: URLフィルタリングカテゴリとレピュテーションルールをDNSルックアップ要求に適用するには、このオプションを有効にします。ルックアップ要求の完全修飾ドメイン名（FQDN）にブロックしているカテゴリやレピュテーションがある場合、システムは DNS 応答をブロックします。ユーザは DNS 解決を受信しないため、ユーザは接続を完了できません。非 Web トラフィックに URL カテゴリおよびレピュテーションフィルタリングを適用するには、このオプションを使用します。詳細については、DNS要求のフィルタリング （14 ページ）を参照してください。

ステップ 4 **[OK]** をクリックします。

アクセス制御ルールの設定

アクセス制御ルールを使用して、ネットワークリソースへのアクセスを制御します。アクセス制御ポリシーに設定されたルールは、上から下への順に評価されます。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）]** > **[アクセス制御（Access Control）]** の順に選択します。

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場合は、[+] ボタンをクリックします。
- 既存のルールを編集する場合は、対象のルールの編集アイコン（  ）をクリックします。

不要になったルールを削除する場合は、対象のルールの削除アイコン（  ）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。ルールの配置を後で変更する場合は、このオプションを編集して配置を変更します。

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。

- [信頼性（Trust）]：どんな種類の検査も行うことなくトラフィックを許可します。
- [許可（Allow）]：ポリシーの侵入およびその他のインスペクション設定に従って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。トラフィックは検査されません。

ステップ 6 以下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/大陸（地理的位置）、アドレスに割り当てられたセキュリティグループタグ（SGT）、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、SGT、プロトコル、およびポートです。送信元/送信先条件 （27 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、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。デフォルトは任意のアプリケーションです。アプリケーション基準 （29 ページ）を参照してください。
- [URL]: WebまたはDNSルックアップ要求のURLまたはURLカテゴリ。デフォルトは任意の URL です。「URL の基準 （31 ページ）」を参照してください。
- [ユーザ（Users）]：アイデンティティ ソース、ユーザまたはユーザ グループ。アイデンティティ ポリシーにより、ユーザおよびグループ情報をトラフィックの照合に使用できる

かどうかを判断します。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 （33 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。

条件をアクセス制御ルールに追加する際は、以下のヒントを参考にしてください。

- ルールごとに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。トラフィックが、基準のいずれかと一致する場合、トラフィックはその条件を満たすことになります。たとえば、単一のルールを使用して、最大 50 のアプリケーションまたはアプリケーション フィルタのアプリケーション制御を適用できます。このように、単一の条件に含まれる基準の間には OR 関係があり、条件のタイプ間（送信元/送信先とアプリケーションの間など）には AND 関係があるということです。
- 一部の機能の使用には、該当する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」アクションを使用するポリシーでは、暗号化されていないトラフィックに対する追加検査を設定できます。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 （34 ページ）を参照してください。
- [ファイル ポリシー（File Policy）]：マルウェアに感染したファイルやブロックする必要があるファイルがないかをトラフィックで検査する場合に選択します。ファイルポリシー設定 （34 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、ルールと一致するトラフィックの接続イベントは生成されません。ただし、ファイル ポリシーを選択した場合はデフォルトでファイル イベントが生成されます。この動作は変更できます。ポリシーと一致するトラフィックをダッシュボードデータまたはイベントビューアに含めるには、ロギングを有効にする必要があります。ロギングの設定 （35 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/送信先条件

アクセスルールの送信元/送信先条件は、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/大陸（地理的位置）、アドレスに割り当てられたセキュリティグループタグ（SGT）、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を定義します。デフォルトは、すべてのゾーン、アドレス、地理的位置、SGT、プロトコル、およびポートです。

条件を変更するには、該当する条件の [+] 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。

ルールに一致する送信元と送信先を識別するのに、次の基準を使用できます。

送信元ゾーン、送信先ゾーン

トラフィックが経由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。どのインターフェイスのトラフィックでも適用するものとして、いずれか、または両方の基準を定義することも、両方とも未定義にすることもできます。

- ゾーン内のインターフェイスからデバイスを発信するトラフィックと一致させるには、そのゾーンを [送信先ゾーン（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着信するトラフィックと一致させるには、そのゾーンを [送信元ゾーン（Source Zones）] に追加します。
- 送信元ゾーンと送信先ゾーンの条件を両方ともルールに追加した場合、指定した送信元ゾーンのいずれかから発信されて、指定した送信先ゾーンのいずれかを経由するトラフィックが一致することになります。

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。

（注） 1 つのルールにパッシブ セキュリティ ゾーンとルーテッド セキュリティ ゾーンを混在させることはできません。さらに、パッシブセキュリティゾーンは送信元ゾーンとしてのみ指定でき、宛先ゾーンとして指定することはできません。

送信元ネットワーク、宛先ネットワーク

ネットワーク アドレスまたはトラフィックの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です。

- IP アドレスまたは地理的位置からのトラフィックを一致させるには、[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一致させるには、[送信先ネットワーク（Destination Networks）] を設定します。
- 送信元と送信先ネットワークの両方の条件をルールに追加すると、一致するトラフィックは指定した IP アドレスのいずれかから送信され、送信先 IP アドレスのいずれかを通って出力されなければなりません。

この条件を追加するには、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。完全修飾ドメイン名（FQDN）を使用してアドレスを定義するオブジェクトを使用できます。このアドレスは DNS ルックアップによって判別されます。
- [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、その大陸内のすべての国が選択されます。地理的位置を直接ルールで選択するほかに、作成した位置情報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、特定の国で使用されているすべての潜在的な IP アドレスを知る必要なく、その国へのアクセスを簡単に制限できます。

（注） 地理的位置の最新データを常にトラフィック フィルタリングで使用できるよう、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推奨します。

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 の場合、ポートが含まれます。ICMP の場合、コードおよびタイプが含まれます。

- 特定のプロトコルまたはポートからのトラフィックと一致させるには、[送信元ポート（Source Ports）] を設定します。送信元ポートに設定できるのは、TCP/UDP のみです。
- プロトコルまたはポートからのトラフィックを一致させるには、[宛先ポート/プロトコル（Destination Ports/Protocols）] を設定します。宛先ポートだけを条件に追加する場合、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、宛先ポートのみで許可されます。送信元ポートでは許可されません。
- 特定の TCP/UDP ポートから特定の TCP/UDP ポートへ発信されるトラフィックを一致させるには、両方のポートを設定します。送信元および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、TCP/80 ポートから TCP/8080 ポートへのトラフィックをターゲットにすることができます。

送信元 SGT グループ、宛先 SGT グループ

Identity Services Engine（ISE）からダウンロードされた、トラフィックに割り当てられた SGT を識別するセキュリティグループタグ（SGT）グループオブジェクト。これらのオブジェクトは、ISE アイデンティティソースを定義する場合にのみ使用できます。それ以外の場合、このセクションは表示されません。アクセス制御のために SGT を使用する方法の詳細については、TrustSec セキュリティ グループ タグを使用したネットワーク アクセスの制御方法 （40 ページ） を参照してください。

- 送信元がグループで定義された SGT のいずれかを持つトラフィックを照合するには、[送信元SGTグループ（Source SGT Groups）] を設定します。
- 宛先がグループで定義された SGT のいずれかを持つトラフィックを照合するには、[宛先SGTグループ（Destination SGT Groups）] を設定します。
- 送信元 SGT 条件と宛先 SGT 条件の両方をルールに追加する場合、指定されたタグのいずれかを持つ送信元から発信され、宛先タグのいずれかに送信されるトラフィックのみが照合されます。

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処理が定義されます。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関連性が低いすべてのアプリケーションを識別してブロックするアクセス制御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。

さらに、シスコはシステムおよび脆弱性データベース（VDB）の更新を通して、頻繁にアプリケーション検出機能の更新や追加を行います。これにより、リスクの高いアプリケーションをブロックするルールが新しいアプリケーションに自動的に適用され、手動でルールを更新する必要がなくなります。

ルールでアプリケーションとフィルタを直接指定するか、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できます。複雑なルールを作成する場合は、オブジェクトを使用すると、システム制限内（基準ごとに 50 項目）に収めることが簡単になります。

アプリケーションとフィルタのリストを変更するには、条件内にある [+] ボタンをクリックし、個別のタブにリストされている必要な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、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。いずれかのタブで [高度なフィルタ（Advanced Filter）] をクリックすると、フィルタ基準の選択、または特定のアプリケーションの検索ができます。アプリケーション、フィルタ、またはオブジェクトの **[x]** をクリックすると、ポリシーから削除されます。[フィルタとして保存（Save As

Filter）]リンクをクリックすると、組み合わせ条件が、新規のアプリケーション フィルタ オブジェクトとして保存されます。

（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た場合は、アプリケーション名の後に「（廃止）」が表示されます。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。削除しないと、それ以降の展開やシステム 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**[高度なフィルタ（Advanced Filter）]**基準を使用して、ルールに一致するアプリケーションや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。「リスクが高いOR非常に高い」という具合です。フィルタ間の関係はANDであり、「リスクが高いOR非常に高いANDビジネスとの関連性は低いOR非常に低い」となります。フィルタを選択するごとに、アプリケーションの一覧が更新され、条件に一致するものだけが表示されます。これらのフィルタを使用して、個別に追加するアプリケーションの検索や、フィルタ基準をルールに追加する際に目的のアプリケーションが対象となっているかを確認できます。

リスク

アプリケーションが、組織のセキュリティ ポリシーに違反して使用される可能性：非常に低い～非常に高い。

ビジネスとの関連性

アプリケーションが、娯楽としてではなく、組織のビジネス活動の範囲内で使用される可能性：非常に低い～非常に高い。

種類

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**：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**：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**：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基本的な機能を表す一般的な分類。

タグ

アプリケーションに関する追加の情報。カテゴリに類似。

暗号化されたトラフィックの場合、システムがトラフィックを識別してフィルタ処理できるのは **SSL プロトコル**のタグが付けられたアプリケーションのみです。このタグが付いてい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可能です。また、システムは**復号トラフィック** タグを、復号されたトラフィックでのみ検出できるアプリケーションに割り当てます。（暗号化されたトラフィックや暗号化されていないトラフィックで検出されるアプリケーションには割り当てない）

アプリケーション一覧（画面下部）

この一覧は、上部のフィルタ オプションを選択するごとに更新されるため、現在のフィルタに一致するアプリケーションのみを確認できます。この一覧を使用することで、フィルタ基準をルールに追加する際に目的のアプリケーションが対象となっているかを確認できます。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 の基準

アクセス ルールの URL の基準は、Web 要求で使用される URL、または要求される URL が属するカテゴリを定義します。カテゴリ照合の場合は、許可またはブロックするサイトの関連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。

DNSルックアップ要求フィルタリングを有効にすると、カテゴリとレピュテーションの設定は、ルックアップ要求の完全修飾ドメイン名(FQDN)にも適用されます。DNS要求フィルタリングには、カテゴリとレピュテーションの設定のみが適用されます。手動URLフィルタリングは無視されます。

URL のカテゴリとレピュテーションにより、アクセス制御ルールの URL 条件を容易に作成できます。たとえば、すべてのギャンブルサイトをブロックしたり、信頼できないソーシャル ネットワーキング サイトをブロックしたりできます。該当するカテゴリとレピュテーションの URL をユーザが参照しようとすると、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 トラフィックを予期されるとおりに制御することが保証されます。さらに、シスコの脅威インテリジェンスは常に更新されて新しい URL が追加され、既存の URL も新しいカテゴリとリスクに更新されるため、システムでは常に最新情報を使用して要求対象のURLがフィルタ処理されます。ただし、セキュリティに対する脅威（マルウェア、スパム、ボットネット、スパム、フィッシングなど）を表す悪意のあ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導入するのが間に合わないこともあります。

URL 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URLカテゴリを選択します。ポリシーからカテゴリやオブジェクトを削除するには、該当する [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、[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、[新しい URL の作成（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、必要なカテゴリを選択し、[OK] をクリックします。

カテゴリの説明については、https://www.talosintelligence.com/categoriesを参照してください。

デフォルトでは、レピューテーションに関係なく、選択した各カテゴリのすべての 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、各カテゴリの下向き矢印をクリックし、[すべて（Any）] チェックボックスをオフにしてから、[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 スライダの左側に許可されるサイトが示され、右側にブロックされるサイトが示されます。レピュテーションの使用方法はルールアクションによって異なります。

- ルールで Web アクセスがブロックまたは監視される場合は、レピュテーション レベルを選択すると、そのレベルよりもシビラティ（重大度）が高いすべてのレピュテーションも選択されます。たとえば、**問題のあるサイト**（レベル 2）をブロックまたは監視するルールを設定する場合、**信頼できない**（レベル1）のサイトも自動的にブロックまたは監視されます。
- 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、**[好ましいサイト（Favorable sites）]**（レベル 4）を許可するルールを設定した場合、**[信頼できる（Trusted）]**（レベル 5）サイトも自動的に許可されます。

レピュテーションが不明な URL をレピュテーション一致に含めるには、[レピュテーションが不明なサイトを含める（Include Sites with Unknown Reputation）] オプションを選択します。通常、新しいサイトは評価されていません。また、その他の理由でサイトのレピュテーションが不明である（または判断できない）場合もあります。

URLのカテゴリを確認します。

特定の URL のカテゴリとレピュテーションを確認できます。[確認するURL]ボックスにURLを入力し、[移動]をクリックします。結果を表示するには、外部の Web サイトに移動します。分類に同意しない場合は、[URLカテゴリの異議を送信する]リンクをクリックしてお知らせください。

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ように、アイデンティティ ポリシーと関連ディレクトリ 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、特定の接続のためにユーザ 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アドレスが識別されたユーザに関連付けられます。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、そのユーザから発信された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が含まれていないため、この IP アドレスからユーザへのマッピングが最良の推測となります。

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ので、個々のユーザを選択するよりも、グループを選択する方が妥当です。たとえば、Engineering グループが開発ネットワークにアクセスできるようにするルールを作成し、その下位ルールとして Engineering グループ以外のすべてのユーザ/グループによる開発ネットワークへのアクセスを拒否するルールを作成するとします。すると、新しいエンジニアにこのルールを適用するには、エンジニアをディレクトリ サーバの Engineering グループに追加するだけですみます。

そのソース内のすべてのユーザに適用するアイデンティティ ソースを選択することもできます。したがって、複数のActive Directoryドメインをサポートする場合は、ドメインに基づいてリソースへの差分アクセスを提供できます。

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。

- [アイデンティティ ソース（Identity Sources）]：AD レルムやローカル ユーザ データベースなど、選択したソースから取得したすべてのユーザにルールを適用するアイデンティティ ソースを選択します。必要なレルムがまだ存在していない場合は、[新しいアイデンティティレルムの作成（Create New Identity Realm）] をクリックします。
- [グループ（Groups）]：目的のユーザ グループを選択します。グループを選択できるのは、ディレクトリ サーバでグループを設定している場合だけです。グループを選択すると、そのグループのすべてのメンバー（サブグループを含む）にそのルールが適用されます。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。
- [ユーザ]: 個々のユーザを選択します。ユーザ名には、Realm\usernameなどのアイデンティティ ソースのプレフィックスが付きます。

  Special-Identities-Realmの下にはいくつかの組み込みユーザがあります。

  - [認証失敗（Failed Authentication）]：ユーザが認証を求められ、有効なユーザ名/パスワードを入力できずに最大試行回数に達しました。認証の失敗により、ユーザがネットワークにアクセスできなくなることはありませんが、このようなユーザに対してネットワーク アクセスを制限するアクセス ルールを作成できます。

- [ゲスト（Guest）]：ゲストユーザは[認証失敗（Failed Authentication）]ユーザと似ていますが、アイデンティティルールでこのようなユーザがゲストと呼ばれるように設定されている点で異なります。ゲストユーザが認証を求められましたが、認証できずに最大試行回数に達しました。
- [認証不要（No Authentication Required）]：ユーザの接続が、認証不要と指定されている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いため、認証失敗の記録がありません。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ないことを意味します。

侵入ポリシーの設定

ファイアウォールシステムには複数の侵入ポリシーが付属しています。Cisco Cisco Talos Intelligence Group（Talos）によって提供されるいくつかの侵入ポリシーはシスコによって設計されています。Talos によって、侵入およびプリプロセッサルール状態と詳細設定が規定されています。トラフィックを許可するアクセス制御ルールでは、侵入ポリシーを選択して、トラフィックにおける侵入およびエクスプロイトを検査することができます。侵入ポリシーにより、デコードされたパケットがパターンに基づいて調査され、悪意のあるトラフィックがブロックまたは除去されます。

Snort 3を実行している場合は、これらのポリシーのいずれかを選択するか、独自の侵入ポリシーを作成できます。

侵入検査を有効化するには、**[侵入ポリシー]**>**[オン]**を選択し、必要なポリシーを選択します。各ポリシーの説明を表示するには、ドロップダウンリストでポリシーの情報アイコンをクリックします。

定義済みポリシーの詳細については、システム定義のネットワーク分析および侵入ポリシーを参照してください。

ファイル ポリシー設定

ファイルポリシーにより、マルウェア防御を使用して悪意のあるソフトウェア（マルウェア）を検出することができます。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。

マルウェア防御は、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 Secure Malware Analytics Cloudを使用します。Secure Malware Analytics Cloud 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 Secure Malware Analytics Cloud 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）：Secure Malware Analytics Cloudはファイルをマルウェア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）：Secure Malware Analytics Cloud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）：Secure Malware Analytics Cloudは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。
- 使用不可（Unavailable）：システムは Secure Malware Analytics Cloudに対し、このファイルの性質を問い合わせることができませんでした。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。「使用不可」イベントが続く場合は、管理アドレスのインターネット接続が正しく機能していることを確認してください。

ファイル ポリシー

次のファイル ポリシーのいずれかを選択できます。

- [なし（None）]：送信されたファイルでマルウェアを評価せず、ファイル固有のブロッキングを実行しません。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）]：Secure Malware Analytics Cloud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）]：Secure Malware Analytics Cloud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。
- **（カスタムファイルポリシー）**：脅威に対する防御 API filepolicies リソース、およびその他の FileAndMalwarePolicies リソース（filetypes、filetypecategories、ampcloudconfig、ampservers、ampcloudconnections など）を使用して、独自のファイルポリシーを作成できます。ポリシーを作成して変更を展開した後、Device Manager でアクセス制御ルールを編集するときにポリシーを選択できます。ポリシーを選択すると、ポリシーの下にポリシーの説明が表示されます。

ロギングの設定

アクセスルールのロギング設定によって、ルールに一致するトラフィックに対する接続イベントを発行す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表示するには、ロギングを有効化する必要があります。一致するトラフィックが、システムのモニタに使用する各種のダッシュボードに反映されるためにも、ロギングを有効化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。生成されるイベントの数を抑えてパフォーマンスを向上させることを目標にする場合は、分析のために重要な意味を持つ接続のロギングだけを有効化してください。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）攻撃中にブロックされたTCP接続のロギングは、複数の同様のイベントでシステムのパフォーマンスに影響を与え、データベースのパフォーマンス低下させる可能性があります。ブロック ルールのロギングを有効化する前に、そのルールの対象がインターネットに接続されているインターフェイスか、それとも DoS 攻撃に脆弱な他のインターフェイスかを考慮します。

次のロギング アクションを設定できます。

[ログ アクションの選択（Select Log Action）]

次のいずれかのアクションを選択できます。

- [接続の始まりと終わりにログ（Log at Beginning and End of Connection）]：接続の始まりと終わりにイベントを発行します。「接続の終わり」イベントには、「接続の始まり」イベントに含まれるものすべてに加えて接続中に収集された情報のすべてが含まれるため、許可するトラフィックにこのオプションを選択するのはお勧めしません。両方のイベントをロギングすると、システムのパフォーマンスに影響を及ぼす可能性があります。一方、ブロックされるトラフィックにはこのオプションのみ許可されています。
- [接続の終わりにログ（Log at End of Connection）]：接続の終わりに接続のロギングを有効化する場合はこのオプションを選択します。許可された、または信頼できるトラフィックには、このオプションを推奨します。
- [接続時にログしない（No Logging at Connection）]：ルールのロギングを無効化するにはこのオプションを選択します。これはデフォルトです。

（注） アクセス制御ルールに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（ルールにおけるロギング設定とは無関係に）侵入が発生した接続の終了を自動的にロギングします。接続で侵入がブロックされると、接続ログ内の接続アクションは [ブロック（Block）]、理由は [侵入のブロック（Intrusion Block）] になります。侵入検査を実行するには許可（Allow）ルールを使用する必要があります。

ファイル イベント（File Events）

禁止されたファイルまたはマルウェアのイベントのロギングを有効化する場合は、[ファイルのログ（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。ルールでファイル ポリシーを選択する場合、

このオプションはデフォルトで有効になっています。このオプションを有効のままにしておくことを推奨します。

禁止されたファイルをシステムが検出した場合、次のうち1種類のイベントがログに記録されます。

- 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。

接続でファイルがブロックされると、接続ログ内で関連付けられるアクションは [ブロック（Block）] になります。ファイル検査とマルウェア検査を実行するには許可（Allow）ルールを使用する必要があります。接続の理由は、[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：（Send Connection Events To）]

外部の 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存在しない場合は、[新しい Syslog サーバの作成（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化するには、サーバのリストから [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、外部の syslog サーバにイベントを送信することにより、長期間ストレージが利用できるようになり、イベントの分析を向上できます。

この設定は、接続イベントのみに適用されます。侵入イベントを syslog に送信するには、侵入ポリシーの設定でサーバを設定します。Syslog にファイル/マルウェア イベントを送信するには、**[デバイス（Device）]** > **[システム設定（System Settings）]** > **[ロギング設定（Logging Settings）]** でサーバを設定します。

アクセス制御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）] ダッシュボードにあるほとんどのデータアクセス制御ポリシーに直接関係します。「トラフィックおよびシステム ダッシュボードのモニタリング」を参照してください。

- **[モニタリング]**>**[アクセスおよびSIルール]**には、最もヒットしたアクセスルールとセキュリティインテリジェンスに相当するルールおよび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。
- ユーザベース統計情報は [ユーザ（Users）] ダッシュボードで確認できます。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。
- 侵入ポリシー統計情報は [攻撃者（Attackers）] および [ターゲット（Targets）] ダッシュボードで確認できます。これらのダッシュボードに情報を表示するには、侵入ポリシー 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。
- 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）]** にはアクセス制御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。

ルール ヒット カウントの調査

各アクセス制御ルールのヒットカウントを表示することができます。ヒットカウントは、接続がルールに一致する頻度を示します。この情報を使用して、最もアクティブなルールとアクティブの度合いが低いルールを特定できます。

このカウントは、再起動やアップグレードの後も維持されます。

また、デバイス CLI で **show rule hits** コマンドを使用してルールヒットカウント情報を表示することもできます。

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 [ヒットカウントの切り替え（Toggle Hit Counts）] アイコン（  ）をクリックします。

[ヒットカウント（Hit Count）] 列は [名前（Name）] 列の右側にあり、ルールの合計ヒット数と最新のヒットの日付と時刻が表示されます。ヒットカウント情報は、切り替えボタンをクリックしたときに取得されます。

ヒットカウントの情報を使用して、次を行うことができます。

- ボタンの左側には、ヒットカウントが最後に更新されたときの情報が表示されます。最新の数字を取得するには、更新アイコン（）をクリックします。
- 特定のルールのヒット カウントの詳細表示を開くには、テーブルのヒット カウント番号をクリックして [ヒットカウント（Hit Count）] ダイアログ ボックスを開きます。ヒット カウント情報には、ヒットの回数と、ルールに一致した最後の接続の日付と時刻が含まれます。カウンタをゼロにリセットするには、[リセット（Reset）] をクリックします。

  一度にすべてのルールのヒットカウントをリセットする場合は、デバイスへの SSH セッションを開き、**clear rule hits** コマンドを発行します。
- 再度 [ヒットカウントの切り替え（Toggle Hit Counts）] アイコン（）をクリックし、テーブルから [ヒットカウント（Hit Count）] 列を削除します。

アクセス制御に関する Syslog メッセージのモニタリング

イベントはイベント ビューアで確認するだけでなく、アクセス制御ルール、侵入ポリシー、ファイル/マルウェア ポリシー、およびセキュリティ インテリジェンス ポリシーを設定してイベントを syslog サーバに送信することができます。イベントでは、次のメッセージ ID が使用されます。

- 430001: 侵入イベント。
- 430002：接続の開始時にログに記録される接続イベント。
- 430003：接続の終了時にログに記録される接続イベント。
- 430004：ファイルイベント。
- 430005：マルウェア イベント。

CLI でのアクセス制御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 rule hits**は、**show access-control-config** および **show access-list** で表示されるカウントよりも正確な、統合されたヒットカウントを表示します。ヒットカウントをリセットするには、**clear rule hits** コマンドを使用します。

- **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を確認してください。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。
- 脅威のブロック方法を確認してください。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。
- マルウェアのブロック方法を確認してください。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）の実装方法を確認してください。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を確認してください。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。
- サブネットの追加方法を確認してください。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。
- ネットワークでトラフィックを受動的にモニタする方法

次に、その他の例を示します。

TrustSec セキュリティ グループ タグを使用したネットワーク アクセスの制御方法

Cisco TrustSec ネットワークでトラフィックを分類するために Cisco Identity Services Engine（ISE）を使用してセキュリティ グループ タグ（SGT）を定義して使用する場合は、一致基準として SGT を使用するアクセス制御ルールを作成できます。これにより、IP アドレスではなく、セ

キュリティ グループ メンバーシップに基づいてアクセスをブロックまたは許可することができます。

セキュリティ グループ タグ（SGT）について

Cisco Identity Services Engine（ISE）では、セキュリティグループタグ（SGT）を作成し、各タグにホストまたはネットワークの IP アドレスを割り当てることができます。また、ユーザアカウントに SGT を割り当て、SGT がユーザのトラフィックに割り当てられるようにすることもできます。ネットワーク内のスイッチとルータがそのように設定されている場合、これらのタグは、ISE、Cisco TrustSec クラウドによって制御されるネットワークに入るときに、パケットに割り当てられます。

Device Manager で ISE アイデンティティソースを設定すると、脅威に対する防御 システムは自動的に ISE から SGT のリストをダウンロードします。その後、アクセス制御ルールでトラフィックの一致条件として SGT を使用できます。

たとえば、[実稼働ユーザ（Production Users）] タグを作成し、192.168.7.0/24 ネットワークをタグに関連付けることができます。これは、ラップトップ、Wi-Fi クライアントなどのユーザエンドポイントにそのネットワークを使用する場合に適しています。実稼働サーバ用に別のタグを作成し、関連するサーバまたはサブネットの IP アドレスをそのタグに割り当てることができます。次に、脅威に対する防御 では、タグに基づいてユーザーネットワークから実稼働サーバーへのアクセスを許可またはブロックすることができます。ISE でタグに関連付けられているホストまたはネットワーク アドレスを後で変更する場合、脅威に対する防御 デバイスに定義されているアクセス制御ルールを変更する必要はありません。

脅威に対する防御 は、アクセス制御ルールのトラフィック一致基準として SGT を評価するときに、次の優先順位を使用します。

1. パケット内で定義されている送信元 SGT タグ（存在する場合）。SGT タグがパケットに含まれるようにするには、ネットワーク内のスイッチおよびルータがそれらを追加するように設定されている必要があります。このメソッドの実装方法については、ISE のマニュアルを参照してください。

2. ISE セッションディレクトリからダウンロードされる、ユーザセッションに割り当てられた SGT。この種の SGT 照合では、セッションディレクトリ情報をリッスンするオプションを有効にする必要がありますが、このオプションは最初に ISE アイデンティティソースを作成するときにデフォルトでオンになっています。SGT は、送信元または宛先に一致させることができます。必須ではありませんが、通常は ISE アイデンティティソースを AD レルムとともに使用してパッシブ認証アイデンティティルールを設定し、ユーザ ID 情報を収集します。

3. SXP を使用してダウンロードされた SGT-to-IP アドレス マッピング。IP アドレスが SGT の範囲内にある場合、トラフィックは SGT を使用するアクセス制御ルールと一致します。SGT は、送信元または宛先に一致させることができます。

   ISE は、セキュリティグループ交換プロトコル（SXP）を使用して、SGT マッピングデータベースをネットワークデバイスに伝播します。ISE サーバを使用するように 脅威に対する防御 デバイスを設定する場合は、ISE から SXP トピックをリッスンするオプションをオンにする必要があります。そのため、脅威に対する防御 デバイスは、ISE からセキュリ

ティグループタグとマッピングについて直接学習し、ISEが更新されたセキュリティグループタグとマッピングを公開するたびに通知を受け取ります。これにより、デバイス上でセキュリティグループタグのリストが最新の状態に維持されるため、脅威に対する防御 は、ISE で定義されたポリシーを効果的に適用できるようになります。

セキュリティ グループ タグ（SGT）に基づくアクセス制御の設定

セキュリティ グループ タグ（SGT）を一致基準として使用するアクセス コントロール ルールを設定するには、最初に ISE サーバから SGT マッピングを取得するようにデバイスを設定する必要があります。

次の手順では、SXP で公開されている SGT から IP アドレスへのマッピングを含め、ISE で定義されているすべてのマッピングを取得するという前提に基づいたエンドツーエンドのプロセスについて説明します。または、下記の手順も実行できます。

- パケット内の SGT 情報のみを使用し、ISE からダウンロードされたマッピングを使用しない場合は、単に SGT グループ ダイナミック オブジェクトを作成し、それらをアクセス制御ルールの送信元 SGT 条件として使用します。この場合、送信元条件としてのみ SGT タグを使用できます。これらのタグは宛先の基準には決して一致しません。
- パケットとユーザセッション SGT のマッピングのみで SGT を使用する場合は、ISE アイデンティティソースの SXP トピックを登録するオプションを有効にする必要はなく、SXP マッピングを公開するように ISE を設定する必要もありません。この情報は送信元と宛先の両方の一致条件に使用できます。

始める前に

ここでは、ネットワークに Cisco TrustSec がすでに設定されていて、ポリシー適用ポイントとして 脅威に対する防御 デバイスを追加するだけであることを前提としています。Cisco TrustSec を展開していない場合は、ISE から開始し、ネットワークを設定してから、この手順に戻ります。Cisco TrustSec の説明は、このドキュメントの範囲外です。

手順

ステップ 1 SGT が定義されていること、ISE が SXP トピックをパブリッシュするように正しく設定されていること、および必要な静的マッピングが設定されていることを確認します。

ISE でのセキュリティグループと SXP パブリッシングの設定 （44 ページ）を参照してください。

ステップ 2 SXP トピックをリッスンするように Identity Services Engine オブジェクトを更新します。

ISE を使用して、ユーザ セッション SGT マッピング、SXP を介したスタティック SGT から IP アドレスへのマッピング、またはその両方を取得できます。デフォルトでは、ISE アイデンティティ ソースを設定すると、ユーザ セッション マッピングのみが取得されます。ISE から SXP トピックをリッスンするには、オプションを有効にする必要があります。

a) **[オブジェクト（Objects）]**>**[アイデンティティ ソース（Identity Sources）]**を選択します。
b) ISE オブジェクトを編集します。まだ設定していない場合は、**[+]**>**[Identity Services Engine]**をクリックし、Identity Services Engine の設定を参照してください。
c) [サブスクライブ対象（Subscribe To）] で、[SXP トピック（SXP Topic）] を選択します。

パッシブ認証を使用している場合またはユーザと SGT のマッピングが必要な場合は、[セッションディレクトリのトピック（Session Directory Topic）] が選択されていることも確認してください。

d) [OK] をクリックします。

ステップ 3 変更を展開し、システムが ISE からタグとマッピングをダウンロードするのを待ちます。

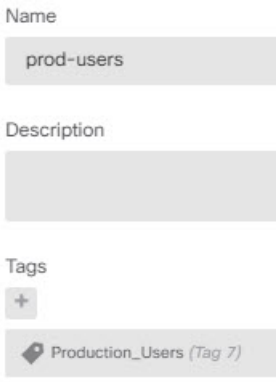
ISE アイデンティティ ソースを設定して変更を展開すると、ISE サーバからセキュリティ グループ タグ（SGT）情報が取得されます。ダウンロードは、変更を展開するまで行われません。

ステップ 4 アクセス制御ルールに必要な SGT グループオブジェクトを作成します。

ISE から取得した情報をアクセス制御ルールで直接使用することはできません。代わりに、ダウンロードした SGT 情報を参照する SGT グループを作成する必要があります。SGT グループは複数の SGT を参照できます。そのため、必要に応じて、関連するタグのコレクションに基づいてポリシーを適用できます。

オブジェクトの数と内容は、作成するアクセス制御ルールによって異なります。次のプロセスを繰り返して、必要なすべてのオブジェクトを作成してください。

a) **[オブジェクト（Objects）]**>**[SGTグループ（SGT Groups）]**を選択します。
b) [+] をクリックして新しいオブジェクトを追加するか、既存のオブジェクトを編集します。
c) 新しいオブジェクトの場合、名前を入力し、任意で説明を入力します。
d) [タグ（Tags）] で、[+] をクリックし、グループに含める必要があるすべてのタグを選択します。



e) [OK] をクリックします。

ステップ 5 SGT グループオブジェクトを使用するアクセス制御ルールを作成します。

たとえば、以下のルールにより、実稼働ユーザから実稼働サーバへのトラフィックが許可されます。ルールはSGTに完全に依存します。送信元/宛先インターフェイスやその他の基準によって制限を受けることはありません。そのため、ルールはさまざまなインターフェイスからのトラフィックに動的に適用され、ISE でセキュリティ グループのメンバーシップを変更するときに適用されます。パケットに送信元 SGT が明示的に含まれていない場合は、パケットの IP アドレスを、ユーザセッション情報または SXP 公開マッピングから取得される、SGT から IP アドレスへのマッピングと比較することによって、送信元/宛先の照合が行われます。

a) **[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** を選択します。
b) [+] をクリックして新しいルールを作成するか、既存のルールを編集します。
c) ルール名を入力し、アクションとして [許可（Allow）] を選択します。
d) [送信元/宛先（Source/Destination）] タブで、**[送信元（Source）]** > **[SGTグループ（SGT Groups）]** の [+] をクリックし、実稼働ユーザ用に作成したオブジェクトを選択します。
e) [送信元/宛先（Source/Destination）] タブで、**[宛先（Destination）]** > **[SGTグループ（SGT Groups）]** の [+] をクリックし、実稼働サーバ用に作成したオブジェクトを選択します。
f) 必要に応じて他のオプションを設定します。たとえば、ロギングを有効にして、侵入ポリシーを適用することができます。
g) [OK] をクリックします。

ステップ 6 設定を展開します。

ISE でのセキュリティグループと SXP パブリッシングの設定

Cisco Identity Services Engine（ISE）では、TrustSec ポリシーとセキュリティ グループ タグ（SGT）を作成するために実行を必要とする設定が多数あります。TrustSecの実装の詳細については、ISEのマニュアルを参照してください。

次の手順では、脅威に対する防御 デバイスがスタティック SGT から IP アドレスへのマッピングをダウンロードして適用できるようにするためにISEで設定する必要があるコア設定のハイライトを示します。これは、アクセス制御ルールでの送信元と宛先 SGT の照合に使用できます。詳細については、ISEのマニュアルを参照してください。

この手順のスクリーンショットは、ISE 2.4に基づいています。これらの機能にアクセスするための正確な手順は後続のリリースで変更される可能性がありますが、概念と要件は同じです。ISE 2.4 以降、特に 2.6 以降が推奨されますが、ISE 2.2 パッチ 1 以降でもこの設定は動作します。

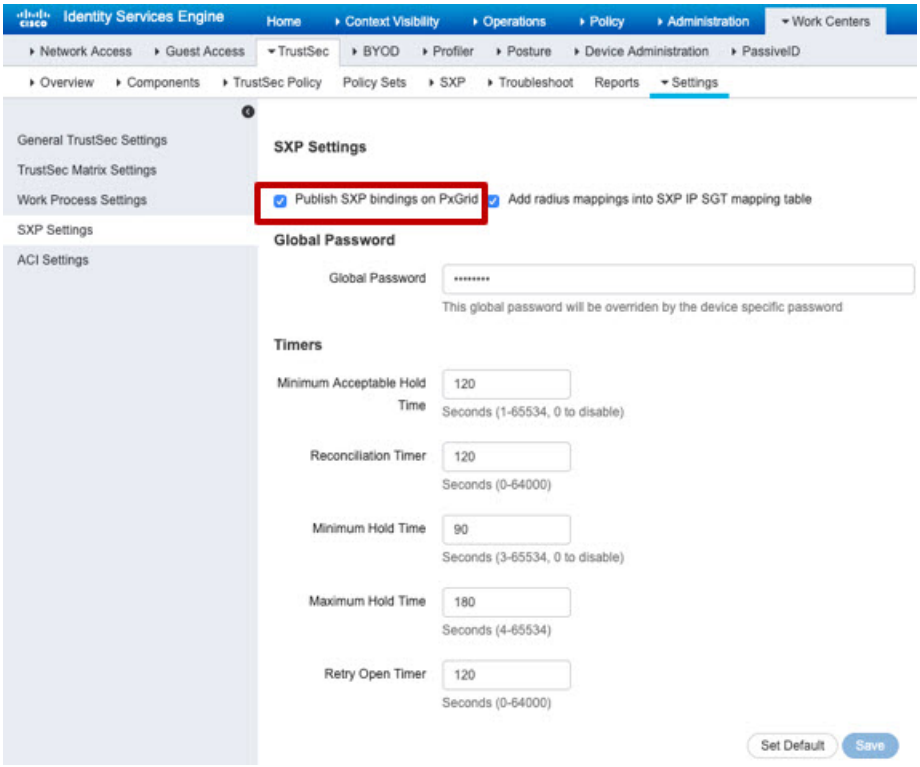
始める前に

SGT から IP アドレスへのスタティックマッピングを公開し、ユーザセッションからと SGT へのマッピングを取得して 脅威に対する防御 デバイスがそれらを受信できるようにするには、ISE Plus ライセンスが必要です。

手順

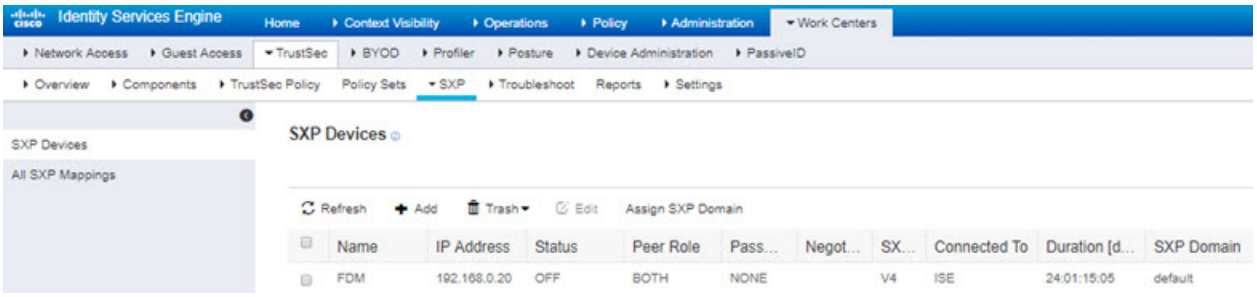
ステップ 1 **[ワークセンター（Work Centers）]** > **[TrustSec]** > **[設定（Settings）]** > **[SXP 設定（SXP Settings）]** を選択し、**[PxGrid で SXP バインディングを公開（Publish SXP Bindings on PxGrid）]** オプションを選択します。

このオプションにより、ISE は SXP を使用して SGT マッピングを送信します。リストから SXP トピックまでを "確認する" には、Threat Defense デバイスに対してこのオプションを選択する必要があります。このオプションは、Threat Defense デバイスが静的 SGT-to-IP アドレスマッピング情報を取得するために選択する必要があります。単に、パケット内で定義された SGT タグ、またはユーザセッションに割り当てられた SGT を使用するのみの場合は、このステップは必要ありません。

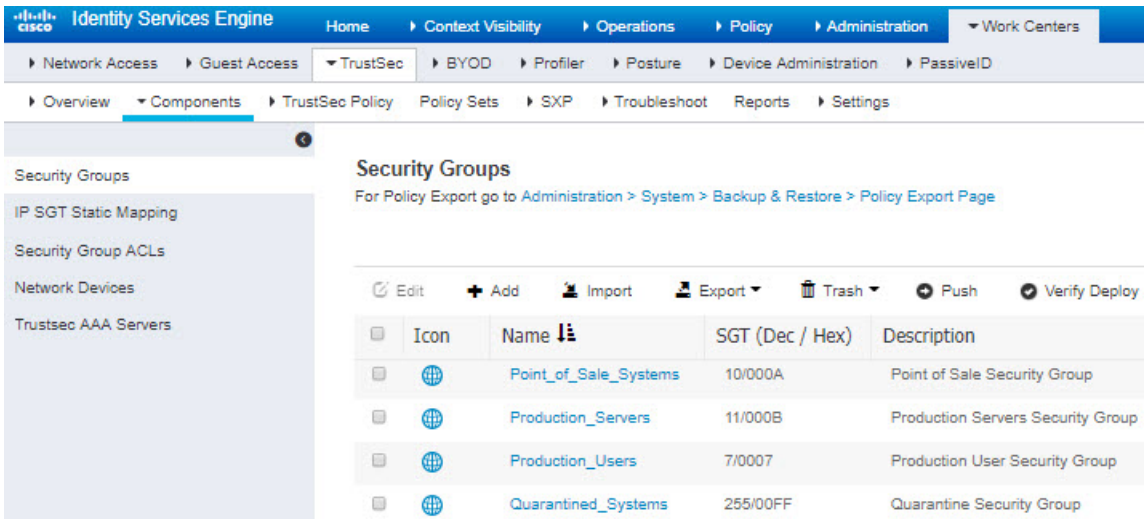


ステップ 2 **[ワークセンター（Work Centers）]** > **[TrustSec]** > **[SXP]** > **[SXPデバイス（SXP Devices）]** を選択し、デバイスを追加します。

これは実際のデバイスである必要はありませんが、脅威に対する防御 デバイスの管理 IP アドレスを使用することもできます。このテーブルには、ISEが静的SGT-to-IPアドレスマッピングをパブリッシュするためのデバイスが1つ以上必要です。単に、パケット内で定義された SGT タグ、またはユーザセッションに割り当てられた SGT を使用するのみの場合は、このステップは必要ありません。

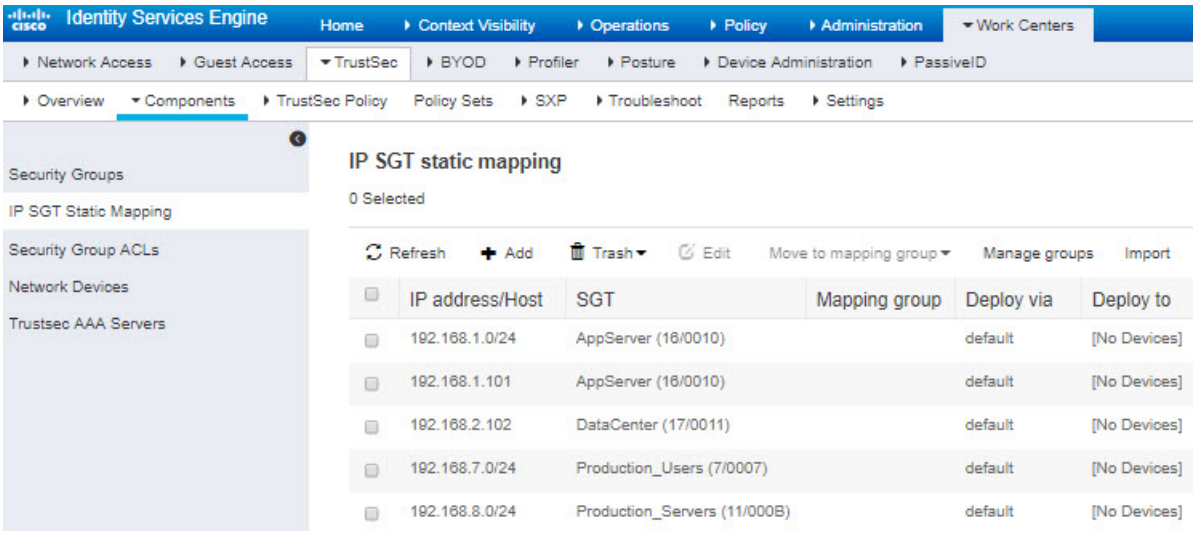


ステップ 3 **[ワークセンター（Work Centers）] > [TrustSec] > [コンポーネント（Components）] > [セキュリティグループ（Security Groups）]** の順に選択し、セキュリティグループタグが定義されていることを確認します。必要に応じて新しいタグを作成します。



ステップ 4 **[ワークセンター（Work Centers）] > [TrustSec] > [コンポーネント（Components）] > [IP SGT スタティックマッピング（IP SGT Static Mapping）]** を選択し、ホストとネットワーク IP アドレスをセキュリティ グループ タグにマッピングします。

単に、パケット内で定義された SGT タグ、またはユーザセッションに割り当てられた SGT を使用するのみの場合は、このステップは必要ありません。


Identity Services Engine
Home
Context Visibility
Operations
Policy
Administration
Work Centers
Network Access
Guest Access
TrustSec
BYOD
Profiler
Posture
Device Administration
PassiveID
Overview
Components
TrustSec Policy
Policy Sets
SXP
Troubleshoot
Reports
Settings
Security Groups
IP SGT Static Mapping
Security Group ACLs
Network Devices
Trustsec AAA Servers
IP SGT static mapping
0 Selected
Refresh
Add
Trash
Edit
Move to mapping group
Manage groups
Import
IP address/Host
SGT
Mapping group
Deploy via
Deploy to
192.168.1.0/24
AppServer (16/0010)
default
[No Devices]
192.168.1.101
AppServer (16/0010)
default
[No Devices]
192.168.2.102
DataCenter (17/0011)
default
[No Devices]
192.168.7.0/24
Production_Users (7/0007)
default
[No Devices]
192.168.8.0/24
Production_Servers (11/000B)
default
[No Devices]

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。