Firepower Management Center 6.3 v1.1 – インスタント デモ

最終更新日：2019 年 2 月 1 日

このデモンストレーションについて

この事前設定済みデモンストレーションのガイドには、次の内容が含まれています。

要件

次の表に、このデモンストレーションの要件の概要を示します。

表 1. 要件

必須	オプション
● ラップトップ	● Cisco AnyConnect

このソリューションについて

FirePOWER システムは、脅威中心型の次世代セキュリティ システムです。ファイアウォール、IPS、および高度なマルウェア防御を利用して、高度な脅威に対する可視性を強化するとともに、非常に強力なセキュリティ制御を可能にします。FirePOWER では、ネットワーク環境、ネットワーク上のホストのタイプ、エンドポイントやサーバで使用されているアプリケーションなどを把握できるため、推測に頼ってポリシーを適用する必要がなくなり、セキュリティ デバイスやセキュリティ サービスの調整にかかる労力が軽減されます。それによってシステムの正確性が向上するため、ネットワークまたはセキュリティ関連のスタッフは、注意を要する問題に意識を集中させることができます。また、ユーザはレトロスペクティブ機能により、脅威やマルウェアがどのようにネットワークに侵入したかを把握し、悪意のあるファイルの移動を追跡できます。

このソリューションの主なコンポーネントは次のとおりです。

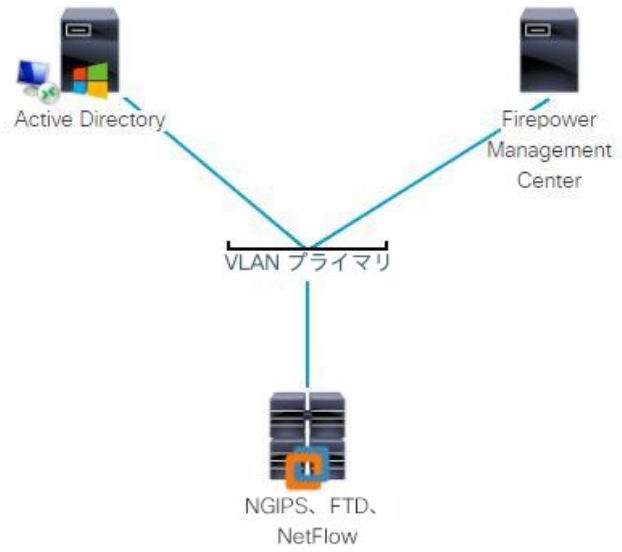
Firepower Management Center（FMC）：FMC は、専用のハードウェア アプライアンス上で、または VMware 内の仮想マシンとして実行される、一元管理およびレポート アプライアンスです。

Cisco FirePOWER：Cisco ASA 適応型セキュリティ アプライアンスのサービスとして実行されるか、専用の FirePOWER アプライアンスとして、または VMware、Amazon Web Service、KVM で仮想アプライアンスとして実行されます。さらに、サポート対象のハードウェアまたは仮想アプライアンスで動作する、Firepower Threat Defense アプライアンスとして実行されます。

トポロジ

このコンテンツには、スクリプト形式のシナリオと、ソリューションの機能を実例で示すために事前設定された管理ユーザとコンポーネントが含まれています。コンポーネントのほとんどは、管理ユーザ アカウントを使用して任意の設定が可能です。コンポーネントへのアクセスに使用する IP アドレスとユーザ アカウント資格情報は、アクティブ セッションの [トポロジ（Topology）] メニューのコンポーネント アイコンをクリックして確認するか、それらを必要とするシナリオ内の手順で確認できます。

図 1. dCloud トポロジ



はじめに

プレゼンテーションの前に

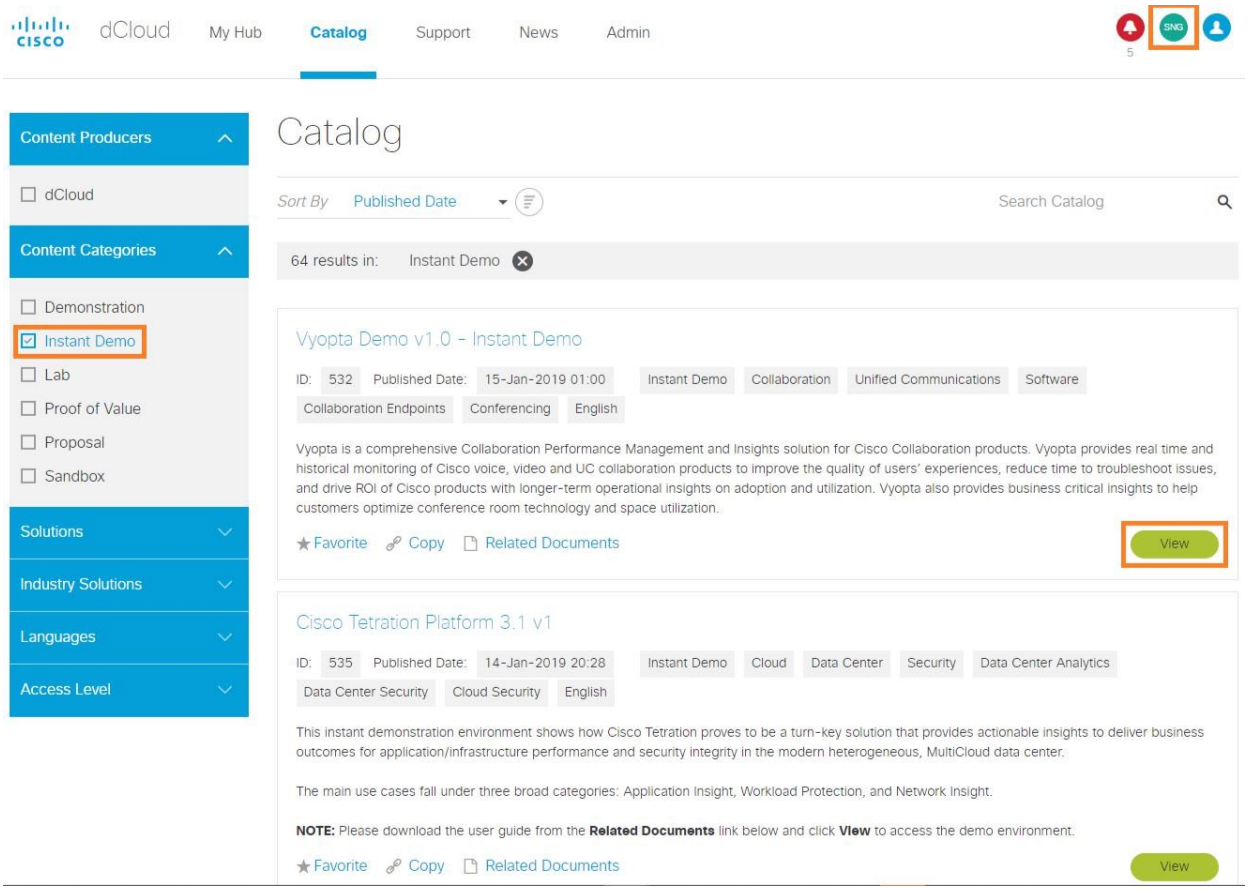
Cisco dCloud では、実際の対象者の前でプレゼンテーションを行う前に、アクティブなセッションを使用して、このドキュメントのタスクを実施しておくことを強く推奨します。そうすることで、ドキュメントとコンテンツの構成に慣れることができます。

場合によっては、環境を元の構成にリセットするため、このガイドのシナリオを完了した後に新しいセッションをスケジュールする必要があります。

プレゼンテーションを成功させるには入念な準備が不可欠です。

次の手順に従ってコンテンツのセッションをスケジュールし、プレゼンテーション環境を設定します。

1. dCloud セッションを開始します。[手順を見る] [英語]
2. ページ右上に表示されているように、最寄りのデータセンターを選択します。[カタログ（Catalog）] をクリックして、サイド バーから [インスタントデモ（Instant Demo）] を選択します。これで、すべての dCloud インスタント デモが一覧表示されます。
3. 該当する [表示（View）] ボタンをクリックします。



シナリオ 1.　Context Explorer の概要

Cisco FirePOWER は、非常に強力なダッシュボードを備えています。Context Explorer は特殊なハイレベル ダッシュボードであり、ネットワークに関する複数のビューを参照できます。これらのビューでは、共通の時間枠とフィルタを適用できます。これらのビューはすべて Context Explorer 内にパネルとして組み込まれています。

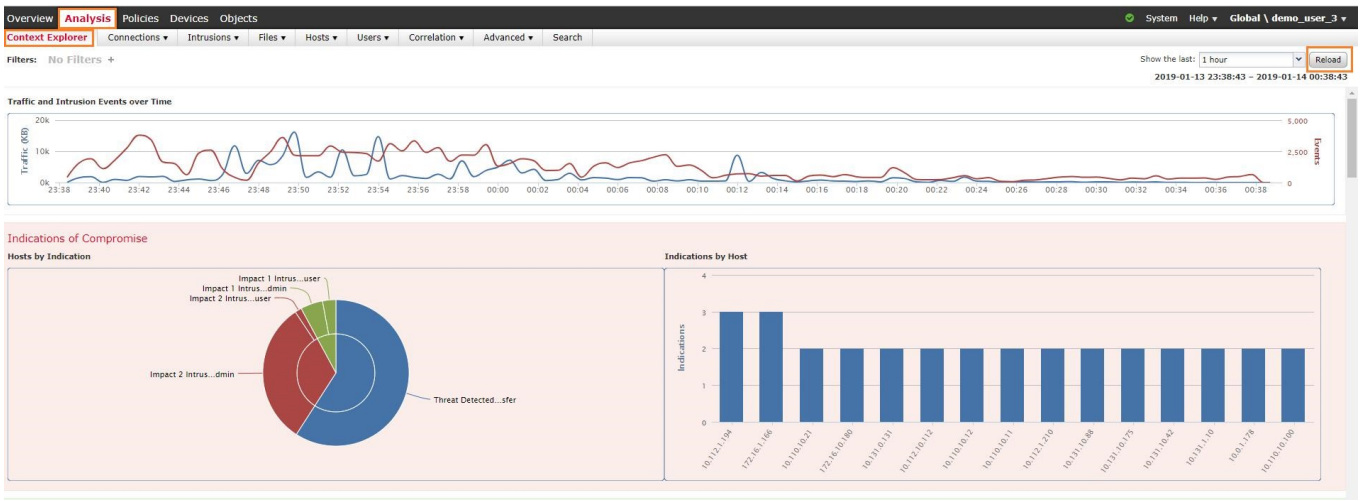
- トラフィックおよび侵入イベントの経時変化
- 侵害の兆候（Indications of Compromise）
- ネットワーク情報（オペレーティング システム情報と、IP アドレスとユーザ名ごとの上位送信者を含む）
- アプリケーション プロトコル情報（Web アプリケーションとクライアント アプリケーションを含む）
- セキュリティ インテリジェンス
- 侵入情報
- ファイル情報（マルウェアを含む）
- 位置情報
- URL 情報

フィルタが適用されるか、時間範囲が変更されると、目的の情報に合わせて各パネルのデータが変化します。用途としては、たとえば特定のユーザのネットワーク アクセスに関するトラブルシューティングを行う場合が挙げられます。ユーザ名はフィルタとして適用でき、また上記のすべてのデータをフィルタリングすることで、該当するユーザ名のネットワーク トラフィックに合致するデータだけがパネルに表示されます。

手順

1. ログインすると、サマリー ダッシュボードが表示されます。メニュー バーの [分析（Analysis）] をクリックすると、Context Explorer が表示されます。

注：何もデータが表示されない場合は、画面右上の [リロード（Reload）] をクリックします。



2. ページ内を上下にスクロールして内容を確認します。個々のパネルには次のような特徴があります。

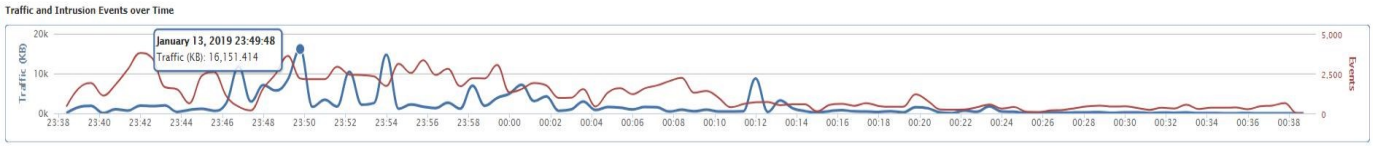
   色分けされている

   グラフとチャートが含まれている

   インタラクティブであり、カーソルを置くと詳細な情報が表示される

   フィルタを追加または削除できる

3. 次の図に、[トラフィックおよび侵入イベントの経時変化（Traffic and Intrusion Events over Time）] グラフを示します。線の上にカーソルを置くと、その時点のイベント数が表示されることを確認できます。

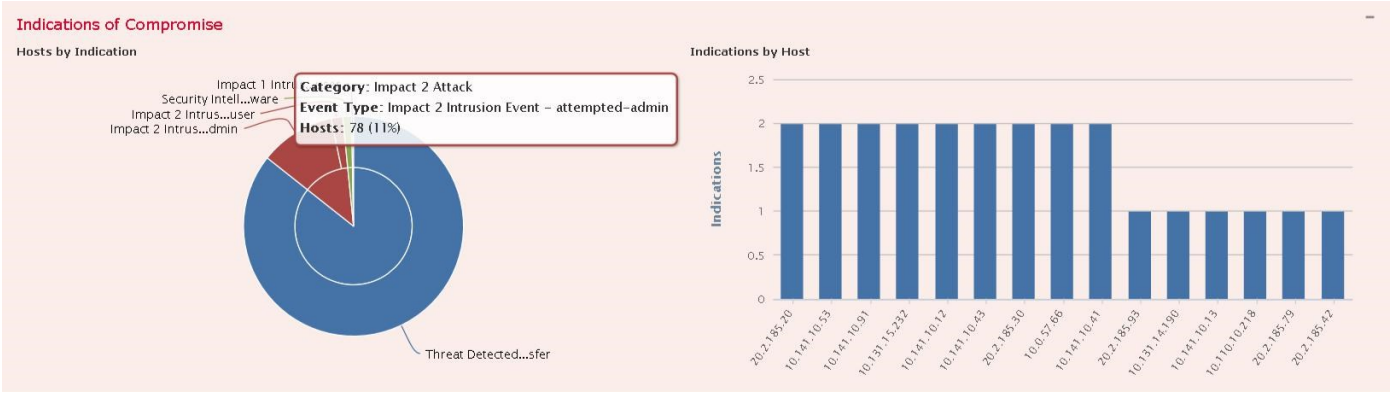


4. 赤色の [侵害の痕跡（Indications of Compromise）] パネルまで下にスクロールすると、次の内容が表示されます。

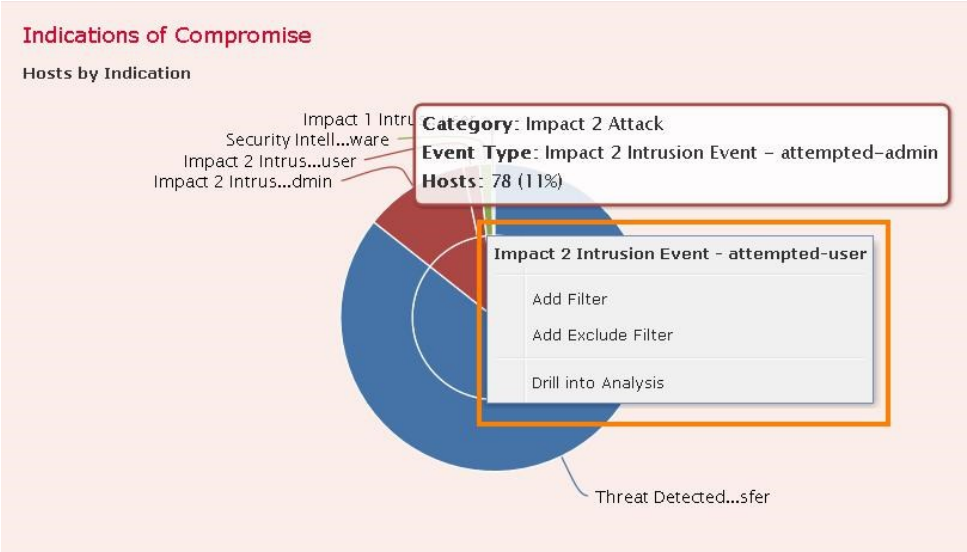
   どのホストが侵害されやすい動作を示したか

5. 現実のネットワークでは、これほど多くの IOC は表示されないと思われますが、ここではホストが侵害されるさまざまな経緯を示すために表示しています。

注：IOC の上にカーソルを置くと、この IOC が確認されているホスト数が表示されます。



6. グラフのセクションを見てください。ここでは IOC にフィルタを適用するか、IOC をトリガーしたイベントにドリルダウンすることができます。この方法ですべてのパネルを操作できます。

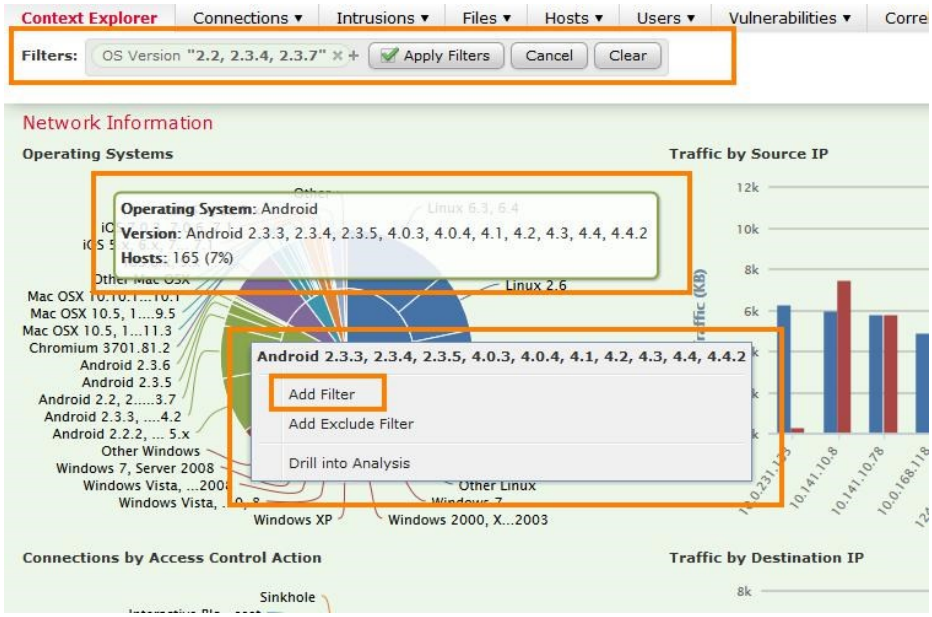


7. 次に [ネットワーク情報（Network Information）] パネルまで下にスクロールします。

   このパネルには、上位のトラフィック送信元と宛先に加えて、ネットワーク上で稼働するデバイスのタイプに関する情報が表示されます。IP アドレスとユーザ情報も簡単に確認できます。

   たとえば、学区全体の Android タブレット使用者に関する情報が必要な場合は、[オペレーティングシステム（Operating Systems）] のグラフ内の項目をクリックして、特定の **Android** デバイスをフィルタに追加できます。

8. [フィルタを適用（Apply Filter）] をクリックすると、グラフに Android に関する情報だけが表示されます。



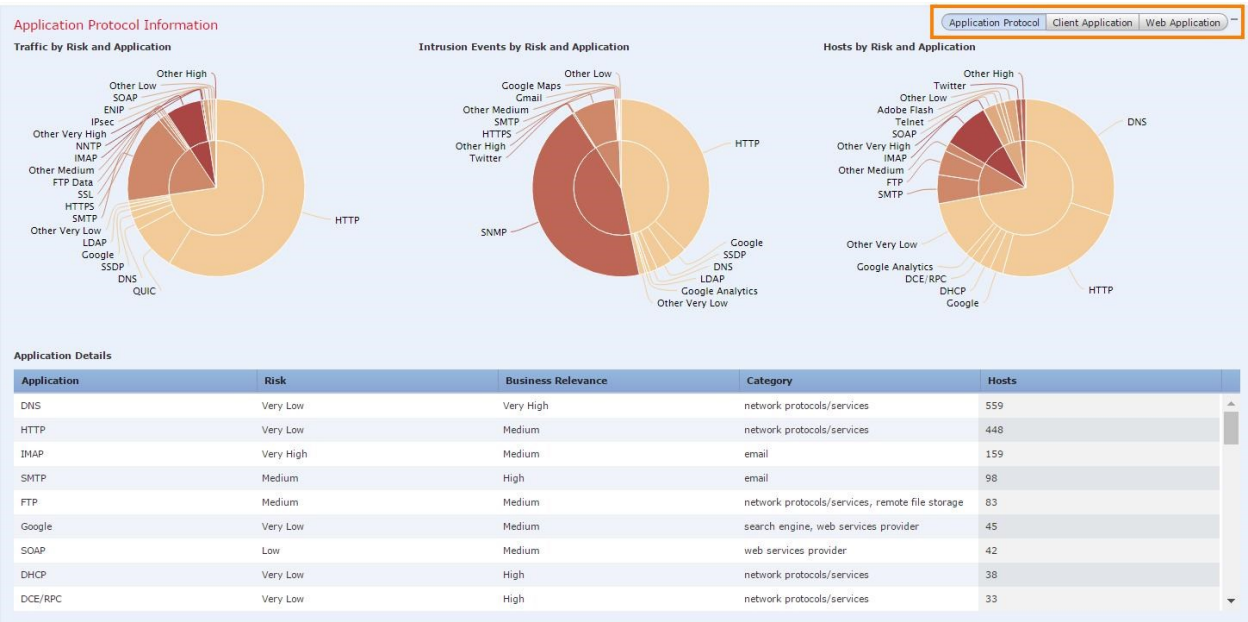
9. [アプリケーションプロトコル情報（Applications Protocol Information）] パネルまで下にスクロールします。画面右上にカーソルを置くと、3 つのパネル オプションが表示されます。

   アプリケーション プロトコル

   クライアント アプリケーション

   Web アプリケーション

デフォルトは [アプリケーションプロトコル（Application Protocol）] です。

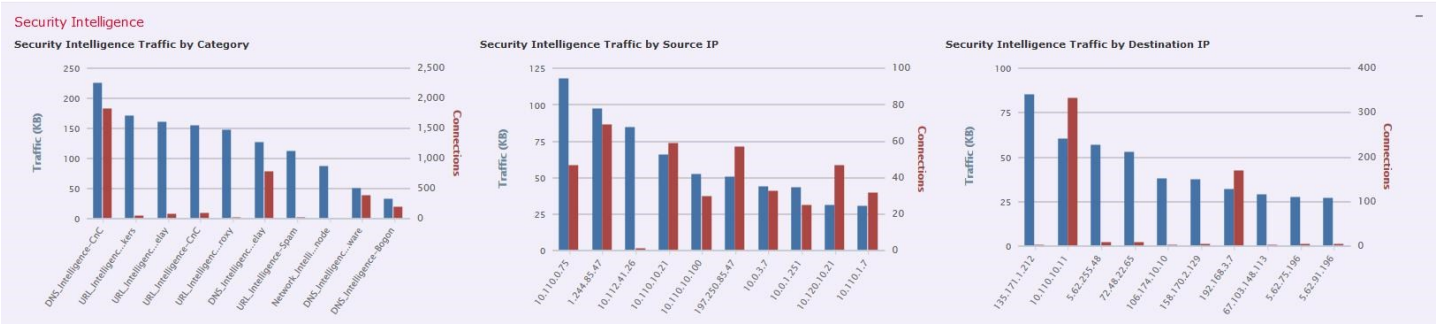


10. [セキュリティインテリジェンス（Security Intelligence）] 情報パネルまでスクロールします。

    セキュリティ インテリジェンス機能の仕組みを理解しておくことが重要です。セキュリティ アプライアンスをリストまたはフィードに登録すると、悪意のあるデバイスの IP アドレス情報を取得できます。この情報を利用して、該当する領域と、その領域で行われるトラフィックについて報告し、またブロックすることが可能になります。

    表示されている情報を見ると、アプライアンスによって、[攻撃者（Attackers）]（インターネット上の他のホストを活発に攻撃していた IP アドレス）や [CnC]（ボットネットのコマンド アンド コントロール アクティビティに参加している IP アドレス）などのカテゴリが、どのようにブロックされているかがわかります。

    これらのフィードを利用することで、セキュリティの有効性が大幅に向上します。Cisco FirePOWER では、シスコやサードパーティが提供するフィード、または自分で作成したフィードなどを含め、制限なくフィードに登録できます。



11. [侵入情報（Intrusion Information）] パネルまで下にスクロールします。このパネルのチャートとグラフでは、侵入防御エンジンによってトリガーされたイベントが示されます。

    FirePOWER IPS の 1 つの特徴として、**影響レベル**が挙げられます。これはパネルの左上に表示されます。

    侵入イベントの分析を容易にするために、また IPS ポリシーを動的に調整するために、FirePOWER では使用中のネットワークとアプリケーションに関する情報を利用します。FirePOWER では他の IPS システムのような雑多な情報が表示されないため、特に注意が必要なイベントに意識を向けることが可能になります。

影響レベルについて次に説明します。

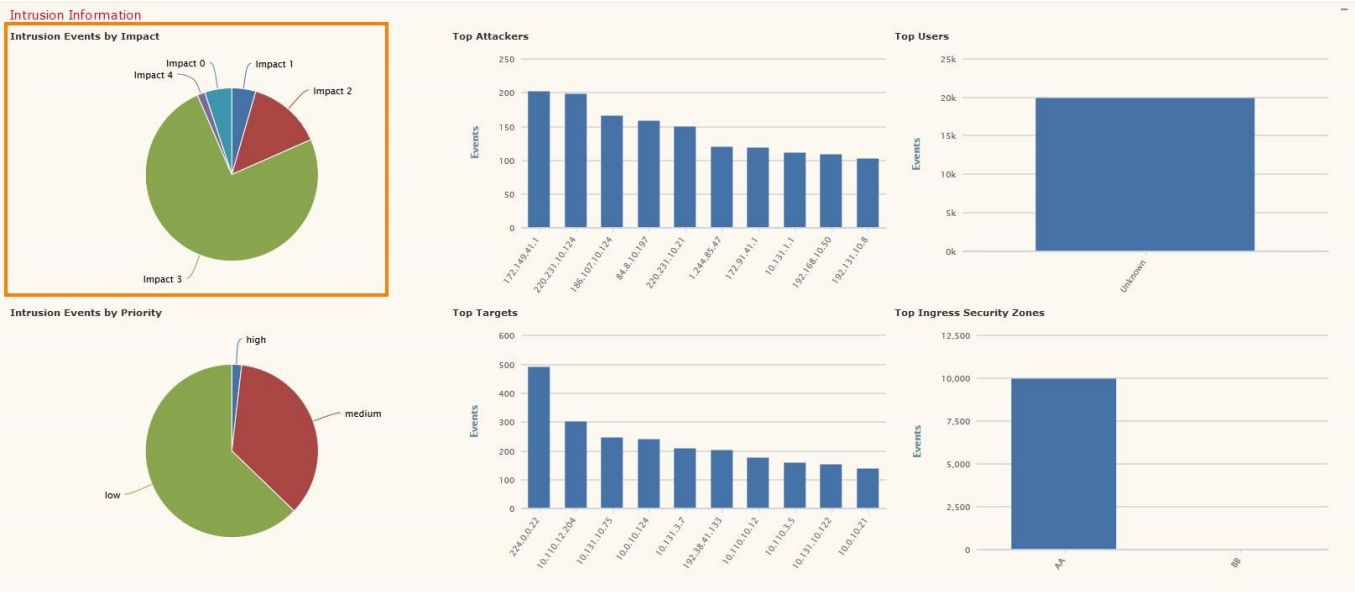
影響レベル 1：オペレーティング システムとアプリケーションを適切な組み合わせで実行しているネットワーク上のホストが、攻撃の影響を受けました。このレベルは攻撃に対して脆弱であると考えられ、注目すべき重要なイベントとなります。

影響レベル 2：ネットワーク上のホストが攻撃の影響を受けました。適切なサービスとアプリケーションを実行していて、攻撃に対して脆弱であるようには見えません。確認しておきたいイベントではありますが、通常は重要ではありません。

影響レベル 3：ネットワーク上のホストが攻撃の影響を受けました。攻撃の対象となったサービスまたはアプリケーションは実行していないようです。この場合、ホストは脆弱ではありません。

影響レベル 4：ネットワーク上のホストが攻撃の影響を受けましたが、ホストが実際にネットワーク上に存在しないか、ホストが新たに追加されたものであるかのどちらかです。脆弱性に関する判断はまだ行われていません。

影響レベル 0：送信元、宛先、IP アドレスのいずれもネットワーク上に存在しません。これらのイベントは調査が必要です。これは FirePOWER システムの設定ミスや、不正なネットワーク トラフィックなどが原因になっています。



12. [ファイル情報（File Information）] パネルまでスクロールします。このパネルでは、ファイル ポリシーが適用された、FirePOWER アプライアンス全体のファイル コピーを確認できます。すべてのファイルを表示するか、FMC 管理者が定義した一部のファイルを表示できます。次のような情報が表示されます。

    ファイルのタイプ

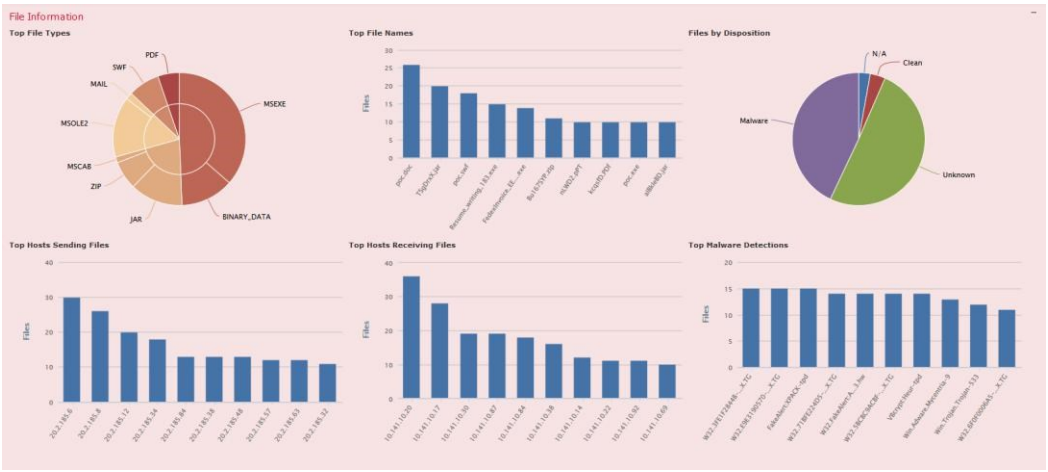
    上位のファイル名

ファイルの送信元または宛先になっている上位のホスト

判定結果別ファイル

マルウェア検出上位件数

高度なマルウェア防御（AMP）では、（他の方法に加えて）構造と動作によってファイルを分析し、どのファイルがホストに損害を与えているかを判定して、悪意のあるファイルがアプライアンスを通過しないようにブロックできます。



13. 下部の 2 つのパネルまでスクロールすると、位置情報と URL 情報を確認できます。

まとめ

Firepower Management Center Context Explorer は、ネットワーク トラフィック、アプリケーション、脅威をすばやく簡単に、さまざまな角度から可視化できる、非常に強力なツールです。

シナリオ 2.　サマリー ダッシュボードの概要

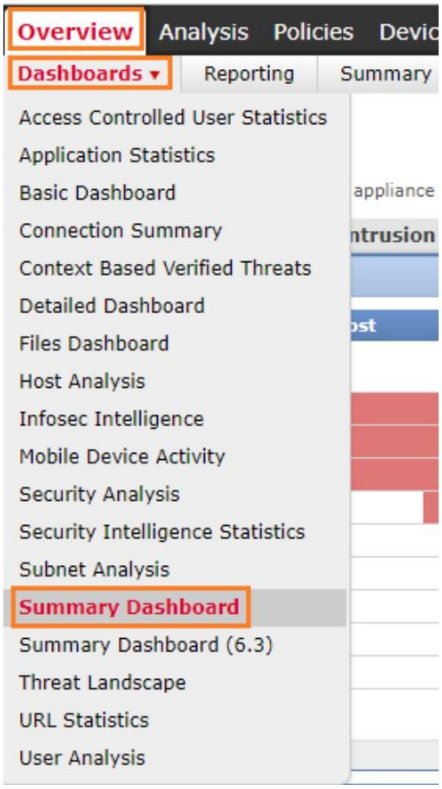
Cisco FirePOWER には、多数の詳細なダッシュボードがあります。これらはすべて高度なカスタマイズが可能で、システムにさらにダッシュボードを追加することができます。それらによって、確認したいネットワーク領域を一目で確認することが可能です。FMC はロール ベースのアクセスを適用できるマルチユーザ システムであるため、ログインした各ユーザは、必要な情報が表示されるダッシュボードを選択して、ログイン時のランディング ページにすることができます。

サマリー ダッシュボードは、ネットワークとアプリケーションの全体像の把握や、検出された脅威の確認ができる最適な場所になります。このダッシュボードは新規ユーザのデフォルトのランディング ページになっています。

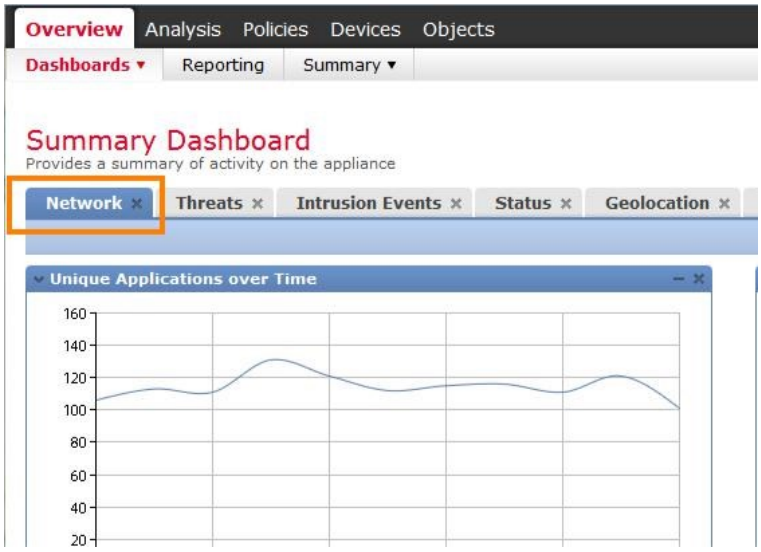
手順

1. メニュー バーの [概要（Overview）] をクリックし、[ダッシュボード（Dashboards）] > [サマリーダッシュボード（Summary Dashboard）] を選択します。

注：ログイン後のデモでは、デフォルトで [サマリーダッシュボード（Summary Dashboard）] ページに移動します。

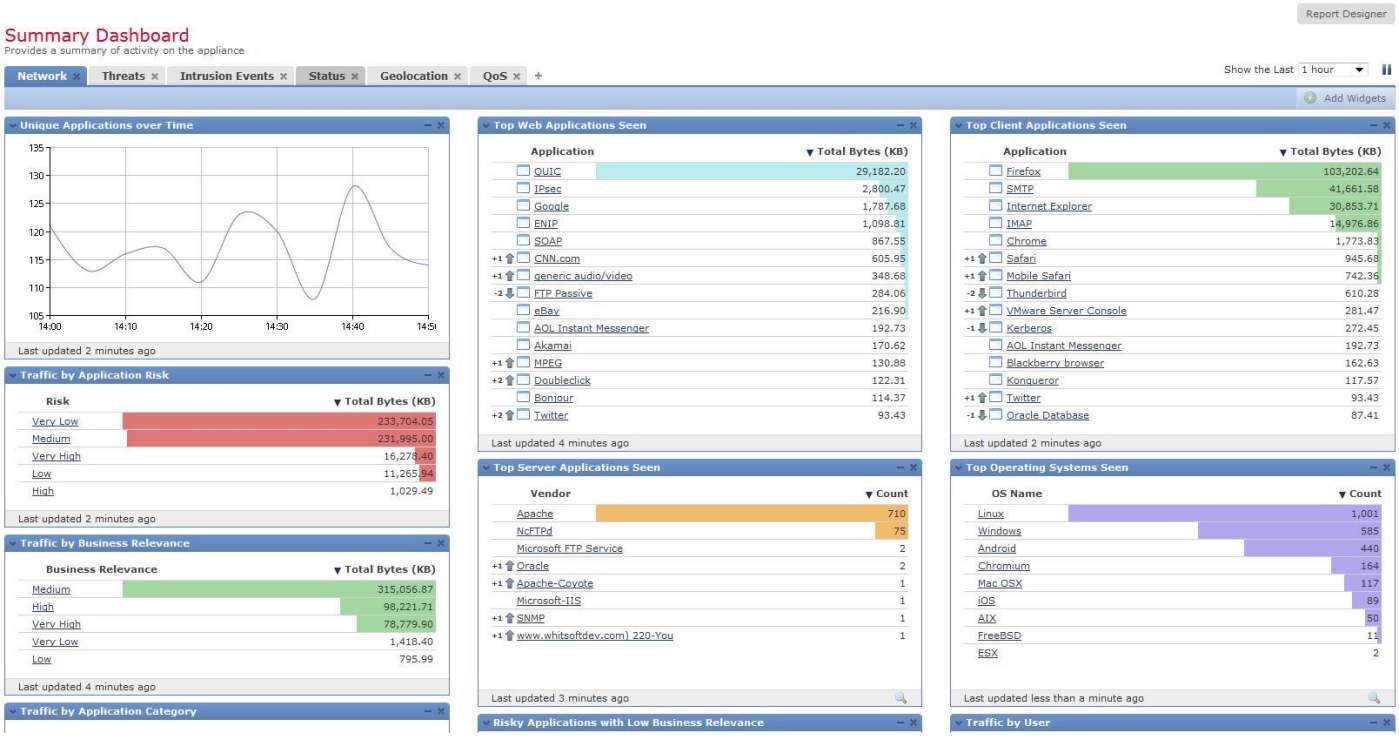


2. 画面がロードされたら、[ネットワーク（Network）] タブを選択します。



3. このダッシュボードでは、ほぼすべてのタイプの情報が含まれたウィジェットの一覧が表示されるため、すべてを一目で確認できます。ダッシュボードとウィジェットは、それぞれ自由にカスタマイズ可能です。各ウィジェットでは、特定のイベント情報を詳細に確認することもできます。

   たとえば、使用率の高いユーザまたはアプリケーションのトラフィックを確認する場合は、ユーザ名またはアプリケーションをクリックするだけで詳細が表示されます。

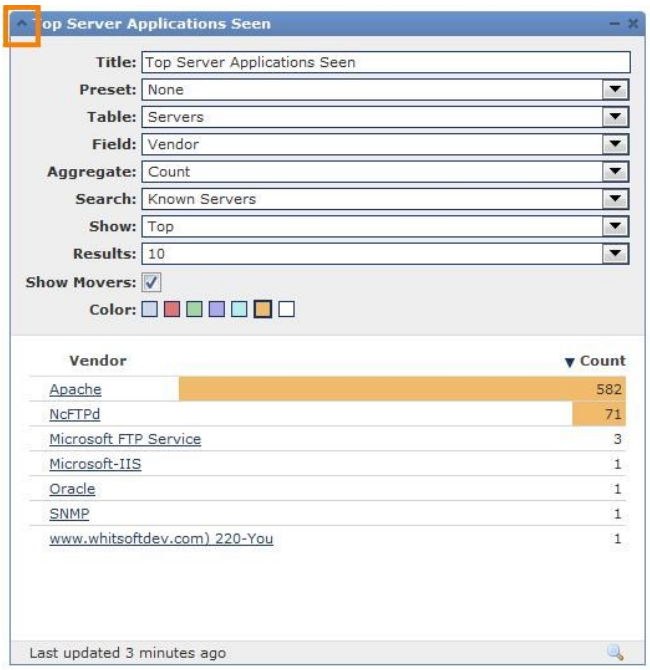


4. [上位のサーバアプリケーション（Top Server Application Seen）] ウィジェット左上の小さな矢印をクリックします。

   これをクリックすると、ウィジェットに表示させる結果の数、グラフの色、使用するデータセットなどのオプションを設定できます。

注：このアカウントを使用している他のデモに影響するため、このデモではデータセットは変更しないでください。

画面上の目的の場所にウィジェットをドラッグ アンド ドロップすることで、各ダッシュボードのレイアウトを変更できます。



5. [脅威（Threats）] タブをクリックします。このタブは悪意のあるトラフィックとファイルに特化していて、どのシステムが侵害されている可能性があるかを確認できるため、非常に有用です。

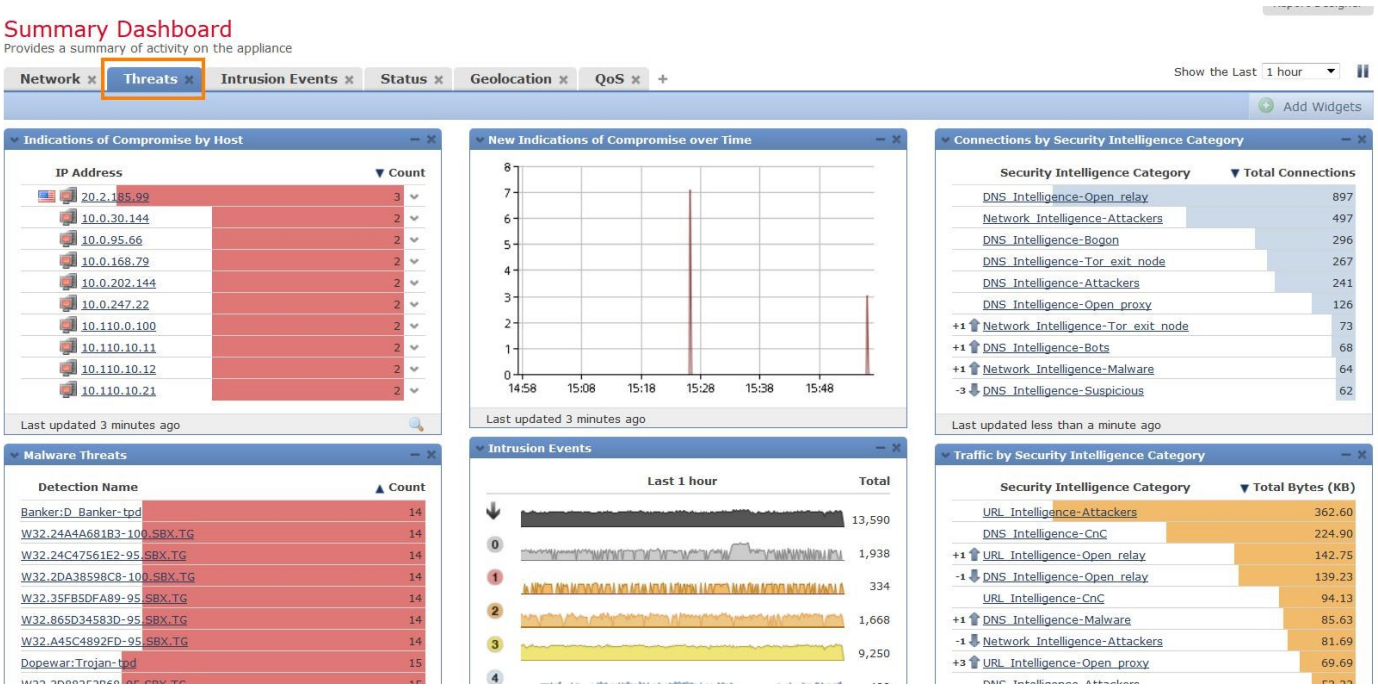
[脅威（Threats）] タブには次の情報が表示されます。

[マルウェアの脅威（Malware Threats）]：高度なマルウェア防御によって検出された、セキュリティ アプライアンスまたはエンドポイント エージェントで実行されているマルウェア ファイルを示します。

[影響レベルごとの侵入イベント（Intrusion Events, by Impact Level）]：通常は許可されるトラフィック タイプで、Snort によって検出された攻撃を示します。

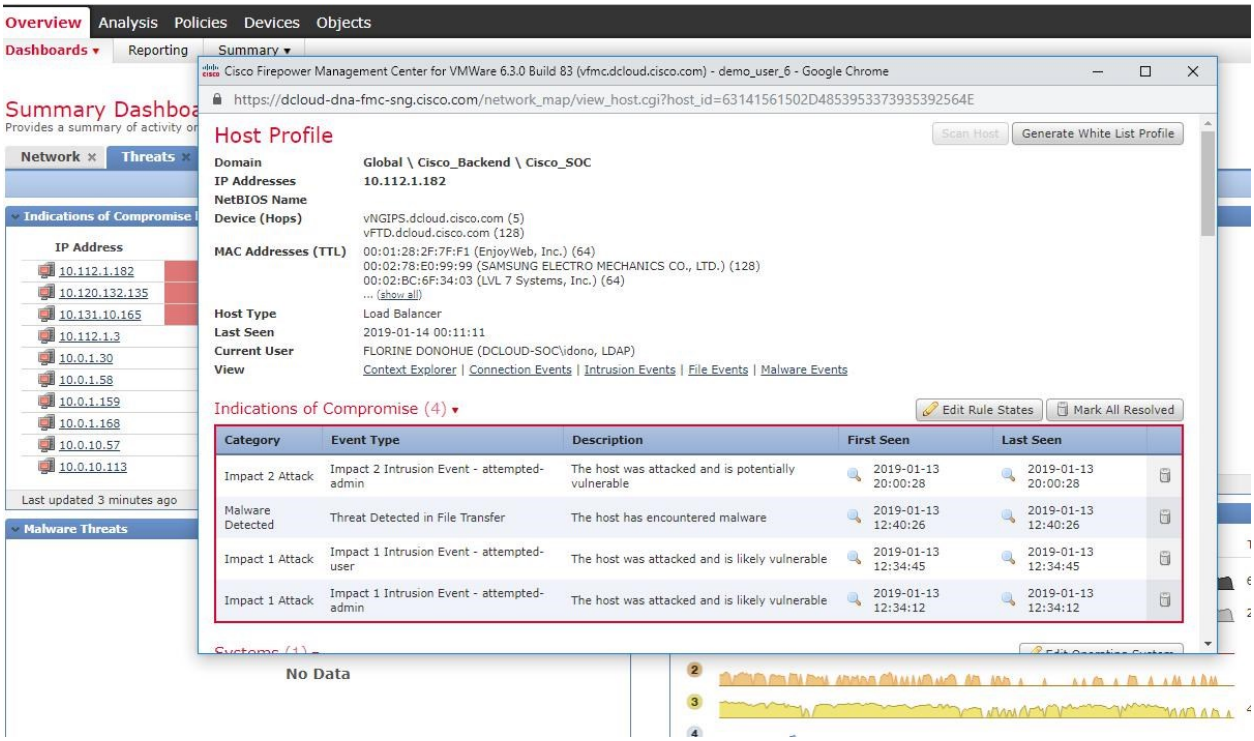
[セキュリティインテリジェンスカテゴリごとの接続とトラフィック（Connections and Traffic by Security Intelligence Category）]：前のシナリオで示したように、送信元または宛先の IP アドレスに基づいて、ネットワーク上で検出された悪意のあるトラフィックのカテゴリを示します。

[侵害の痕跡（Indications of Compromise）]：侵害の原因になった、アクティビティに関与したホストを示します。多くの場合、マルウェア ファイルにアクセスする動作が示されます。



6. [脅威（Threats）] タブでは、侵害の痕跡（IoC）を示すホストに関する詳細な情報を簡単に確認できます。いずれかの IP アドレスの横にある赤色のホスト アイコンをクリックすると、ホスト プロファイルが表示されます。

7. それによって新しいウィンドウが開き、デバイスに現在ログインしているユーザや、ホストに関連する IoC などの関連情報が表示されます。



8. さらに下にスクロールすると、オペレーティング システム情報、使用されているアプリケーション、そのデバイスにログインしたことがあるユーザの履歴などを確認できます。

まとめ

Cisco FirePOWER には、使いやすい強力なダッシュボードが用意されています。それによってネットワーク管理者やセキュリティ管理者は、ネットワーク上のアプリケーションや脅威の状況を完全に把握できます。ダッシュボードに表示される情報は、ポリシー エンジンでネットワーク ポリシーの適用に使用できます。これにより、他社製品を凌ぐ最も強力かつ正確な次世代セキュリティ システムが実現します。

シナリオ 3.　次世代ファイアウォール ポリシーの構築

最初の 2 つのシナリオでは、可視性とレポートに注目しました。このシナリオでは、次世代ポリシーの適用について説明します。従来のセキュリティ アプライアンスでは、IP アドレス、プロトコル、およびポートに基づいてトラフィックを適用していました。次世代セキュリティ アプリケーションでは、それらの機能に加えて、コンテキスト情報が追加されます。シスコの次世代セキュリティ アプライアンスでは、次のような多数の属性に基づいたポリシーがサポートされています。

- 位置情報
- VLAN
- Active Directory 内のユーザ名またはグループ
- アプリケーションまたはクライアント アプリケーション
- URL のカテゴリとレピュテーション
- セキュリティ グループ タグ
- ネットワーク デバイス タイプ

トラフィックの許可とブロックなどの従来型の制御に加えて、シスコの次世代セキュリティ ポリシーでは、微調整された IPS ポリシー、SSL 復号、高度なマルウェア防御ポリシーを、アクセス制御を通じて適用できます。

手順

1. 最上部のバーで [ポリシー（Policies）] をクリックします。デフォルトのポリシー タイプである [アクセスコントロール（Access Control）] ポリシーが表示されます。
2. [サンプル企業の複雑な NGFW AC ポリシー（Sample Corporate Complex NGFW AC Policy）] という、入力が完了した事前定義済みのポリシーをリストから選択します。

3. このサンプル ルールでは、次のようなタイプの制御を使用できます。

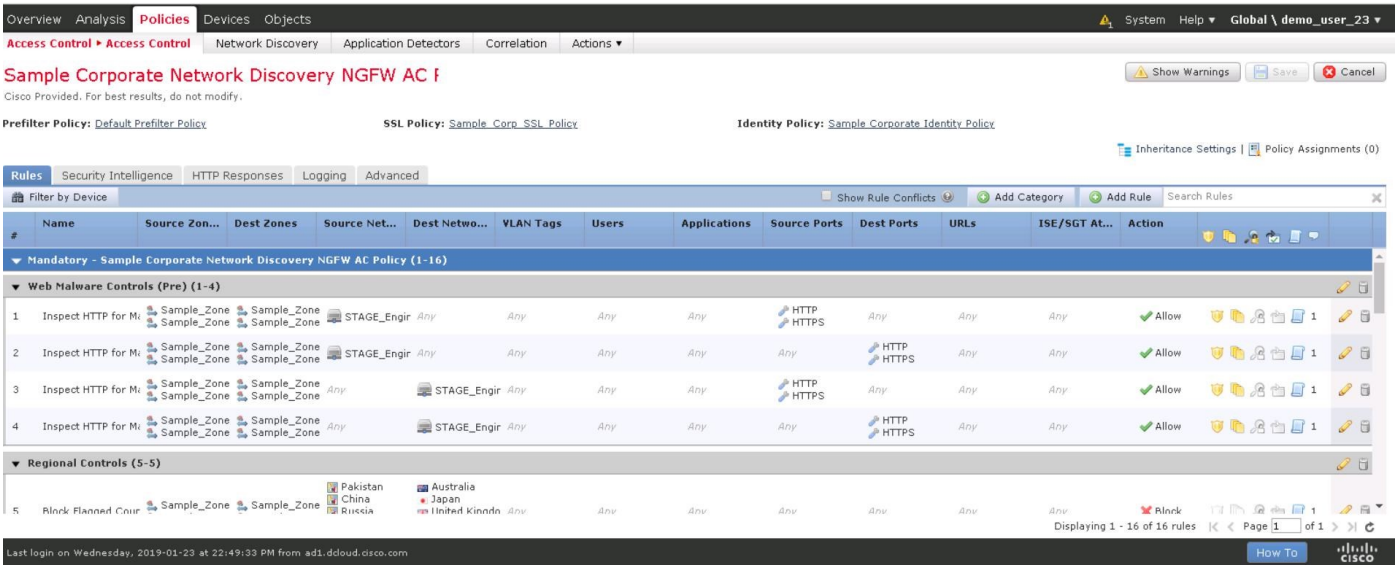
    ポートおよびプロトコル ベースのルール

    アプリケーション専用ルール

    ユーザ ベース ルール（ルール 6 または 27 を参照）

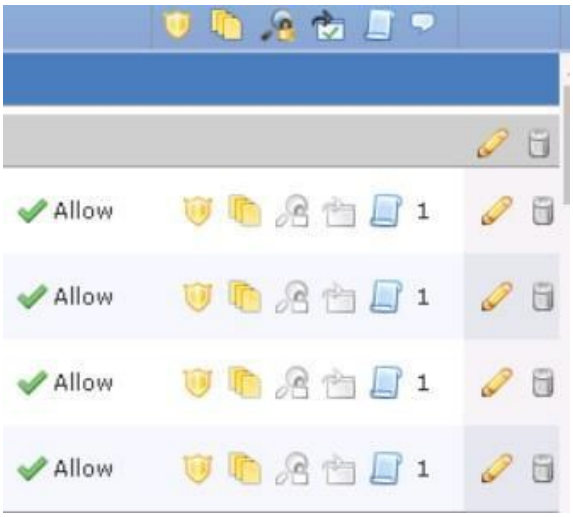
    URL カテゴリのフィルタリング ルール

    位置情報ルール



4. 画面の右側を見てください。特定のルールがトラフィックを許可するかブロックするかをすばやく確認できます。

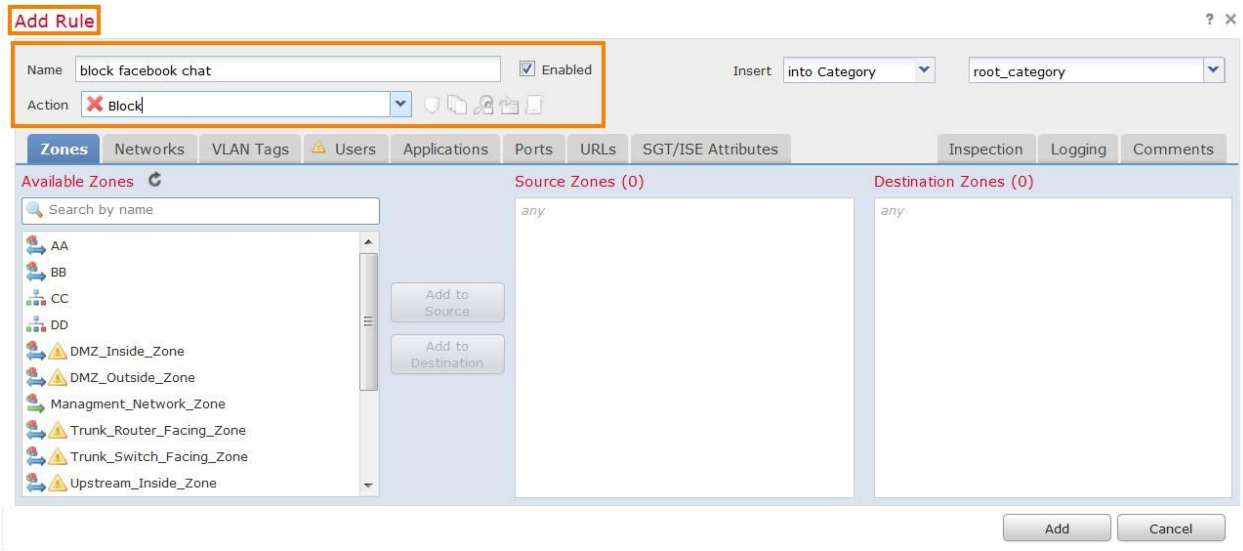
    各ルールに対して有効になっている凡例で、**黄色い盾アイコン** は侵入ポリシーを、**紙の束アイコン** はファイル ポリシーを、**鍵の付いた虫めがねアイコン** は SafeSearch ポリシーを、**緑色のチェック マークの付いた画面アイコン** は YouTube EDU ポリシーを、**紙のスクロール アイコン** はルールのログが有効になっていることを、末尾の数字はルールにコメントが追加されたことを示しています。



新しい機能の **SafeSearch** と **YouTube EDU** アクセス コントロール ポリシーの参照については、ルール番号 15 および 16 を参照してください。正式なドキュメントを参照するには、こちらをクリックしてください。

5. このポリシーを確認したら、画面右側の [ルールの追加（Add Rule）] をクリックしてルールを追加します。

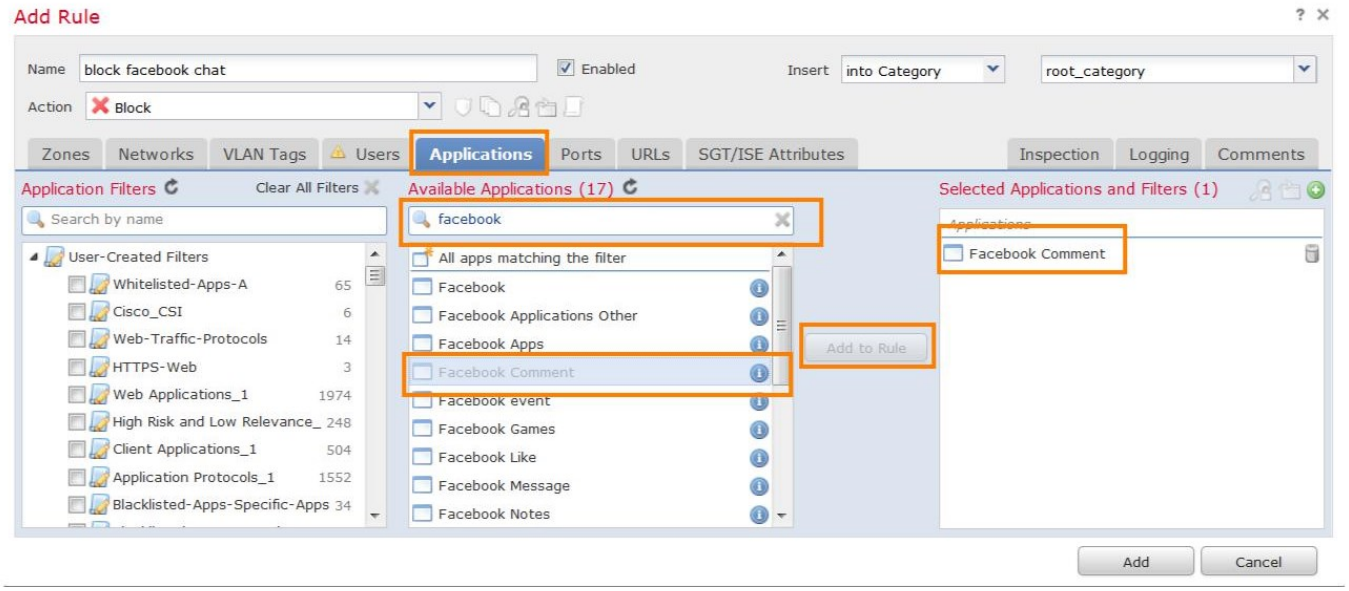
6. このルールに「**block Facebook chat（Facebook チャットをブロック）**」という名前を付け、アクションを [ブロック（Block）] に設定します。



7. [アプリケーション（Applications）] タブを選択して、新しいルールをアプリケーション ルールに指定します。

8. [使用可能なアプリケーション（Available Applications）] フィールドに「**Facebook**」と入力します。これによって結果にフィルタが適用され、Facebook アプリケーションのタイプだけが表示されるようになります。

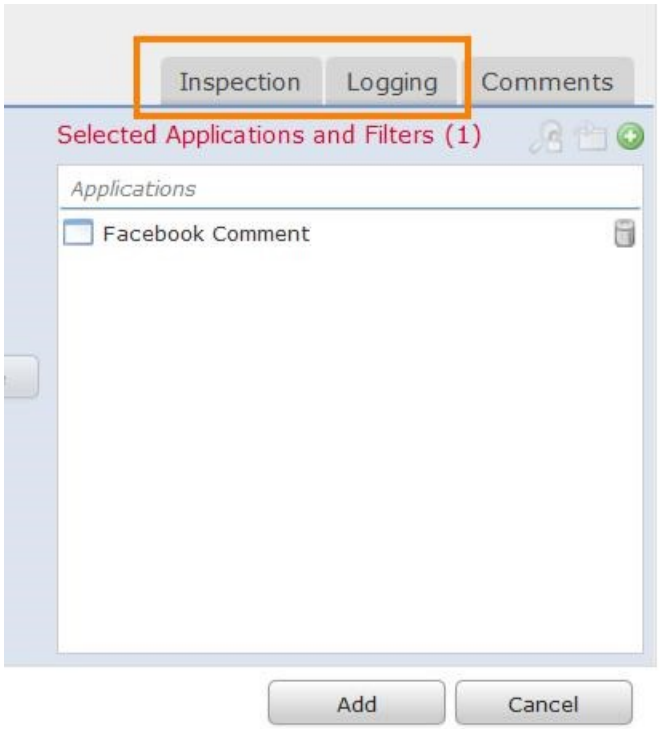
9. [Facebook のコメント（Facebook Comment）] を選択し、[ルールに追加（Add to Rule）] をクリックします。



10. これによって、このポリシーが適用されているアプリケーションで Facebook のコメントをブロックするルールが作成されます。

    必要に応じて、ウィンドウ右側の [検査（Inspection）] タブと [ロギング（Logging）] タブを使用して、検査機能を追加し、ルールが実行された場合にログに記録されるようにすることができます。

    ブロックするトラフィックを検査する意味はありません。ただし、新しいルールで許可する場合は、トラフィックのマルウェアを検査することができます。



11. 次世代ファイアウォール ルールの作成は、このように簡単に行うことがわかったので、[キャンセル（Cancel）] をクリックしてこの変更を破棄します。

まとめ

Cisco FirePOWER、Firepower Threat Defense、および Cisco ASA with FirePOWER Services は、いずれもお客様に最高水準の保護を提供する、非常に強力で使いやすい次世代セキュリティ ソリューションです。Firepower Management Center では、クライアント アプリケーション、プラグイン、または Java などが不要なインターフェイスを管理用コンピュータで確認でき、すべての FirePOWER テクノロジーの集中管理とレポートを行うことができます。

Firepower Management Center と各種の FirePOWER テクノロジーを導入すれば、管理オーバーヘッドを削減しながら、ネットワークのセキュリティと可視性を劇的に向上させることができます。

お問い合せ先

シスコシステムズ合同会社

〒107 - 6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp