ホワイトペーパー

Cisco Tetration：ほぼリアルタイムでネットワーク ポリシーのシミュレーション、テスト、検証を実行

概要

アプリケーション、セキュリティ、およびインフラストラクチャのアーキテクトは、相互に関連する 2 つの重要な課題を抱えています。1 つはアプリケーション導入および関連するインフラストラクチャの変更を迅速に行わなければならないこと、もう 1 つはこのようなアプリケーションおよび関連するビジネス データを、急速に進化するセキュリティ上の脅威から保護しなければならないことです。

これらの 2 つの大規模な変化に対処するため、インフラストラクチャ アーキテクトは、意図に基づくクラウド アーキテクチャへの移行を進めています。このアーキテクチャでは、ビジネスおよびアプリケーション ポリシーは、論理的な方法で明確に定義された上でオンプレミスまたはオフプレミス インフラストラクチャの組み合わせに実装されます。ビジネスおよびアプリケーションのセキュリティ ポリシーを形式的な論理記述で使用できるので、アプリケーション、セキュリティ、およびネットワークの各管理者は、ビジネスで要求されるガバナンス ルールとポリシーの構築と維持に専念できます。また、インフラストラクチャ ツールでさまざまなデバイスを詳細に構成できます。

Puppet、Ansible、Chef などの構成管理ツール、Openstack などの IaaS プラットフォーム、さらには Amazon Web サービスまたは Cisco® アプリケーション セントリック インフラストラクチャなどの機能を完備したクラウドおよびアプリケーション プログラマブル インターフェイス（API）駆動プラットフォームといった、多彩なメカニズムがこの移行を支援するために使用されていますが、次のような重大な問題も残されています。

自動化システム（または自動化以前の手動プロセス）によって実行されていたインフラストラクチャの構成が論理レイヤによって定義された意図を忠実に表現していることを、いかにして確認するか。ネットワーク トラフィックはポリシーに従って正しく転送されているか。アプリケーション コンポーネントは適切に導入されているか。セキュリティ ルールはプログラムおよび遵守されているか。新規または既存のポリシーへの移行および変更をどのように実施するか。

この問題は現代のデータセンターにとって目新しいものではありません。頻繁に変更が行われ、要求されるセキュリティの厳密さが増すなかで、機械学習や分析プラットフォームによる先進的な機能を活用しなければ、このような問題への回答を得るのはほとんど不可能です。

このドキュメントでは、以下のトピックについて説明します。

- ポリシー コンプライアンスが応答性に優れた安全なデータセンターにとって重要となる理由
- ベースライン設定アプリケーションの重要性
- Cisco Tetration Analytics™ アプリケーション インサイトを使用してポリシー ベースラインを生成する方法
- what-if シミュレーションで次のことをモデリングおよびテストする方法
  - アプリケーションのローカル、リモート、クラウドへの移行
  - 新規ポリシーの調整
  - ホワイトリストベースのセキュリティ適用への移行
  - Cisco® アプリケーション セントリック インフラストラクチャ（Cisco ACI™）プラットフォームへの移行

- ライブ トラフィックをほぼリアルタイムで監視して、次のことを検出する方法
  - 許可されたトラフィック
  - 誤って廃棄されたトラフィック
  - エスケープされたトラフィック
  - 廃棄されたトラフィック

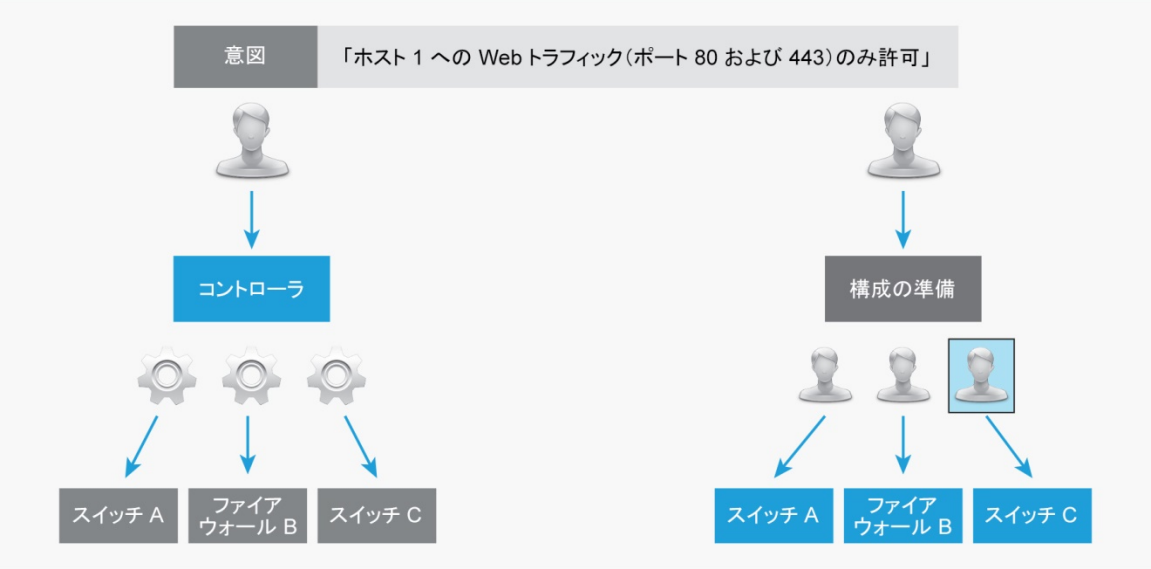
ポリシー コンプライアンスの使用事例

自動化によって、ネットワーク オペレータの自由度が高まり、コスト効率が高くスケーラブルで、継続可能なデータセンターを導入できるようになります。ただし、このアプローチでは、オペレータは基盤となるデバイスのハードウェアとの直接的な関係を失います。ほとんどの自動化ではこのような抽象化が伴い、多くの場合、構成はコントローラによって生成される（おそらく人間が読み取れない形式で）という状況で、管理者は、どのように要件がハードウェアに正しくプログラムされたかを確認できるのでしょうか。実際に何が起きているかを確認する自動化された手法がなければ、セキュリティは幻想にすぎず、何ヵ月も後になって重大な問題が発生してから脆弱性が表面化することになります。

しかし、大規模な、明示的ではないポリシーベースのネットワーク（スタンドアロン ネットワーク アーキテクチャ）にも同様の問題があります。この場合は、ビジネスおよびセキュリティ ポリシーの適用についてはネットワーク チームの責務です（データセンターが従う論理ポリシーが常に存在します）。このチームは通常、分散した各種のコンフィギュレーション ファイルのセットを手動で維持し、目的のエンドツーエンドのポリシーをネットワークに提供する必要があります。構成が適切に機能していることを検証する必要性と、セキュリティ ポリシーの精度については、同じです。

図 1 に両方のアプローチを示します。

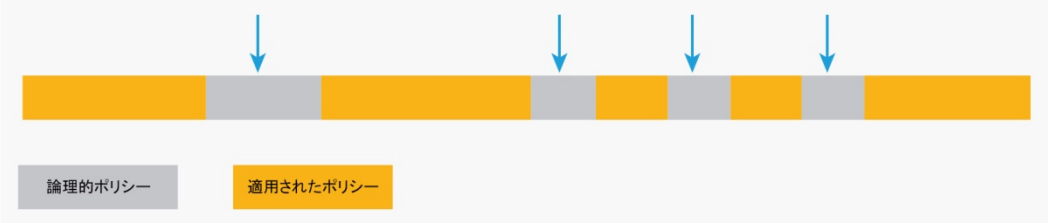
図 1. 同じビジネス意図を、コントローラベースのアプローチを使用して適用した場合と、オペレータ主導のアプローチを使用して適用した場合



この文脈での「ポリシー」という用語は、ネットワーク オペレータの意図を指しています。Cisco Application Policy Infrastructure Controller（APIC）などのコントローラは、このような意図を単に形式的な方法で捉えており、必要なハードウェアまたはソフトウェア デバイスに構成をレンダリング（適用）するプロセスは自動化されます。データセンターは作成時点からポリシーに基づいて構築されていますが、この用語は必ずしも使用されるわけではありません。従来のモデルでは、オペレータは、ポリシーの意図の理解と、デバイスへの適用の両方の役割を担っています（各デバイスに該当するコンフィギュレーション ファイルを構築し、1 つずつ適用する）。

ポリシーの適用方法にかかわらず（コントローラの使用の有無を問わず）、エンドツーエンドの意図が実現されていると形式的に証明することは困難です。それでも検証しなければ、気が付かないうちにネットワーク中にポリシーのギャップが生じる可能性があります（図 2）。

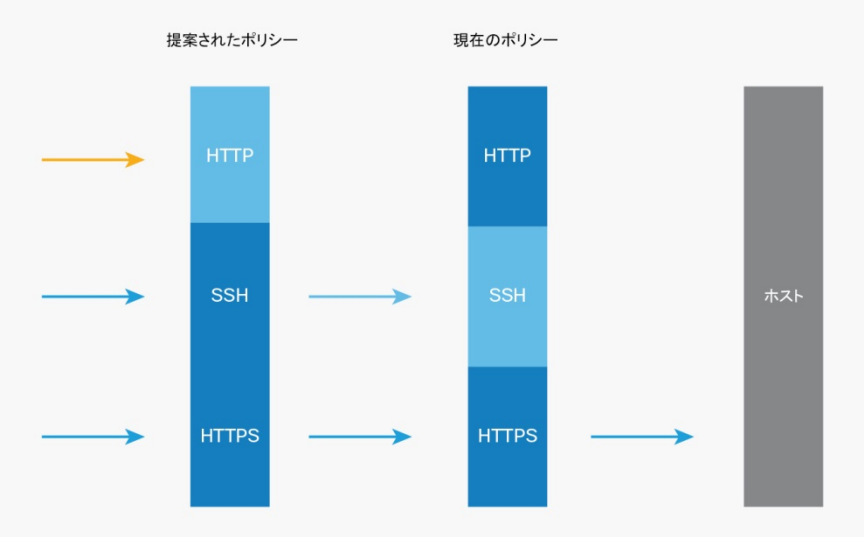
図 2. 論理ポリシー（意図）と、適用プロセス中に発生する可能性のあるセキュリティ ギャップの概念的な表現：たとえば、アクセス コントロール リストの不適切な設定によって過剰な数のポートが開く



また、ポリシーの細部を変更したことで生じる連鎖的な影響についてはどのように評価できるでしょうか。特にホワイトリストベースのネットワーク セキュリティ アプローチでは、ポリシーの精度を検証することが不可欠です。検証しなければ、新しいポリシーを導入した後に、アプリケーションの重要な部分に到達できないことに気付くはめになりかねません。問題の対応策として、変更の完全なロールバックが必要となることがあります。この場合、貴重なエンジニアリング時間が消費され、ネットワークの強固さが幻影となり、アプリケーション チームは、ネットワークが必要な変更に対してタイムリーに対応できるという確信を失います。

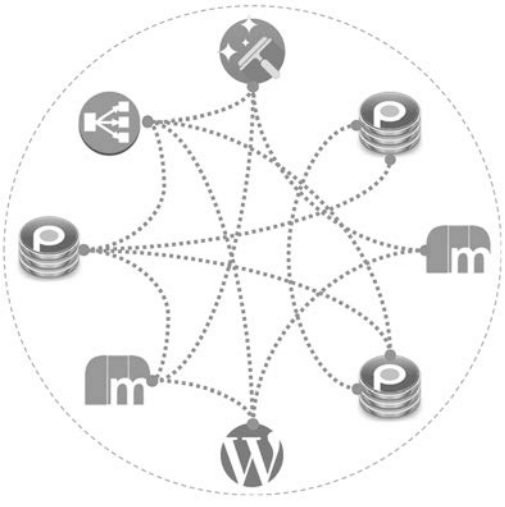
2 つのポリシー反復の転送結果を比較すれば、予測と検証が可能な変更の導入が実現します。図 3 の例では、HTTPS トラフィックは引き続き許可されます（予測どおり、ホストに向かう青い矢印）。Secure Shell（SSH）トラフィックは新しいポリシー反復で許可され（論理セキュリティ ポリシーでの潜在的な回帰、水色の矢印）、HTTP トラフィックは誤って拒否されるので、アプリケーションの重要な部分が到達不可能になります（黄色の矢印）。

図 3. Web アプリケーションにサービスを提供するホストに対する現在のポリシーと提案されたポリシーの比較例



これまで、この問題への対処はほぼ不可能でした。正当なワークロードがどこに存在するかを、通常の運用条件でアプリケーションから発生する通信パターンのすべてを追跡しながら特定することは手作業ではできないほど、現代のデータセンターの規模と複雑さが増大してしまったからです。そしてこの問題は、アプリケーション ベースがクライアント/サーバのベアメタルと仮想マシン ベースのアプリケーションからスケールアウト コンテナ ベースのモデルへの移行を進めるにつれ、悪化しています（図 4）。

図 4. シンプルな 3 層 Web アプリケーションのアプリケーション依存関係グラフのサンプル：小規模でも、依存関係グラフは急速に複雑化する



Cisco Tetration Analytics プラットフォームには、この問題の解決に向けて設計された、まったく新しい分析ベースのアーキテクチャが採用されています。

重要なフローの検出

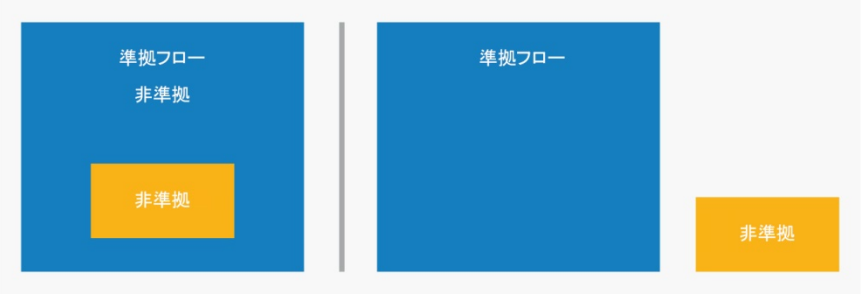
もし干し草の山から針を見つけるよう頼まれた場合、針を干し草の山から取り除く方法があるとしたら、それを試すでしょうか。普通の状況で分別のある人ならそうするでしょう。

しかし、何が干し草で何が針であるか、どうやって判別するのでしょうか。探しているものが針ではなくて、これまで見たことのないものだとしたら、どうでしょうか。

干し草の特長を、茎の 1 本 1 本にいたるまで知り尽くせば、針を明らかに異なるものとして即座に見分けることができます。

同じ考え方が、ポリシー コンプライアンスにも適用できます。目的のポリシーをきわめて詳細なレベルで理解すると、違反の特性をこれまでに確認したことや把握したことがなくても、ポリシーからのあらゆる違反を容易に検出できるのです（図 5）。

図 5. Cisco Tetration Analytics の分析で、準拠フローを非準拠フローから容易に分離できる



この新しいアプローチによって、応答時間が分単位に短縮され、問題の検出と修復をこれまで以上に迅速に実施できるようになります。アプリケーションのダウンタイムを防止し、ユーザのデータのセキュリティを確保し、不正なネットワーク アクティビティに起因する高額なコストを回避できます。

アプリケーション インサイトの適用

Cisco Tetration Analytics アプリケーション インサイト（詳細は、本書末尾にある参考資料を参照してください）により、アプリケーションが適切かつ安全に機能するために適用が必要なポリシーを、正確に検出します。このポリシーをエクスポートして、任意の数のコントローラにインポートできます。オープン形式なので、コントローラの種類は問いません。

アプリケーション インサイトでは無人の機械学習を使用して、類似したエンドポイントを正確にクラスタリングし、安全なアプリケーション通信に必要なホワイトリスト ポリシーも生成します。つまり、「干し草を学習」するのです。

ホワイトリストは、オーストラリア政府情報セキュリティ部門などの一部の機関では、標的型サイバー侵入を防御する第一の軽減戦略であると考えられています（Australian Government, 2014）。ただし、ホワイトリストの実装にはコストがかかり、維持するのも困難です。ホワイトリストは従来のブラックリストによるセキュリティ手法の対極にあり、エンドポイント間の通信は必要に応じて明示的に許可され、その他すべてのトラフィックはデフォルトで拒否されます。

アプリケーション インサイトからの推奨ポリシーをポリシー コンプライアンス パイプラインに公開し、履歴のシミュレーションとライブ分析を容易に実施できます。アプリケーション ポリシーは JSON、XML、YAML など、多数のオープン形式で公開できます。エクスポートされたポリシーには、検出されたクラスタの定義とそれぞれのクラスタ間で必要な通信ポリシーが含まれます。ポリシーはオープンで汎用性があるので、ほぼすべてのネットワーク インフラストラクチャと互換性があります。

過去のシミュレーションから将来をテストする

将来を計画するために最適な方法は、過去を学習することです。多くのデータセンターでは、多大な時間と資金を費やしてアプリケーションをただ稼働させるに留まり、多くのデータセンターにはビジネス ニーズに迅速に対応する柔軟性がありません。データセンターが新しいニーズに迅速に対応できない主な理由の 1 つは、提案された変更のテストが困難か、不可能だということです。そのため、プロジェクトの完了が遅れ、ロールアウトが長期にわたることになります。

Cisco Tetration Analytics には各フローの完全なアーカイブが備わっているので、新しいポリシー変更が起きてもその影響をシミュレーションできます。

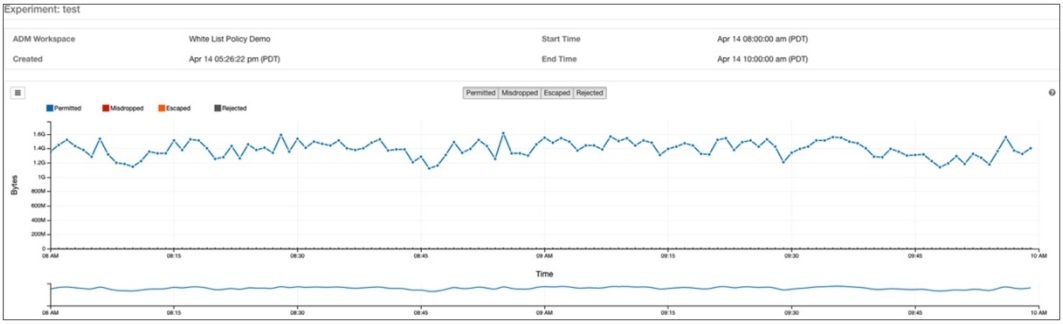
技術レベルでは、Cisco Tetration Analytics は、アプリケーション インサイトによって検出されたルールに基づいて仮想ポリシー ルックアップ テーブル（VPLT）を構築します。履歴トラフィックがルックアップ テーブルに対して再生され、ポリシー判定が監視されます。このアプローチは、同じフローが実稼働ワークロードで生成され、ネットワーク デバイスで適用された場合に見られる動作を、正確に模倣します（図 6）。

図 6. 複数のサンプル フローに対する転送判断の詳細を示す VPLT

プロトコル	プロトコル	送信元ポート	宛先 IP	宛先ポート	意思決定
TCP	192.168.0.10	5581	172.16.30.25	8080	
TCP	10.1.0.20	9396	172.16.30.25	443	→
TCP	172.16.90.100	85811	172.16.30.25	22	
UDP	10.0.0.50	4921	10.0.0.1	123	→

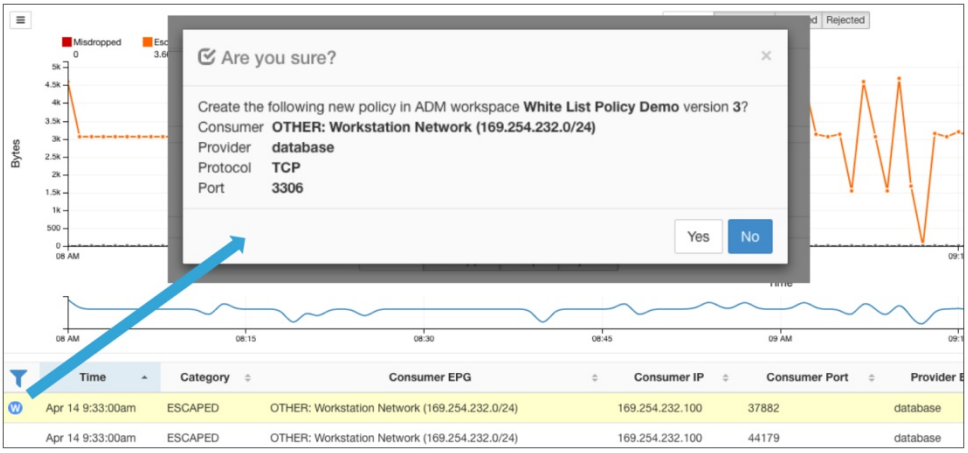
ユーザには、シミュレーション結果の特性を示す時系列グラフが表示されます（図 7）。許可されたトラフィックはグラフから除外でき、オペレータは誤廃棄、エスケープ、却下されたトラフィックに注目できます。これらのフローは、対処しなければビジネスに直接影響を及ぼすことになります。相互に通信できない必要なコンポーネント、ポリシー ルール セットでの潜在的なセキュリティ ホール、悪意のあるトラフィックを生成している侵害されたホストなどを示しています。

図 7. ポリシー分析結果グラフのサンプル



オペレータが許可済み(「干し草の一部」)と識別した中に非準拠フローがあれば、アプリケーション インサイト機能に即座に戻され、ポリシーを調整して機械学習アルゴリズムを改善できます(図 8)。

図 8. 分析後にアプリケーション インサイト ポリシーを即座に調整する



テストは、規模の大小を問わず、ポリシーの変更が発生した後に実行でき、データセンターのオペレータは即座に変更を有効にしてテストし、高い信頼度で導入することができます。

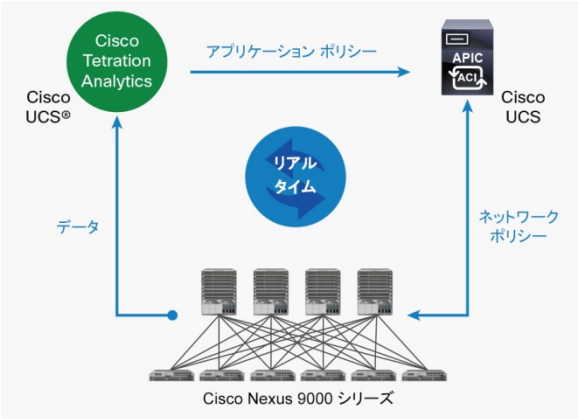
ポリシーの適用

Cisco Tetration Analytics プラットフォームは、ネットワークの運用とセキュリティ保護に必要なポリシーを生成し、テストします。ただし、ポリシーの適用は行いません。ポリシーを使用したネットワーク セキュリティの強化においては、さまざまなテクノロジーを利用可能です。

Cisco Tetration Analytics は Cisco ACI とは本質的にはリンクされていませんが、Cisco Tetration Analytics が生成するポリシーは、オープンソースの Cisco ACI ツールキットをシンプルなミドルウェア コンポーネントとして使用することで、ボタンをクリックするだけでアプリケーション インフラストラクチャ コントローラにインポートできます。実際には、アプリケーションとクラスタは、Cisco ACI での契約として構築された通信ポリシーで、アプリケーション プロファイルおよびエンドポイント グループ(EPG)として設定されます。

Cisco ACI を使用していない導入、たとえば Cisco Nexus® 9000 シリーズ スタンドアロン スイッチを使用した導入では、ポリシーはアクセス コントロール リストおよびその他の構成オプションを使用して、ネットワーク オペレータが手動で、またはネットワーク管理ツールを使用して適用できます(図 9)。

図 9. ポリシーのフィードバック ループは Cisco APIC および Tetration Analytics を使用して簡単に実装できる

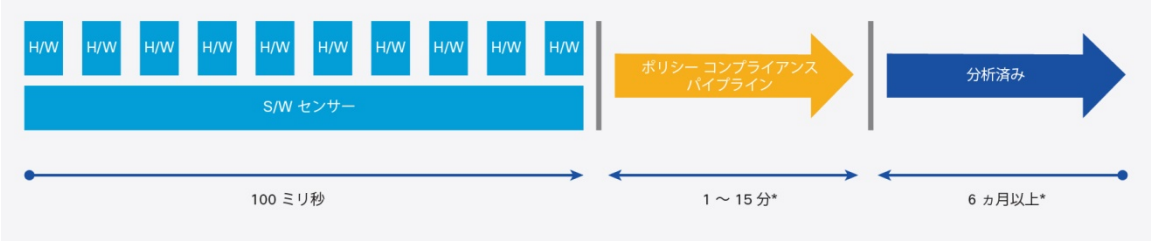


Cisco Tetration Analytics プラットフォームを使用して、ファイアウォール内またはネットワーク アクセスをレイヤ 4 で制限できないネットワーク デバイスで、フィルタ ルールを作成することもできます。プラットフォームでは、サードパーティ ベンダーのスイッチ、ルータ、ファイアウォール、セキュリティ アプライアンス向けに生成されたポリシーを禁止しません。また、Cisco Nexus 9000 シリーズ スイッチによるテレメトリ情報の収集も不要で、プラットフォームのオープンな性質を強化します。

問題に集中する

ポリシー コンプライアンスをシミュレートした後、ネットワークのコンプライアンスをほぼリアルタイムで監視できます。テレメトリ情報は、1 秒未満の間隔で分析クラスタにストリーミングされ、入力から 15 分以内に分析されます。一般的には、5 分未満で処理されます。このようにエンドツーエンドの遅延時間がきわめて短いため、データセンターの所有者はネットワークの問題をアクティブに管理して修復する機会を得られます（図 10）。

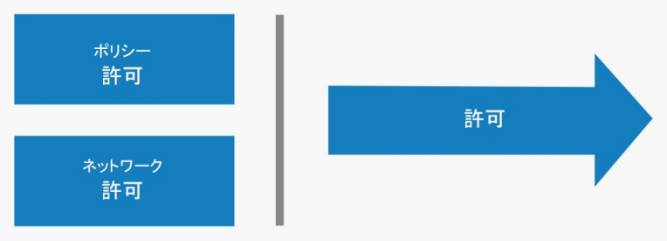
図 10. ポリシー分析のスケジュール：テレメトリ情報の取得から結果を得るまで



繰り返しますが、Cisco Tetration Analytics は、トラフィックの分類に、許可、誤廃棄、エスケープ、却下という 4 つの区分を使用する VPLT を構築します。履歴シミュレーションの代わりに（実際のネットワークの結果を参照していない場合）、ここではポリシー、つまり実際のネットワークの転送判断を、VPLT が表現するポリシーの実際の意図と比較します（図 11）。

ネットワークで許可されるトラフィックを VPLT と比較できます。結果は一致しているでしょうか。一致するならば、これは通常のアプリケーション トラフィックです。一致しなければ、それはなぜかをすぐに突き止めなければなりません。

図 11. ポリシーの「許可」とネットワークの「許可」はフローの許可を示す：トラブルシューティングの場合でも異常フローの調査の場合でも、許可されたトラフィックは不要な背景雑音になる



ネットワークに許可されたトラフィックがあるはずなのに実際にはない場合、誤って廃棄されたフローがあります（図 12）。

図 12. ポリシーの「許可」とネットワークの「拒否」または「廃棄」の組み合わせは、誤って破棄されたフローを示す

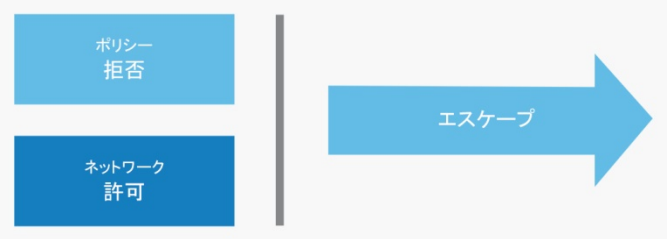
Cisco Tetration Analytics が対処する次の重要な質問は、なぜ廃棄が発生するか、です。

廃棄が発生する理由は主に 2 つあります。ポリシーの適用エラーと転送エラーです。正確な理由（廃棄）は、Cisco Nexus 9000 シリーズ スイッチのハードウェア センサーから報告され、オペレータに提供されます。

トラフィックがポリシー適用エラーによって廃棄された場合、適用されたポリシーが正当なトラフィック フローを取得して拒否している可能性があります。このシナリオは、アプリケーションの一部が相互に接続すべき場面で接続できないことを示します。トラフィックが転送エラーによって廃棄された場合、ネットワーク上でパケットを転送できないため、アプリケーションが影響を受け、運用チームによる調査が必要な問題が発生します。

ネットワークに拒否されたトラフィックがあるはずなのにない場合、ネットワークにエスケープされたフローがあります（図 13）。

図 13. ポリシーの「拒否」とネットワークの「許可」の組み合わせはエスケープされたフローを示す



エスケープされたフローは潜在的に危険を伴い、少なくとも、異常なフローといえます。迅速な対処が必要です。Cisco ACI 契約で開いているポートが多すぎる、論理セキュリティ ポリシーに意図しないギャップがあるなど、構成エラーを示すことがあります。また、悪意のあるユーザが、ネットワーク適用を強制的に排除または回避している可能性があります。これは Cisco Tetration Analytics センサーで必ず検出されます。

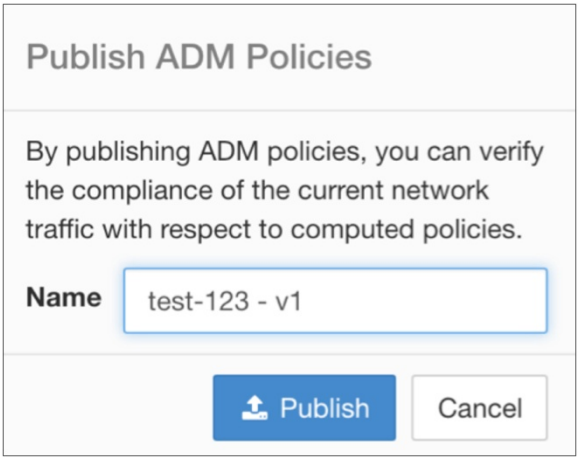
ネットワークがフローを廃棄すべき状態で実際に廃棄している場合、却下されたフローは正しく拒否されています。この動作によって、データセンター チームはポリシーの意図がすべてのデバイスによって適切に適用されていることを再確認できます。それでも、侵害されたホストが感染を広めようとするアクティビティである場合や、悪意のあるユーザが本来アクセス権のないリソースにアクセスを試みている場合が考えられるため、全チームによる慎重な調査が必要です（図 14）。

図 14. ポリシーの「拒否」とネットワークの「拒否」の組み合わせは正常に却下されたフローを示す

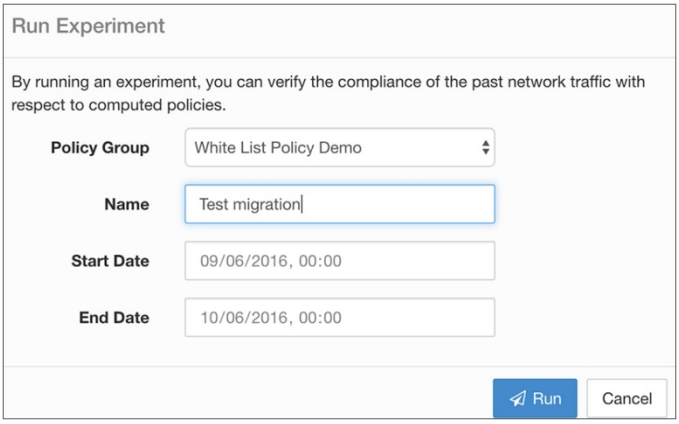
Cisco Tetration Analytics のポリシー コンプライアンスの仕組み

Cisco Tetration Analytics によるポリシー コンプライアンスの仕組みを理解するには、以下のプロセスを順に確認してください。

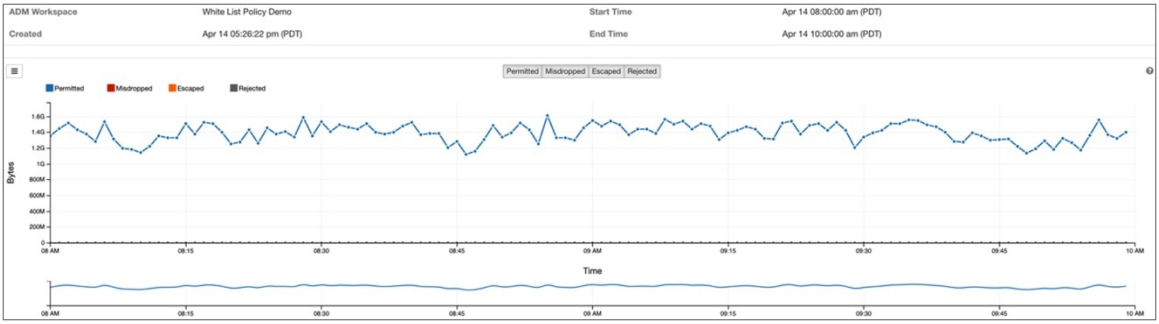
1. アプリケーション インサイトからのポリシーがポリシー コンプライアンスに公開されます。



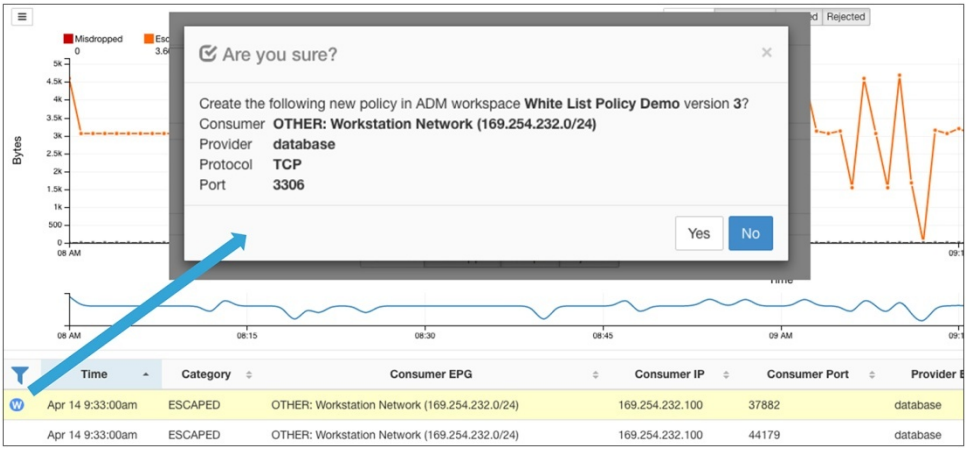
2. アプリケーション インサイトによって履歴フローから検出されたポリシーをシミュレートするには、仮想ポリシー ルックアップ テーブルを使用して、テストするポリシー グループとテストする期間を選択します。



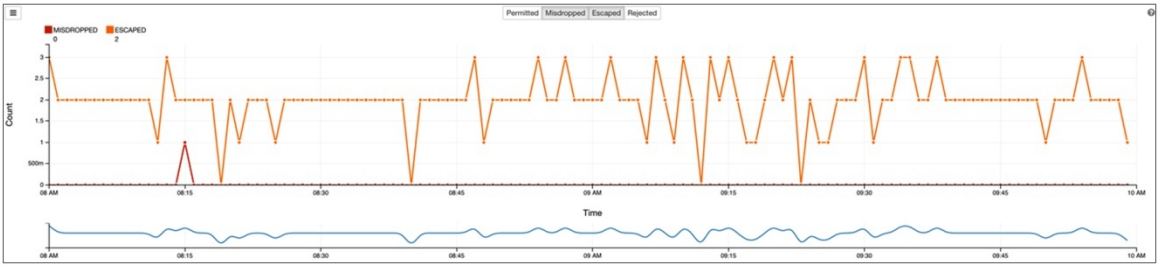
3. 許可、誤廃棄、エスケープ、却下されたトラフィックの時系列グラフを確認します。



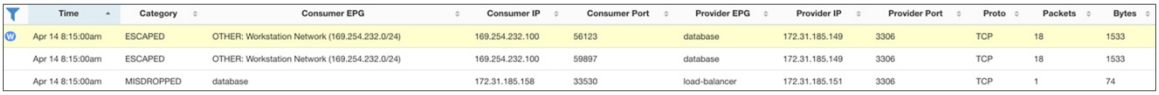
4. ポリシー コンプライアンス ツールから直接、アプリケーション インサイト ポリシーを調整します。



5. トラフィックのアプリケーション インサイト ポリシーの遵守状況をほぼリアルタイムで監視します。



6. 許可、誤廃棄、エスケープ、却下されたトラフィックの時系列グラフの詳細を確認します。



まとめ

知識は能力であると考えるならば、Cisco Tetration Analytics プラットフォームは、これまで手にすることができなかったデータセンターに関する知識を提供し、今までにない新たな能力を身に付けられます。データセンターをこれまでとはまったく違う新しいレベルで運用する能力が手に入ります。必要な変更や変化するネットワーク環境に迅速に対応し、追加されたポリシーが検出、テスト、適用、検証されるたびに日々セキュリティが強化されていきます。

関連情報

- Cisco Tetration Analytics：http://www.cisco.com/jp/go/tetration
- 動作ベースのアプリケーション インサイト：データセンターの状況の分析と把握に役立つソリューション
- Cisco Advantage Series White Papers: Flow Telemetry in Cisco ASICs（Cisco Advantage シリーズ ホワイト ペーパー：シスコの ASIC におけるフロー テレメトリ）

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

C11-737376-00JA 16.07