



Secure Workload の AI ポリシーの統計

AI Policy Statistics in Cisco Secure Workload utilizes the AI engine to track and analyze policy performance trends over time. This feature offers users insights into policy effectiveness and facilitates efficient audits. 詳細な統計と AI で生成された条件により、ユーザーは注意が必要なポリシーを特定、設定、および対処できます。トラフィックなし（30日間を超えてポリシーがフローに影響を与えない場合の条件を設定します。特定のポリシーが別のポリシーによってオーバーシャドウされている場合）および **Broad**（ポリシーの送信元フィルタまたは宛先フィルタが使用されている場合の条件を設定します。



注目 最近の GUI の更新により、ユーザーガイドで使用されているイメージやスクリーンショットの一部に、製品の現在の設計が完全に反映されていない可能性があります。最も正確に視覚的に参照するには、このガイドを最新バージョンのソフトウェアと組み合わせて使用することを推奨します。

- [Secure Workload の AI ポリシーの統計, on page 1](#)
- [AI ポリシー 統計情報の前提条件, on page 6](#)
- [AI ポリシー設定のセットアップ \(6 ページ\)](#)
- [よく寄せられる質問 \(7 ページ\)](#)

Secure Workload の AI ポリシーの統計

Secure Workload の AI ポリシー統計情報機能は、次の主要な機能を提供します。

- **Policy trend analysis:** Users can view the performance trends of policies over a specific time period while comparing the expected number of flows to the actual performance of the policies.
- **Policy conditions:** The AI engine identifies and flags policies that meet specific conditions and require user attention.

Note that a policy condition rule cannot be in more than one condition at a time. For example, a rule can either be in **Broad** or **Overshadowed** condition at a time, but not in both the conditions at the same time.

- No Traffic—policy that does not affect any flow for a configured period.

Figure 1: Policy condition—No Traffic

Protocol and Port

Rank	Priority	Action
Default	100	Allow

Consumer: Tetratation : Workloads : Collector
Provider: Tetratation

Protocol and Port: TCP : 11410 **No Traffic**
Last Used On: Never used since Oct 15, 2024

⚠️ This policy has never seen any traffic. [Analyzed Flows](#)

Description:

[Show advanced options](#)

[Analyzed Flows](#) [Enforced Flows](#) [Conversations](#) [Cancel](#) [Update](#)

- Overshadowed—a policy that overshadows another policy.

Figure 2: Policy Condition–Overshadowed

Protocol and Port

Rank	Priority	Action
Default	100	Allow

Consumer: Tetration : Workloads : Collector Provider: Tetration

Protocol and Port
TCP : 50010 **Overshadowed**

⚠ Overshadowed by the following policy:

Tetration : Workloads → Tetration
Absolute - 90 **Allow** TCP : 50010
Workspace: Tetration:Workloads [p1] Tetration : Workloads

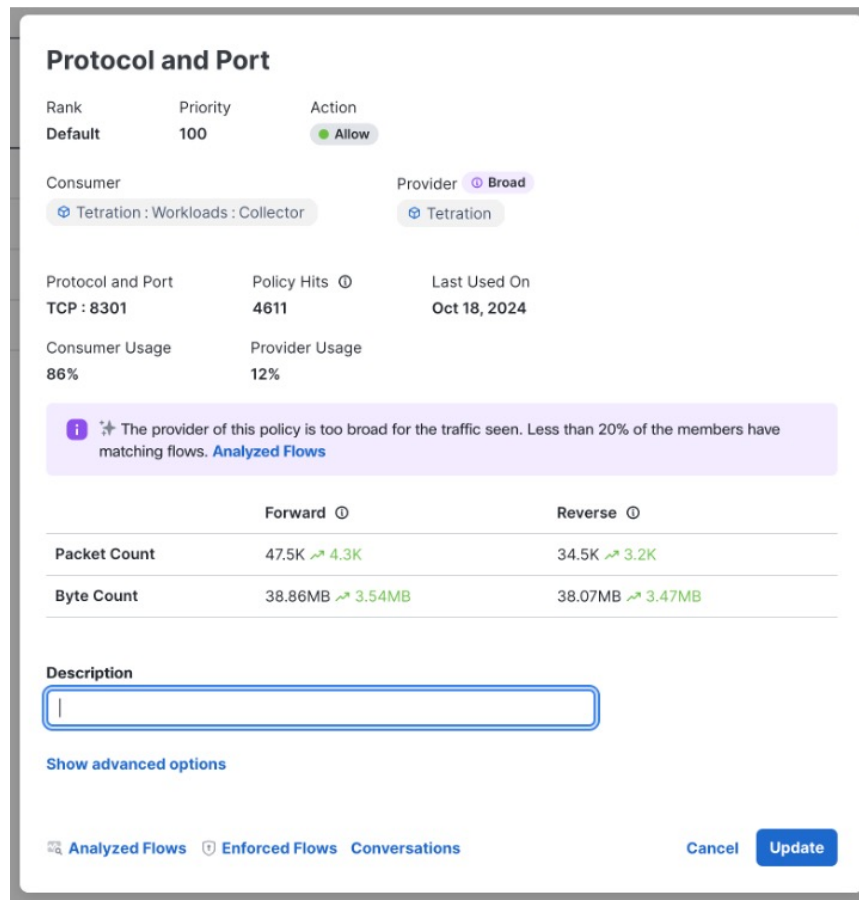
Description

Show advanced options

Analyzed Flows Enforced Flows Conversations Cancel Update

- **Broad** : 十分に活用されていないポリシーフィルタの送信元フィルタまたは宛先フィルタ。たとえば、フィルタが 10 個のインベントリで構成されており、10 個のインベントリのうち 2 個だけがポリシーの影響を受けるフローに参加する場合、フィルタの使用率は 20% だけになります。

Figure 3: Policy Condition–Broad



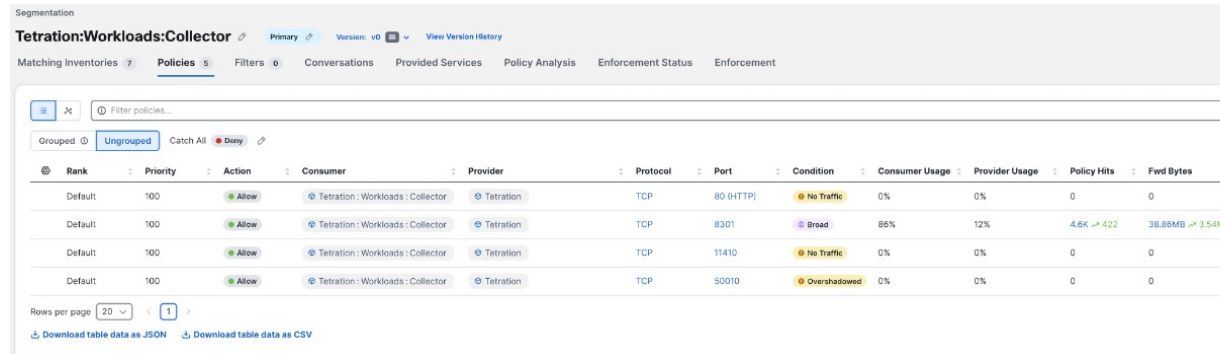
トラフィック フローの AI ポリシー統計情報

トラフィックフローに対するポリシーの統計情報またはヒット数は、各ポリシーの影響を受けるフローの数に基づきます。The hit count is for the deployed policy and not for policy versions that are in draft form or have not been published yet.



Note The **First Scanned On** and **Last Used On** columns represent the timestamps when the AI engine first scanned a particular policy and the last time it scanned the same policy.

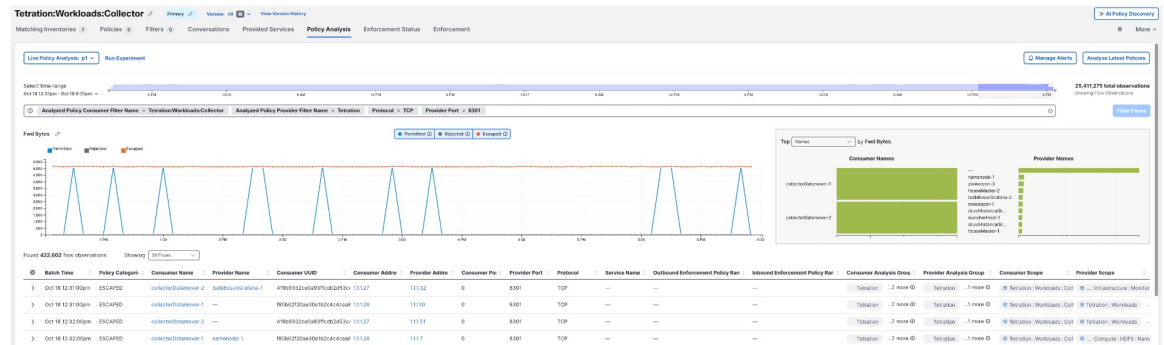
Figure 4: AI ポリシー統計



トラフィック フローの大量トレンド

ピーク イベント時にトラフィックの大量の傾向を把握するために、システムはネットワークトラフィックの異常なパターンの特定に重点を置いてデータを処理します。AI エンジンは、履歴データを使用して通常のトラフィックパターンのベースラインを確立します。大量のイベント中に、このベースラインからの大幅な偏差が検出され、異常の可能性があるものとしてフラグが立てられます。ポリシーに関するインサイトにより、ポリシーのパフォーマンスに関するリアルタイムデータが得られます。このデータを使用して、イベントのピーク時のトラフィックスパイクを監視して対応することができます。システムの分析アルゴリズムでは、ネットワークトラフィックの動的な性質が考慮されており、誤検出を生成することなく、異常を正確に特定して報告します。

Figure 5: フローでのポリシーの傾向



ポリシー統計を計算

ポリシー統計またはヒットカウントは、ポリシーの基準に一致するフローの数に基づいて計算されます。ポリシーの統計情報は、1週間のウィンドウにわたって6時間ごとに更新されます。AI の側面では、機械学習アルゴリズムを使用してヒット数のパターンと傾向を特定することが含まれており、ファイアウォールでの単純なヒット数と比較して、ポリシーパフォーマンスの微妙な理解が得られます。

AI ポリシー 統計情報の前提条件

AI ポリシー統計情報機能を活用する前に、次の前提条件が満たされていることを確認してください。

- 公開されたポリシー：AI エンジンが統計情報をスキャンして計算するには、ポリシーを Cisco Secure Workload 内でアクティブに公開する必要があります。非公開ポリシーは分析に含まれません。
- AI エンジンのアクティブ化：Secure Workload 環境内で AI エンジンが実行され、構成されている必要があります。AI 構成が最適に構成されていることを確認します。AI 構成を確認し、結果が期待どおりでない場合はデフォルトに戻します。
- ユーザーアクセス権限：ユーザーが、ポリシー統計と傾向データを表示するために必要なロールベース アクセス コントロール (RBAC) 権限を持っていることを確認します。

AI ポリシー設定のセットアップ

AI エンジンを使用すると、ポリシー統計情報とワークスペースに適用されるポリシールールを表示できます。AI エンジンの高度な機能を活用して、以下を理解できます。

- AI ポリシー ディスカバリ機能を使用した継続的なポリシー検出。
- ポリシーの有効性に関するポリシー条件の傾向分析。
- エスケープされたフローに基づくリアルタイムポリシー更新。
- 経時的なポリシーパフォーマンスの詳細な統計。
- ポリシー改善のための AI 支援の推奨事項。



(注) ポリシー統計は、ポリシーが公開された後にのみ表示されます。

手順

ステップ 1 Cisco Secure Workload アプリケーションにログインし、ナビゲーションウィンドウで、[**防御 (Defend)**] > [**セグメンテーション (Segmentation)**] の順に選択します。

- a) ポリシーがどのように分析されるかを確認するには、ワークスペースを選択します。
- b) このワークスペースに接続されているポリシーと、AI エンジンによって分析のために考慮されているポリシーを確認するには、[**ポリシーの管理 (Manage Policies)**] をクリックします。

ポリシーの作成方法については、[ポリシーの手動作成](#) を参照してください。

- c) すでに分析されたポリシーを確認するには、[**ポリシー分析 (Policy Analysis)**] タブをクリックして、[**最新のポリシーの分析 (Analyze Latest Policies)**] をクリックします。

ポリシーは、十分な分析が行われた後のみ公開する必要があることに注意してください。

ステップ 2 ワークロードで分析されたポリシーを確認するには、ナビゲーション ペインから、[**防御 (Defend)**] > [**セグメンテーション (Segmentation)**] から、[**AI 設定のポリシー (Policy AI Settings)**] をクリックします。

ポリシー分析後、AI エンジンは 6 時間ごとにポリシー統計情報を計算します。デフォルトでは、ポリシー統計情報は、1 週間にわたって収集および分析されたデータを反映します。ただし、必要な間隔を更新するには、[**ポリシー AI 設定 (Policy AI Settings)**] で期間を変更できます。

図 6: AI 設定のポリシー

次のタスク

トラフィックがポリシーにヒットしたときに通知がトリガされるように、ポリシーのアラートを作成します。通知に基づいて、問題を分析して修正し、脆弱なワークロードへのトラフィックを復元できます。詳細については、「[アラートの設定](#)」を参照してください。

よく寄せられる質問

このセクションでは、AI エンジンの使用中に発生する可能性のある潜在的なシナリオをいくつか示します。

- 質問：ワークスペースのポリシーを表示できないのはなぜですか。

回答：ポリシーが公開されているかどうかを確認します。AI エンジンがポリシーをスキャンするには、ポリシーを公開する必要があります。

- 質問：ポリシー統計はどのくらいの頻度で更新されますか？

回答：ポリシーの統計情報は 6 時間ごとに更新されます。これは、ユーザーが構成できないことに注意してください。

- 質問：ポリシー提案を受け取った後、すぐにポリシー提案を適用できますか？

回答：ポリシー条件は提案であり、提案に基づいてアクションを実行する前に確認する必要があります。

- 質問：結果が予期したとおりではない場合はどうすればよいのですか。

回答：AI ポリシー設定を確認します。結果が期待どおりでない場合は、デフォルトに戻して最適な使用をしてください。

- 質問：ここで使用されるモデルに関するお客様向けのドキュメントはありますか？AI 関連サービスが使用されている場所の詳細はありますか。

回答：大型言語モデル（LLM）は使用していません。すべての結果は、意思決定ツリーとデータ処理から得られています。AI 関連サービスは、VM 上の Secure Workload クラスタ内で実行されているサーバプロセスであり、これは Yarn ジョブではありません。

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。