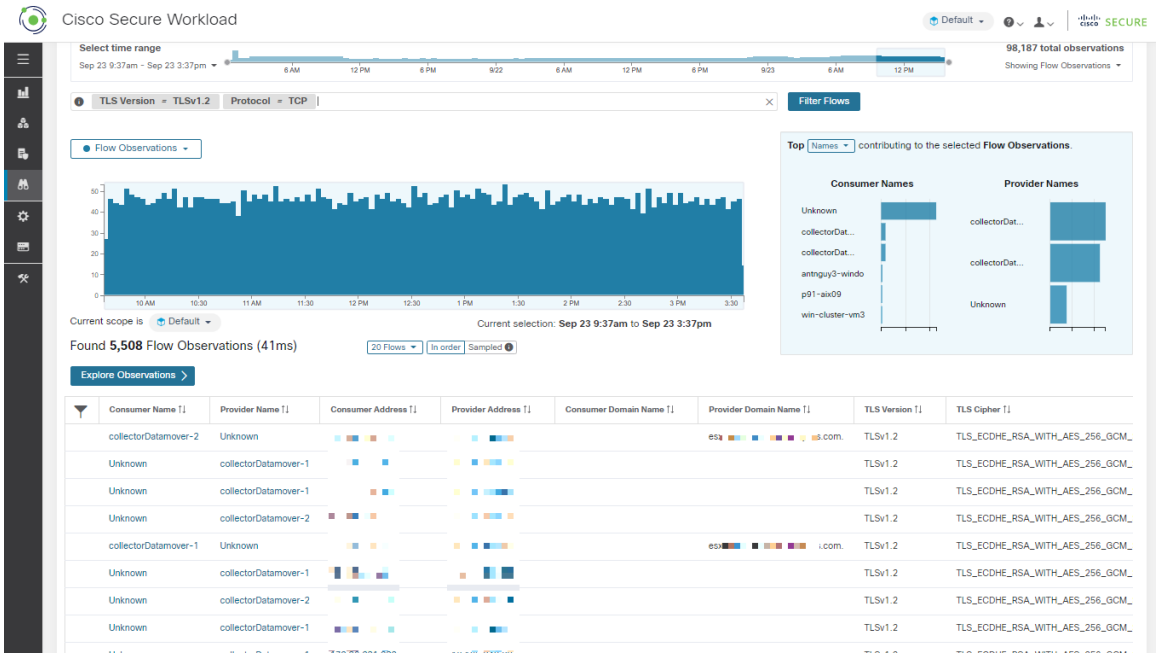
フロー

左側のナビゲーションメニューの**[調査（Investigate）]**>**[トラフィック（Traffic）]**オプションから[フローの検索（Flow Search）]ページに移動します。このページでは、フローコーパスをすばやくフィルタリングおよびドリルダウンできます。基本単位となる「フロー観測データ」は、固有のフローごとに分単位で集計されます。フローには「コンシューマ」側と「プロバイダー」側の 2つがあり、コンシューマ側でフローが開始され、プロバイダーはコンシューマに応答します（例：それぞれ「クライアント」と「サーバー」になります）。それぞれの観測では、フローの各方向のパケット数、バイト数、およびその他のメトリックが分間隔で追跡されます。フローを迅速にフィルタリングできるだけでなく、[観測結果の確認（Explore Observations）]ボタンを使用してフローを可視化できます。フロー観測結果のリストをクリックして、そのフローのライフタイム全体を通した遅延、パケット数、バイト数などのフローの詳細情報を表示できます。

警告 優れた可視化エージェントや適用エージェントを備えたホストの場合、Secure Workload はフローデータをそのフローを提供または利用するプロセスと関連付けることができます。その結果、プロセスの起動に使用される**データベースやAPIのクレデンシャルといった機密情報**を含む可能性のあるすべてのコマンドライン引数を分析や表示に利用できます。

図 *1:* フローの概要



- コーパスセレクタ （2 ページ）
- 列とフィルタ （3 ページ）
- フィルタ処理された時系列 （9 ページ）
- 上位 N 件チャート （11 ページ）
- 観測リスト （12 ページ）
- 観測結果の確認 （14 ページ）
- クライアントサーバーの分類 （16 ページ）
- カンバセーションモード （20 ページ）

コーパスセレクタ

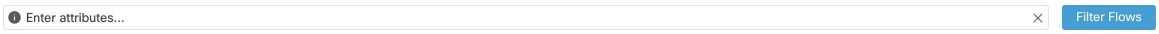
図 *2:* コーパスセレクタ

これは、コーパス全体における現在の [範囲（Scope）] の、フィルタ処理されていない要約された時系列データです。このコンポーネントの目的は、表示されている日付範囲を把握し、コンポーネント内をドラッグしてその日付範囲を簡単に変更できるようにすることです。チャート内のデータは、選択すべき時間範囲の決定に役立つ場合があります。表示するメトリックの種類は選択できます。デフォルトでは、[フロー観測（flow observations）] の数が表示されます。

コーパスセレクタは、現在およそ [20億のフロー観測（2 billion flow observations）] を選択できるようになっています。

列とフィルタ

図 *3:* フィルタ入力



ここで、検索結果を絞り込むためのフィルタを定義します。[フィルタ（Filters）] という単語の横にある [(?)] アイコンをクリックすると、すべての次元が表示されます。ユーザーラベルデータについては、これらの列も適切な間隔で使用できます。この入力は and、or、not、および括弧などのキーワードもサポートしており、これらを使用してより複雑なフィルタを表現します。たとえば、IP 1.1.1.1 と 2.2.2.2 の間の指示に依存しないフィルタは次のように記述できます。

Consumer Address = 1.1.1.1 and Provider Address = 2.2.2.2 or Consumer Address = 2.2.2.2 and Provider Address = 1.1.1.1

And to additionally filter on Protocol = TCP:

Consumer Address = 1.1.1.1 and Provider Address = 2.2.2.2 or Consumer Address = 2.2.2.2 and Provider Address = 1.1.1.1

フィルタ入力機能は、「-」を範囲クエリに変換することで、ポート、コンシューマアドレス、プロバイダーアドレスの「,」と「-」もサポートします。以下に有効なフィルタの例を示します。

図 *4:* 例：フィルタ入力でコンシューマアドレスの「,」がサポートされている

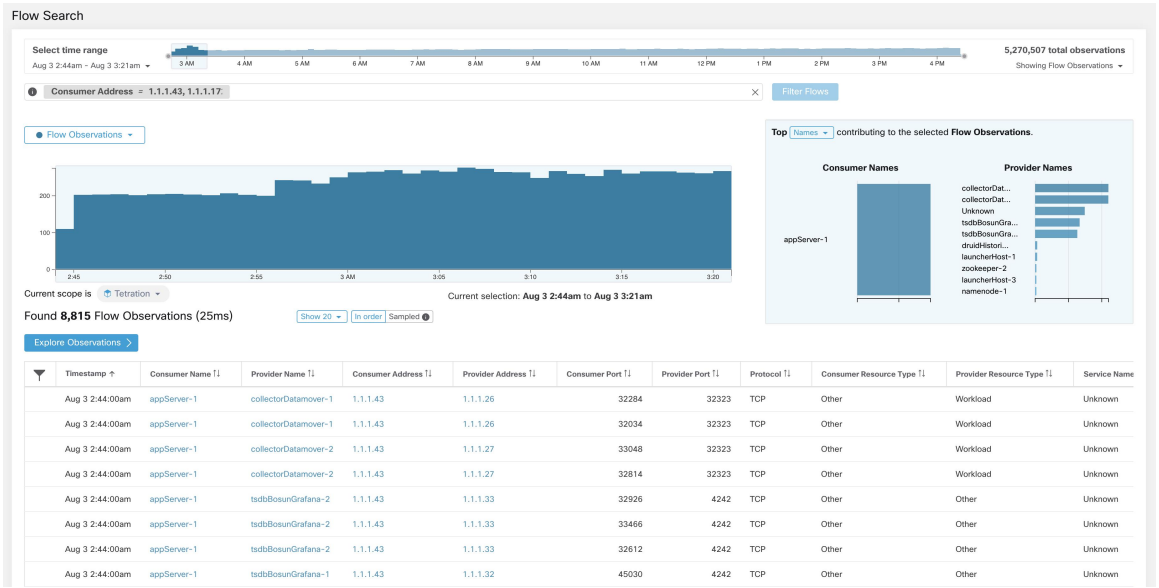


図 *5:* 例：フィルタ入力でコンシューマアドレスの範囲クエリがサポートされている

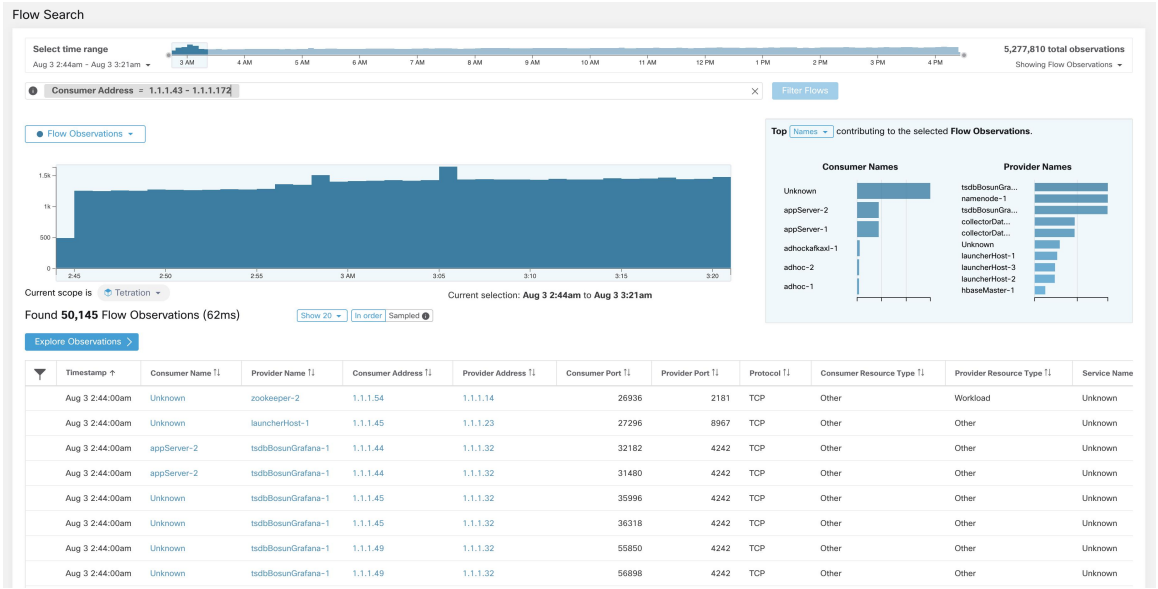


表 *1:* 利用可能な列とフィルタ

列（API で公開される名前）	説明	ソース（Source）
[コンシューマアドレス（Consumer Address）]（src_address）	CIDR 表記を使用してサブネットまたは IP アドレスを入力します（例：10.11.12.0/24）。コンシューマアドレスが入力された IP アドレスまたはサブネットと重複するフロー観測を一致させます。	ソフトウェアエージェントと Ingest アプライアンス
[プロバイダーアドレス（Provider Address）]（dst_address）	CIDR 表記を使用してサブネットまたは IP アドレスを入力します（例：10.11.12.0/24)。プロバイダーアドレスが入力された IP アドレスまたはサブネットと重複するフロー観測を一致させます。	ソフトウェアエージェントと Ingest アプライアンス
[コンシューマドメイン名（Consumer Domain Name）]	（コンシューマ IP アドレス/サブネットに関連付けられている）コンシューマドメイン名が入力されたコンシューマドメイン名と重複するフロー観測を一致させます。	ソフトウェアエージェントと Anyconnect
[プロバイダードメイン名（Provider Domain Name）]	（プロバイダー IP アドレス/サブネットに関連付けられている）プロバイダードメイン名が入力されたプロバイダードメイン名と重複するフロー観測を一致させます。	ソフトウェアエージェントと Anyconnect

列（API で公開される名前）	説明	ソース（Source）
[コンシューマホスト名（Consumer Hostname）]（src_hostname）	コンシューマホスト名が入力されたホスト名と重複するフローを一致させます。	ソフトウェアエージェントと Anyconnect
[プロバイダーホスト名（Provider Hostname）（dst_hostname）	プロバイダーのホスト名が入力されたホスト名と重複するフローを一致させます。	ソフトウェアエージェントと Anyconnect
[コンシューマ適用グループ（Consumer Enforcement Group）]（src_enforcement_epg_name）	コンシューマ適用グループは、コンシューマに一致する適用ポリシー内のフィルタ（範囲、インベントリフィルタ、またはクラスタ）の名前です。	内線
[プロバイダー適用グループ（Provider Enforcement Group）]（dst_enforcement_epg_name）	プロバイダー適用グループは、プロバイダーに一致する適用ポリシー内のフィルタ（範囲、インベントリフィルタ、またはクラスタ）の名前です。	内線
[コンシューマ分析グループ（Consumer Analysis Group）]	コンシューマ分析グループは、コンシューマに一致する分析済みポリシー内のフィルタ（範囲、インベントリフィルタ、またはクラスタ）の名前です。	内線
[プロバイダー分析グループ（Provider Analysis Group）]	プロバイダー分析グループは、プロバイダーに一致する分析済みポリシー内のフィルタ（範囲、インベントリフィルタ、またはクラスタ）の名前です。	内線
[コンシューマ範囲（Consumer Scope）（src_scope_name）	指定された範囲にコンシューマが属するフローを一致させます。	内線
[プロバイダー範囲（Provider Scope）]（dst_scope_name）	指定された範囲にプロバイダーが属するフローを一致させます。	内線
[コンシューマポート（Consumer Port）]（src_port）	コンシューマポートが入力されたポートと重複するフローを一致させます。	ソフトウェアエージェント、ERSPAN および NetFlow
[プロバイダーポート（Provider Port）]（dst_port）	プロバイダーポートが入力されたポートと重複するフローを一致させます。	ソフトウェアエージェント、ERSPAN および NetFlow

列（API で公開される名前）	説明	ソース（Source）
[コンシューマの国（Consumer Country）]（src_country）	コンシューマの国が入力された国と重複するフローを一致させます。	内線
[プロバイダーの国（Provider Country）]（dst_country）	プロバイダーの国が入力された国と重複するフローを一致させます。	内線
[コンシューマの下位区分（Consumer Subdivision）]（src_subdivision）	コンシューマの下位区分が入力された下位区分（都道府県）と重複するフローを一致させます。	内線
[プロバイダーの下位区分（Provider Subdivision）]（dst_subdivision）	プロバイダーの下位区分が入力された下位区分（都道府県）と重複するフローを一致させます。	内線
[コンシューマ自律システム構成（Consumer Autonomous System Organization）]（src_autonomous_system_organization）	コンシューマ自律システム構成が入力された自律システム構成（ASO）と重複するフローを一致させます。	内線
[プロバイダー自律システム構成（Provider Autonomous System Organization）]（dst_autonomous_system_organization）	プロバイダー自律システム構成が入力された自律システム構成（ASO）と重複するフローを一致させます。	内線
[プロトコル（Protocol）]（proto）	フロー観測をプロトコルタイプ（TCP、UDP、ICMP）でフィルタ処理します。	ソフトウェアエージェントと Ingest アプライアンス
[アドレスタイプ（Address Type）]（key_type）	フロー観測をアドレスタイプ（IPv4、IPv6、DHCPv4）でフィルタ処理します。	ソフトウェアエージェントと Ingest アプライアンス
[順方向TCPフラグ（Fwd TCP Flags）]	フロー観測をフラグ（SYN、ACK、ECHO）でフィルタ処理します。	ソフトウェアエージェント、ERSPAN および NetFlow

列（API で公開される名前）	説明	ソース（Source）
[逆方向TCPフラグ（Rev TCP Flags）]	フロー観測をフラグ（SYN、ACK、ECHO）でフィルタ処理します。	ソフトウェアエージェント、ERSPAN および NetFlow
[順方向プロセスUID（Fwd Process UID）]（fwd_process_owner）	フロー観測をプロセス所有者 UID（root、admin、yarn、mapred）でフィルタ処理します。	ソフトウェアエージェント
[逆方向プロセスUID（Rev Process UID）]（rev_process_owner）	フロー観測をプロセス所有者 UID（root、admin、yarn、mapred）でフィルタ処理します。	ソフトウェアエージェント
[順方向プロセス（Fwd Process）]（fwd_process_string）	フロー観測をプロセス（java、hadoop、nginx）でフィルタ処理します。「プロセス文字列の可視性の警告」を参照してください。	ソフトウェアエージェント
[逆方向プロセス（Rev Process）]（rev_process_string）	フロー観測をプロセス（java、hadoop、nginx）でフィルタ処理します。「プロセス文字列の可視性の警告」を参照してください。	ソフトウェアエージェント
[収集ルールのコンシューマ（Consumer In Collection Rules?）]	内部コンシューマのみを一致させます。	内線
[収集ルールのプロバイダー（Provider In Collection Rules?）]	内部プロバイダのみを一致させます。	内線
[SRTT使用可能（SRTT Available）]	「true」または「false」の値を使用して、使用可能な SRTT 測定値を持つフローを一致させます（これは SRTT > 0 に相当します）。	内線
Bytes	バイトトラフィックバケットでフロー観測をフィルタ処理します。バイトトラフィックバケット値が=、<、>（2の累乗（0、2、64、1024）でバケット化）であるフローを一致させます。	ソフトウェアエージェントと Ingest アプライアンス

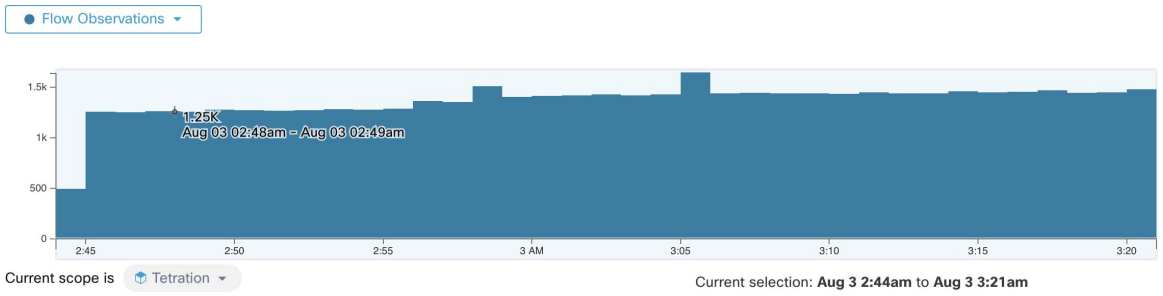
列（API で公開される名前）	説明	ソース（Source）
Packets	パケット トラフィック バケットでフロー観測をフィルタ処理します。パケット トラフィック バケット値が =、<、>（2 の累乗（0、2、64、1024）でバケット化）であるフローを一致させます。	ソフトウェア エージェントと Ingest アプライアンス
[フロー持続時間（マイクロ秒）（Flow Duration (µs)]	フロー持続時間バケットでフロー観測をフィルタ処理します。フロー持続時間バケット値が =、<、>（2 の累乗（0、2、64、1024）でバケット化）であるフローを一致させます。	内線
[データ持続時間（マイクロ秒）（Data Duration (µs)）]	データ持続時間バケットでフロー観測をフィルタ処理します。データ持続時間バケット値が =、<、>（2 の累乗（0、2、64、1024）でバケット化）であるフローを一致させます。	内線
[SRTT（マイクロ秒）（SRTT (µs)）]（srtt_dim_usec）	SRTTバケットでフロー観測をフィルタ処理します。SRTT バケット値が =、<、>（2 の累乗（0、2、64、1024）でバケット化）であるフローを一致させます。	ソフトウェア エージェント
[順方向パケットの再送信（Fwd Packet Retransmissions）]（fwd_tcp_pkts_retransmitted）	パケット再送信バケットでフロー観測をフィルタ処理します。パケット再送信バケット値が =、<、>（2 の累乗（0、2、64、1024）でバケット化）であるフローを一致させます。	ソフトウェア エージェント
[逆方向パケットの再送信（Rev Packet Retransmissions）]（rev_tcp_pkts_retransmitted）	パケット再送信バケットでフロー観測をフィルタ処理します。パケット再送信バケット値が =、<、>（2 の累乗（0、2、64、1024）でバケット化）であるフローを一致させます。	ソフトウェア エージェント
[ユーザーラベル（User Labels）]（* または user_ プレフィックス）	手動でアップロードされたカスタムラベルに関連付けられたユーザー定義データ。UI ではプレフィックスが * で、OpenAPI では user_ です。	CMDB
TLS バージョン	フローで使用される SSL プロトコルバージョン。	ソフトウェア エージェント
[TLS暗号方式（TLS Cipher）]	フローで SSL プロトコルによって使用されるアルゴリズムのタイプ。	ソフトウェア エージェント

列（API で公開される名前）	説明	ソース（Source）
[コンシューマエージェントタイプ（Consumer Agent Type）]	コンシューマ エージェント タイプを指定します。	内線
[プロバイダーエージェントタイプ（Provider Agent Type）]	プロバイダー エージェント タイプを指定します。	内線
[コンシューマリソースタイプ（Consumer Resource Type）]	ソースからコンシューマへのリソースのフローを表します。ワークロード、ポッド、サービスなどがあります。	内線
[プロバイダーリソースタイプ（Provider Resource Type）]	プロバイダーからコンシューマへのリソースのフローを表します。ワークロード、ポッド、サービスなどがあります。	内線

（注） フローデータは取り込み時にのみユーザーラベルでラベル付けされるため、ユーザーラベルを有効化してもすぐには表示されません。フロー検索でラベルが表示されるまでに数分かかる場合があります。また、使用可能なユーザーラベルは、[コーパスセレクタ（Corpus Selector）] で選択した部分によって異なります。有効化されたラベルがさまざまな時点で変更されている可能性があるためです。

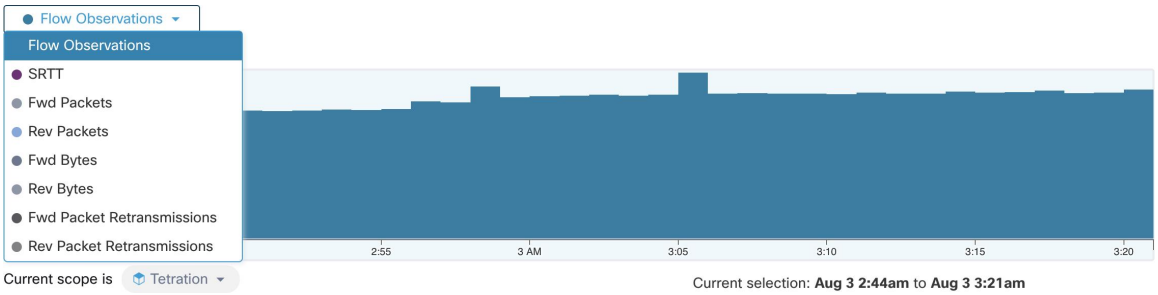
フィルタ処理された時系列

図 *6 :* フィルタ処理された時系列



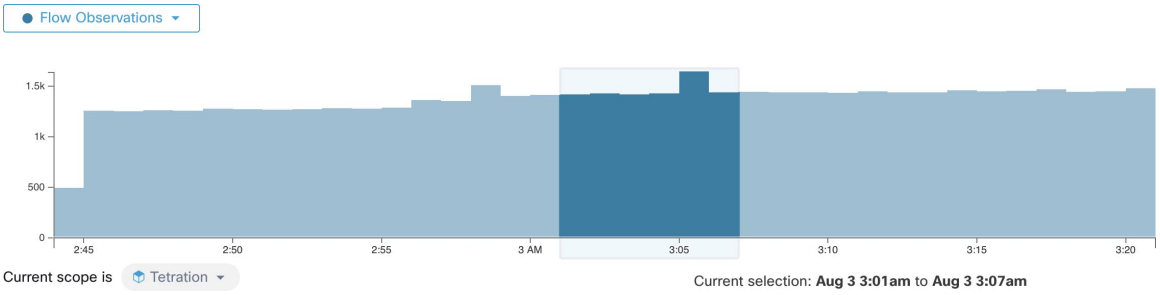
このコンポーネントは、選択した間隔（前述のコーパスセレクタ（2ページ）で行った選択）のさまざまなメトリックの集約合計を表示します。ドロップダウンを使用して、表示されるメトリックを変更します。

図 *7 :* [時系列（*Timeseries*）] ドロップダウン



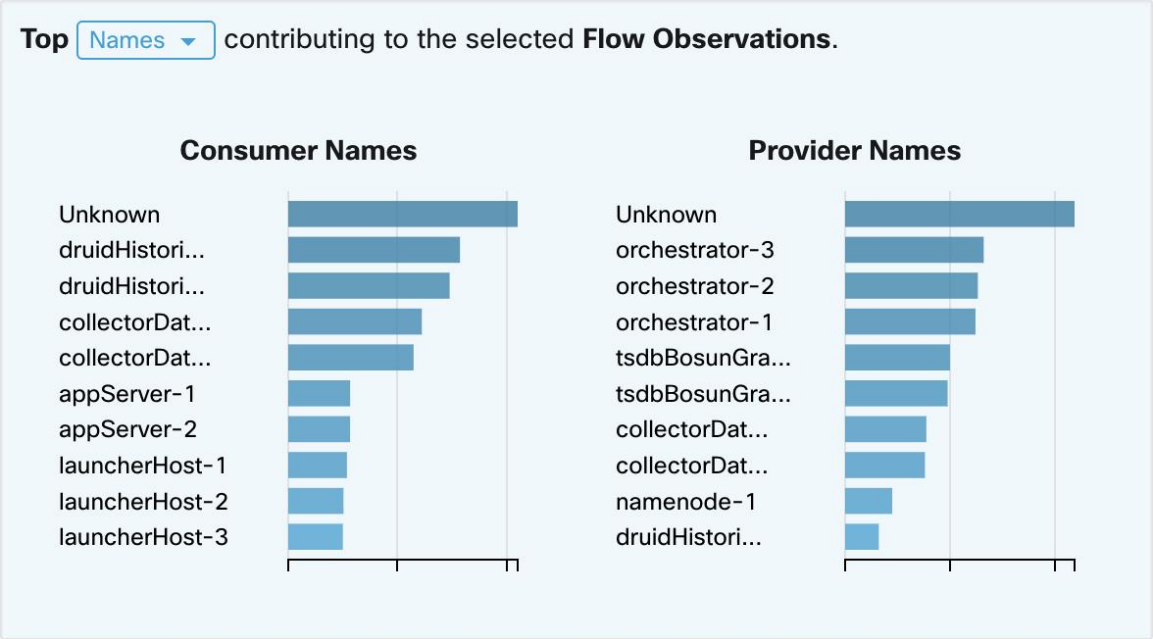
このコンポーネントでは、選択した間隔をさらに狭めることもできます。注目したいグラフの領域をクリックするだけで、上位Nチャートとその下のデータがすべて更新され、選択した間隔のデータのみが含まれます。

図 *8 :* 選択範囲による時系列チャート



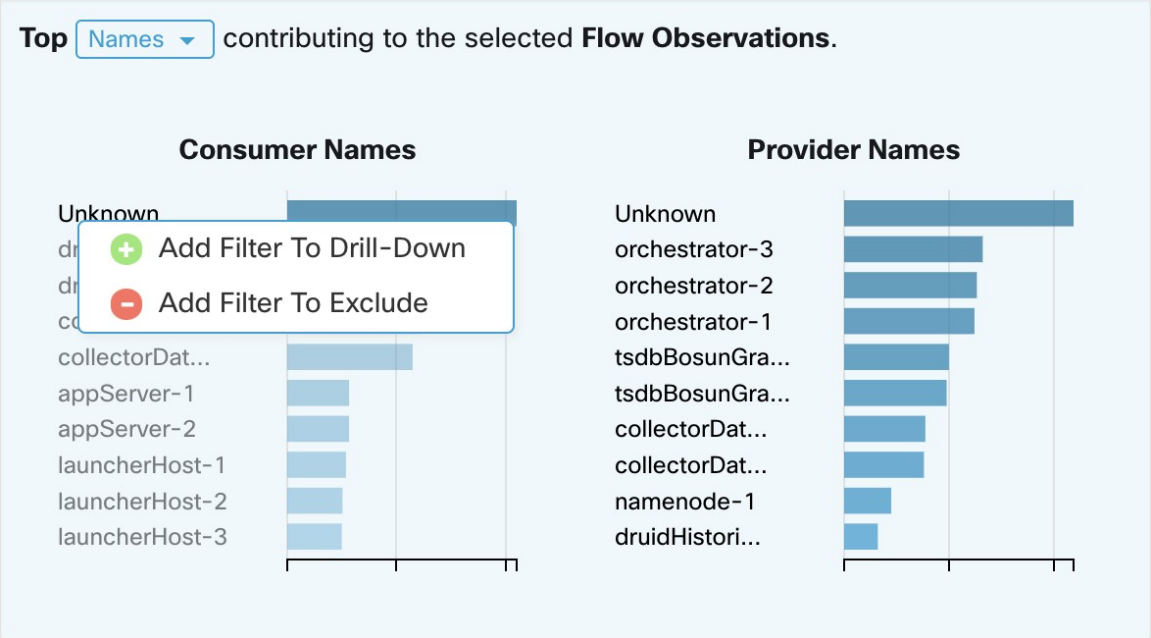
上位 N 件チャート

図 *9 :* 上位 *N* 件チャート



このチャートには、左側のフィルタ済みの時系列チャートの選択に影響を与える上位N件の値が表示されます。時系列チャートのフロー観測でピークを選択し、上位N件チャートでホスト名を選択すると、それらのフロー観測に最も影響を与えるホスト名（コンシューマとプロバイダー）のリストが表示されます。また、時系列チャートがSRTTを表示するように設定されている場合、上位のホスト名には、選択したSRTTに最も影響を与えるものが表示されます。

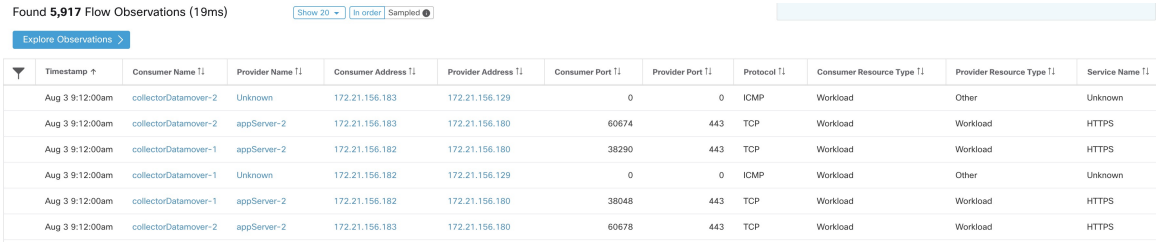
図 *10 :* ドリルダウンおよび除外



上位N件チャートのいずれかの項目をクリックすると、その値を「ドリルダウン」または「除外」できるメニューが表示されます。[ドリルダウン（Drill-down）] をクリックすると、結果をその値だけに限定するフィルタが追加されます。[除外（Exclude）]をクリックすると、結果からその値を除外するフィルタが追加されます。

（注） [ドリルダウン（Drill-down）] または [除外（Exclude）] をクリックした後、フィルタを有効にするには、[フィルタ（Filter）]ボタンを押す必要があります。これは、ページが途中で繰り返し更新されることなく、複数の「除外」アクションをすばやく実行できるようにするためです。

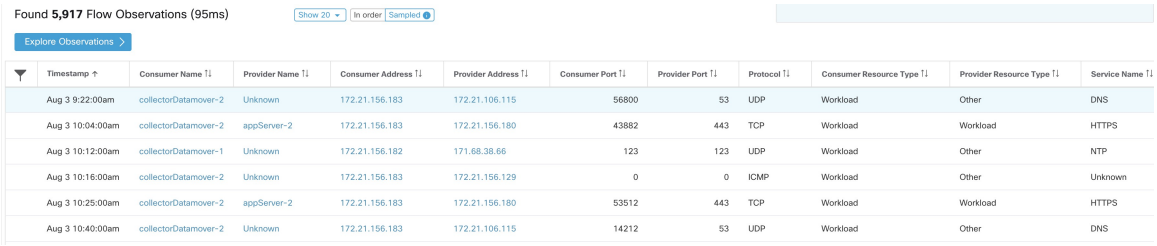
観測リスト



これは、上のページのフィルタおよび選択と一致する、実際の[フロー観測（Flow Observations）] のリストです。デフォルトでは、間隔の最初から 20 個がロードされます。 ドロップダウンを使用すると、ロードされる数を増やせます。[順番（In Order）] ではなく [サンプル（Sampled）]

を使用して、選択された間隔からフロー観測のランダムセットの読み込みも可能です。[サンプル（Sampled）]設定は、間隔の最初から順番に読み込むのではなく、選択した間隔からより代表的なフロー観測のセットを取得するのに役立ちます。

図 *11* : サンプル



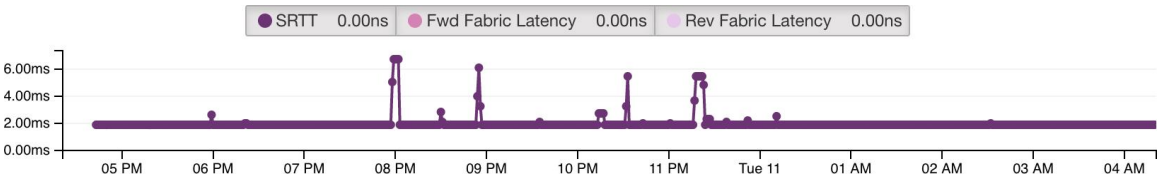
フローの詳細

いずれかの行をクリックすると、その行の下にある [フローの詳細（Flow Details）] セクションが展開されます。フローの概要と、そのフローの存続期間中のさまざまなメトリックのグラフが表示されます。存続期間の長いフローの場合、サマリーチャートが下部に表示され、時系列データを表示するさまざまな間隔を選択できるようになります。

図 *12* : フローの詳細

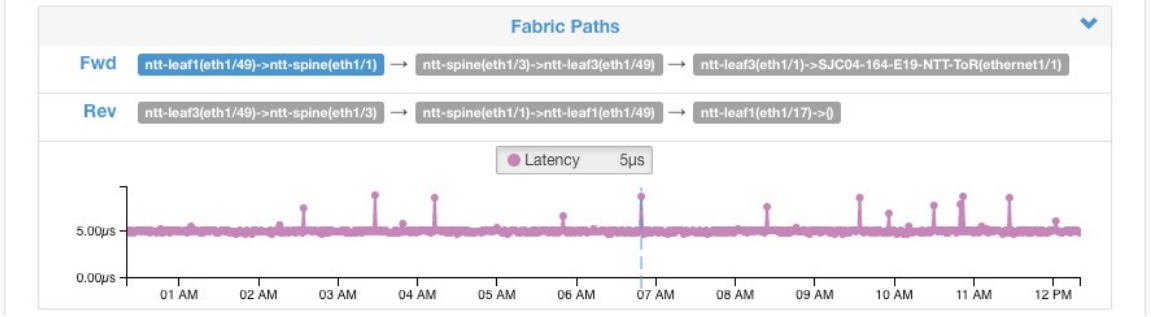
ファブリックパス情報でラベル付けされたフローの場合、[順方向/逆方向ファブリックレイテンシ（Fwd/Rev Fabric Latency）] と [SRTT] が使用可能になります。[順方向/逆方向バーストインジケータ（Fwd/Rev Burst Indicators）] および [順方向/逆方向バースト+ドロップインジケータ（Fwd/Rev Burst+Drop Indicators）] など、他のメトリックの時系列グラフが表示される場合があります。「可視性の警告」を参照してください。

図 *13* : 遅延



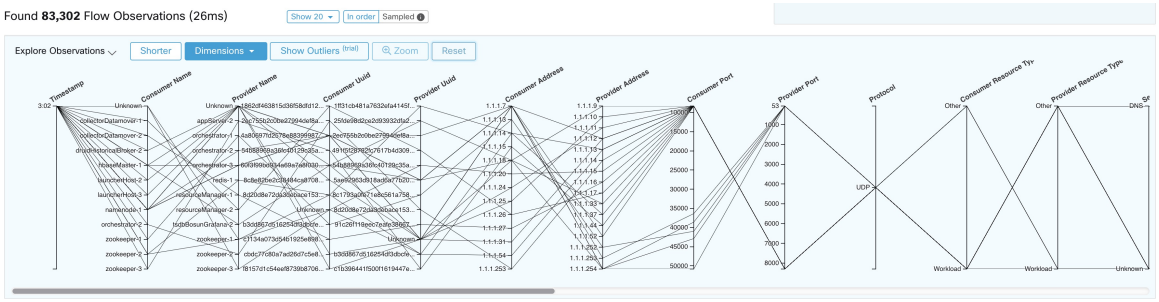
さらに、[順方向/逆方向ファブリックパス（Fwd/Rev Fabric Path）] に関する詳細が利用可能になります。各リンクをクリックして、[レイテンシ（Latency）] および [ドロップインジケータ（Drop Indicators）] の時系列チャートの切り替えができます（ゼロでない場合）。[順方向（Fwd）] または [逆方向（Rev）] をクリックすると、フローの [ファブリックパスのオーバーレイ（Fabric Path Overlay）] ページのドリルダウンに移動します。

図 *14* : ファブリックパス



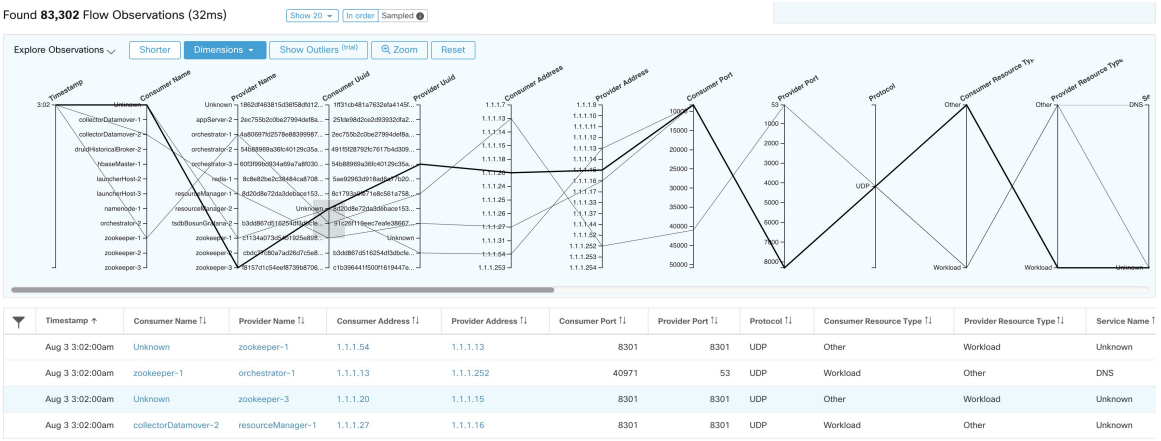
観測結果の確認

図 *15* : 観測結果の確認



青色の [観測結果の確認（Explore Observations）] ボタンをクリックすると、チャートビューが有効になり、高次元データ（別名「平行座標」チャート）をすばやく分析できます。最初は少し難しく感じるかもしれませんが、関心のある次元のみを有効にする場合（[次元（Dimensions）] ドロップダウンの項目のチェックを外す）や、次元の順序を並べ替える場合、このチャートは非常に便利です。このチャートの 1 本の線は 1 つの観測値を表し、その線がさまざまな軸と交差する場所は、その次元での観測値を示しています。より明確にするには、チャートの下にある観測結果のリストにカーソルを合わせます。これにより、チャート内の観測結果を示す線が強調表示されます。

図 *16 :* フローの観測結果にカーソルを合わせた場合



Timestamp	Consumer Name	Provider Name	Consumer Address	Provider Address	Consumer Port	Provider Port	Protocol	Consumer Resource Type	Provider Resource Type	Service Name
Aug 3 3:02:00am	Unknown	zookeeper-1	1.1.1.54	1.1.1.13	8301	8301	UDP	Other	Workload	Unknown
Aug 3 3:02:00am	zookeeper-1	orchestrator-1	1.1.1.13	1.1.1.252	40971	53	UDP	Workload	Other	DNS
Aug 3 3:02:00am	Unknown	zookeeper-3	1.1.1.20	1.1.1.15	8301	8301	UDP	Other	Workload	Unknown
Aug 3 3:02:00am	collectorDatamover-2	resourceManager-1	1.1.1.27	1.1.1.16	8301	8301	UDP	Workload	Other	Unknown

Download table data as JSON

フローデータの高次元の性質により、このチャートはデフォルトでかなり幅が広く、チャート全体を表示するには右にスクロールする必要があります。このため、関心のある次元以外はすべて無効にすると便利です。

サンプリング観測と順次観測の比較

[観測結果の確認（Explore Observations）]では、**サンプリング**を有効にして、より多くのフローを対象にすることを推奨します。これにより、選択した期間内に発生したさまざまなフローをより多く確認できます。したがって、上の時系列チャートで200万件のフロー観測を選択した場合、1000件のサンプルが期間全体で均一にロードされます。一方、フローの**順次**ロードでは、期間の最初から1000件のフロー観測データがロードされます。：

図 *17 : 1000* 件の順次データ

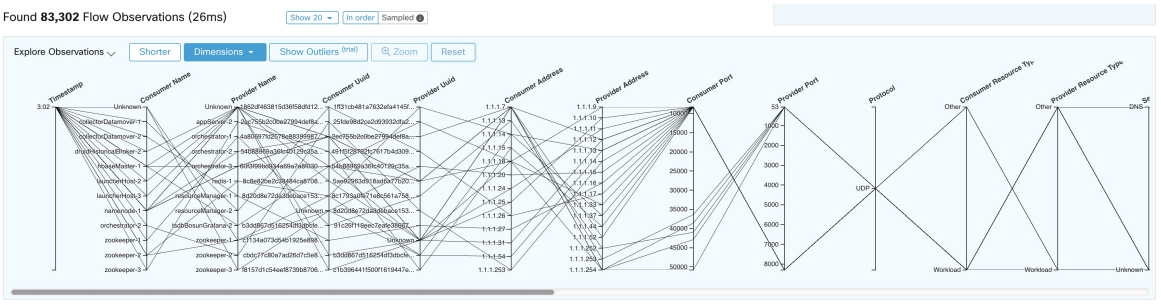
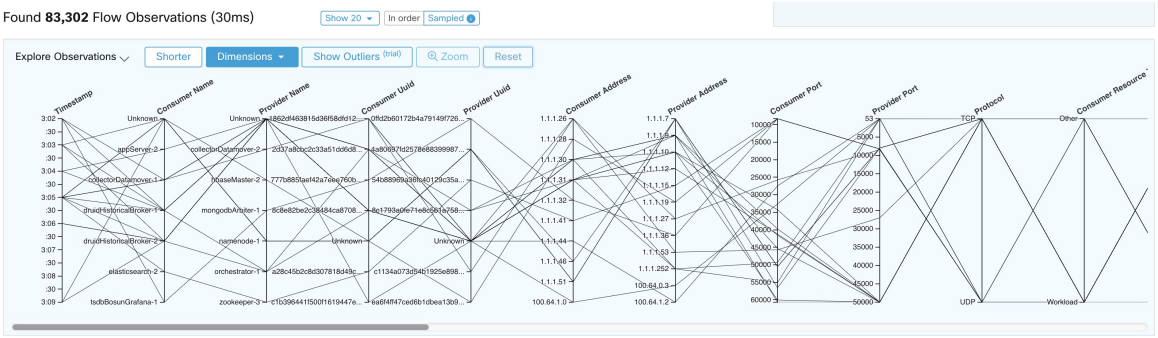


図 *18 : 1000* 件のサンプルデータ

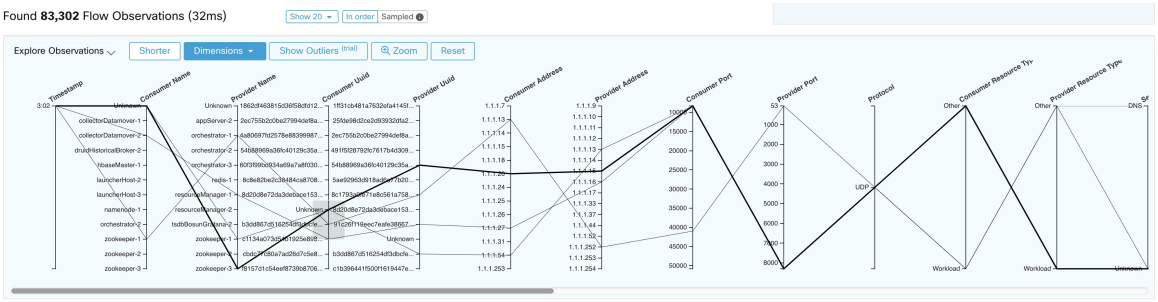


順序どおりの観測データの場合は、すべて**タイムスタンプ**が 9:09 から始まる点や、サンプリングの場合は観測データが選択された期間全体で均等に分散されている点に注目してください。

フィルタリング

いずれかの軸に沿ってカーソルをドラッグすると、選択範囲が作成され、その選択範囲に一致する観測データのみが表示されるようになります。軸を再度クリックすると、いつでも選択範囲を解除できます。一度に任意の数の軸を選択できます。観測データのリストが更新され、選択した観測データのみが表示されます。

図 *19 :* 選択範囲による確認



Timestamp	Consumer Name	Provider Name	Consumer Address	Provider Address	Consumer Port	Provider Port	Protocol	Consumer Resource Type	Provider Resource Type	Service Name
Aug 3 3:02:00am	Unknown	zookeeper-1	1.1.1.54	1.1.1.13	8301	8301	UDP	Other	Workload	Unknown
Aug 3 3:02:00am	zookeeper-1	orchestrator-1	1.1.1.13	1.1.1.252	40971	53	UDP	Workload	Other	DNS
Aug 3 3:02:00am	Unknown	zookeeper-3	1.1.1.20	1.1.1.15	8301	8301	UDP	Other	Workload	Unknown
Aug 3 3:02:00am	collectorDatamover-2	resourceManager-1	1.1.1.27	1.1.1.16	8301	8301	UDP	Workload	Other	Unknown

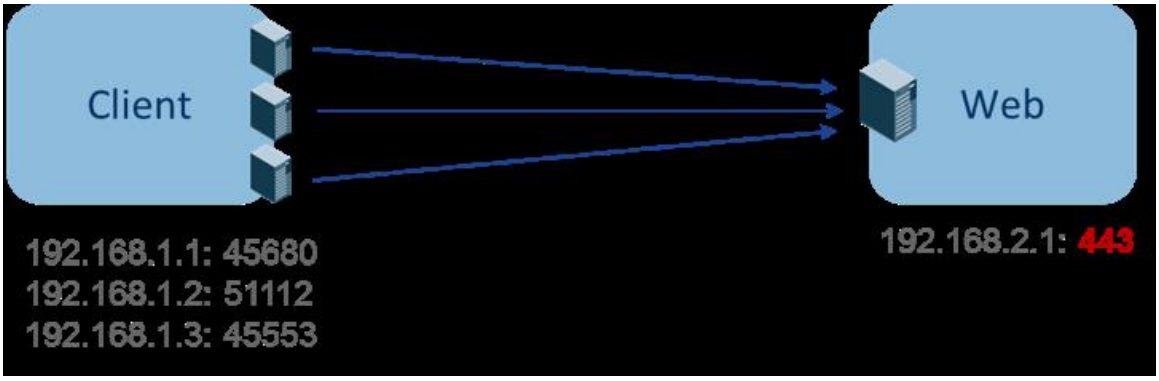
Download table data as JSON

クライアントサーバーの分類

フローの方向（クライアント/サーバーまたはプロバイダー/コンシューマの分類）は、可視性、自動ポリシー検出、および適用にとって重要です。すべてのユニキャストフローには、クライアントとサーバーの分類があります。

たとえば、HTTPS を使用して Web サーバー（192.168.2.1）にアクセスするクライアント（192.168.1.1 ～ 192.168.1.3）がある場合、通常、送信元ポートは 1025 ～ 65535 の範囲のエフェメラルポートであり、宛先ポートは 443 です。

図 *20* : クライアントサーバーの分類



正確なクライアントサーバーの方向は次のとおりです。

- クライアント：192.168.1.1 ～ 3
- サーバー：192.168.2.1
- サービス：TCP ポート 443

自動ポリシー検出によって生成されたポリシーは、以下の図に示されています（左側のエンドポイントがグループ化されています）。

図 *21* : 生成されたポリシー

ここで、クライアントとサーバーの方向の判断が逆になった場合（不正確な分類）、次のようになります。

- クライアント：192.168.2.1
- サーバー：192.168.1.1 ～ 3
- サービス：エフェメラルポートのリスト（45680、51112、45553）

次に、上記の不正確な分類では、生成されたポリシーは次の図のようになる可能性があります。

図 *22 :* 不正確な分類

この結果、ポリシーの適用に関してより多くのリソースが消費されます。さらに、ポリシーの適用方法によっては、192.168.1.1 ～ 3 では当該エフェメラルポートを使用しても、192.168.2.1 にアクセスできません。たとえば、Secure Workload ソフトウェアセンサーの適用を使用する場合、前述のクライアントから Web（ESTAB）への適用ポリシーは、Web 宛てのクライアントによって生成されたトラフィック（NEW、ESTAB）と一致しません。

タイムスタンプと TCP フラグは、クライアントとサーバーの方向を判断するために Secure Workload で使用されます。たとえば、パケットが UDP/ICMP である可能性があるか、方向信号をサポートしていない HW センサーが使用されているため、TCP フラグ情報（SYN、SYN/ACK）がない場合、ユーザー定義のオーバーライドルール、タイムスタンプ、およびその他のヒューリスティックは、フローの方向を推測するために使用されます。定義上、ヒューリスティックでは 100% の精度は保証されません。クライアントとサーバーの精度は、使用されるセンサーのタイプと、センサーの使用条件の関数で得られます。ユーザーは、Cisco Secure Workload の REST-API（OpenAPI）を使用してクライアントとサーバーのオーバーライドルールを挿入し、Secure Workload が誤った方向を取得したフロータイプのサーバーポートを識別できます。次に、Secure Workload はそれらのルールを適用してキャプチャされた新しいフローデータを処理し、フローの方向が固定されている期間にポリシーを生成します。オーバーライドルールを指定する API の詳細については、クライアントサーバー構成を参照してください。ポリシーを手動で定義し、不要なポリシーを調査または削除することもできます。ポリシーを参照してください。

センサータイプの推奨事項

優れた可視性エージェントまたは適用ソフトウェアエージェントは、Secure Workload クライアントサーバー分類アルゴリズムに最適な信号を提供します。優れた可視性エージェントまたは適用エージェントの展開を検討することを強く推奨します。これらのエージェントは、適切なクライアント/サーバー分類を推進するために必要なすべての信号を取得します。一部のワークロードで優れた可視性エージェントまたは適用エージェントを展開できない場合は、ERSPAN センサーを使用し、そこで停止して自動ポリシー検出を行うことを推奨します。そのためには Secure Workload が役立ちます。また、シスコではフィードバックに基づいてヒューリスティック アルゴリズムを継続的に改善しています。

正しいクライアントサーバーの指示情報が利用できない場合、Secure Workload はユーザー定義のオーバーライドまたはヒューリスティックを使用して、指示の内容を推測します。定義上、ヒューリスティックは 100% の精度を保証しません。使用するセンサーの種類や使用条件により精度は低下します。

以下は、ポリシー生成のユースケースにおけるクライアント/サーバーの決定で推奨される順序です。

- [優れた可視性エージェントまたは適用エージェント （Deep visibility or enforcement agents）]：最良の結果を得るには、ソフトウェアセンサー（優れた可視性エージェントまたは適用エージェント）を使用します。センサーが起動する前に開始されたトラフィックフローは、以下で説明するヒューリスティックによって処理されます。
- [F5/Citrix/. ..エージェントのようなADCセンサー（ADC Sensors like F5/Citrix/. . . agents）]：これらのエージェントは、ADC デバイスからクライアントサーバーの状態を収集し、その信頼できる情報源を Cisco Secure Workload にストリーミングします。
- [ERSPANセンサー（ERSPAN sensors）]：ERSPAN センサーを使用する場合、ユーザーは問題があるワークロードとの間のトラフィックを完全に可視化し、ERSPANセンサーがすべてのスパンされたトラフィックを認識できるようにする必要があります。また、ワークロードのネットワーク通信の可視性を低下させないため、 ERSPAN センサーのオーバーサブスクライブもしないでください。さらに、ERSPANセンサーのパケットドロップを最小限に抑える必要があります。オペレータには、自動ポリシー検出のネットワークフロー情報を含むプロセス情報は見えません。

以下にリストされている Netflow センサーを使用している場合、ユーザーはポリシー分析に関するより多くの手動作業にサインアップし、例外ルールを生成する必要があります。定義上、Secure Workload は 100% 正確ではないヒューリスティックを多用します。

- [Netflowセンサー（Netflow Sensor）]：NetFlow は、サンプリングされ、集約されたフローデータを提供します。集約およびサンプリングのプロセスでは、クライアントサーバーの指示情報が失われます。指示情報が失われると、自動ポリシー検出とポリシー生成の結果に影響し、問題をより困難にします。NetFlow データは、高度な可視性に優れています。Secure Workloadはヒューリスティックにフォールバックする必要がありますが、正しくない場合はオペレータに代わってより多くの手動作業が必要になります（たとえば、Cisco Secure Workload の例外ルールを定義するなど）。NetFlow データも一部の短いフローを見逃しており、信号品質は NetFlow データを生成するデバイスに依存します。アプリケーション デリバリ コントローラ（またはサーバーロードバランサ）など、L3/L4 NAT デバイスを介したスティッチングフローのような特殊なユースケースでは、Secure Workload で NetFlow を使用して、どのフローが他のどのフローに関連しているかを Secure Workload で可視化することを推奨します。

クライアントサーバーの指示分析の詳細は、次のとおりです。

フローのプロデューサー（別名サーバー）とコンシューマ（別名クライアント）の識別

サーバーを検出するために使用される方法（多くの場合、ヒューリスティック）は複数あります。

- センサーが SYN ハンドシェイクを検出すると、サーバーを特定できます。

- 時間ベース：接続のイニシエータがクライアントと見なされます。
- 度合いモデル：通常、サーバーは多くのクライアントと通信します。対照的に、クライアントポートの利用度合いは、はるかに少ないと予想されます。

優先順位は、SYN_ANALYSIS/NETSTAT > USER_CONFIG > DEGREE_MODEL の順です。

SYN_ANALYSIS にユーザー設定よりも高い優先順位が与えられるのは、ユーザー設定は古くなる可能性があり、センサーがグラウンドトゥルースを確立するための最良の監視ポイントを持っていると考えられるからです。DEGREE_MODEL は学習/ヒューリスティックが機能する場所であり、精度を 100% 保証することはできません。

クライアントサーバー検出のヒューリスティックは、この分野でシスコが最善を尽くし、継続的にアルゴリズムを改良しているにも関わらず、うまく機能しない場合があります。こうした場合は、OpenAPIインターフェイスを使用して、既知のサーバーポートにアクセスできます。この設定は過去のフローには適用されず、その時点以降（つまり、今後）のフローのマーキングにのみ影響します。これは、通常の対処方法ではなく、フォールバックの最後の手段として使用できます。

また、特定のフローの全期間中、クライアントサーバーのマーキングを繰り返し切り替えないようにすることも重要です（間違っていたり、内部モデルが変更された場合でも、フローパターンがより多く観測/分析されるにつれて、時間の経過とともに変化します）。同等以上の優先順位の更新により、低い優先順位の更新を上書きできます（既存のフローのクライアントサーバーも切り替わります）。言い換えれば、「フローの存続期間中」のマーキングの粘着性は、度合いモデルベースのマーキングにのみ適用されます。

カンバセーションモード

デフォルトでは、エージェントのフロー分析忠実度モードは「詳細」です。従来は、これが利用可能な唯一のモードであり、観測されたすべてのフローがそれらのフローに関する詳細な統計とともにエージェントによってレポートされていました。統計には、パケット数とバイト数、TCP フラグ、接続統計、ネットワーク遅延、SRTT などが含まれます。

この種のレポートは多くの場合望ましいものですが、レポートと処理のための計算負荷が大きくなります。また、主要なユースケースがセグメンテーションのみの場合は厳密な要件ではない可能性があります。

カンバセーションモードは、従来の詳細モードよりも軽量な代替モードになります。カンバセーションモードのエージェントは、可能な限り（つまり、クライアントとサーバーを正確に分類できる場合はいつでも）フローではなくカンバセーションをレポートすることを目指します。これは、TCP、UDP、および ICMP フローに適用されます。

詳細モードでは、TCP/UDP フローの場合、5 タプルフロー（送信元と宛先の IP、送信元と宛先のポート、およびプロトコル）をレポートします。

一方で、カンバセーションモードでは、送信元ポートは（新しく接続されるたびに変更される）エフェメラルポートであるため、エージェントは送信元ポートを省略し、4 タプルフローにします。

（注） フローを4タプルとして検出することは、クライアントサーバー検出アルゴリズムにも依存しています。このアルゴリズムは、サーバー/宛先ポートがウェルノウンポート（0 ～ 1023）であることに依存しています。

そのため、ウェルノウンサーバー/宛先ポートを使用しないカスタムアプリケーションを使用している場合は、OpenAPIインターフェイスを使用してウェルノウンサーバーポートにアクセスできます。この設定は過去のフローには適用されず、その時点以降（つまり、今後）のフローのマーキングにのみ影響します。サーバーポートを最適化するには、「Client Server Configuration」を参照してください。

カンバセーションモードのエージェントレポートには、トリミングされた情報が含まれています。省略されたフィールドの完全なリストは次のとおりです。TCP/UDP送信元ポート（エフェメラルポート）、順方向/逆方向TCPボトルネック、TCPハンドシェイクバケット、SRTT（マイクロ秒）、順方向/逆方向パケット再送信、利用可能なSRTT、削減された順方向/逆方向輻輳ウィンドウ、変更された順方向/逆方向MSS、順方向/逆方向TCP受信Window Zero、順方向/逆方向バーストインジケータ、順方向/逆方向最大バーストサイズ（KB）。

カンバセーションモードを有効にするには、「ソフトウェアエージェントの設定」に含まれる「フローの可視性設定」セクションを参照してください。

（注） エージェントをカンバセーションモードでレポートするように変更することで得られる確実な利点は、TCPフローのパーセンテージ、既定のサービスポートでリッスンするサービスの数、エージェントのメモリ制限など、複数の要因によって異なる場合があります。

（注） 一部のエージェントの「カンバセーション」モードをオンにすると、フロー検索ページの観測結果にカンバセーションとフローが混在する場合があります。

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。