Firepowerデータパスのトラブルシューティング：概要

内容

概要

このガイドの目的は、Firepower Threat Defense(FTD)デバイスまたはAdaptive Security Appliance(ASA)with FirePOWER Servicesがネットワークトラフィックの問題を引き起こしているかどうかを迅速に特定できるようにすることです。また、Cisco Technical Assistance Center(TAC)に連絡する前に、調査する必要のあるFirepowerコンポーネントと収集するデータを絞り込む際にも役立ちます。

すべてのFirepowerデータパストラブルシューティングシリーズの記事のリスト。

Firepowerデータパスのトラブルシューティングフェーズ1:パケット入力

https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/214574-firepower-data-path-troubleshooting-phas.html

Firepowerデータパスのトラブルシューティングフェーズ2:DAQレイヤ
https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/214575-firepower-data-path-troubleshooting-phas.html

Firepowerデータパスのトラブルシューティングフェーズ3:セキュリティインテリジェンス

https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/214576-firepower-data-path-troubleshooting-phas.html

Firepowerデータパスのトラブルシューティングフェーズ4:アクセス コントロール ポリシー
https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/214577-firepower-data-path-troubleshooting-phas.html

Firepowerデータパスのトラブルシューティングフェーズ5:SSLポリシー
https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/214581-firepower-data-path-troubleshooting-phas.html

Firepowerデータパスのトラブルシューティングフェーズ6:アクティブ認証
https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw-virtual/214608-firepower-data-path-troubleshooting-phas.html

Firepowerデータパスのトラブルシューティングフェーズ7:侵入ポリシー
https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/214609-firepower-data-path-troubleshooting-phas.html

Firepowerデータパスのトラブルシューティングフェーズ8:ネットワーク分析ポリシー

https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/214610-firepower-data-path-troubleshooting-phas.html

前提条件

- この記事では、FTDおよびASAプラットフォームに関する基本的な知識があることを前提としています。
- オープンソースsnortの知識は推奨されますが、必須ではありません。

インストールおよび構成ガイドを含むFirepowerのドキュメントの完全なリストについては、ドキュメントのロードマップページを参照してください。

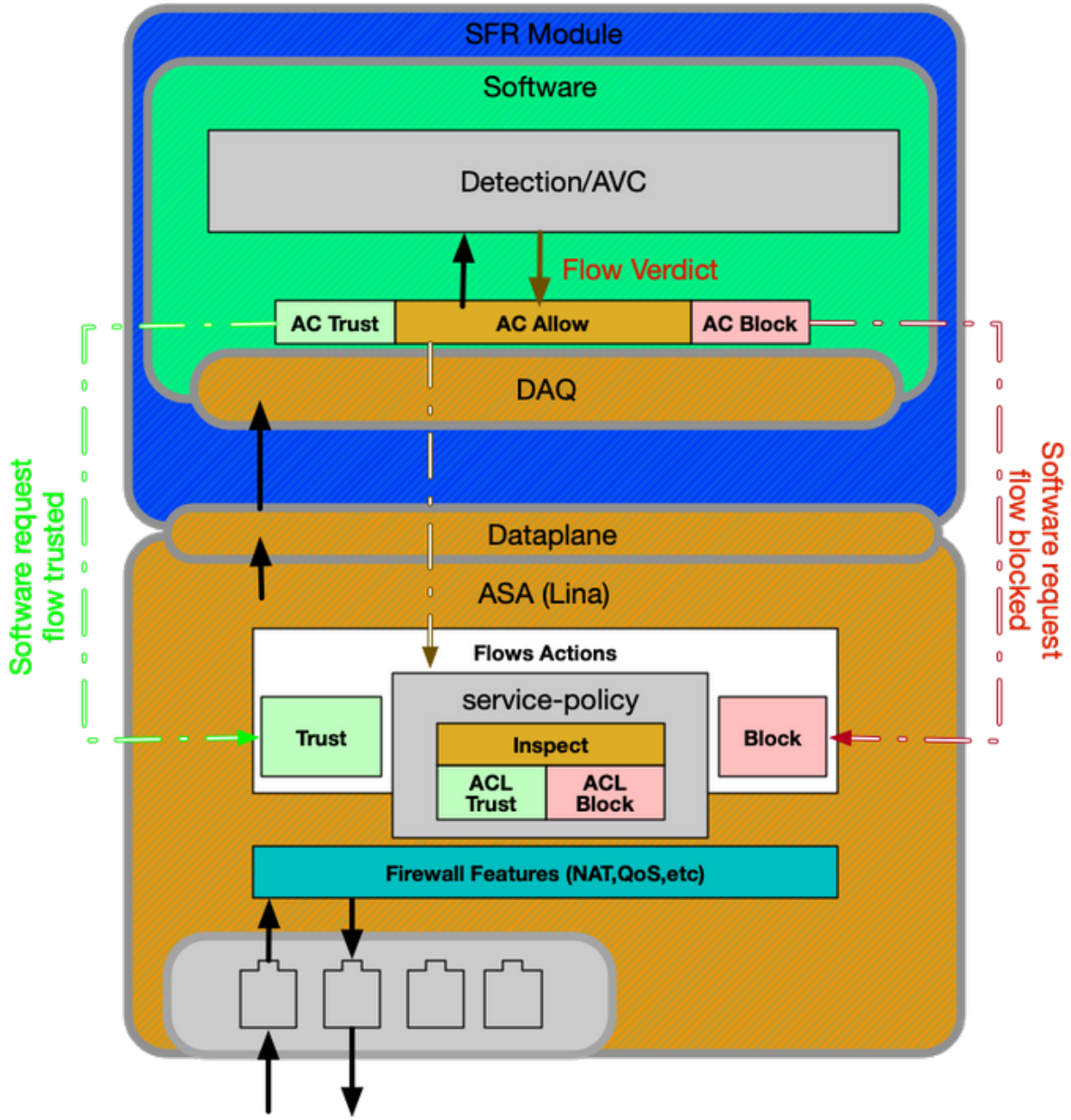
データパスのアーキテクチャの概要

次のセクションでは、さまざまなFirepowerプラットフォームのアーキテクチャデータパスについて説明します。アーキテクチャを念頭に置いて、Firepowerデバイスがトラフィックフローをブロックしているかどうかを迅速に判断する方法に進みます。

> **注**：この記事では、従来のFirepower 7000および8000シリーズデバイス、およびNGIPS（非FTD）仮想プラットフォームについては扱いません。これらのプラットフォームのトラブルシューティングについては、テクニカルノートのページを参照してください。

ASA with FirePOWERサービス（SFRモジュール）プラットフォーム

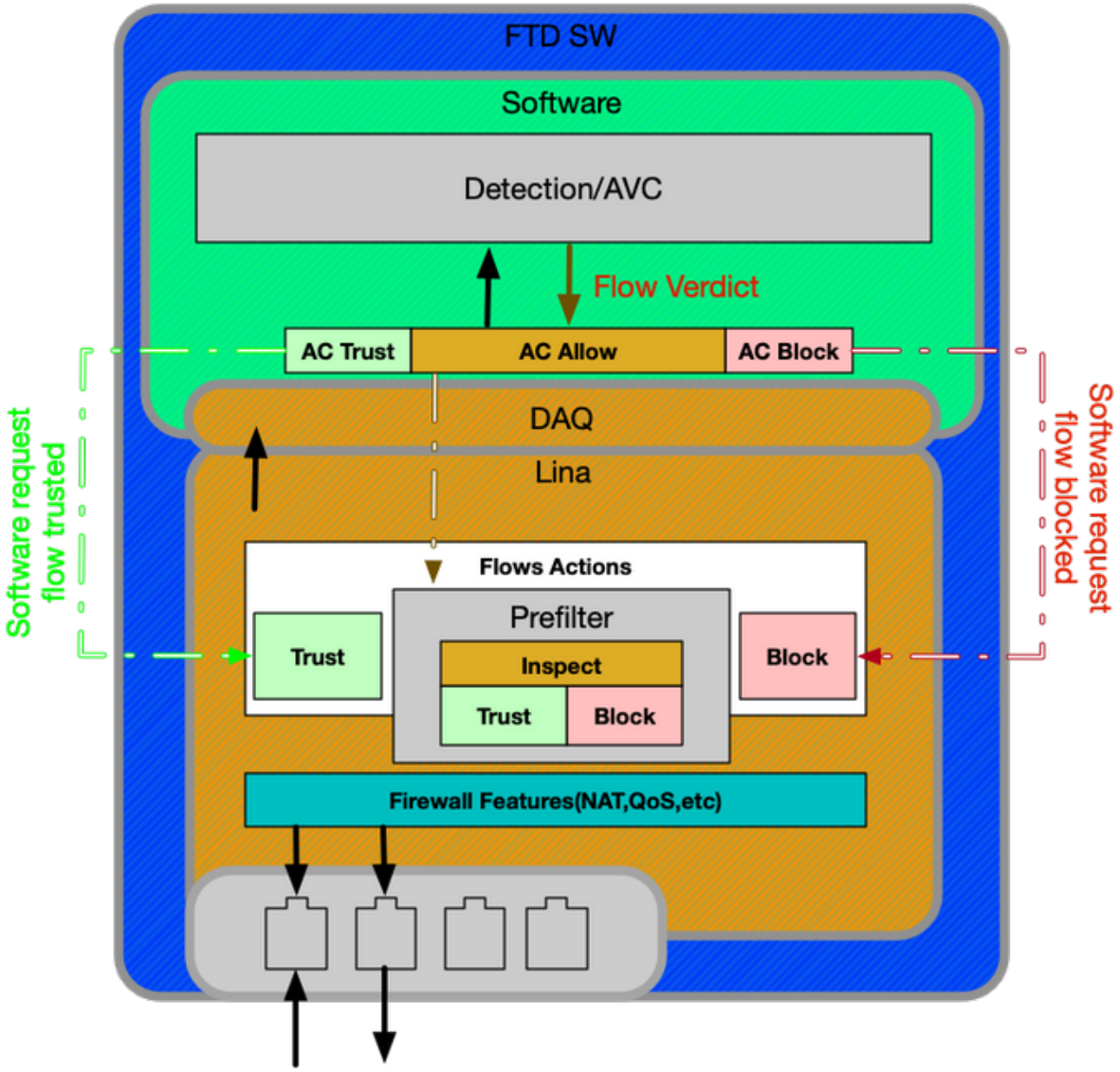
FirePOWERサービスプラットフォームは、SFRモジュールとも呼ばれます。これは基本的に、5500-X ASAプラットフォームで稼働する仮想マシンです。



ASAのサービスポリシーによって、SFRモジュールに送信されるトラフィックが決まります。Firepower Data Acquisition(DAQ)エンジンとの通信に使用されるデータプレーン層があります。このレイヤは、Snortが理解できる方法でパケットを変換するために使用されます。

ASA500-Xおよび仮想FTDプラットフォームでのFirepower Threat Defense

FTDプラットフォームは、Lina(ASA)コードとFirepowerコードの両方を含む1つのイメージで構成されます。このモジュールとSFRモジュールプラットフォームの大きな違いは、LinaとSnortの間の効率的な通信が可能であるということです。

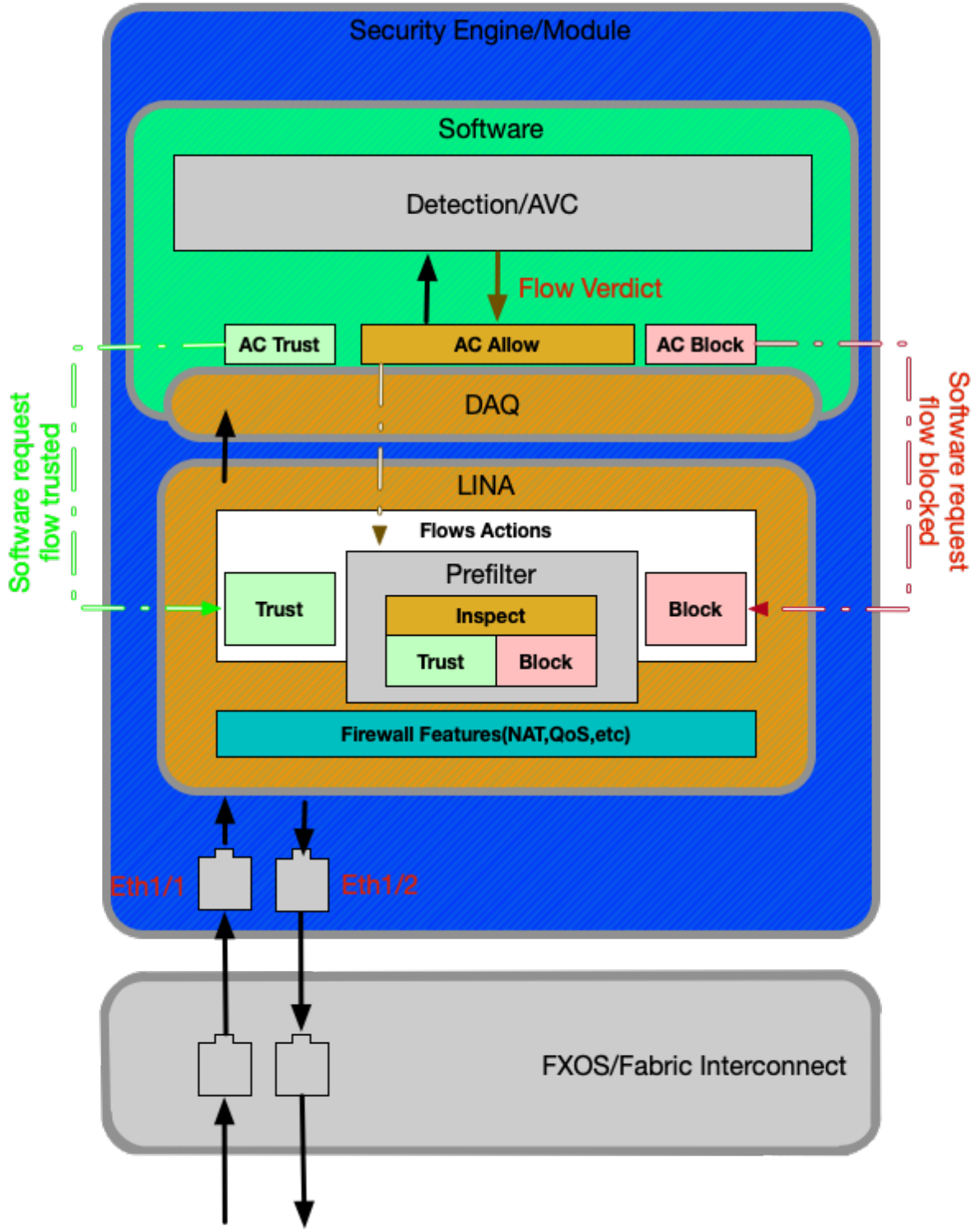


SSPプラットフォームでのFTD

セキュリティサービスプラットフォーム(SSP)モデルでは、FTDソフトウェアは、シャーシハードウェアを管理し、論理デバイスとして知られるさまざまなアプリケーションをホストするために使用される基盤となるOperable System(FXOS)プラットフォーム上で動作します。

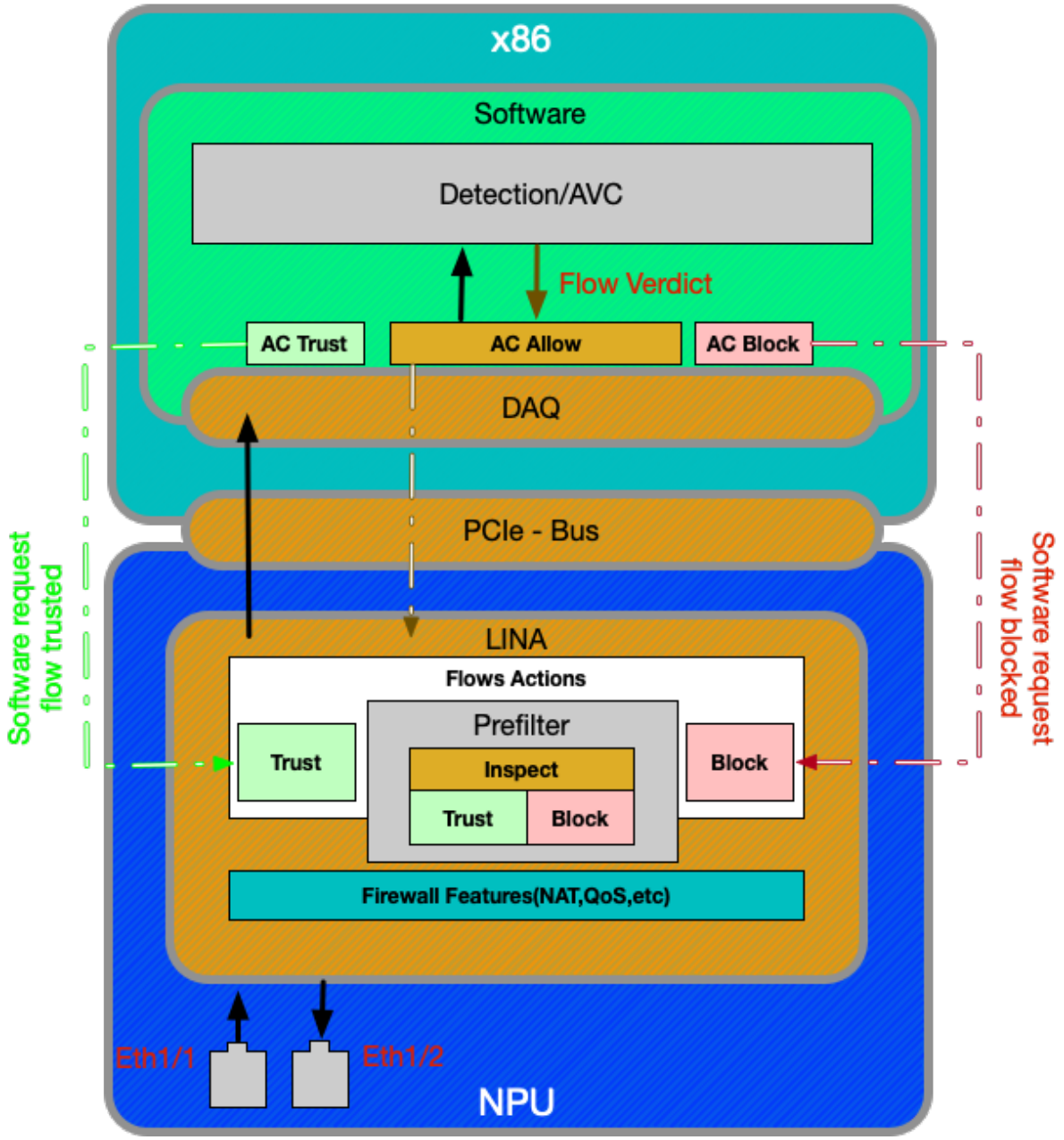
SSPプラットフォーム内には、次の図と説明に示すように、モデル間に違いがあります。

Firepower 9300および4100アプライアンス



Firepower 9300および4100プラットフォームでは、入力パケットと出力パケットは、FXOSファームウェア（ファブリックインターコネクト）によって給電されるスイッチによって処理されます。 その後、パケットは論理デバイスに割り当てられたインターフェイス（この場合はFTD）に送信されます。 その後、パケット処理は非SSP FTDプラットフォーム上と同じです。

Firepower 2100アプライアンス



Firepower 2100デバイスは、非SSP FTDプラットフォームと同様に機能します。9300および4100モデルに存在するファブリックインターコネクトレイヤは含まれません。ただし、2100シリーズのデバイスは他のデバイスと大きく異なり、特定用途向け集積回路(ASIC)が存在します。 従来のASA機能(Lina)はすべてASIC上で実行され、次世代ファイアウォール(NGFW)機能（Snort、URLフィルタリングなど）はすべて従来のx86アーキテクチャ上で実行されます。このプラットフォームでLinaとSnortが通信する方法は、Peripheral Component Interconnect Express(PCIe)経由でパケットキューを介する方法です。他のプラットフォームは、Direct Memory Access(DMA)を使用してパケットをSnortにキューイングします。

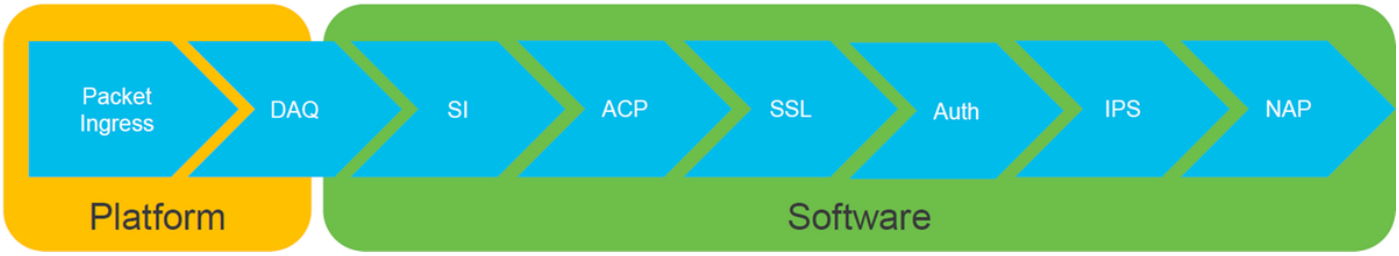
> **注**：FTD非SSPプラットフォームのトラブルシューティングと同じ方法は、FPR-2100プラットフォームで行います。

Firepowerデータパスのトラブルシューティングに推奨されるプロセス

ここでは、固有のトラフィックの識別方法と、Firepowerプラットフォームの基本的なデータパスアーキテクチャについて説明しました。ここでは、パケットをドロップできる特定の場所につい

て説明します。データパスに関する記事では、8つの基本コンポーネントについて説明しています。これらのコンポーネントは、パケット廃棄の可能性を体系的に判断するためにトラブルシューティングを行うことができます。802.11 の標準規格には以下があります。

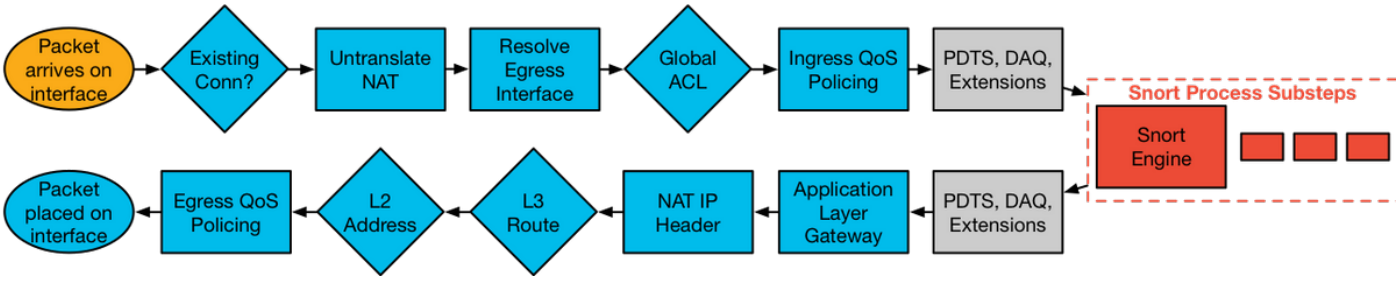
1. パケット入力
2. Firepower DAQレイヤ
3. セキュリティインテリジェンス
4. アクセス コントロール ポリシー
5. SSLポリシー
6. アクティブ認証機能
7. 侵入ポリシー（IPSルール）
8. ネットワーク分析ポリシー（Snortプリプロセッサ設定）



注：これらのコンポーネントは、Firepower処理の正確な操作順序に記載されていませんが、推奨されるトラブルシューティングワークフローに従って発注されます。パケットダイアグラムの実際のパスについては、次の図を参照してください。

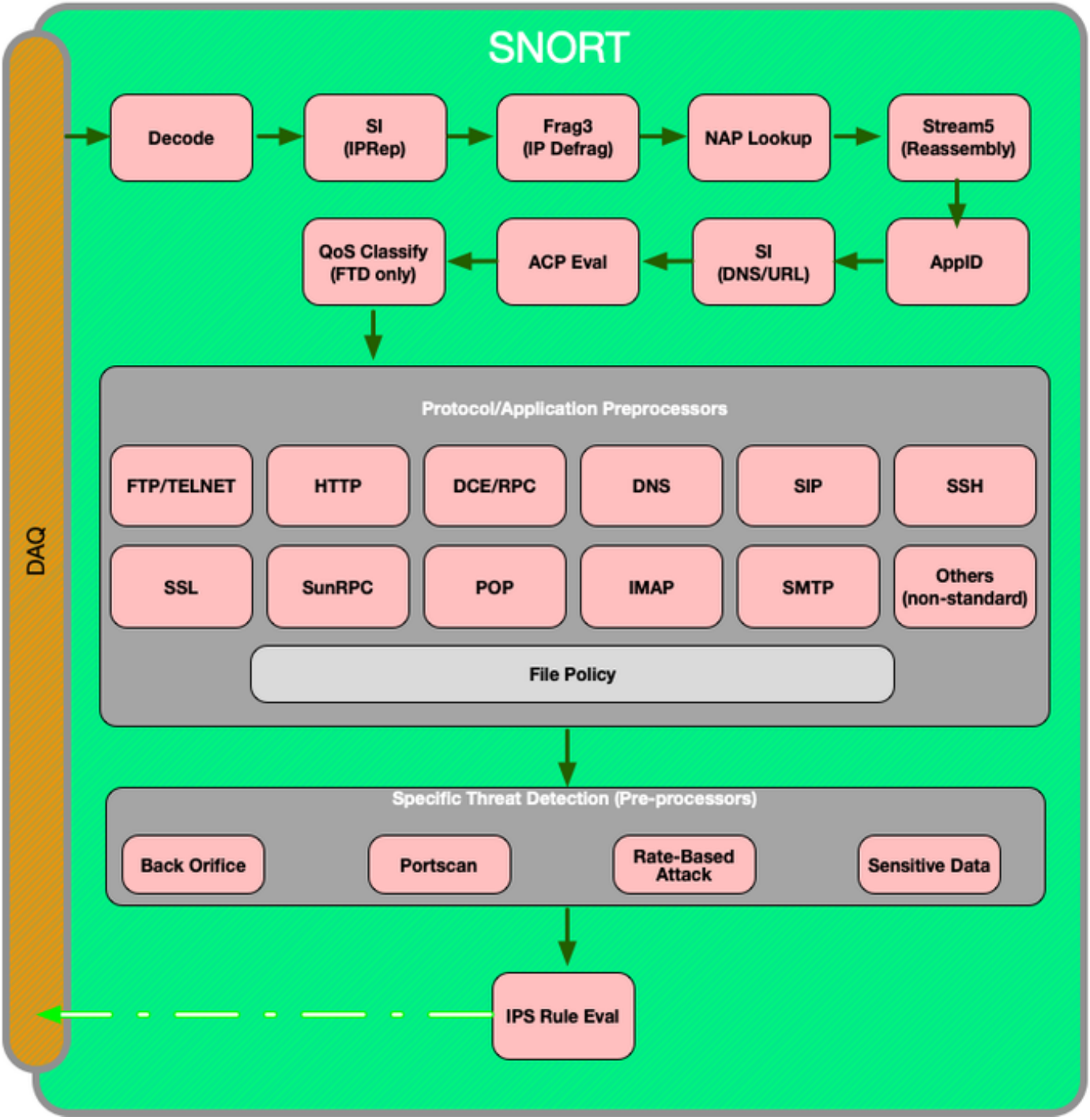
FTDを通過するパケットの実際のパス

次の図は、FTDを通過するパケットの実際のパスを示しています。



Snortパケットパス

次の図は、Snort工ンジンを通過するパケットのパスを示しています。



パケットの入出力

最初のデータパスのトラブルシューティング手順は、パケット処理の入力または出力ステージでドロップが発生していないことを確認することです。パケットが入力されているにもかかわらず出力されない場合は、そのパケットがデータパス内のどこかの場所でデバイスによってドロップされていることを確認できます。

この記事では、Firepowerシステムでのパケットの入出力のトラブルシューティング方法について説明します。

Firepower DAQレイヤ

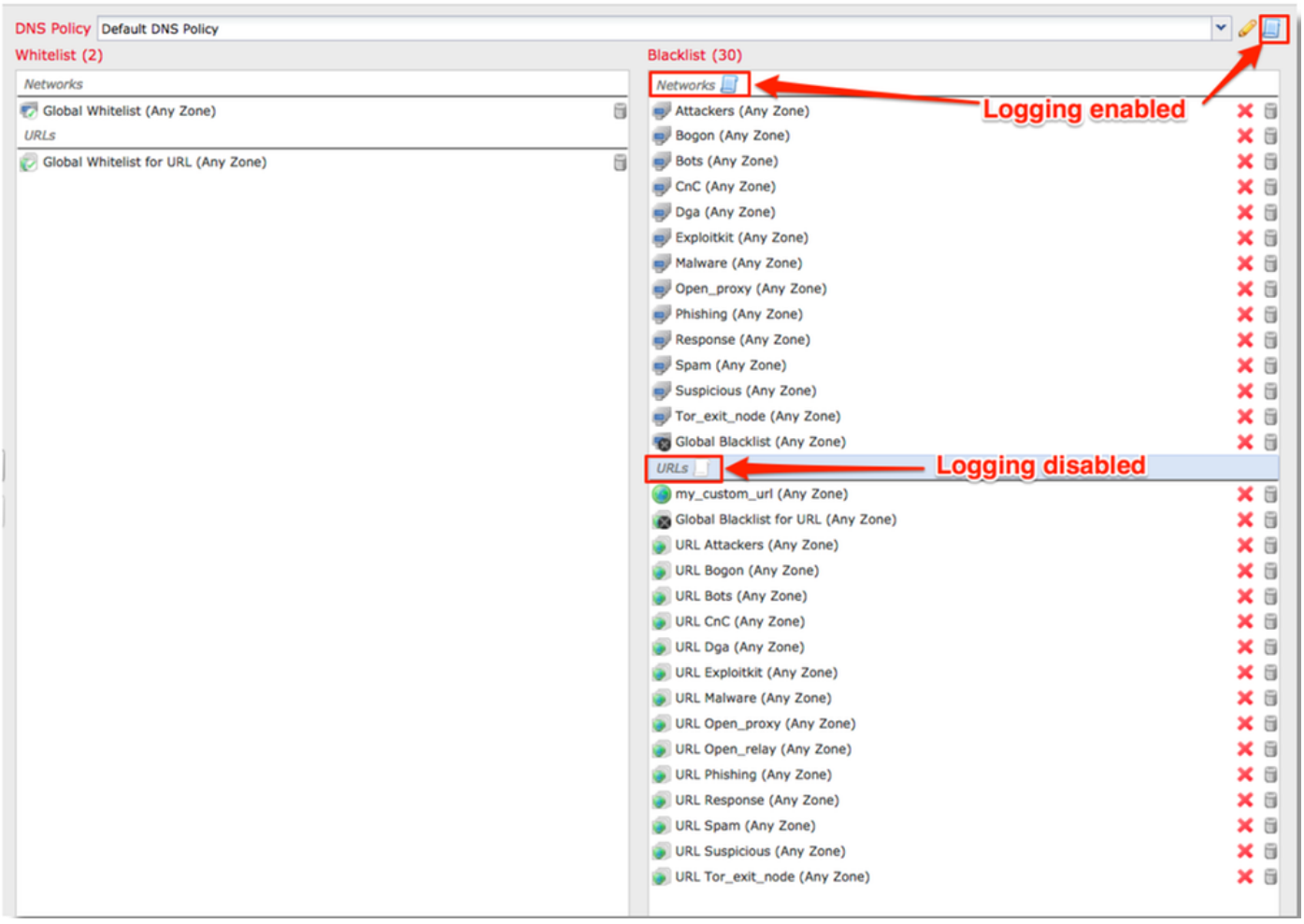
パケットが入り込んでいるが出て来ないと判断された場合は、Firepower DAQ(Data Acquisition)レイヤでデータパスのトラブルシューティングの次のステップを行い、対象のトラフィックがFirepowerに送信されていることを確認します。

この記事では、Firepowerによるトラフィックの初期処理と、アプライアンス全体で行われているパスのトラブルシューティング方法について説明します。

また、Firepowerデバイスを完全にバイパスして、Firepowerコンポーネントがトラフィックの問題の原因であるかどうかを判断する方法についても説明します。

セキュリティインテリジェンス

セキュリティインテリジェンスは、トラフィックを検査するFirepower内の最初のコンポーネントです。このレベルのブロックは、ロギングが有効である限り簡単に判別できます。これは、FMCのGUIで、[Policies] > [Access Control] > [Access Control Policy]の順に移動**して確認できます**。該当するポリシーの横にある編集アイコンをクリックした後、[セキュリティインテリジェンス]**タブに移動**します。

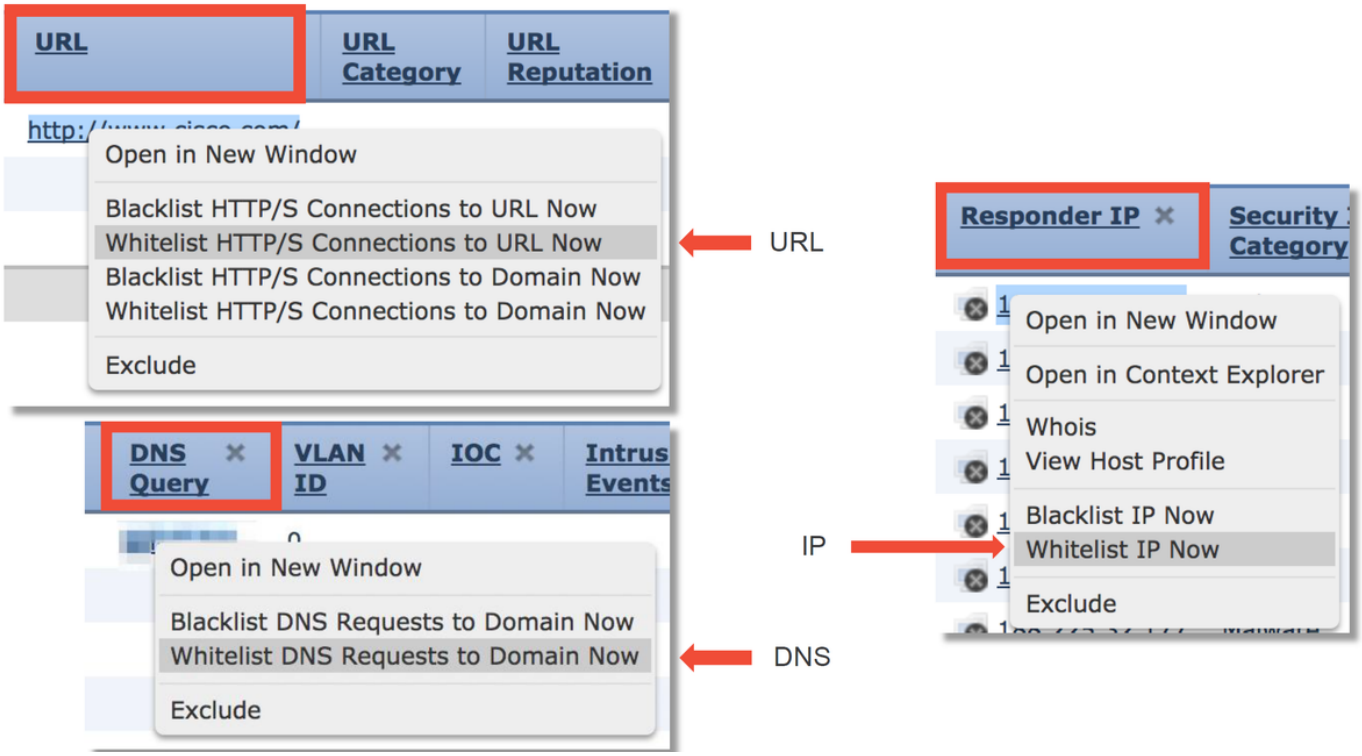


ロギングを有効にすると、[Analysis] > [Connections] > [Security Intelligence Events]の下に

Security Intelligence Events**が表示されます**。トラフィックがブロックされている理由は明確である必要があります。

First Packet	Last Packet	Action	Reason	Initiator IP	Responder IP	Security Intelligence Category
2017-05-16 17:00:16		Domain Not Found	DNS Block	192.168.1.95		DNS Response
2017-05-16 16:57:50	2017-05-16 16:57:50	Block	URL Block	192.168.1.95	10.83.48.40	my_custom_url
2017-05-16 16:50:05		Block	IP Block	192.168.1.95		Malware

簡単な対応策として、セキュリティインテリジェンス機能によってブロックされているIP、URL、またはDNSクエリを右クリックし、ホワイトリストオプションを選択できます。



ブラックリストに誤って何かが入ったと思われる場合、またはレピュテーションの変更を要求する場合は、次のリンクでCisco Talosから直接チケットを開くことができます。

https://www.talosintelligence.com/reputation_center/support

また、TACにデータを提供して、ブロックされている内容をレポートし、ブラックリストから削除されたエントリを持っている可能性もあります。

セキュリティインテリジェンスコンポーネントの詳細なトラブルシューティングについては、関連するデータパスのトラブルシューティングの記事を参照してください。

アクセス コントロール ポリシー

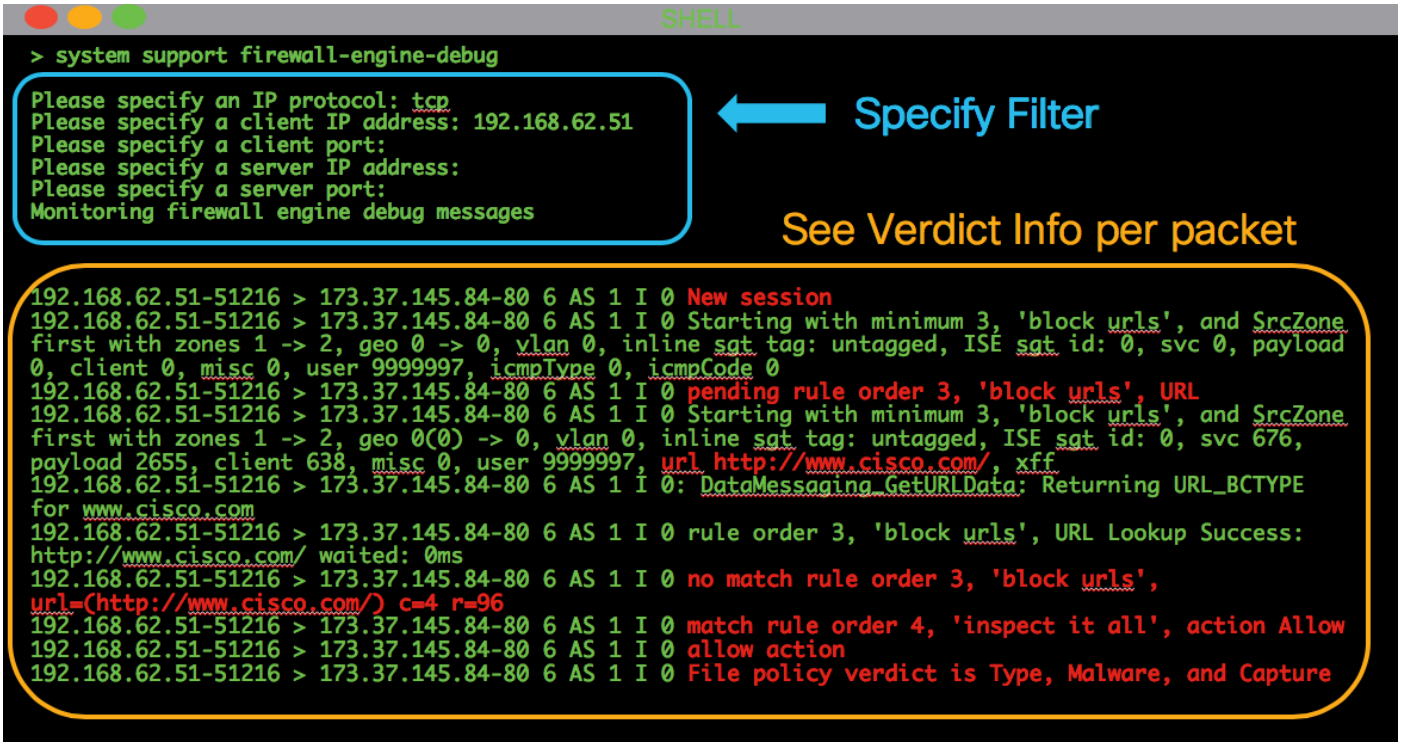
Security Intelligence機能がトラフィックをブロックしていないと判断された場合は、次にAccess Control Policy（ACE；アクセスコントロールポリシー）ルールをトラブルシューティングして、「ブロック」アクションを持つルールがトラフィックをドロップしているかどうかを確認することを推奨します。

コマンド「firewall-engine-debug」を使用するか、トレースを使用してキャプチャすることを推奨

します。一般的に、これらのツールを使用すると、すぐに回答を得ることができ、トラフィックがどのルールに達しているか、どのような理由でトラフィックが到達しているかを伝えることができます。

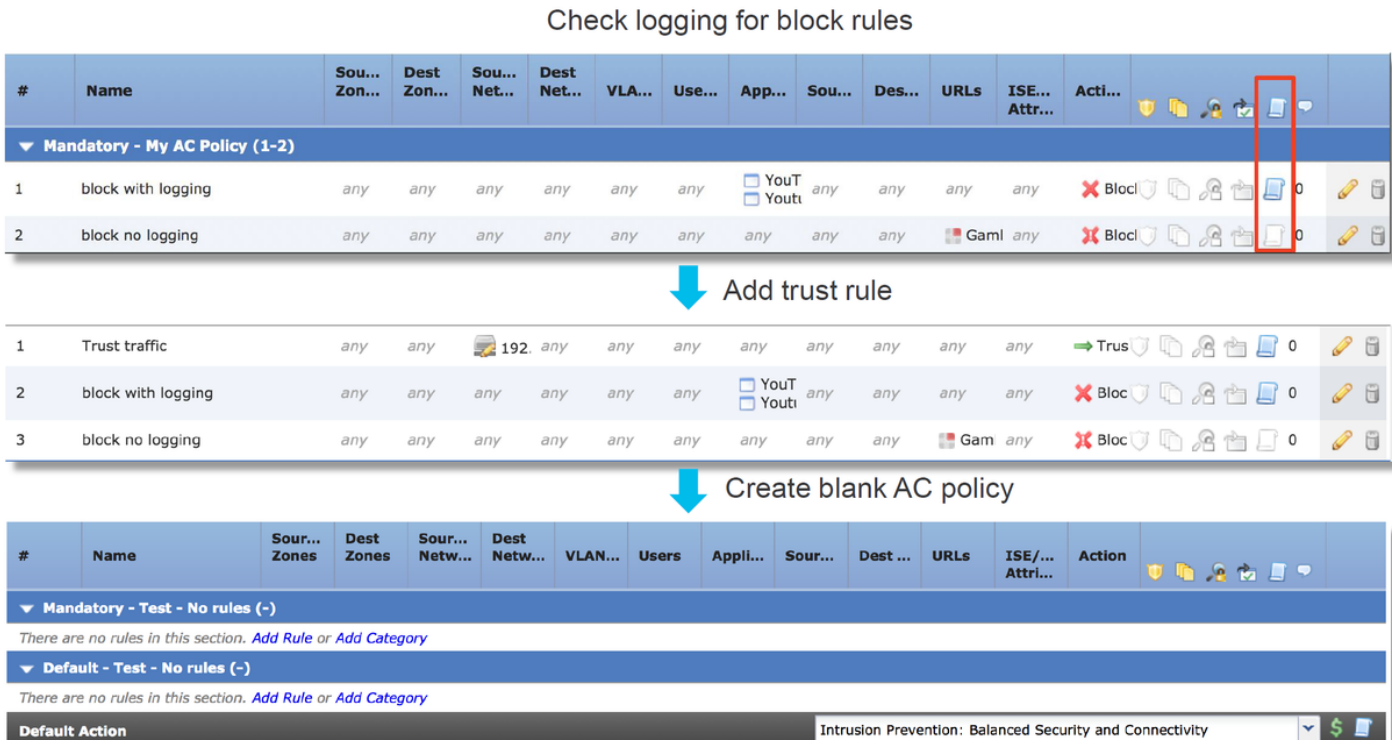
- 次のコマンドを使用して、Firepower CLIでデバッグを実行し、トラフィックをブロックしているルールを確認します（可能な限り多くのパラメータを入力してください）。**> system support firewall-engine-debug**
- デバッグ出力は、分析のためにTACに提供できます

次に、アクセスコントロールルールと一致するトラフィックのルール評価と「Allow」のアクションを示す出力例を示します。



どのアクセスコントロール(AC)ルールが一致しているかを判別できない場合、または上記のツールを使用してACポリシーが問題であるかどうかを判別できない場合は、アクセスコントロールポリシーのトラブルシューティングの基本的な手順を次に示します（ポリシーの変更や導入が必要です）。

- 「ブロック」アクションを使用するルールのロギングを有効にする
- それでもトラフィックの接続イベントが表示されず、トラフィックがブロックされている場合は、次に緩和ステップとして、該当するトラフィックの信頼ルールを作成します
- トラフィックの信頼ルールでも問題が解決せず、ACポリシーに問題があると疑われる場合は、次に、[Block All Traffic]以外のデフォルトアクションを使用して、可能であれば新しい空のアクセスコントロールポリシーを作成します

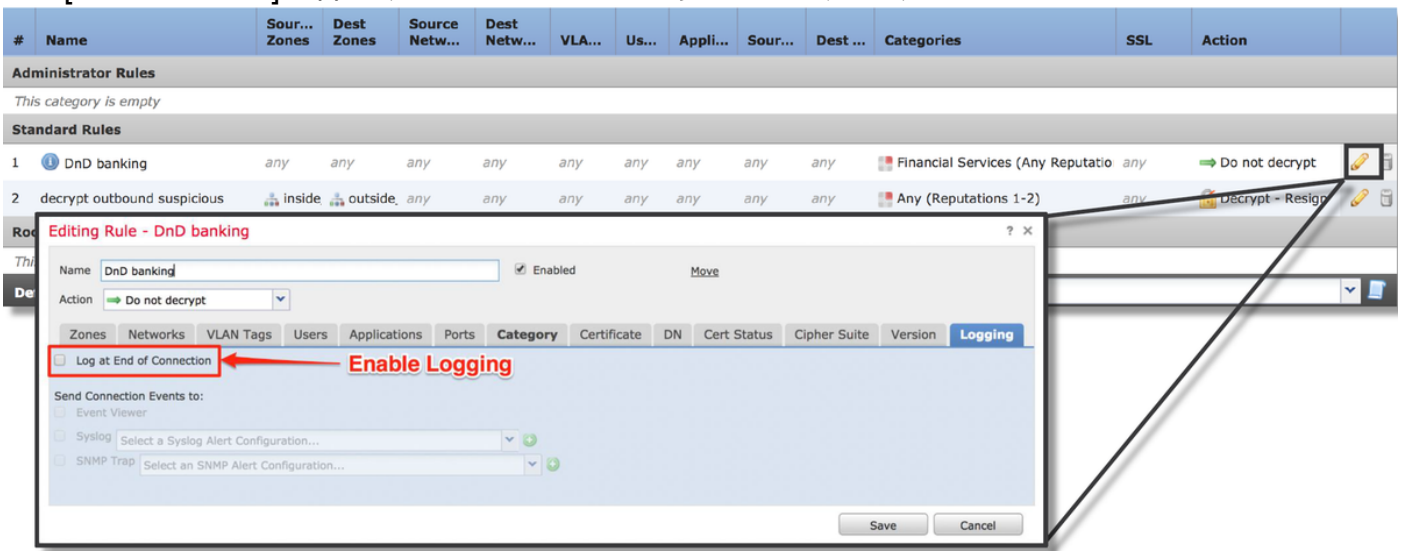


アクセスコントロールポリシーの詳細なトラブルシューティングについては、関連するデータパスのトラブルシューティング記事を参照してください。

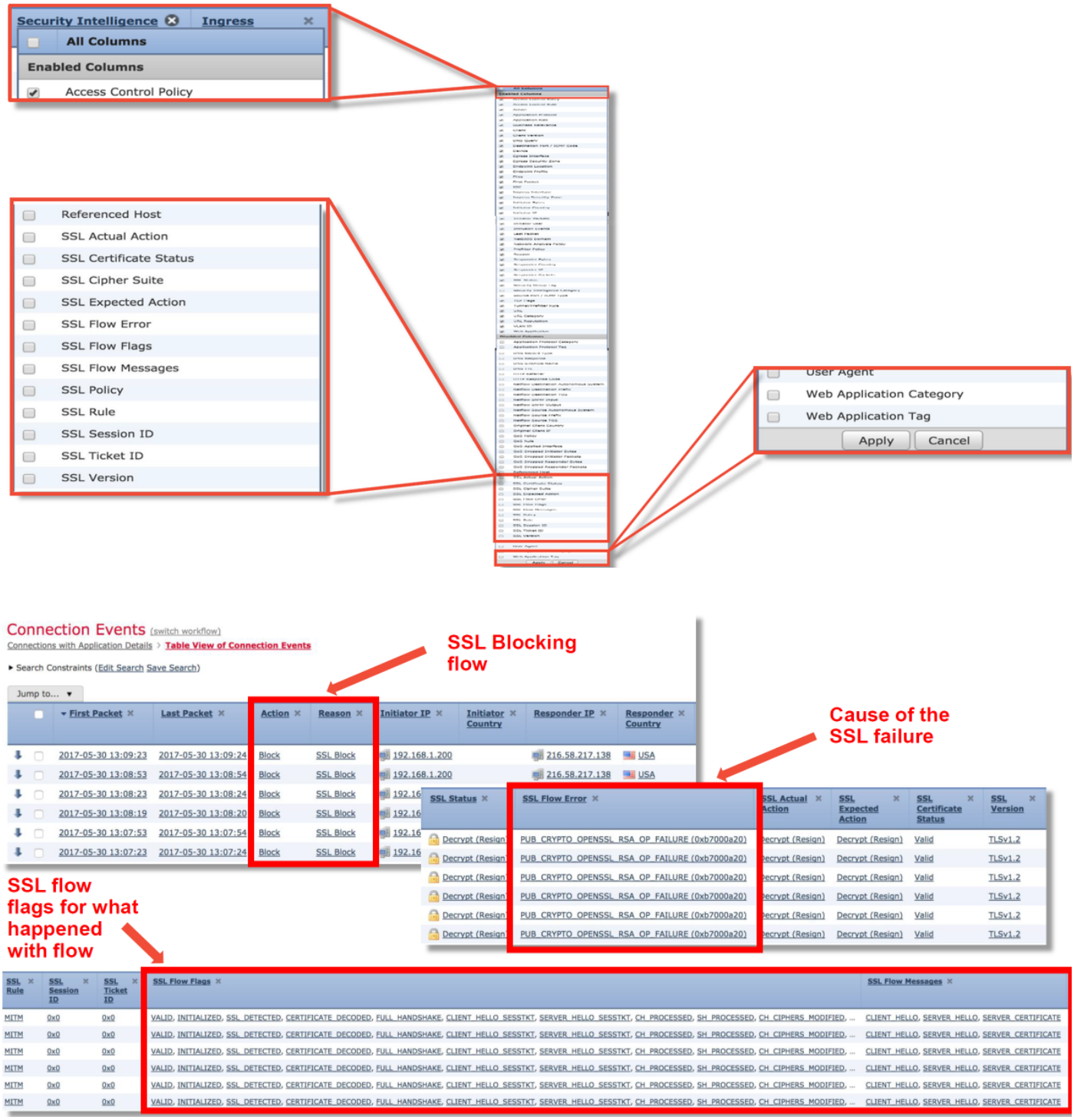
SSLポリシー

SSLポリシーが使用されている場合、トラフィックがブロックされている可能性があります。SSLポリシーのトラブルシューティングの基本的な手順を次に示します。

- [Default Action]を含むすべてのルールのロギングを有効にする



- [Undecryptable Actions]タブで、トラフィックをブロックするオプションが設定されているかどうかを確認します
- [Connection events]セクションで、名前に「SSL」が含まれるすべてのフィールドをチェックします
  ほとんどの機能はデフォルトで無効になっており、任意の列名の横にある十字をクリックして[接続イベント]ビューアで有効にする必要があります



- 軽減ステップとして[Do not Decrypt]をデフォルトアクションとして使用して、空のSSLポリシーを作成します
- 緩和ステップとして、アクセスコントロールポリシーからSSLポリシーを削除します これは[詳細設定]タブで設定します

SSLポリシーはトラフィックのドロップの疑いがあり、ポリシー設定とともに接続イベントをTACに送信できます。

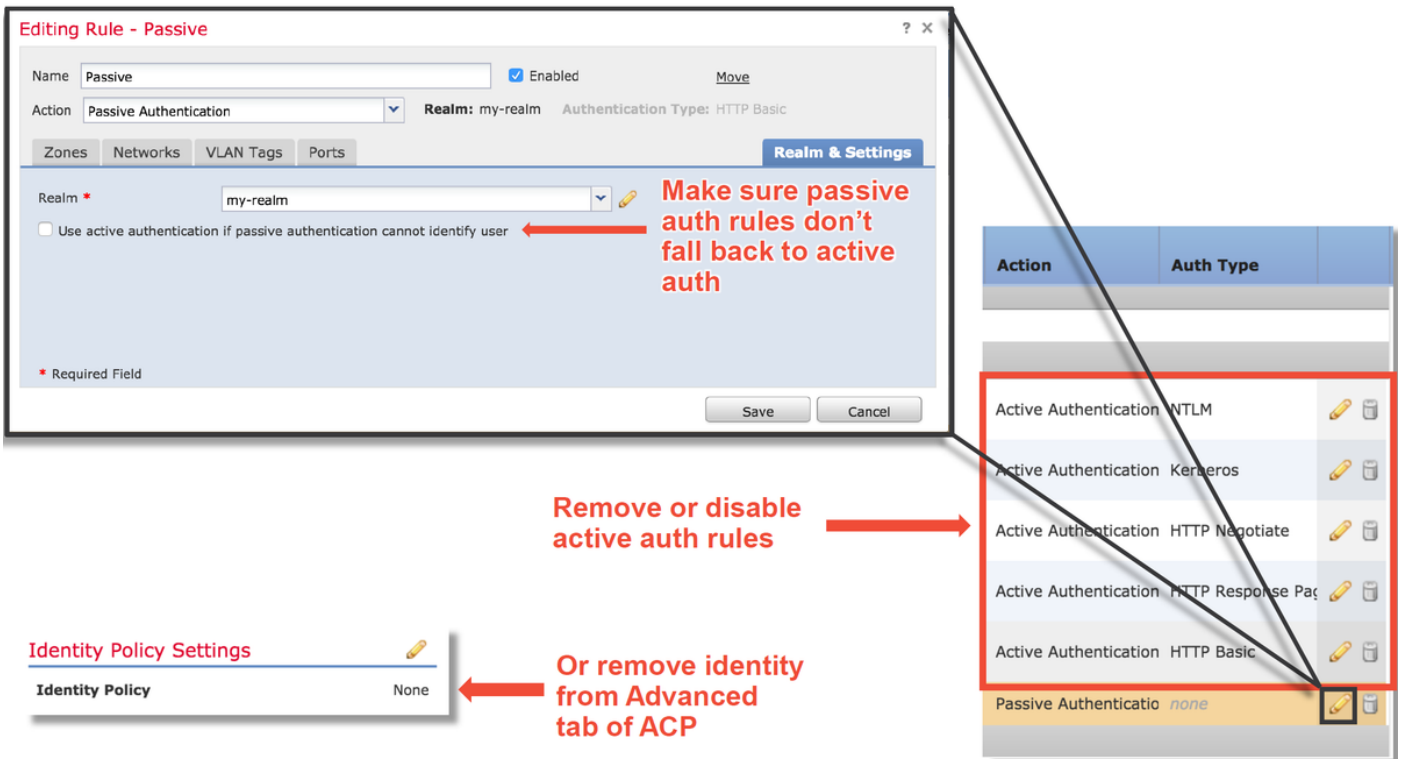
SSLポリシーの詳細なトラブルシューティングについては、関連するデータパスのトラブルシューティング記事を参照してください。

アクティブ認証

アイデンティティポリシーでアクティブ認証を使用すると、何らかの問題が発生した場合に許可する必要があるトラフィックをドロップできます。アクティブ認証機能自体は、ユーザの認証が必要と判断された場合、これらはすべてHTTPプロトコルでのみ行われるため、すべてのHTTP/HTTPSトラフィックに直接影響を与える可能性があります。つまり、ユーザに基づいてブロックする特定のアクセスコントロールルールがあり、ユーザがFTDのアクティブ認証サービスを介して認証できない場合を除き、アクティブ認証は他のネットワークサービス（DNS、ICMPなど）に影響を与えません。ただし、これはアクティブな認証機能の直接的な問題ではありませんが、ユーザが認証できず、認証されていないユーザをブロックするポリシーを持つことの結果です。

迅速な緩和手順は、「アクティブ認証」のアクションでアイデンティティポリシー内のルールを無効にすることです。

また、[Passive Authentication]アクションを実行するルールで、[Use active authentication if passive authentication cannot identify user]オプションがオンになっていないことを確認します。



アクティブ認証の詳細なトラブルシューティングについては、関連するデータパスのトラブルシューティングの記事を参照してください。

侵入ポリシー

侵入ポリシーがトラフィックをドロップしているか、ネットワーク遅延を引き起こしている可能性があります。侵入ポリシーは、アクセスコントロールポリシー内の次の3つの場所のいずれかで使用できます。

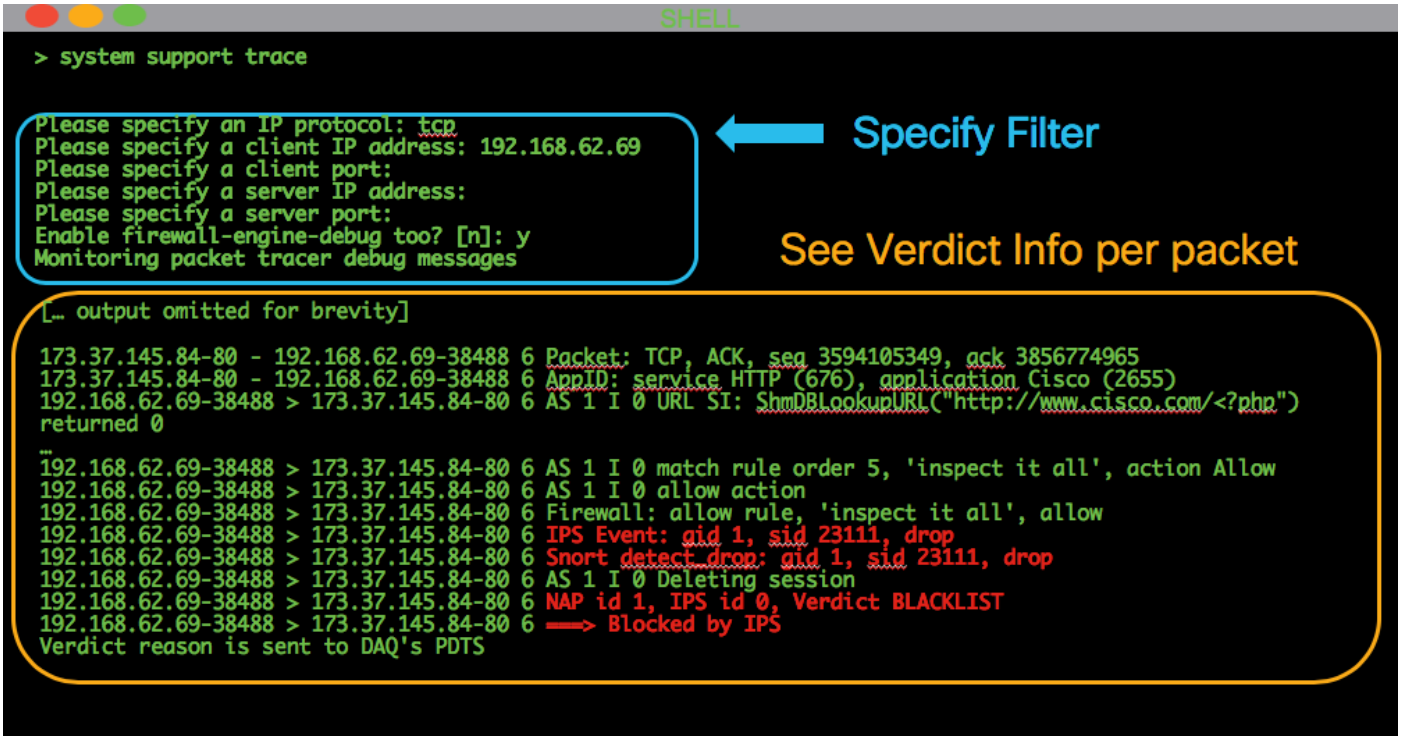
- アクセスコントロールルールの[Inspection]タブ内
- デフォルトアクション
- [Advanced]タブの**[Network Analysis and Intrusion Policies] > [Intrusion Policy used before Access Control rule is determined]セクションで、**

侵入ポリシールールがトラフィックをブロックしているかどうかを確認するには、FMCの**[Analysis] > [Intrusion] > [Events]**ページに移動します。**[Table View of Intrusion Events]ビューは**

、イベントに関連するホストに関する情報を提供します。イベント分析に関する情報については、関連するデータパスのトラブルシューティング記事を参照してください。

侵入ポリシーシグニチャ(IPS)がトラフィックをブロックしているかどうかを判断するための最初の推奨手順は、FTDのCLIから**>システムサポートトレース機能を使用する**ことです。このdebugコマンドは、firewall-engine-debugと同様の方法で動作し、トレースと共にfirewall-engine-debugを有効にするオプションも提供します。

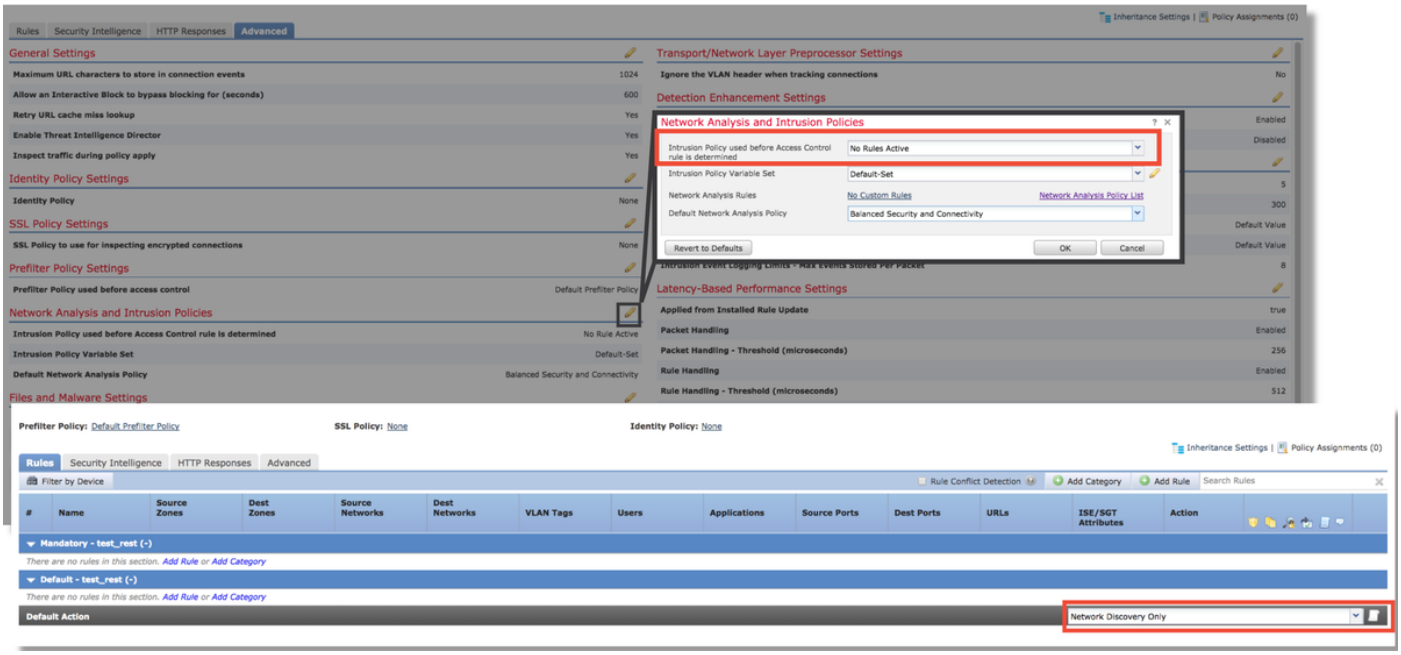
次の図は、侵入ルールによりパケットがブロックされたことを示すシステムサポートトレースツールの使用例を示しています。これにより、GID(Group Identifier)、SID(Signature Identifier)、NAP(Network Analysis Policy) ID、IPS IDなどのすべての詳細が表示されるため、このトラフィックをブロックしているポリシー/ルールを正確に確認できます。



IPSがトレース出力をブロックしているかどうかは判別できないが、カスタム侵入ポリシーによりIPSがドロップしていると疑われる場合は、侵入ポリシーを「Balanced Security and Connectivity」ポリシーまたは「Connectivity over Security」ポリシーに置き換えます。これらは、シスコが提供する侵入ポリシーです。この変更を行うことで問題が解決した場合は、以前に使用したカスタム侵入ポリシーをTACでトラブルシューティングできます。デフォルトのシスコポリシーがすでに使用されている場合は、ルールが少ないため、デフォルトをセキュリティの低いポリシーに変更してみてください。そのため、範囲を絞り込むことができます。たとえば、トラフィックがブロックされ、バランスの取れたポリシーを使用している場合は、セキュリティポリシーを介した接続に切り替えて問題が解決すると、バランスの取れたポリシーでドロップに設定されていないトラフィックをドロップするルールが存在する可能性があります。

アクセスコントロールポリシー内で次の変更を行い、すべての侵入ポリシーインスペクションブロックの可能性を排除できます（セキュリティの有効性を変えないように可能な限り少ない変更を行うことをお勧めします。ポリシー全体でIPSを無効にすることはお勧めします）。

- すべてのアクセスコントロールルール（または特定のトラフィックが一致するルールのみ）で、[Inspection]タブから侵入ポリシーを削除します
- [Advanced]タブの**[Network Analysis and Intrusion Policies] > [Intrusion Policy used before Access Control rule is determined]セクションで、[No Rules Active]ポリシーを選択します。**



それでも問題が解決しない場合は、ネットワーク分析ポリシーのトラブルシューティングに進んでください。

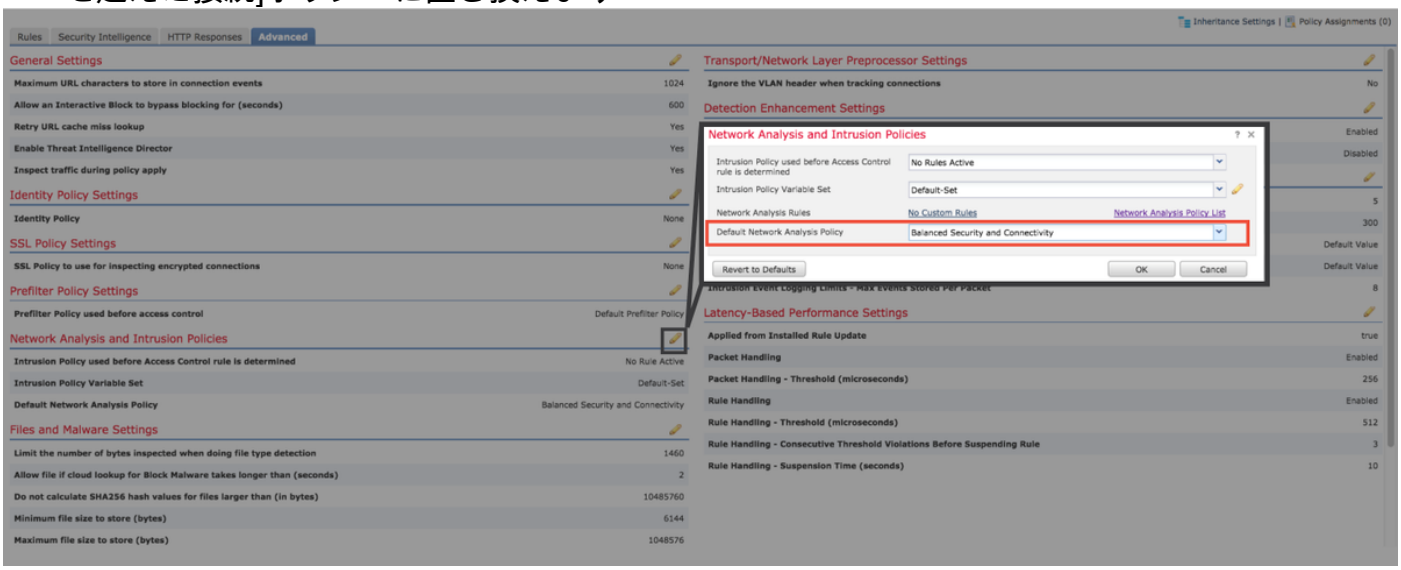
侵入ポリシー機能の詳細なトラブルシューティングについては、関連するデータパスのトラブルシューティング記事を参照してください。

ネットワーク分析ポリシー

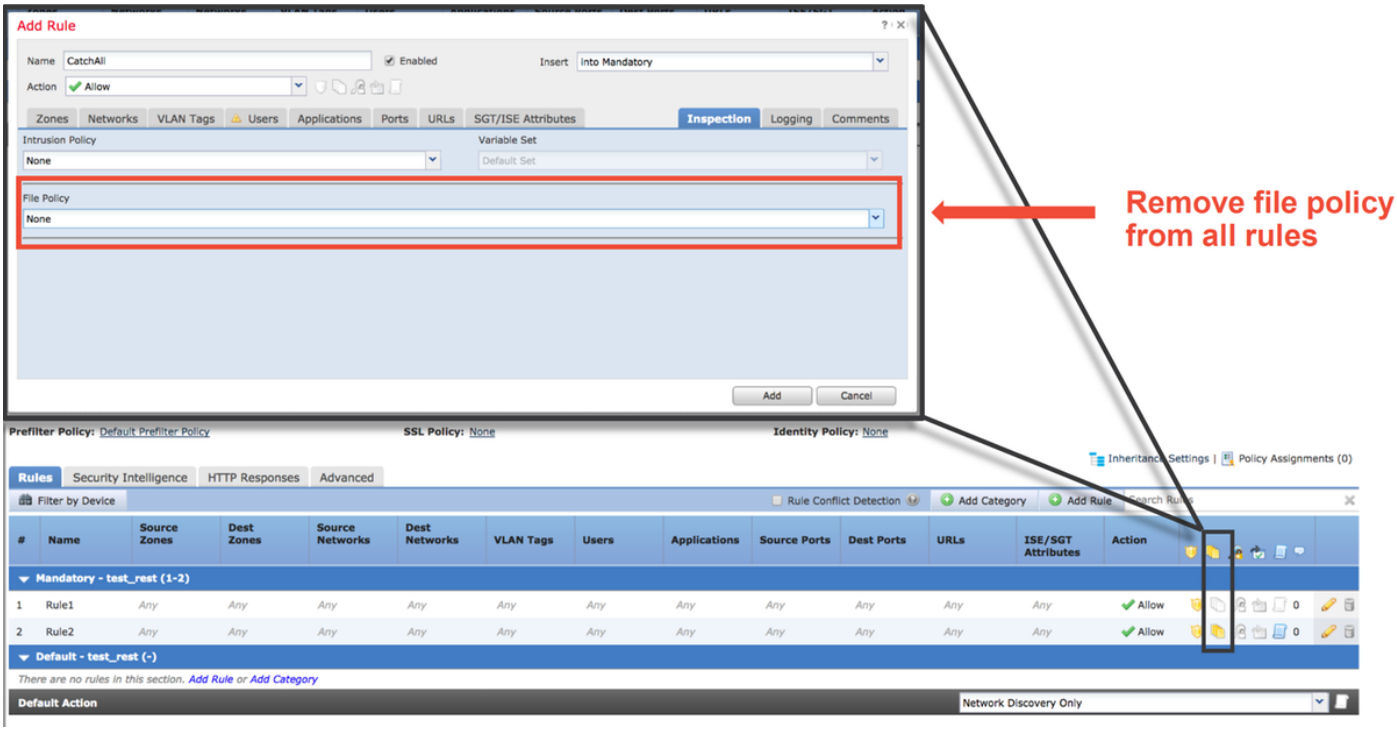
ネットワーク分析ポリシー(NAP)にはFirepowerのプリプロセッサ設定が含まれており、一部の設定ではトラフィックがドロップされる可能性があります。これをトラブルシューティングするための最初の推奨ステップは、IPSのトラブルシューティングと同じです。これは、**> system support traceツールを使用して、Snortでトラフィックをブロックしている内容を検索する**方法です。このツールと使用例の詳細については、上記の「侵入ポリシー」セクションを参照してください。

NAPで発生する可能性のある問題を迅速に軽減するには、次の手順を実行します。

- カスタムNAPを使用している場合は、[セキュリティと接続のバランス]または[セキュリティを超えた接続]ポリシーに置き換えます



- [カスタムルール]が使用されている場合は、NAPを上記のいずれかのデフォルトに設定してください
- アクセスコントロールルールでファイルポリシーが使用されている場合は、ファイルポリシーを一時的に削除します。ファイルポリシーは、バックエンドでプリプロセッサ設定を有効にできますが、GUIには反映されません



ネットワーク分析ポリシー機能の詳細なトラブルシューティングについては、この記事で確認できます。

関連情報

Firepowerドキュメントへのリンク

https://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-roadmap.html