

Firepowerデータパスのトラブルシューティング : 概要

内容

[概要](#)

[前提条件](#)

[データパスのアーキテクチャの概要](#)

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

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

[SSPプラットフォームでのFTD](#)

[Firepower 9300および4100アプライアンス](#)

[Firepower 2100アプライアンス](#)

[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](#)

[FTDを通過するパケットの実際のパス](#)

[Snortパケットパス](#)

[パケットの入出力](#)

[Firepower DAQレイヤ](#)

[セキュリティインテリジェンス](#)

[アクセスコントロール ポリシー](#)

[SSLポリシー](#)

[アクティブ認証](#)

[侵入ポリシー](#)

[ネットワーク分析ポリシー](#)

[関連情報](#)

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、調査する必要がある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](#)。

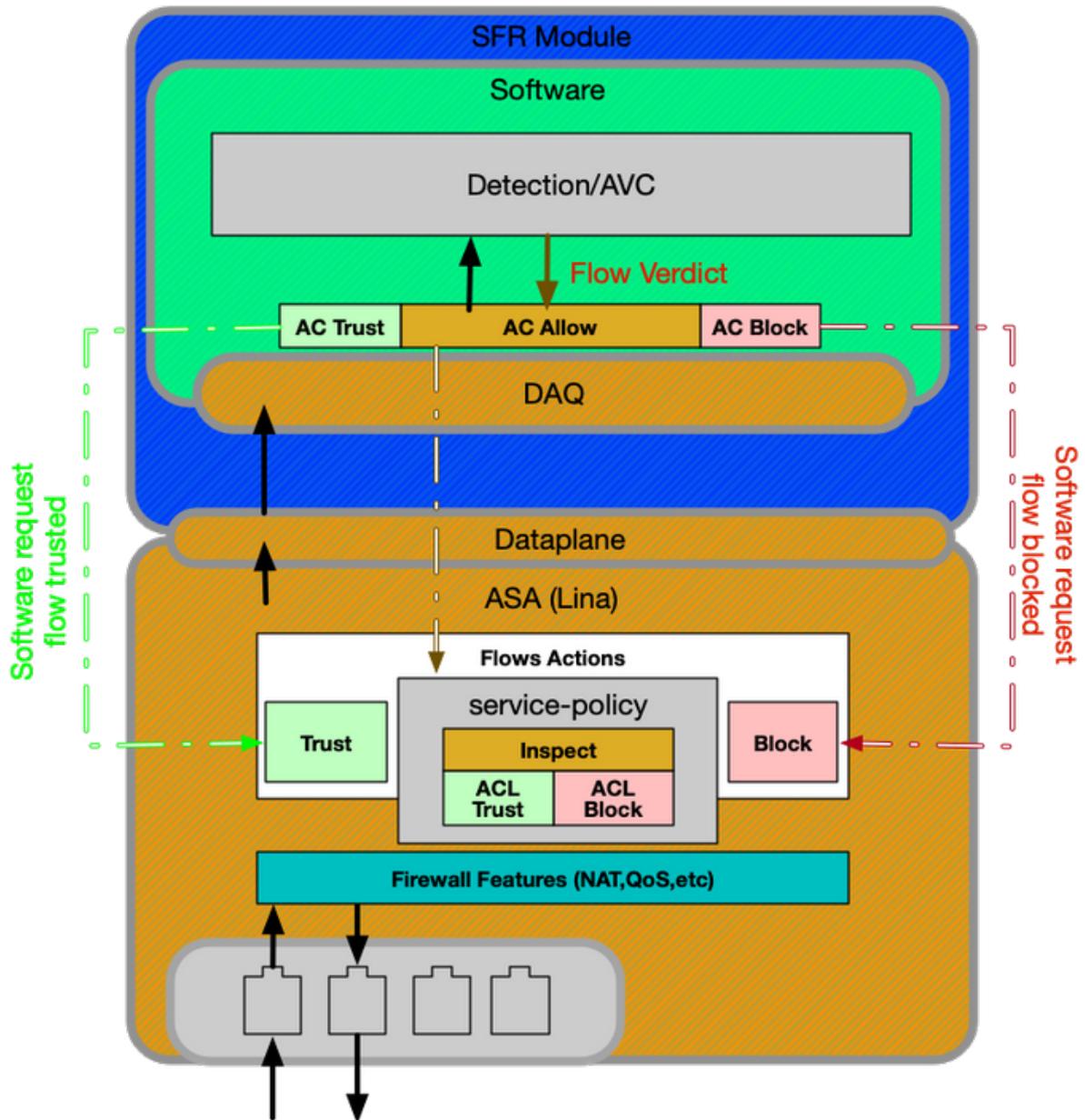
データパスのアーキテクチャの概要

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

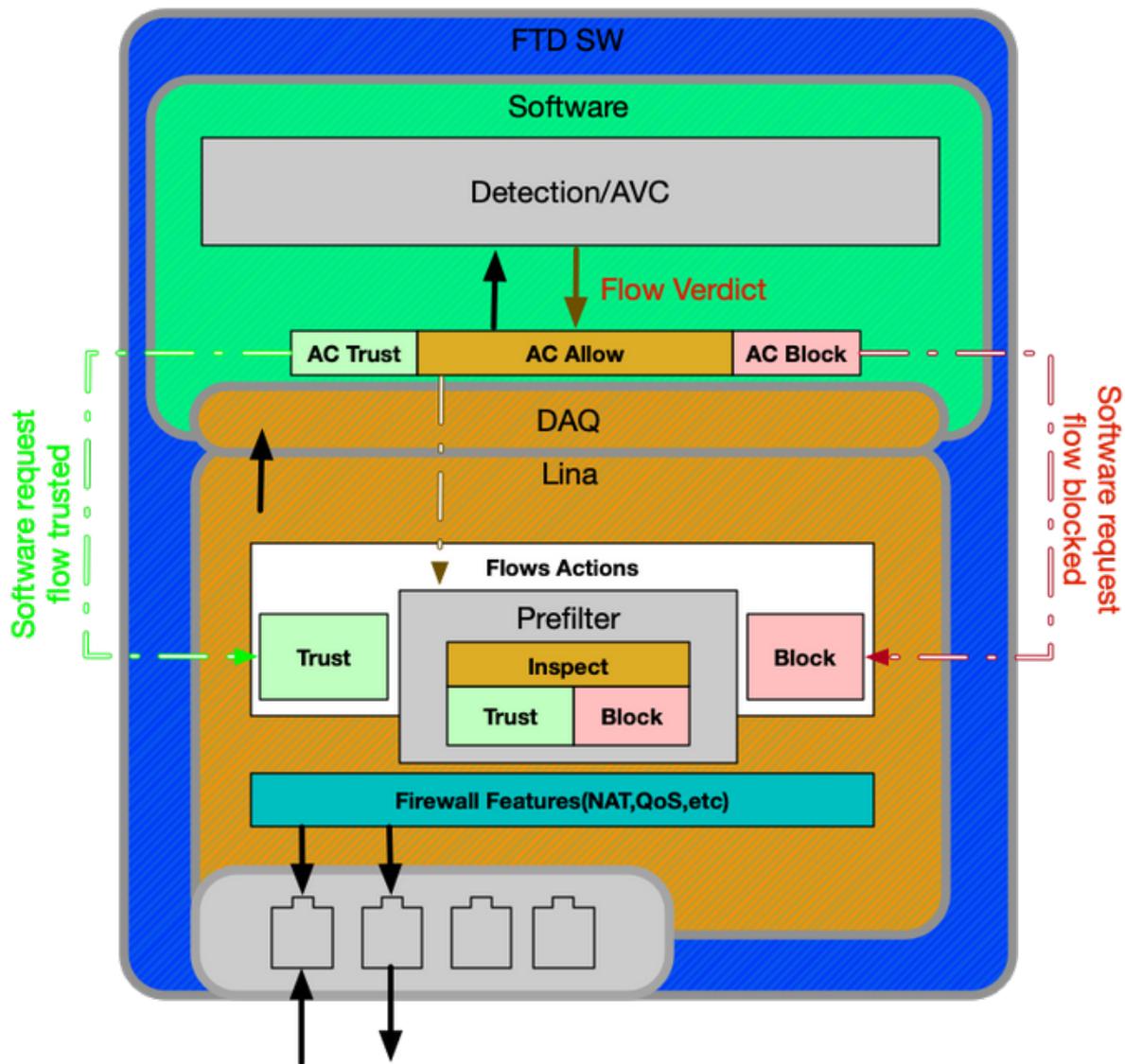
FirePOWERサービスプラットフォームは、SFRモジュールとも呼ばれます。これは基本的に、5500-X ASAプラットフォームで稼働する仮想マシンです。



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。

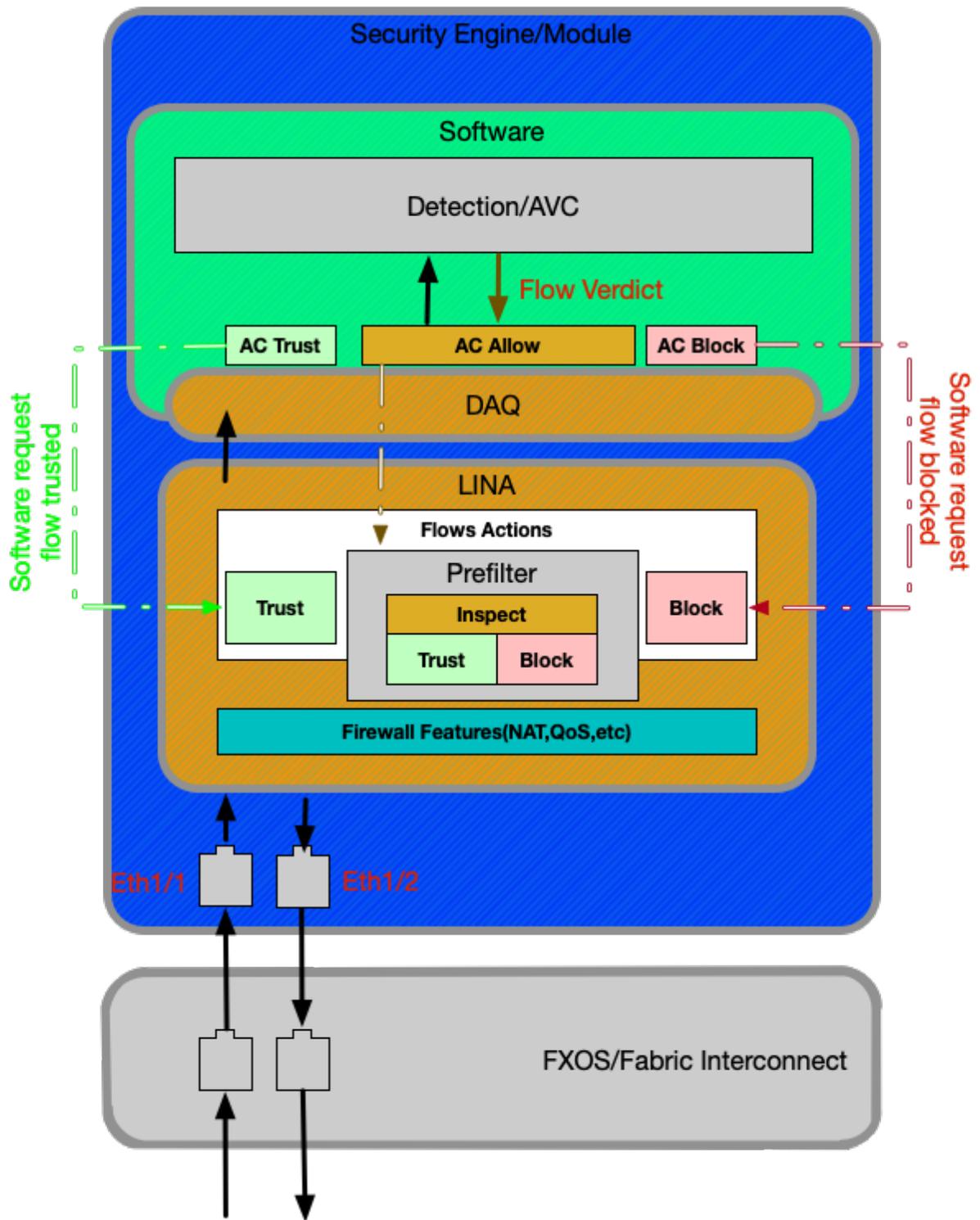


SSPプラットフォームでのFTD

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。

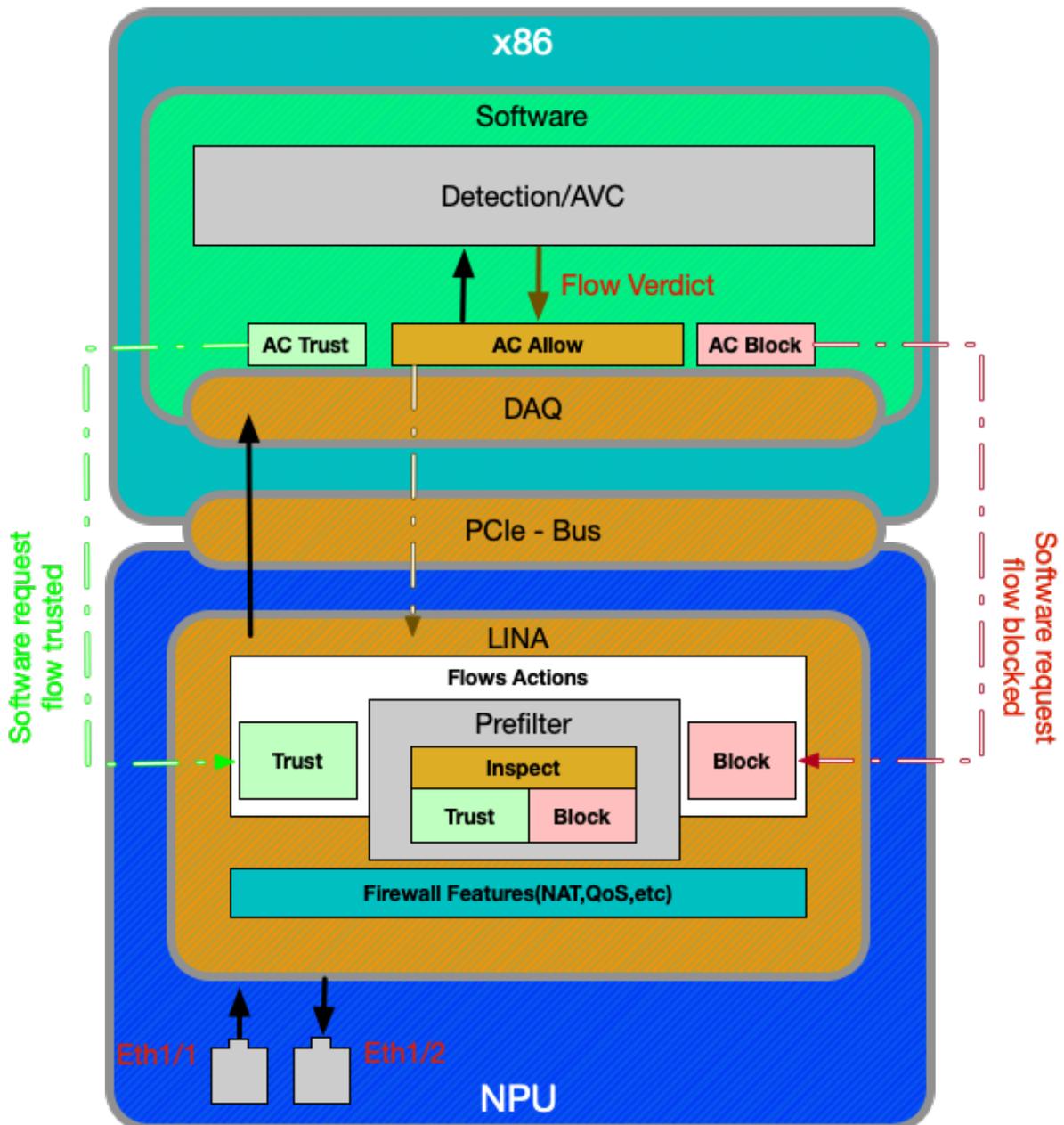
SSPプラットフォーム内には、次の図と説明に示すように、モデル間に違いがあります。

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(PCle)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

で説明します。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。

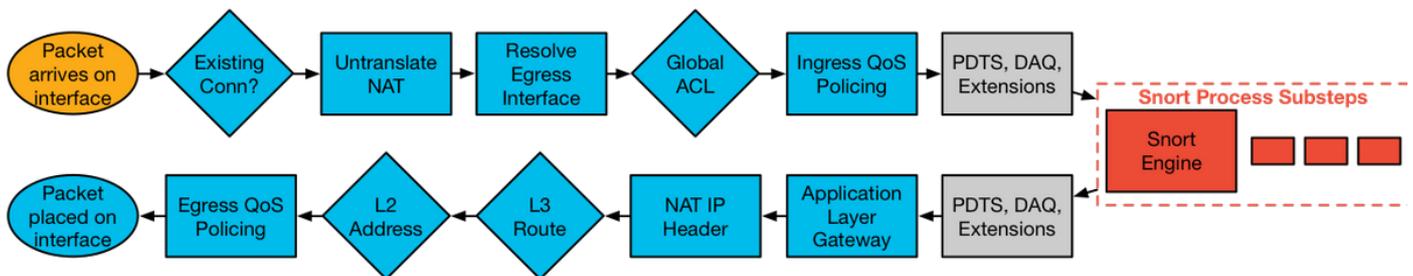
1. パケット入力
2. Firepower DAQレイヤ
3. セキュリティインテリジェンス
4. アクセスコントロールポリシー
5. SSLポリシー
6. アクティブ認証機能
7. 侵入ポリシー (IPSルール)
8. ネットワーク分析ポリシー (Snortプリプロセッサ設定)



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。

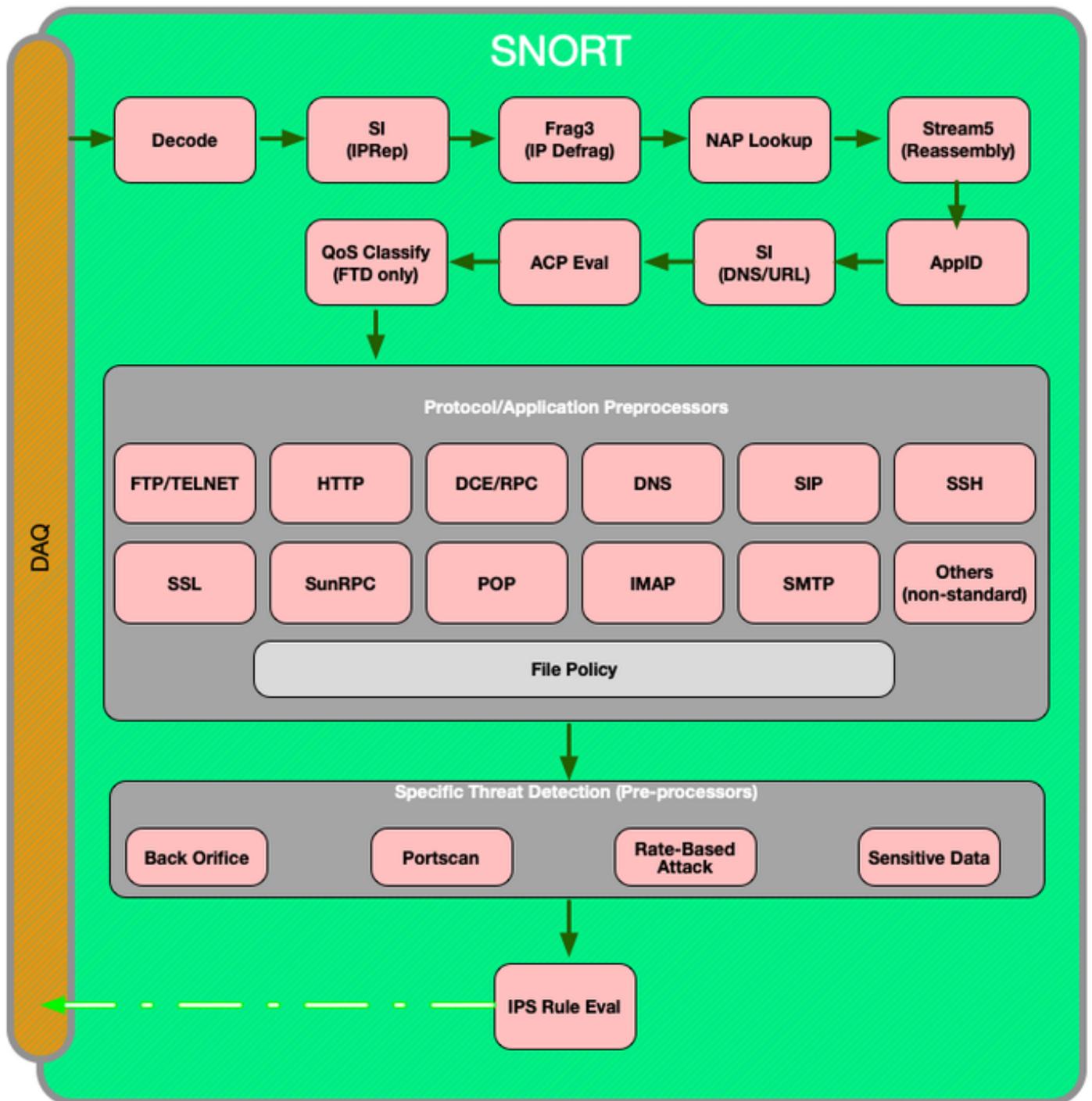
FTDを通過するパケットの実際のパス

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エンジンを通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で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。

The screenshot shows the Firepower GUI with the 'Security Intelligence' tab selected. The 'Blacklist (30)' section is expanded, showing a list of categories. A red arrow points to the 'Logging enabled' status for the 'Networks' category, and another red arrow points to the 'Logging disabled' status for the 'URLs' category.

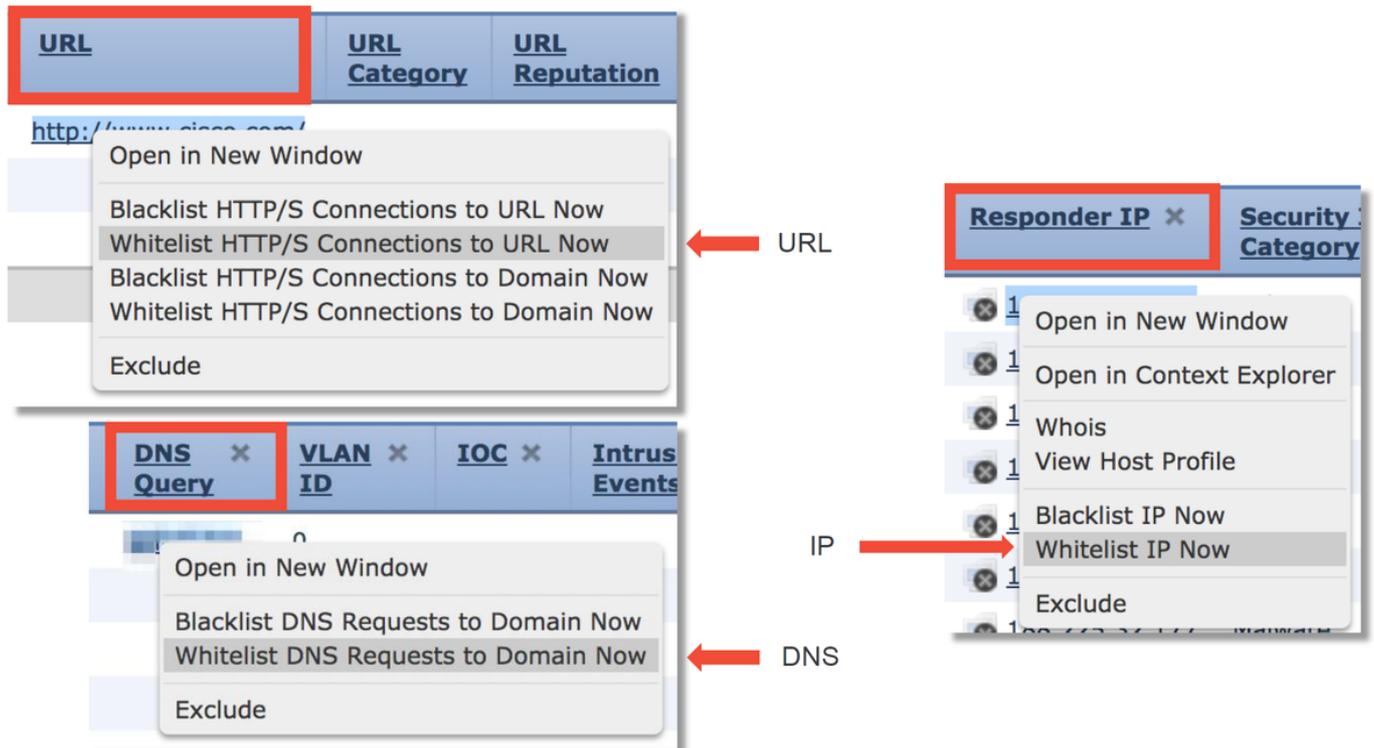
Category	Logging Status
Networks	Logging enabled
Attackers (Any Zone)	Logging disabled
Bogon (Any Zone)	Logging disabled
Bots (Any Zone)	Logging disabled
CnC (Any Zone)	Logging disabled
Dga (Any Zone)	Logging disabled
Exploitkit (Any Zone)	Logging disabled
Malware (Any Zone)	Logging disabled
Open_proxy (Any Zone)	Logging disabled
Phishing (Any Zone)	Logging disabled
Response (Any Zone)	Logging disabled
Spam (Any Zone)	Logging disabled
Suspicious (Any Zone)	Logging disabled
Tor_exit_node (Any Zone)	Logging disabled
Global Blacklist (Any Zone)	Logging disabled
URLs	Logging disabled
my_custom_url (Any Zone)	Logging disabled
Global Blacklist for URL (Any Zone)	Logging disabled
URL Attackers (Any Zone)	Logging disabled
URL Bogon (Any Zone)	Logging disabled
URL Bots (Any Zone)	Logging disabled
URL CnC (Any Zone)	Logging disabled
URL Dga (Any Zone)	Logging disabled
URL Exploitkit (Any Zone)	Logging disabled
URL Malware (Any Zone)	Logging disabled
URL Open_proxy (Any Zone)	Logging disabled
URL Open_relay (Any Zone)	Logging disabled
URL Phishing (Any Zone)	Logging disabled
URL Response (Any Zone)	Logging disabled
URL Spam (Any Zone)	Logging disabled
URL Suspicious (Any Zone)	Logging disabled
URL Tor_exit_node (Any Zone)	Logging disabled

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。

```
SHELL
> system support firewall-engine-debug

Please specify an IP protocol: tcp
Please specify a client IP address: 192.168.62.51
Please specify a client port:
Please specify a server IP address:
Please specify a server port:
Monitoring firewall engine debug messages

192.168.62.51-51216 > 173.37.145.84-80 6 AS 1 I 0 New session
192.168.62.51-51216 > 173.37.145.84-80 6 AS 1 I 0 Starting with minimum 3, 'block urls', and SrcZone
first with zones 1 -> 2, geo 0 -> 0, vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc 0, payload
0, client 0, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.62.51-51216 > 173.37.145.84-80 6 AS 1 I 0 pending rule order 3, 'block urls', URL
192.168.62.51-51216 > 173.37.145.84-80 6 AS 1 I 0 Starting with minimum 3, 'block urls', and SrcZone
first with zones 1 -> 2, geo 0(0) -> 0, vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc 676,
payload 2655, client 638, misc 0, user 9999997, url http://www.cisco.com/, xff
192.168.62.51-51216 > 173.37.145.84-80 6 AS 1 I 0: DataMessaging_GetURLData: Returning URL_BCTYPE
for www.cisco.com
192.168.62.51-51216 > 173.37.145.84-80 6 AS 1 I 0 rule order 3, 'block urls', URL Lookup Success:
http://www.cisco.com/ waited: 0ms
192.168.62.51-51216 > 173.37.145.84-80 6 AS 1 I 0 no match rule order 3, 'block urls',
url=(http://www.cisco.com/) c=4 r=96
192.168.62.51-51216 > 173.37.145.84-80 6 AS 1 I 0 match rule order 4, 'inspect it all', action Allow
192.168.62.51-51216 > 173.37.145.84-80 6 AS 1 I 0 allow action
192.168.62.51-51216 > 173.37.145.84-80 6 AS 1 I 0 File policy verdict is Type, Malware, and Capture
```

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

Check logging for block rules

#	Name	Sou... Zon...	Dest Zon...	Sou... Net...	Dest Net...	VLA...	Use...	App...	Sou...	Des...	URLs	ISE... Attr...	Acti...					
▼ Mandatory - My AC Policy (1-2)																		
1	block with logging	any	any	any	any	any	any	<input type="checkbox"/> YouT <input type="checkbox"/> YouTi	any	any	any	any	✗ Bloc					
2	block no logging	any	any	any	any	any	any		any	any	any	Gam	any	✗ Bloc				



Add trust rule

1	Trust traffic	any	any	192.	any	any	any		any	any	any	any	→ Trus					
2	block with logging	any	any	any	any	any	any	<input type="checkbox"/> YouT <input type="checkbox"/> YouTi	any	any	any	any	✗ Bloc					
3	block no logging	any	any	any	any	any	any		any	any	any	Gam	any	✗ Bloc				



Create blank AC policy

#	Name	Sour... Zones	Dest Zones	Sour... Netw...	Dest Netw...	VLAN...	Users	Appli...	Sour...	Dest ...	URLs	ISE... Attr...	Action					
▼ Mandatory - Test - No rules (-)																		
There are no rules in this section. Add Rule or Add Category																		
▼ Default - Test - No rules (-)																		
There are no rules in this section. Add Rule or Add Category																		
Default Action												Intrusion Prevention: Balanced Security and Connectivity						

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、関連するデータベー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

#	Name	Sour... Zones	Dest Zones	Source Netw...	Dest Netw...	VLA...	Us...	Appli...	Sour...	Dest ...	Categories	SSL	Action					
Administrator Rules																		
This category is empty																		
Standard Rules																		
1	DnD banking	any	any	any	any	any	any	any	any	any	Financial Services (Any Reputatio	any	→ Do not decrypt					
2	decrypt outbound suspicious	inside	outside	any	any	any	any	any	any	any	Any (Reputations 1-2)	any	Decrypt - Resign					

Editing Rule - DnD banking

Name: DnD banking Enabled [Move](#)

Action: Do not decrypt

Logging

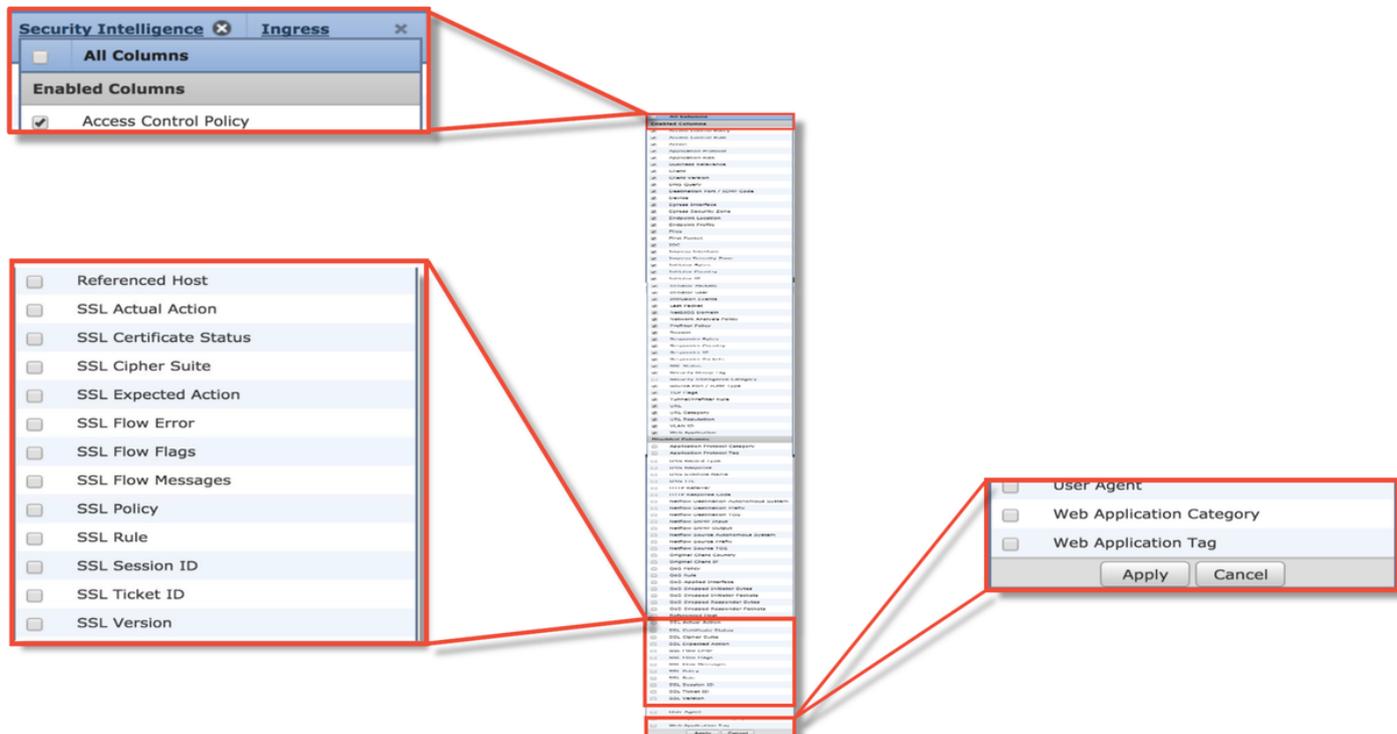
Log at End of Connection **Enable Logging**

Send Connection Events to:

- Event Viewer
- Syslog [Select a Syslog Alert Configuration...](#)
- SNMP Trap [Select an SNMP Alert Configuration...](#)

[Save](#) [Cancel](#)

- [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



Connection Events (switch workflow)
 Connections with Application Details > **Table View of Connection Events**
 Search Constraints (Edit Search Save Search)

SSL Blocking flow

First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Responder IP	Responder Country
2017-05-30 13:09:23	2017-05-30 13:09:24	Block	SSL Block	192.168.1.200		216.58.217.138	USA
2017-05-30 13:08:53	2017-05-30 13:08:54	Block	SSL Block	192.168.1.200		216.58.217.138	USA
2017-05-30 13:08:23	2017-05-30 13:08:24	Block	SSL Block	192.168.1.200		216.58.217.138	USA
2017-05-30 13:08:19	2017-05-30 13:08:20	Block	SSL Block	192.168.1.200		216.58.217.138	USA
2017-05-30 13:07:53	2017-05-30 13:07:54	Block	SSL Block	192.168.1.200		216.58.217.138	USA
2017-05-30 13:07:23	2017-05-30 13:07:24	Block	SSL Block	192.168.1.200		216.58.217.138	USA

Cause of the SSL failure

SSL Status	SSL Flow Error	SSL Actual Action	SSL Expected Action	SSL Certificate Status	SSL Version
Decrypt (Resign)	PUB_CRYPTOPENSSL_RSA_OP_FAILURE (0xb7000a20)	Decrypt (Resign)	Decrypt (Resign)	Valid	TLSv1.2
Decrypt (Resign)	PUB_CRYPTOPENSSL_RSA_OP_FAILURE (0xb7000a20)	Decrypt (Resign)	Decrypt (Resign)	Valid	TLSv1.2
Decrypt (Resign)	PUB_CRYPTOPENSSL_RSA_OP_FAILURE (0xb7000a20)	Decrypt (Resign)	Decrypt (Resign)	Valid	TLSv1.2
Decrypt (Resign)	PUB_CRYPTOPENSSL_RSA_OP_FAILURE (0xb7000a20)	Decrypt (Resign)	Decrypt (Resign)	Valid	TLSv1.2
Decrypt (Resign)	PUB_CRYPTOPENSSL_RSA_OP_FAILURE (0xb7000a20)	Decrypt (Resign)	Decrypt (Resign)	Valid	TLSv1.2
Decrypt (Resign)	PUB_CRYPTOPENSSL_RSA_OP_FAILURE (0xb7000a20)	Decrypt (Resign)	Decrypt (Resign)	Valid	TLSv1.2

SSL flow flags for what happened with flow

SSL Rule	SSL Session ID	SSL Ticket ID	SSL Flow Flags	SSL Flow Messages
MITM	0x0	0x0	VALID, INITIALIZED, SSL_DETECTED, CERTIFICATE_DECODED, FULL_HANDSHAKE, CLIENT_HELLO_SESSTKT, SERVER_HELLO_SESSTKT, CH_PROCESSED, SH_PROCESSED, CH_CIPHERS_MODIFIED, ...	CLIENT_HELLO, SERVER_HELLO, SERVER_CERTIFICATE
MITM	0x0	0x0	VALID, INITIALIZED, SSL_DETECTED, CERTIFICATE_DECODED, FULL_HANDSHAKE, CLIENT_HELLO_SESSTKT, SERVER_HELLO_SESSTKT, CH_PROCESSED, SH_PROCESSED, CH_CIPHERS_MODIFIED, ...	CLIENT_HELLO, SERVER_HELLO, SERVER_CERTIFICATE
MITM	0x0	0x0	VALID, INITIALIZED, SSL_DETECTED, CERTIFICATE_DECODED, FULL_HANDSHAKE, CLIENT_HELLO_SESSTKT, SERVER_HELLO_SESSTKT, CH_PROCESSED, SH_PROCESSED, CH_CIPHERS_MODIFIED, ...	CLIENT_HELLO, SERVER_HELLO, SERVER_CERTIFICATE
MITM	0x0	0x0	VALID, INITIALIZED, SSL_DETECTED, CERTIFICATE_DECODED, FULL_HANDSHAKE, CLIENT_HELLO_SESSTKT, SERVER_HELLO_SESSTKT, CH_PROCESSED, SH_PROCESSED, CH_CIPHERS_MODIFIED, ...	CLIENT_HELLO, SERVER_HELLO, SERVER_CERTIFICATE
MITM	0x0	0x0	VALID, INITIALIZED, SSL_DETECTED, CERTIFICATE_DECODED, FULL_HANDSHAKE, CLIENT_HELLO_SESSTKT, SERVER_HELLO_SESSTKT, CH_PROCESSED, SH_PROCESSED, CH_CIPHERS_MODIFIED, ...	CLIENT_HELLO, SERVER_HELLO, SERVER_CERTIFICATE
MITM	0x0	0x0	VALID, INITIALIZED, SSL_DETECTED, CERTIFICATE_DECODED, FULL_HANDSHAKE, CLIENT_HELLO_SESSTKT, SERVER_HELLO_SESSTKT, CH_PROCESSED, SH_PROCESSED, CH_CIPHERS_MODIFIED, ...	CLIENT_HELLO, SERVER_HELLO, SERVER_CERTIFICATE

- 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。

Editing Rule - Passive

Name: Passive Enabled Move

Action: Passive Authentication Realm: my-realm Authentication Type: HTTP Basic

Zones Networks VLAN Tags Ports Realm & Settings

Realm * my-realm

Use active authentication if passive authentication cannot identify user

* Required Field

Save Cancel

Make sure passive auth rules don't fall back to active auth

Remove or disable active auth rules

Action	Auth Type	
Active Authentication	NTLM	
Active Authentication	Kerberos	
Active Authentication	HTTP Negotiate	
Active Authentication	HTTP Response Pa	
Active Authentication	HTTP Basic	
Passive Authentication	none	

Identity Policy Settings

Identity Policy None

Or remove identity from Advanced tab of ACP

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、関連するデータベー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。

```
SHELL
> system support trace

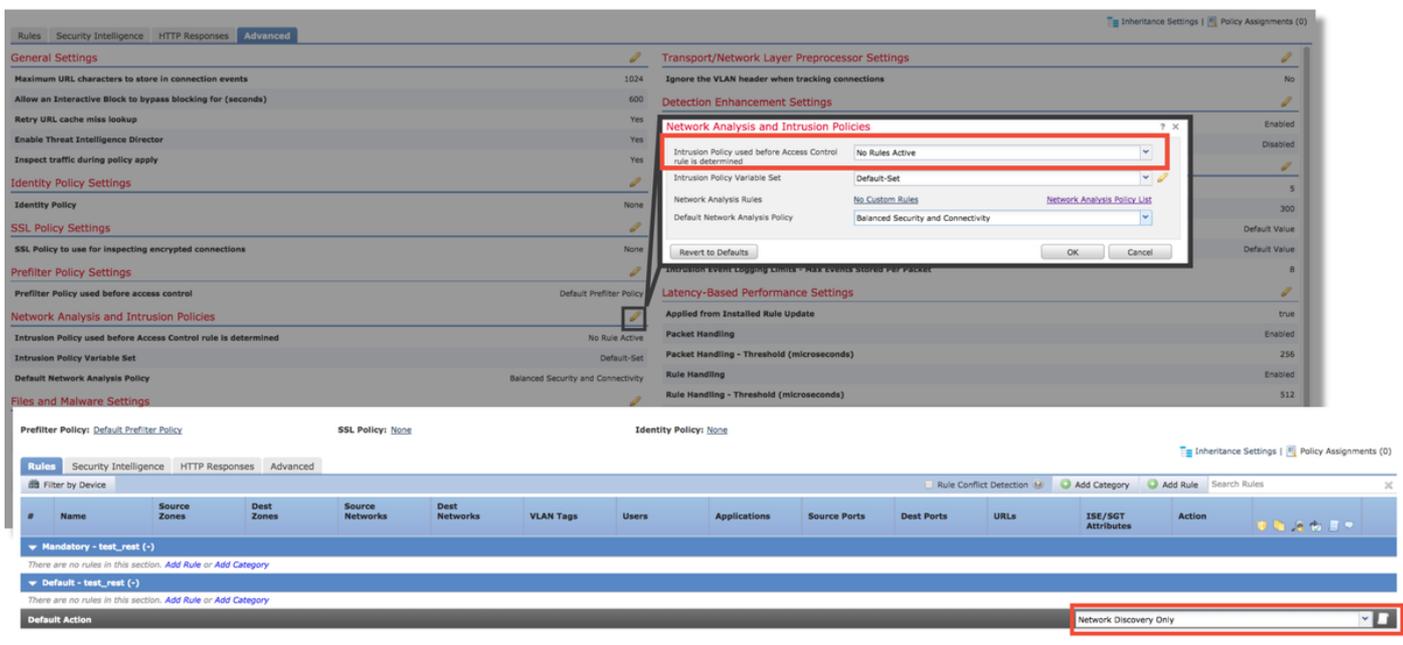
Please specify an IP protocol: tcp
Please specify a client IP address: 192.168.62.69
Please specify a client port:
Please specify a server IP address:
Please specify a server port:
Enable firewall-engine-debug too? [n]: y
Monitoring packet tracer debug messages

[... output omitted for brevity]
173.37.145.84-80 - 192.168.62.69-38488 6 Packet: TCP, ACK, seq 3594105349, ack 3856774965
173.37.145.84-80 - 192.168.62.69-38488 6 AppID: service HTTP (676), application Cisco (2655)
192.168.62.69-38488 > 173.37.145.84-80 6 AS 1 I 0 URL SI: ShmDBLookupURL("http://www.cisco.com/<?php")
returned 0
...
192.168.62.69-38488 > 173.37.145.84-80 6 AS 1 I 0 match rule order 5, 'inspect it all', action Allow
192.168.62.69-38488 > 173.37.145.84-80 6 AS 1 I 0 allow action
192.168.62.69-38488 > 173.37.145.84-80 6 Firewall: allow rule, 'inspect it all', allow
192.168.62.69-38488 > 173.37.145.84-80 6 IPS Event: gid 1, sid 23111, drop
192.168.62.69-38488 > 173.37.145.84-80 6 Snort detect drop: gid 1, sid 23111, drop
192.168.62.69-38488 > 173.37.145.84-80 6 AS 1 I 0 Deleting session
192.168.62.69-38488 > 173.37.145.84-80 6 NAP id 1, IPS id 0, Verdict BLACKLIST
192.168.62.69-38488 > 173.37.145.84-80 6 -> Blocked by IPS
Verdict reason is sent to DAQ's PDTS
```

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せん）。

- 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。

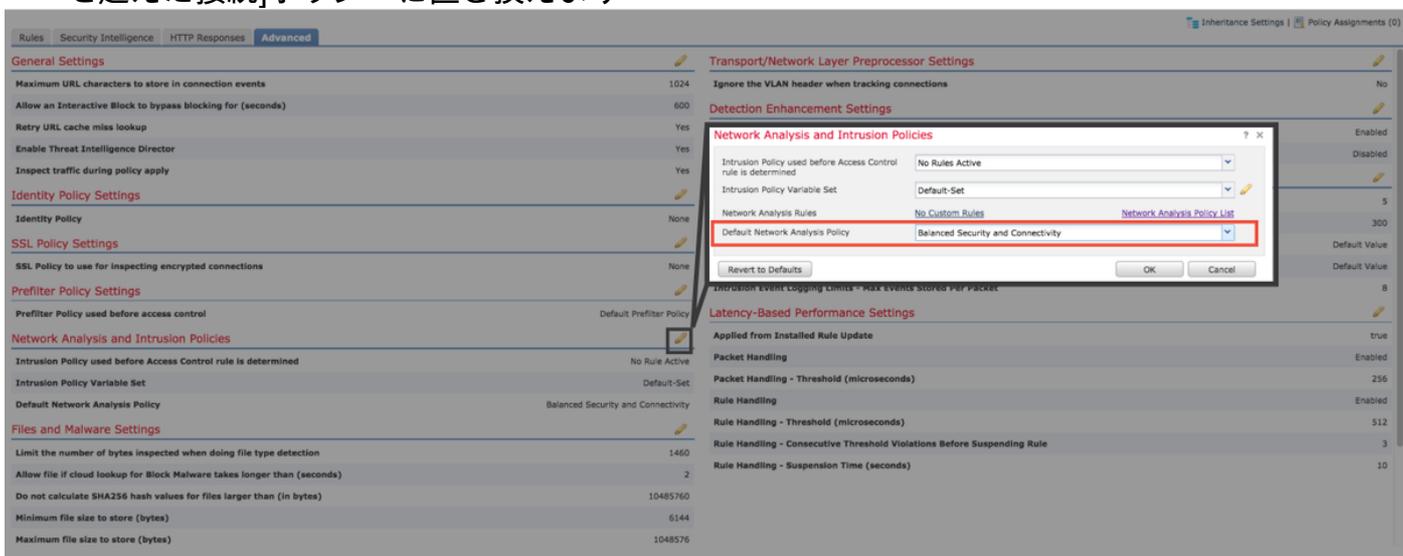
侵入ポリシー機能の詳細なトラブルシューティングについては、関連するデータパスのトラブルシューティング記事を参照してください。

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

The screenshot shows the 'Add Rule' dialog box in the Cisco Firepower GUI. The 'File Policy' dropdown menu is highlighted with a red box, and a red arrow points to it with the text 'Remove file policy from all rules'. Below the dialog, the 'Rules' table is visible, showing two rules: 'Rule1' and 'Rule2', both with 'Allow' actions.

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applications	Source Ports	Dest Ports	URLs	ISE/SGT Attributes	Action
Mandatory - test_rest (1-2)													
1	Rule1	Any	Any	Any	Any	Any	Any	Any	Any	Any	Any	Any	Allow
2	Rule2	Any	Any	Any	Any	Any	Any	Any	Any	Any	Any	Any	Allow
Default - test_rest (-)													

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>