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

内容

概要

この記事は、Firepowerシステムのデータパスを体系的にトラブルシューティングし、Firepowerのコンポーネントがトラフィックに影響を与えているかどうかを判断する方法を説明する一連の記事の一部です。Firepowerプラットフォームのアーキテクチャに関する情報や、その他のデータパスのトラブルシューティングに関する記事へのリンクについては、概要記事を参照してください。

この記事では、Firepowerのデータパスのトラブルシューティングの3番目の段階であるセキュリティインテリジェンス機能について説明します。

前提条件

- この記事は、現在サポートされているすべてのFirepowerプラットフォームに関連しています
- URLおよびDNSのセキュリティインテリジェンスは、バージョン6.0.0で導入されました

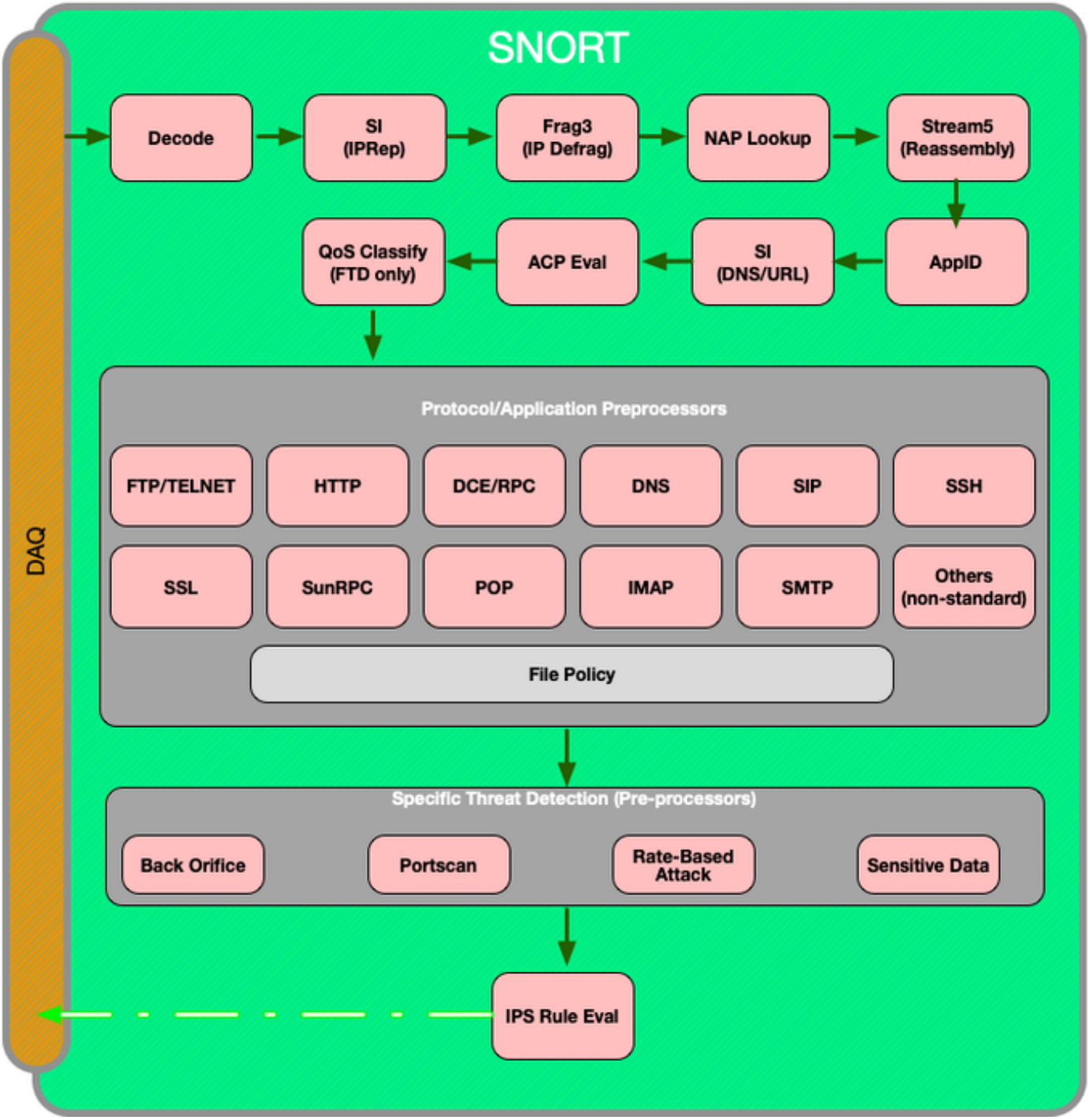
Firepowerセキュリティインテリジェンスフェーズのトラブルシューティング

セキュリティインテリジェンスは、次の項目に対してブラックリストとホワイトリストの両方に対して検査を実行する機能です。

- IPアドレス（UIの特定の部分では「ネットワーク」とも呼ばれる）
- Uniform Resource Locators(URL)
- ドメインネームシステム(DNS)クエリ

セキュリティインテリジェンス内のリストは、シスコが提供するフィードや、ユーザが設定したリストやフィードによって入力できます。

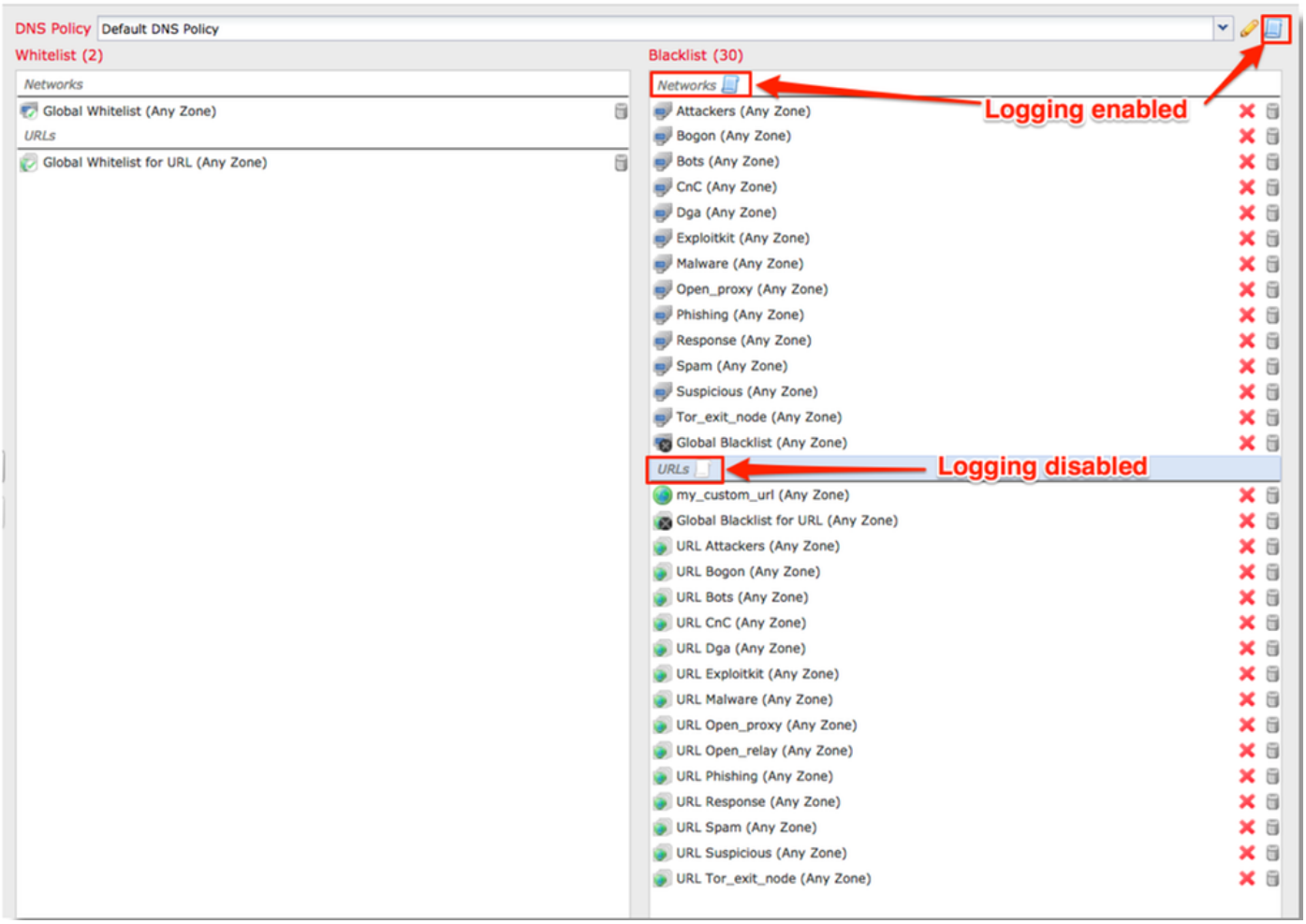
IPアドレスに基づくセキュリティインテリジェンスレピュテーションは、トラフィックを検査するFirepower内の最初のコンポーネントです。URLおよびDNSセキュリティインテリジェンスは、関連するアプリケーションプロトコルが検出されるとすぐに実行されます。Firepowerソフトウェアのインスペクションワークフローの概要を次に示します。



セキュリティインテリジェンスイベントに対してロギングが有効

になっていることを確認する

Security Intelligenceレベルのブロックは、ロギングが有効になっている限り簡単に判別できます。これは、Firepower Management Center(FMC)ユーザインターフェイス(UI)で、[ポリシー(Policies)] > [アクセスコントロール(Access Control)] > [アクセスコントロールポリシー(Access Control Policy)]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。



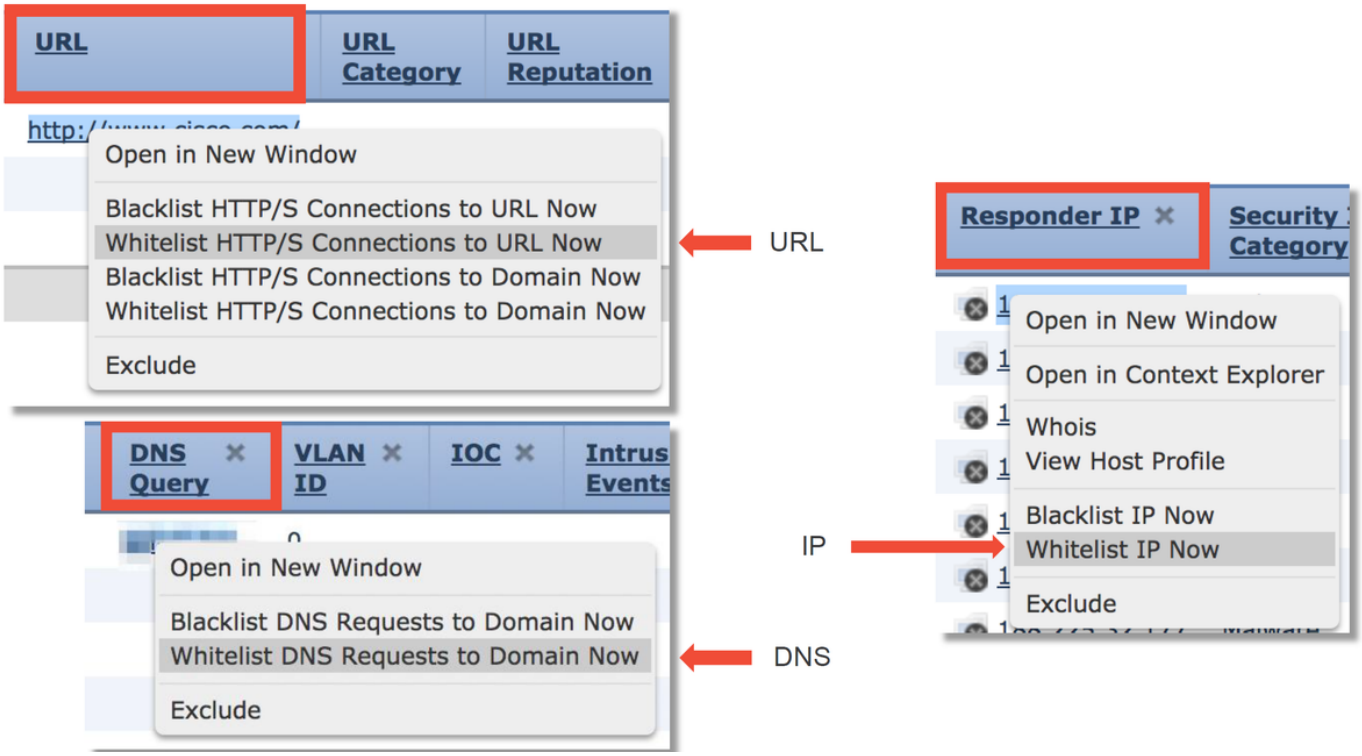
セキュリティインテリジェンスイベントの確認

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

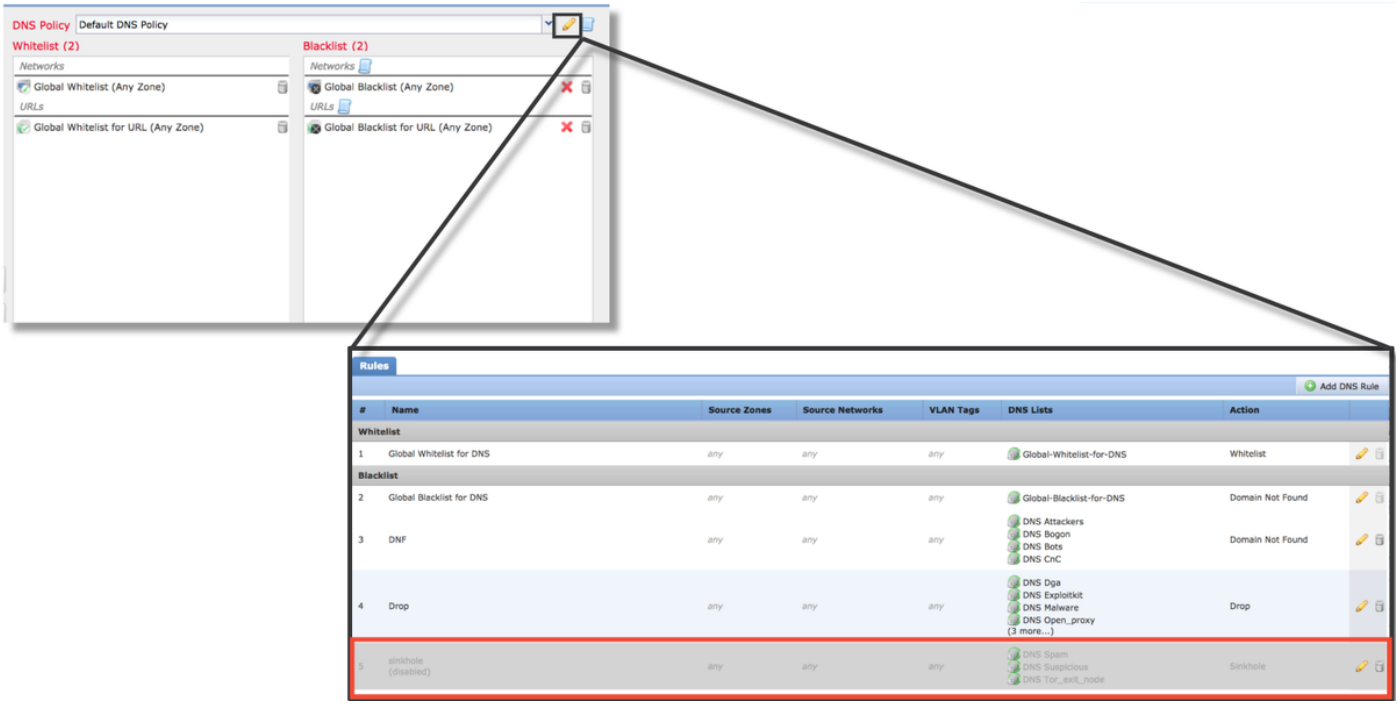
ブラックリストから項目を削除する必要があるかどうかを調査するために、Cisco Technical Assistance Center(TAC)にデータを提供することもできます。

> **注**：ホワイトリストに追加すると、対象のセキュリティインテリジェンスホワイトリストにエントリのみが追加されます。つまり、オブジェクトはセキュリティインテリジェンスチェックに合格できます。ただし、他のすべてのFirepowerコンポーネントは引き続きトラフィックを検査できます。

セキュリティインテリジェンス設定を削除する方法

Security Intelligenceの設定を削除するには、前述のように[Security Intelligence]**タブ**に移動します。3つのセクションがあります。1つはネットワーク、URL、およびDNSのポリシーです。

そこから、リストとフィードを削除するには、ごみ箱の記号をクリックします。



上のスクリーンショットでは、グローバルブラックリストとホワイトリストを除くすべてのIPおよびURL Security Intelligenceリストが削除されています。

DNSセキュリティインテリジェンスの設定が保存されているDNSポリシー内で、いずれかのルールが無効になります。

> **注**：グローバルブラックリストとホワイトリストの内容を表示するには、[Objects] > [Object Management] > [Security Intelligence]に移動します。次に、対象のセクション（ネットワーク、URL、DNS）をクリックします。 リストを編集すると、内容が表示されますが、アクセスコントロールポリシー内で設定を実行する必要があります。

バックエンドの設定の確認

セキュリティインテリジェンスの設定は、CLIで**> show access-control-configコマンドを使用して確認できます**。このコマンドは、Firepowerデバイスで実行されているアクティブなアクセスコントロールポリシーの内容を表示します。

```
> show access-control-config

==================[ My AC Policy ]==================
Description              :
Default Action            : Allow
Default Policy            : SOC
Logging Configuration
   DC                   : Enabled
   Beginning             : Disabled
   End                  : Enabled
Rule Hits                 : 0
Variable Set              : Default-Set

===[ Security Intelligence - Network Whitelist ]====
   Name                 : Global-Whitelist (List)
   IP Count             : 0
   Zone                 : any

===[ Security Intelligence - Network Blacklist ]====
Logging Configuration     : Enabled
   DC                   : Enabled


--------------------[ Block ]---------------------
   Name                 : Attackers (Feed)
   Zone                 : any

   Name                 : Bogon (Feed)
   Zone                 : any
…[omitted for brevity]
```

上記の例では、ロギングがNetwork Blacklist（NBLK；ネットワークブラックリスト）に設定されており、ブラックリスト（攻撃者およびBogon）に少なくとも2つのフィードが含まれていることに注意してください。

個々のアイテムがセキュリティインテリジェンスリストにあるかどうかは、エキスパートモードで確認できます。次の手順を参照してください。

```
> expert
$ grep <ip.addr> /var/sf/iprep_download/*
/var/sf/iprep_download/23f2a124-8278-4c03-8c9d-d28fe08b5e98.blf:<ip.addr>

$ head -1 /var/sf/iprep_download/23f2a124-8278-4c03-8c9d-d28fe08b5e98.blf
#Cisco intelligence feed: Malware



$ grep <url> /var/sf/siurl_download/*
/var/sf/siurl_download/00000000-0000-0ed3-0000-073014445223.lf:<url>

$ head -1 /var/sf/siurl_download/00000000-0000-0ed3-0000-073014445223.lf
#URL object: my_custom_url



$ grep <dns.hostname> /var/sf/sidns_download/*
/var/sf/sidns_download/032ba433-c295-11e4-a919-d4ae5275b77b.lf: <dns.hostname>

$ head -1 /var/sf/sidns_download/032ba433-c295-11e4-a919-d4ae5275b77b.lf
#Cisco DNS and URL intelligence feed: DNS Response
```

IP SI lists are in /var/sf/iprep_download/

URL SI lists are in /var/sf/siurl_download/

DNS SI lists are in /var/sf/sidns_download/

各セキュリティインテリジェンスリストには、一意のUUIDを持つファイルがあります。上記の例は、**head -n**1コマンドを使用してリストの名前を識別する方法を示しています。

TACに提供するデータ

Data	手順
トラフィックを検査するFMCおよびFirepowerデバイスからのファイルのトラブルシューティング	http://t
イベントのスクリーンショット（タイムスタンプを含む）	手順に
CLIセッションからのテキスト出力	手順に
偽の正のケースを送信する場合は、問題の項目（IP、URL、ドメイン）を指定します。	紛争を

次のステップ

セキュリティインテリジェンスコンポーネントが問題の原因ではないと判断された場合、次のステップは、アクセスコントロールポリシールールのトラブルシューティングです。

次の記事に進むには、ここをクリックしてください。