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

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4番目の段階であるアクセスコントロールポリシー(ACP)について説明します。 この情報は、現在サポートされているすべてのFirepowerプラットフォームおよびバージョンに適用されます。

アクセスコントロールポリシー(ACP)フェーズのトラブルシューティング

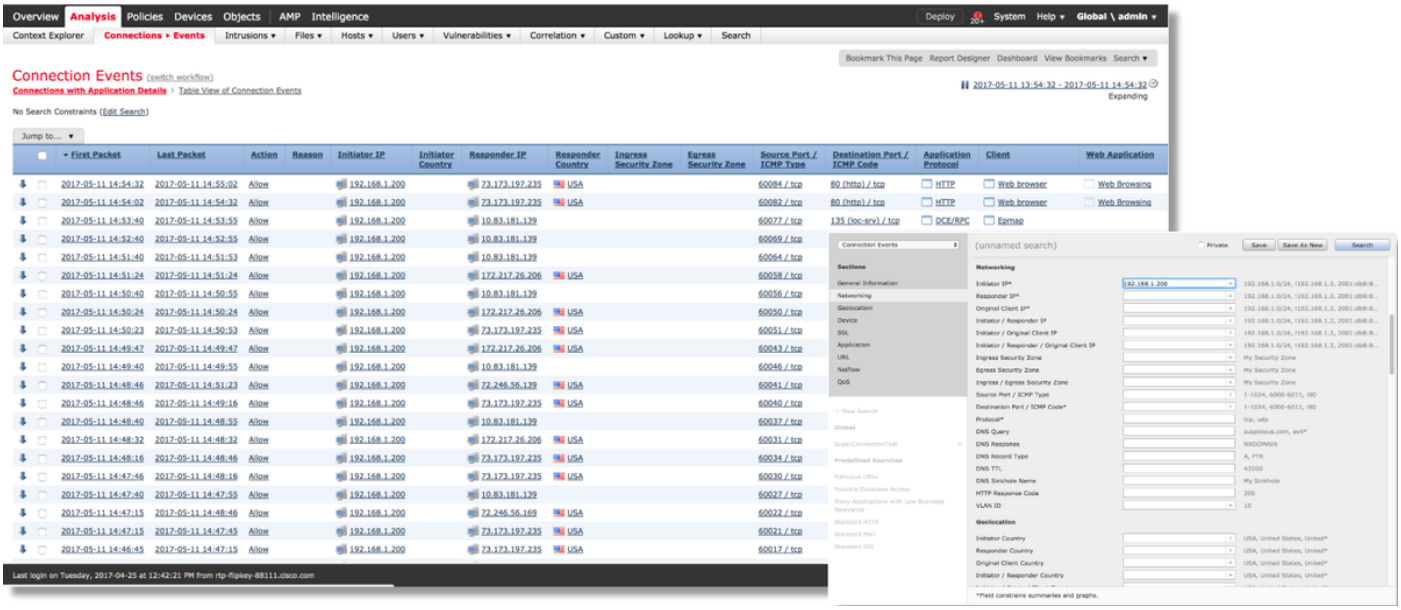
一般的に、フローが一致するACPルールを決定することは、非常に簡単です。接続イベントを確認して、どのルール/アクションが適用されているかを確認できます。ACPがトラフィックに対して何を行っているかが明確に示されていない場合は、Firepowerコマンドラインインターフェイス(CLI)でデバッグを実行できます。

接続イベントの確認

入力インターフェイスと出力インターフェイスを確認した後、トラフィックとフロー情報が一致する必要があります。Firepowerがフローをブロックしているかどうかを確認する最初のステップは、該当するトラフィックの接続イベントを確認することです。これらは、Firepower

Management Centerの[Analysis] > [Connections] > [Events]で表示できます。

> **注**：接続イベントを確認する前に、ACPルールでロギングが有効になっていることを確認してください。ロギングは、各アクセスコントロールポリシールールの[Logging]タブおよび[Security Intelligence]タブで設定します。疑わしいルールが「イベントビューア」にログを送信するように設定されていることを確認します。 これは、デフォルトアクションにも適用されます。



[Edit Search（検索の編集）]をクリックし、一意のソース（イニシエータ）IPでフィルタリングすると、Firepowerによって検出されたフローを確認できます。[Action]列には、このホストのトラフィックの[Allow]が表示されます。

Firepowerが意図的にトラフィックをブロックしている場合、アクションには「ブロック」という単語が含まれます。 [接続イベントのテーブルビュー]をクリックすると、さらに多くのデータが表示されます。アクションが「ブロック」の場合、接続イベントの次のフィールドを確認できます。

-原因

– アクセスコントロールルール

迅速な緩和手順

ACPルールが原因と考えられる問題を迅速に緩和するには、次の手順を実行します。

- 該当するトラフィックに対して「Trust」または「Allow」のアクションを使用してルールを作成し、それをACPの一番上、またはすべてのブロックルールの上に配置します。
- 「ブロック」という単語を含むアクションを使用して、ルールを一時的に無効にします
- [Default Action]が[Block All Traffic]に設定されている場合は、一時的に[Network Discovery Only]に切り替えます

> **注**：これらの迅速な緩和策には、すべての環境で実現できない可能性があるポリシーの変更が必要です。ポリシーを変更する前に、まずシステムサポートトレースを使用して、トラフィックが一致するルールを判別することを推奨します。

ACPのデバッグ

ACP操作に対する詳細なトラブルシューティングは、> system support firewall-**engine-debug CLIユーティリティを使用して実行**できます。

> **注**：Firepower 9300および4100プラットフォームでは、問題のシェルに次のコマンドでアクセスできます。
>
> **# connect module 1 console**
> Firepower-module1> **connect ftd**
> **>**
>
> マルチインスタンスの場合、論理デバイスのCLIには次のコマンドでアクセスできます。
> **# connect module 1 telnet**
> Firepower-module1> **connect ftd ftd1**
> コンテナftd(ftd1)コンソールに接続しています… 「exit」と入力してブートCLIに戻ります
> **>**

システム**サポートのfirewall-engine-debugユーティリティ**には、ACPで評価される各パケットのエントリがあります。ルールの評価プロセスが実行され、ルールが一致するか一致しないかが表示されます。

> **注**：バージョン6.2以降では、システムサポート**トレースツ**ールを実行できます。同じパラメータを使用しますが、詳細も含まれます。「Enable **firewall-engine-debug too?」というプロンプトが表示されたら、必ず「y」と入力してください。**

例 1：信頼ルールに一致するトラフィック

次の例では、SSHセッションの確立は、**system support firewall-engine-debugを使用して評価されます。**

これは、Firepowerデバイスで実行されているACPです。

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN ...	Users	Applic...	Sourc...	Dest P...	URLs	ISE/S... Attrib...	Acti...
Mandatory - JG AC (all) (1-6)													
1	Trust ssh for host	Any	Any	192.168.0.7	Any	Any	Any	Any	Any	SSH	Any	Any	Trust
2	inspect	Any	Any	10.0.0.0/8	Any	Any	Any	Any	Any	Any	Any	Any	Allow
3	trust server backup	Any	Any	192.168.62.3	10.123.175.22	Any	Any	Any	Any	Any	Any	Any	Trust

ACPには3つのルールがあります。

1. 1つ目のルールは、SSHで使用される宛先ポートを持つ192.168.0.7からのトラフィックを信頼することです。
2. 2番目のルールは、10.0.0.0/8から送信され、ネットワーク基準がXFFヘッダーデータに基づいて一致するすべてのトラフィックを検査します（ネットワークオブジェクトの横のアイコンで示されます）
3. 3番目のルールは、192.168.62.3から10.123.175.22へのすべてのトラフィックを信頼します

トラブルシューティングシナリオでは、192.168.62.3から10.123.175.22へのSSH接続を分析しています。

セッションがACルール3の「信頼サーバのバックアップ」と一致することが期待されます。 問題は、このセッションでこのルールに一致するために必要なパケットの数です。ACルールまたは複数のパケットを決定するために最初のパケットに必要な情報はすべて必要ですか。必要な場合は何ですか。

Firepower CLIで、ACPルール評価プロセスを確認するために次のように入力します。

```
>system support firewall-engine-debug

Please specify an IP protocol: tcp
Please specify a client IP address: 192.168.62.3
Please specify a client port:
Please specify a server IP address: 10.123.175.22
Please specify a server port: 22
Monitoring firewall engine debug messages
```

> **ヒント**：**firewall-engine-debug**を実行する際は、できるだけ多くのパラメータを入力して、対象のデバッグメッセージだけを画面に出力することをお勧めします。

次のデバッグ出力では、セッションの最初の4つのパケットが評価されています。

SYN

SYN、ACK

ACK

最初のSSHパケット（クライアントからサーバ）

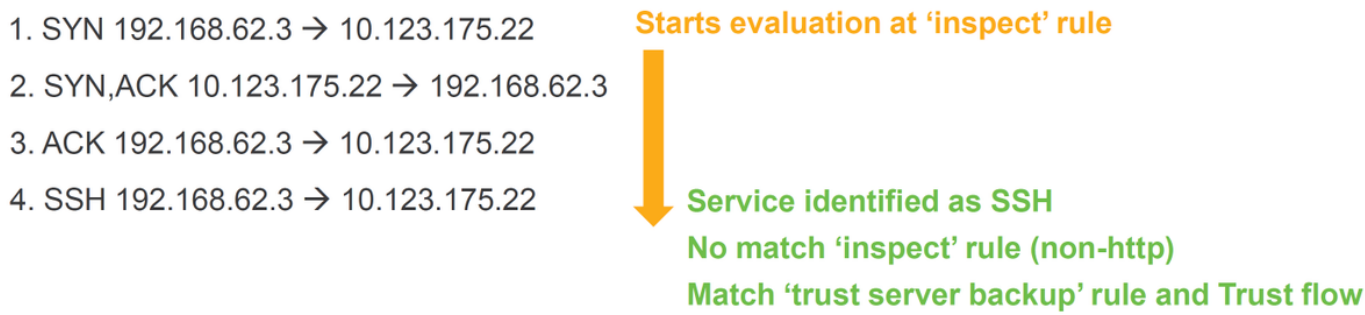
```
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 New session
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 Starting with minimum 4, 'inspect', and IPProto first with zones 1 -> 2, geo 0 -> 0, vlan 0,
inline sgt tag: untagged, ISE sgt id: 0, svc 0, payload 0, client 0, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 pending rule order 4, 'inspect', XFF wait for AppId

192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 Starting with minimum 4, 'inspect', and IPProto 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
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 pending rule order 4, 'inspect', XFF wait for AppId

192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 Starting with minimum 4, 'inspect', and IPProto 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
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 pending rule order 4, 'inspect', XFF wait for AppId

192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 Starting with minimum 4, 'inspect', and IPProto first with zones 1 -> 2, geo 0 -> 0, vlan 0,
inline sgt tag: untagged, ISE sgt id: 0, svc 846, payload -1, client 2000000846, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 no match rule order 4, 'inspect', XFF non-http
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 match rule order 5, 'trust server backup', action Trust
```

これは、デバッグロジックをさらに詳しく説明したチャートです。



このフローでは、デバイスがルールに一致するために4パケットかかります。

デバッグ出力の詳細な説明を次に示します。

- IPアドレスが要件に一致しないため、「trust ssh for host」ルールが一致しないため、ACP評価プロセスは「inspect」ルールから開始されます。このルールが一致する必要があるかどうかを判断するために必要なすべての情報が最初のパケット（IPおよびポート）に存在するため、これは迅速に一致します
- HTTPアプリケーショントラフィックにX-Forwarded-For(XFF)情報が見つかっており、アプリケーションはまだ認識されていないため、セッションはルール2（保留中のアプリケーションデータ）の保留状態になります。
- 4番目のパケットでアプリケーションが識別されると、「inspect」ルールは一致しません。これは、アプリケーションがHTTPではなくSSHであるためです
- 次に、IPアドレスに基づいて「信頼サーバのバックアップ」ルールが照合されます。

要約すると、接続はセッションに一致するために4パケットを要します。これは、ルール2にアプリケーションの制約があるため、ファイアウォールがアプリケーションを識別するまで待機する必要があるためです。

ルール2に送信元ネットワークしかなく、XFFでない場合、セッションに一致するために1パケットが必要でした。

レイヤ1 ~ 4のルールは、ポリシー内の他のすべてのルールの上に常に配置する必要があります。これは、通常、これらのルールが決定を行うために1パケットが必要になるためです。ただし、レイヤ1 ~ 4のルールだけで、ACルールに一致するパケットは1パケット以上になる可能性があります。その理由はURL/DNSセキュリティインテリジェンスです。これらのイネーブルのいずれかがある場合、ファイアウォールはACポリシーによって評価されるすべてのセッションのアプリケーションを決定する必要があります。これは、アプリケーションがHTTPかDNSかを決定する必要があるためです。次に、ブラックリストに基づいてセッションを許可するかどうかを決定する必要があります。

firewall-engine-debugコマンドの出力の一部を次に示します。このコマンドに関連するフィールドが赤で強調表示されています。特定されたアプリケーションの名前を取得するために使用するコマンドに注意してください。

```
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 New session
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 Starting with minimum 4, 'inspect', and IPProto 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
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 pending rule order 4, 'inspect', XFF wait for AppId

[…omitted for brevity]

192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 Starting with minimum 4, 'inspect', and IPProto first with zones 1 -> 2, geo 0 -> 0, vlan 0,
inline sgt tag: untagged, ISE sgt id: 0, svc 846, payload -1, client 2000000846, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 no match rule order 4, 'inspect', XFF non-http
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 match rule order 5, 'trust server backup', action Trust


[! How to map service/application ID to name]
> expert
$ grep "^846[^0-9]" /var/sf/appid/odp/appMapping.data
846 SSH 32 0 0 ssh
```

例 2：信頼ルールに一致するトラフィックがブロックされる

一部のシナリオでは、ACPの信頼ルールが一致していても、トラフィックをブロックできます。次の例では、同じアクセスコントロールポリシーとホストのトラフィックを評価します。

```
192.168.62.3-54650 > 10.123.175.22-22 6 AS 1 I 0 New session
192.168.62.3-54650 > 10.123.175.22-22 6 AS 1 I 0 Starting with minimum 4, 'inspect', and IPProto 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
192.168.62.3-54650 > 10.123.175.22-22 6 AS 1 I 0 pending rule order 4, 'inspect', XFF wait for AppId
192.168.62.3-54650 > 10.123.175.22-22 6 AS 1 I 0 Deleting session

[!Session was deleted because we hit a drop IPS rule and blacklisted the flow.
This happened before AC rule was matched (Intrusion policy before AC rule match dropped).
Firewall engine will re-evaluate from top of AC policy to find a rule for logging decision]

192.168.62.3-54650 > 10.123.175.22-22 6 AS 1 I 0 Starting with minimum 0, id 0 and IPProto first with zones 1 -> 2, geo 0 -> 0, vlan 0, inline
sgt tag: 0, ISE sgt id: 0, svc -1, payload -1, client -1, misc -1, user 9999997, icmpType 102, icmpCode 22
192.168.62.3-54650 > 10.123.175.22-22 6 AS 1 I 0 no match rule order 3, 'Trust ssh for host', src network and GEO
192.168.62.3-54650 > 10.123.175.22-22 6 AS 1 I 0 no match rule order 4, 'inspect', XFF non-http
192.168.62.3-54650 > 10.123.175.22-22 6 AS 1 I 0 match rule order 5, 'trust server backup', action Trust
```

Action	Reason	Initiator IP	Responder IP	Source Port / ICMP Type	Destination Port / ICMP Code	Application Protocol	Client	Intrusion Events	Access Control Policy	Access Control Rule
Block	Intrusion Block	192.168.62.3	10.123.175.22	55654 / tcp	22 (ssh) / tcp				JG AC (all)	trust server backup

上記のように、**firewall-engine-debugの出力**は、トラフィックが「信頼」に一致していることを示しています。一方、接続イベントは、侵入ポリシールールによるブロックのアクションを示します(理由カラムが侵入ブロックを示すため**に決定されます**)。

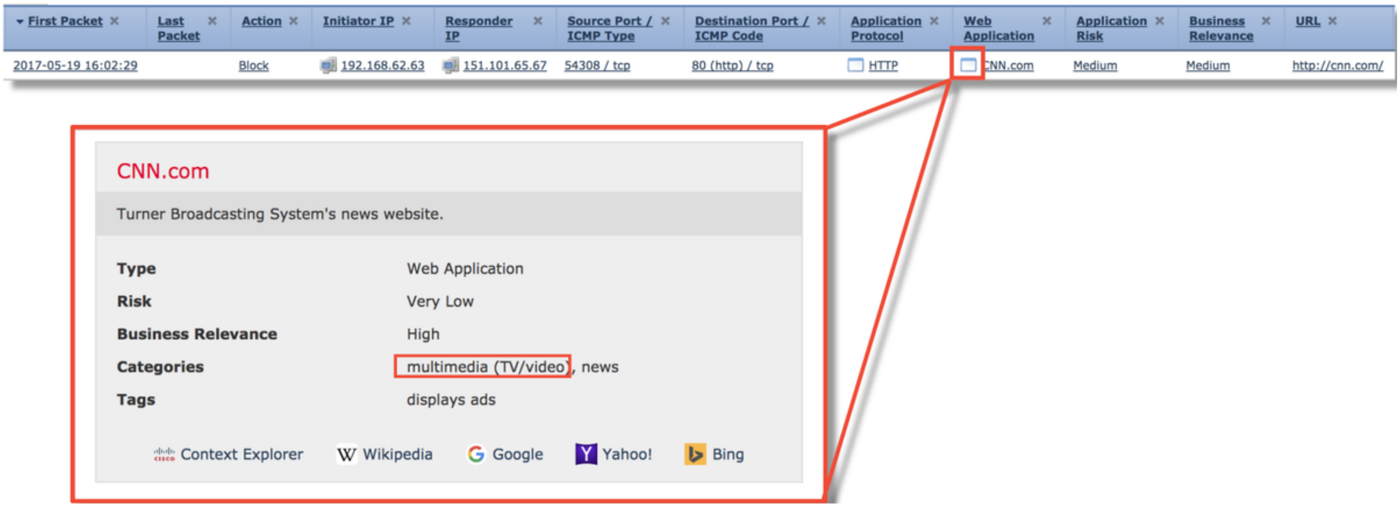
この問題が発生する理由は、ACPの[詳細設定]タブでアクセス制御ルールが設定される前に使用される侵入ポ**リシー**が原因です。ルールアクションごとにトラフィックが信頼される前に、対象の侵入ポリシーがパターン一致を特定し、トラフィックをドロップします。ただし、IPアドレスが「信頼サーバーのバックアップ」ルールの基準と一致しているため、ACPルールの評価は信頼ルールと一致します。

トラフィックが侵入ポリシー検査を受けないようにするには、信頼ルールを「検査」ルールの上に配置します。これは、どちらの場合でもベストプラクティスです。アプリケーションIDは「inspect」ルールの一致と非一致に必要なため、アクセスコントロールルールの前に使用される侵入ポリシーが決定さ**れ、同じルールで評価されるトラフィックに使用されます**。「trust server backup」ルールを「inspect」ルールの上に配置すると、最初のパケットが見つかった場合にトラフィックがルールと一致します。これは、最初のパケットで決定できるIPアドレスに基づいてルールが作成されるためです。したがって、アクセス制**御ルールの前に使用される侵入ポリシーを使用する**必要がないと判断されます。

シナリオ 3：アプリケーショントグによってブロックされるトラフィック

このシナリオでは、cnn.comがブロックされているとユーザが報告します。しかし、CNNをブロックする特定のルールはありません。Connection Eventsと**firewall-engine-debugの出力は**、ブロックの理由を示しています。

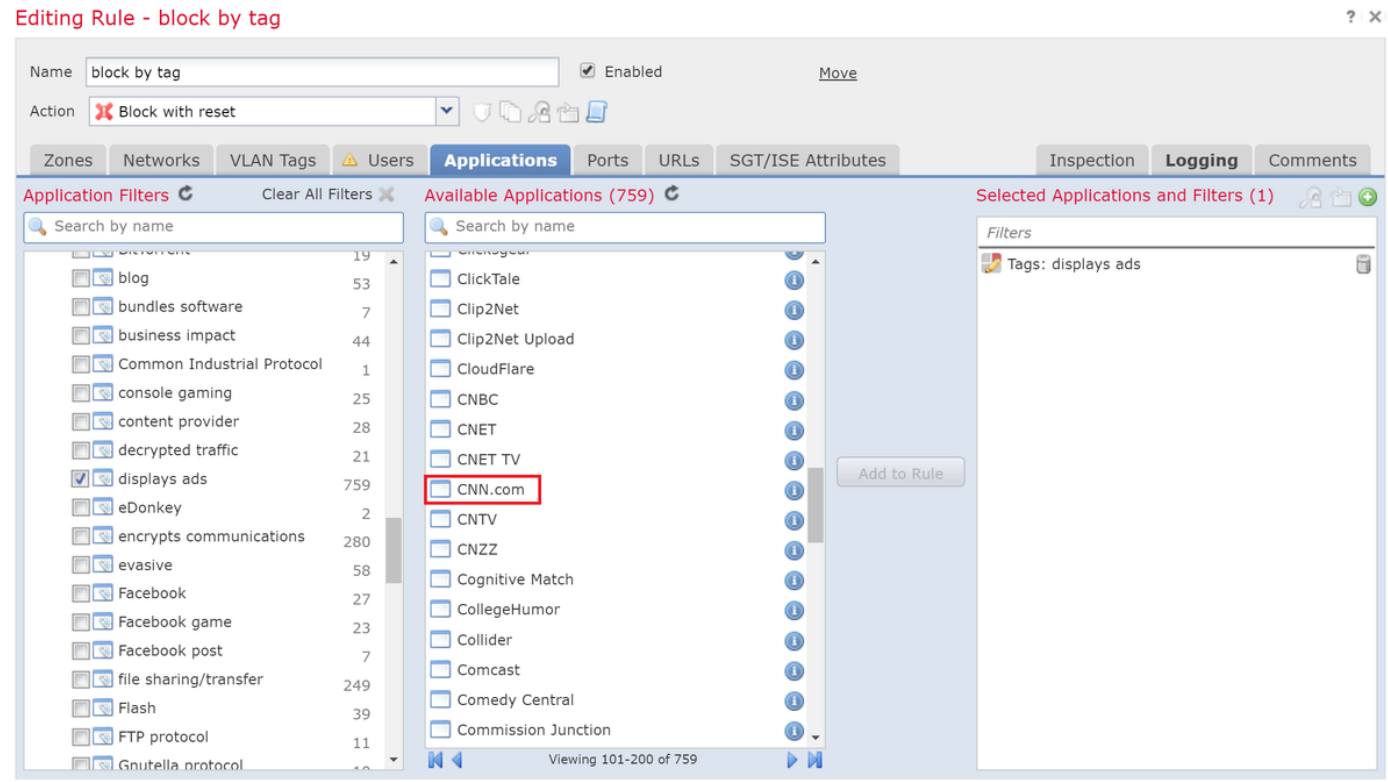
最初に、接続イベントには、アプリケーションに関する情報と、Firepowerがアプリケーションを分類する方法を示すアプリケーションフィールドの横に情報ボックスがあります。



この情報を念頭に置いて、**firewall-engine-debugが実行**されます。デバッグ出力では、トラフィックはアプリケーションタグに基づいてブロックされます。

```
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 New session
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 Starting with minimum 4, 'block by tag', 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
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 pending rule order 4, 'block by tag', AppID
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 Starting with minimum 4, 'block by tag', 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
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 pending rule order 4, 'block by tag', AppID
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 Starting with minimum 4, 'block by tag', 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
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 pending rule order 4, 'block by tag', AppID
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 URL SI: ShmDBLookupURL("http://cnn.com/") returned 0
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 Starting with minimum 4, 'block by tag', and SrcZone first with zones 1 -> 2, geo 0(0) -> 0,
vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc 676, payload 1190, client 638, misc 0, user 9999997, url http://cnn.com/, xff
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 match rule order 4, 'block by tag', action Block
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 sending block response of 605 bytes
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 Deleting session
```

http://cnn.comを明示的にブロックするルールがない場合でも、タグ付き表示**広告はACPルールのApplicationsタ**ブ内でブロックされています。



TACに提供するデータ

Data	手順
トラフィックを検査するFirepowerデバイスからのファイルのトラブルシューティング **system support firewall-engine-debugおよびsystem-support-trace出力** アクセスコントロールポリシーのエクスポート	http://www.cisco.c 手順については、 [システム(System ルポリシー(Acces

> **注意**：ACPにSSLポリシーが含まれている場合は、ACPからSSLポリシーを削除してから、機密PKI情報の開示を避けてください

次の手順：SSLポリシーレイヤのトラブルシューティング

SSLポリシーが使用中で、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で問題が明らかでない場合は、次のステップとしてSSLポリシーのトラブルシューティングを行います。