False positive 不正侵入を減らすオプション

目次

はじめに
False positive アラートを減らすオプション
1. Cisco テクニカル サポートに報告して下さい
2. ルールを信頼するか、または許可して下さい
3. 不必要なルールを無効に して下さい
4. しきい値 (Threshold)
5. 抑制
6. ファスト パス ルール
7. ルールを渡して下さい
8. SNORT_BPF 変数

概要

Intrusion Prevention System は警告 しますある特定の Snort ルールの余分生成するかもしれません。 アラートは true positive または false positive である可能性があります。 多くの false positive アラートを受け取る場合、それらを減らすあなたのために利用可能な複数のオプションがあります。 この技術情報は各オプションの利点と欠点の要約を提供します。

False positive アラートを減らすオプション

> **注:** これらのオプションは通常特定の状況のもとで最もよい選択、唯一のソリューションである場合もありますではないです。

1. Cisco テクニカル サポートに報告して下さい

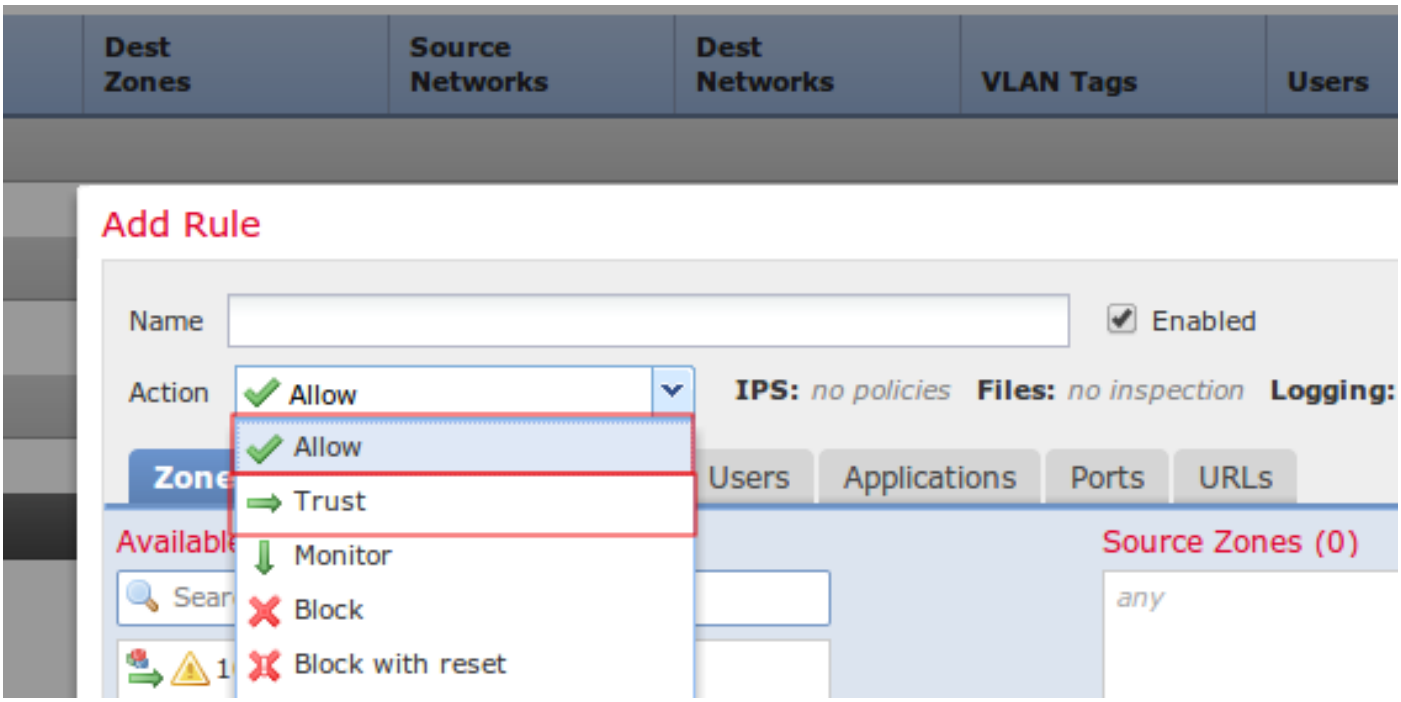
トリガーは良性トラフィックの警告 すること Snort ルールを見つけたら、Cisco テクニカル サポートにそれを報告して下さい。 報告されて、カスタマ サポート エンジニアは脆弱性調査チーム (VRT) に問題を増やします。 VRT はルールに可能性のある機能強化を研究します。 改善されたルールは利用可能である、また次の公式ルール アップデートに追加されますとすぐレポーターにふつう利用でき。

2. 信頼か割り当てルール

パススルーへの信頼されたトラフィックを許可するための最もよいオプションは関連する不正侵入ポリシーなしでインスペクションのない Sourcefire アプライアンス**信頼**または**割り当て**操作をイネーブルにしています。 信頼または割り当てルールを、ナビゲート **ポリシー > アクセス制御 > ルール**。 に設定するため Add

> **注:** そのようなルールが FirePOWER ハードウェアで処理することができるのでトラフィック ユーザを一致するために設定されない一致する信頼または割り当てルールにアプリケーション、または URL に Sourcefire アプライアンスの全体的なパフォーマンスの最小限の影

響があります。



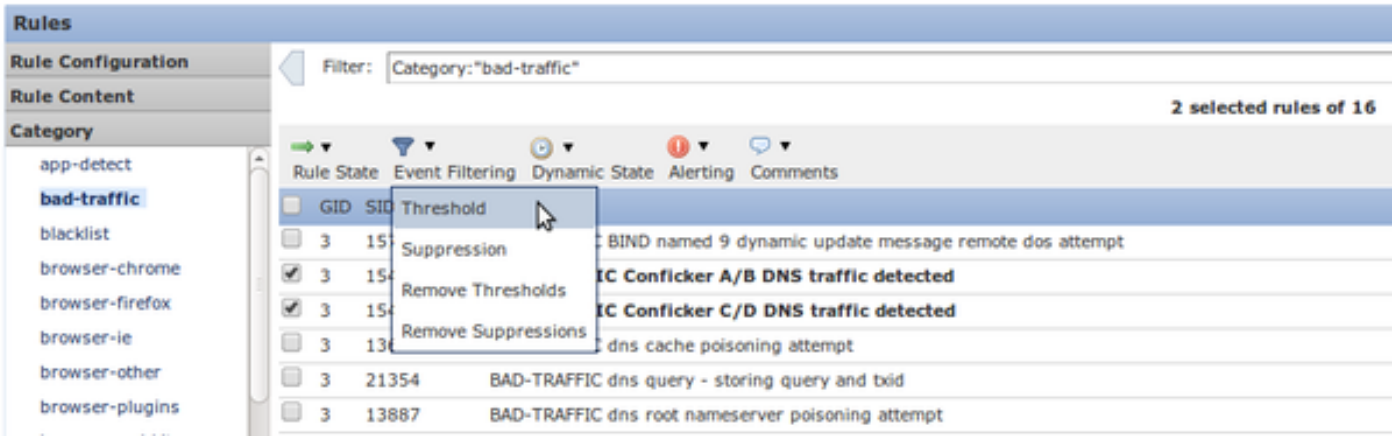
図： 信頼ルールの設定

3. ディセーブル不必要なルール

古く、修正された脆弱性を目標とする Snort ルールを無効に することができます。 それはパフォーマンスを改善し、false positive を減らします。 SireSIGHT を使用する推奨事項はこのタスクと助けることができます。 さらに、頻繁に名誉棄損とならない低優先順位アラートかアラートを生成するルールは不正侵入ポリシーからの削除のためのよい候補であるかもしれません。

4. しきい値 (Threshold)

不正侵入イベントの数を減らすのに**しきい値を**使用できます。 これは一定量のパケットより多くがルールを一致する場合規則的に正常なトラフィックのイベントの限られた数を誘発するとルールが期待されるで問題の示す値である可能性がありますとき設定するべきよいオプション。 騒々しいルールによって引き起こされるイベントの数を減らすのにこのオプションを使用できます。



図： しきい値の設定

5. 抑制

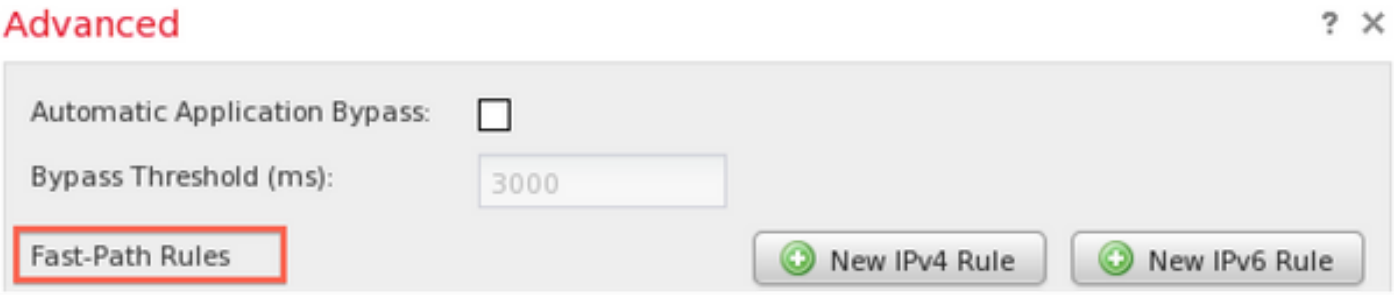
完全にイベントの通知を除去するのに**抑制を**使用できます。 それは**しきい値**オプションへの設定された類似したです。

> **注意**： 抑制はイベントが生成されない間、Snort がまだトラフィックを処理しなければならないのでパフォーマンス上の問題を導くことができます。

> **注:** 抑制はトラフィックの廃棄からのドロップするルールを防ぎません、従ってドロップするルールと一致するときトラフィックは無言で廃棄されるかもしれません。

6. ファスト パス ルール

類似したアクセス制御ポリシーのルールを許可するために信頼し、ファスト パス ルールはバイパス インスペクションまたできます。 Cisco テクニカル サポートは通常アクセス制御ルールがほとんど常に十分な間、**Device ページ**の **Advanced ウィンドウ**でファスト パス ルールを使用することを設定される推奨しないし、ので容易に見落とされるかもしれません。



図： ファスト パスは Advanced ウィンドウのオプションを支配します。

ファスト パス ルールの使用への唯一の長所はすばらしい最大トラフィック量を処理できることです。 ファスト パス ルールはハードウェア レベルでトラフィックを（NMSB として知られている）処理し、トラフィックの 200 Gbps まで論理上処理できます。 それに対して、**信頼**のルールはネットワーク 流 れ エンジン（NFE）にアクションを促進され、トラフィックの 40 Gbps の最高値を処理できます**可能にし**。

> **注:** ファスト パス ルールは 8000 シリーズ デバイスおよび 3D9900 だけで利用できます。

7. ルールを渡して下さい

トラフィックで引き起こすことからの特定のルールをある特定のホストから防ぐために（そのホストからの他のトラフィックが検査される必要がある間、）、パス型 Snort ルールを使用して下さい。 実際、これはそれを達成する唯一の方法です。 パス ルールが有効な間、パス ルールが手動で書かれているので維持し非常ににくい場合もあります。 パス ルールのオリジナル ルールがルール アップデートによって修正されればさらに、すべての関連パス ルールは手動でアップデートされる必要があります。 さもなければそれらは非効果的になるかもしれません。

8. SNORT_BPF 変数

不正侵入ポリシーの `Snort_BPF` 変数はインスペクションをバイパスすることをある特定のトラ

フィックが可能にします。 この変数がレガシー ソフトウェア バージョンの最初の選択の 1 つの間、Cisco テク二カル サポートは粒状、より目に見える、および設定することはもっと簡単であるのでインスペクションをバイパスするアクセス制御ポリシー ルールを使用するために推奨します。