NGFW ポリシーの運用順序

初版発行日：2018 年 5 月 22 日
最終更新日：2018 年 6 月 15 日

目次

ポリシーの運用順序 2
はじめに：目的： 2
ポリシー ファイアウォール：ファンネル アプローチ（脅威の嵐）： 3
よくある誤解： 3
ファイアウォール ファンネル モデル： 3
運用順序におけるベスト プラクティス： 5
パケットおよびポリシー チェックポイントのパス： 6
ポリシー順序のベスト プラクティス： 7
ポリシーの継承： 8
脅威ポリシーの多様性： 8
セキュリティ インテリジェンス（IP ベース）： 9
セキュリティ インテリジェンス (URL)： 9
セキュリティ インテリジェンス (DNS)： 9
アプリケーションの検出： 10
マルウェアおよびファイルの検出： 11
侵入防御： 11
IPS 変数の考慮事項： 11
IPS 変数をレビューする理由： 13

© 2018 Cisco Systems, Inc. All rights reserved.

Firepower 推奨の考慮事項： 13
アーキテクチャにおける考慮事項： 14
NG 4100/9300： 15
特別なプラットフォームの考慮事項： 15
プラットフォーム固有のベスト プラクティス： 16
NG 2100： 16
特別なプラットフォームの考慮事項： 16
プラットフォーム固有のベスト プラクティス： 17
vFTD/ASA 5500-X FTD 17
特別なプラットフォームの考慮事項： 17
プラットフォーム固有のベスト プラクティス： 17
運用順序に与える影響 18
法的情報： 18

ポリシーの運用順序

はじめに：目的：

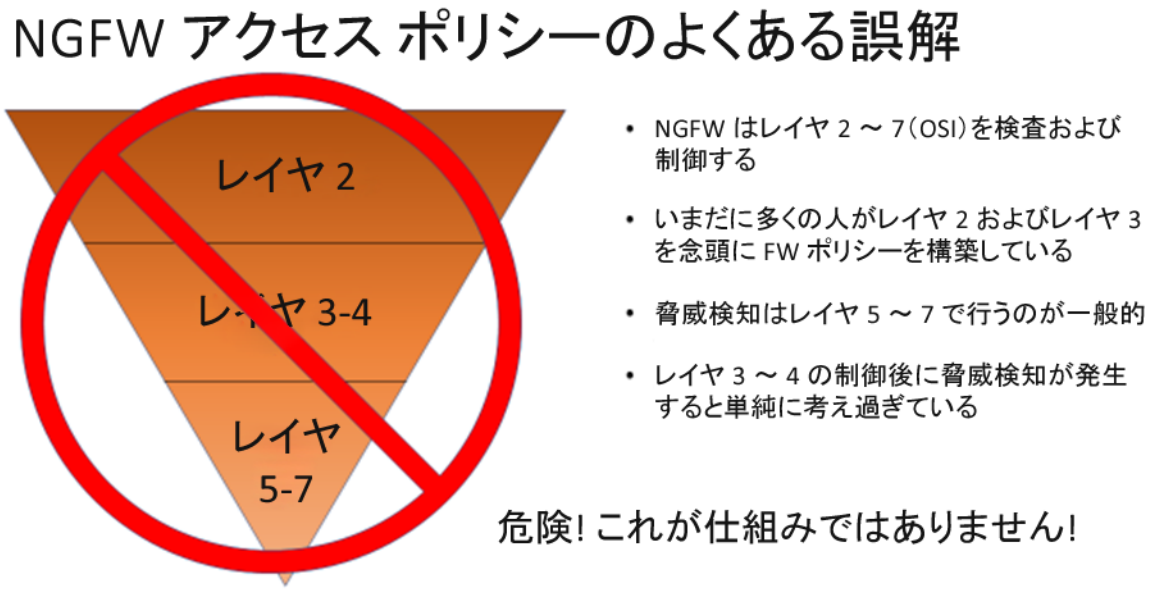
セキュリティの効果とデバイスのパフォーマンスの両方で起こりうる課題を避けるには、アクセス コントロール ポリシー内でルールを正しい順序に並べることが重要です。アーキテクチャの制約を理解せずにルールの順序を間違えると、不要なレイヤ 5 ～ 7 インスペクションが原因でパフォーマンスが低下したり、デバイスのセキュリティ効果が低下したりする可能性があります。このドキュメントの目的は、アーキテクチャの制約を考慮したうえで、Firepower システムのアクセス コントロール ポリシー内の順序についてのベスト プラクティスを包括的に理解することです。このドキュメントを読み終えると、ポリシーの運用順序に関するベスト プラクティス、およびアクセス コントロール ポリシーの設計時に重視すべきアーキテクチャの考慮事項について理解できるようになります。

© 2018 Cisco Systems, Inc. All rights reserved.

ポリシー ファイアウォール：ファンネル アプローチ（脅威の嵐）：

よくある誤解：

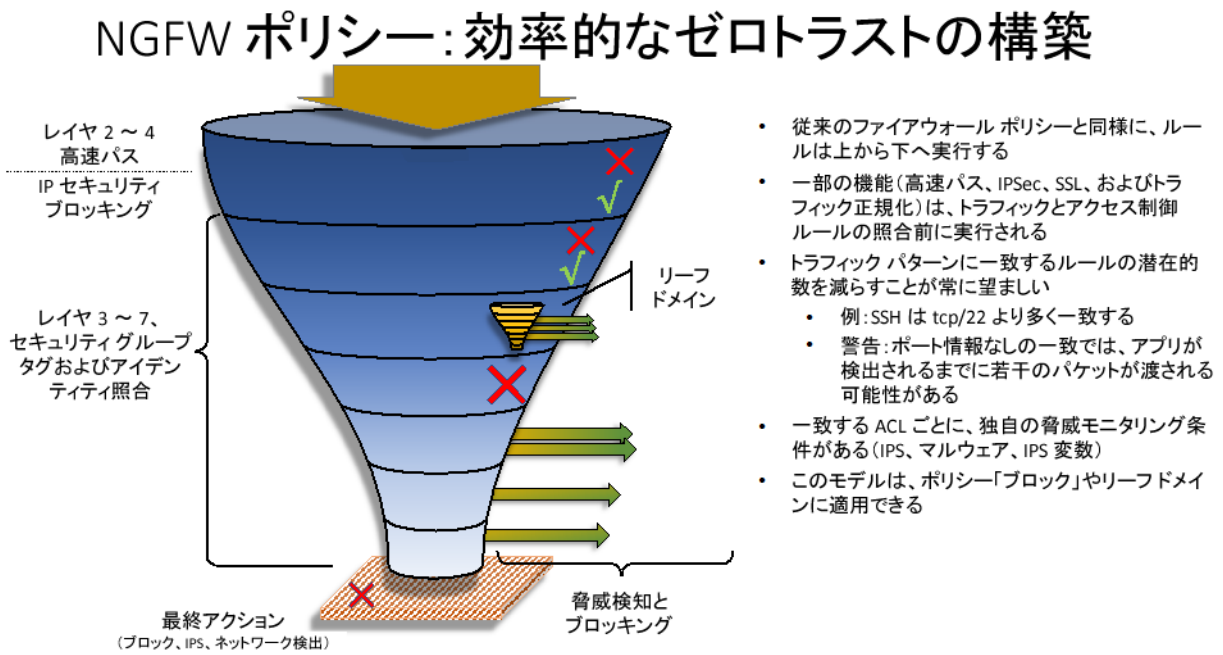
脅威のモニタリングや脅威の制御に関するテクノロジーを追加した結果、ファイアウォール ポリシーの実装方法に予期していなかった副作用が生じました。ファイアウォール ポリシーの最適化では、ファイアウォール ルール スタックの最上位でできるだけ多くのブロックを最適化するということがよく知られています。その結果、脅威の検出をファイアウォールの ACL ルールの前または後で発生するアクションであると捉えるユーザが出てきました。このような誤解は、パフォーマンスのさらなる悪化につながり、さらには「許可」アクセス ルールに一致するトラフィックに潜む可能性のある脅威シナリオを見落としてしまうリスクがあります。



ファイアウォール ファンネル モデル：

ファイアウォール ファンネル モデルは、ファイアウォールおよびセキュリティに対する脅威の管理者が、一貫したアプローチ構築と次世代ファイアウォール ポリシーを視覚化できる方法として作成されました。

© 2018 Cisco Systems, Inc. All rights reserved.



上図は、ファイアウォールのアクセス コントロール ポリシーをファンネルとしてモデル化したものです。ファンネルの考え方は、ブロックできるトラフィックや、脅威検知をさらに必要としないトラフィックを早期に削除する、というものです。下側のレイヤになるほど、下へ進む必要のあるトラフィック パターンが段階的に少なくなることが、このモデルからわかります。これは特にアプリケーションベースのトラフィック照合で当てはまります（例：HTTP トラフィックに一致するルールと TCP ポート 80 トラフィックに一致するルール）。ファンネルの最上位レイヤは、レイヤ 2 ～ 4 のトラフィックのみを評価します。アプリケーション検出、URL、アイデンティティなどさらに多くの条件が含まれると、追加のプロセスを使用してそれらの条件を特定します。最上位レイヤは 2 つのポリシー要素で処理されます。1 つ目は高速パス ポリシーで、照合がハードウェア内だけで実行され、2 つ目はアクセス コントロール ポリシーで、照合がソフトウェア内で実行されます。

セッション トラフィックがアクセス制御ルールにマッピングされると、照合セッションに追加の脅威検出機能を適用できます。この脅威検知は、IPS エンジン、ファイル/マルウェア検出エンジン、またはその両方で実行できます。つまり、許可されたセッション内で発生しうる検出パターンのみが確実に使用される IPS ポリシー（Snort 変数設定や IPS ルール選択など）を配備できるような最適化の考慮事項がさらにあるということです。

© 2018 Cisco Systems, Inc. All rights reserved.

運用順序におけるベスト プラクティス：

アクセス コントロール ポリシーを設計するときの目標は、情報がアクセス制御ルールに一致するまでの所要時間を最低限に留めることです。また、不要なレイヤ 7 インスペクションが発生する回数を制限することです。

シナリオ例：

ポート 443 宛てのすべてのトラフィックをブロックするには、そのルールが、アプリケーション フィルタや待つ必要のある情報が含まれるルールよりも下にならないようにします。

以下のようなアクセス コントロール ポリシーの例を見てみましょう。

ルール 1：Google Drive のトラフィックを許可し、IPS で検査する
ルール 2：ポート 22 を信頼する
ルール 3：ポート 443 をブロックする
ルール 4：その他すべてのトラフィックをブロックする

このアクセス コントロール ポリシーを宛先ポート 443 の TCP 接続に適用すると、パケット フローおよびパケット アクションは次のようになります。

パケット 1：Syn <- 保留中ルール 1
パケット 2：Syn-Ack <- 保留中のルール 1
パケット 3：Ack <- 保留中のルール 1
パケット 4：SSL クライアント Hello <- 保留中のルール 1 で Google 証明書または Google Drive URI を探す
+ これは Google Drive のサブジェクト名識別子で一致する可能性がある
パケット 5：ルール 3 が一致し、トラフィックがブロックされる

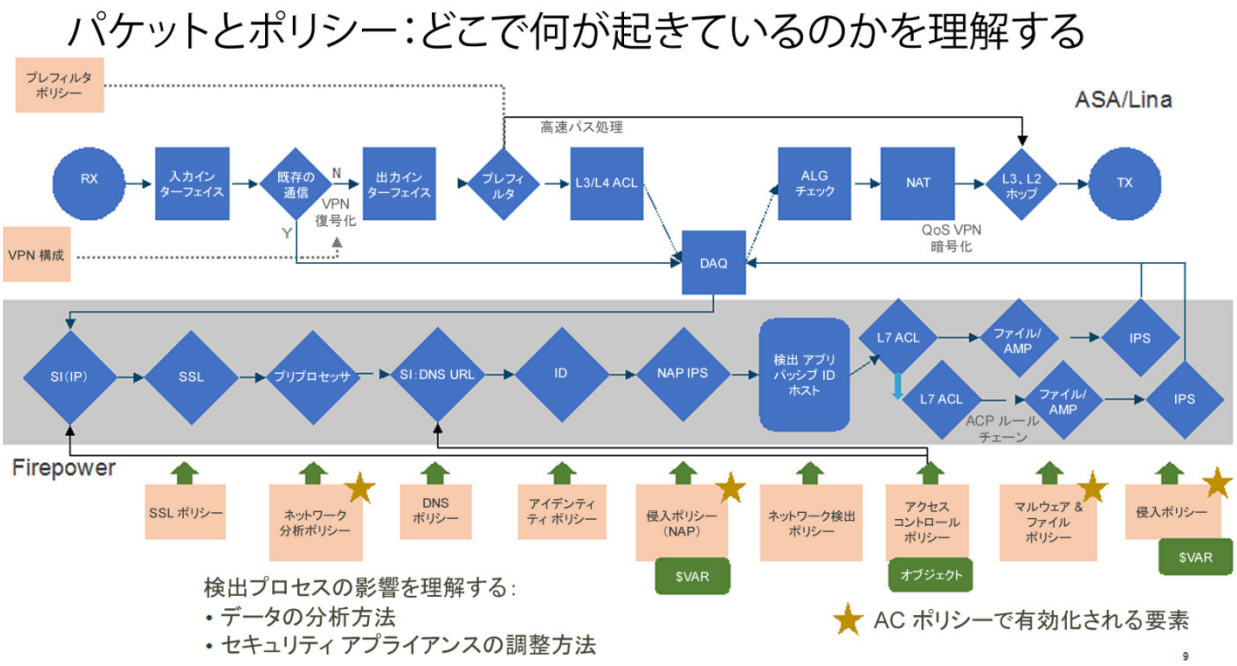
ポート 443 トラフィックをブロックしたいにもかかわらず、このパケット フローの先頭 4 パケットはブロックされません。また、このトラフィックは未検査の状態で送信することはできず、アクセス コントロール ポリシーの [詳細 (Advanced)] セクションで設定される「アクセス制御ルールの決定前に使用された侵入ポリシー」へ送信されます。つまり、最初のパケットに基づいてフローをブロックする場合と比べて、このトラフィックがネットワークに影響を及ぼすリスクもパフォーマンスへの影響も大きくなります。

© 2018 Cisco Systems, Inc. All rights reserved.

効率性を高め、セキュリティ効果を向上させるには、ルール 3 とルール 2 をルール 1 より上にしなければなりません。

一般的に望ましい順序としては、レイヤ 1 ～ 4 のブロック、1 ～ 4 の信頼ルール、レイヤ 5 ～ 7 の明示的ブロック、レイヤ 1 ～ 7 の許可ルール、そして最後にデフォルトのブロック アクションにします。こうすることで、トラフィックのインスペクションにおいてアクセス制御ルールに一致するかどうかの情報を待つための時間が削減されます。

パケットおよびポリシー チェックポイントのパス：



パケット（および関連フロー）が Firepower Threat Defense を通過する際の詳細なパスを理解すると、検出の最適化も簡単になります。このモデルは、各エンジン（および関連する設定ポリシー）が最終的にパケットに対して何らかの分析や制御を実行する様子を示しています。

© 2018 Cisco Systems, Inc. All rights reserved.

注意すべき最適化の重要ポイントをいくつか示します。

- 一致する可能性があり、ブロックされる（または高速パスで信頼されるために許可される）レイヤ 2 ～ 4 のトラフィックは、ハードウェア内だけでトラフィックを処理します。
- セキュリティ インテリジェンス（IP ベース）は、Firepower 層で発生する最初の検出条件です。このトラフィックはすべてブロックされ（ブロック状態に設定されている場合）、インスペクションはその後発生しません。その結果、攻撃分析をさらに必要としないアクティブな脅威キャンペーンを停止することで、脅威モニタリングを実質的に最適化できます。
- 多くのユーザが考慮しない追加の IPS ポリシーとして、アプリケーション検出の前に侵入ポリシーが発生します。このポリシーは、アクセス コントロール ポリシーの [詳細 (Advanced)] タブで設定し、アプリケーション検出フローでまだ一致していないトラフィックに対して脅威検出を実行します。通常、この状態に気付くのは、特定の IPS ポリシー内で IPS ブロックを無効化しようとしていて、Firepower Threat Defense がトラフィックをブロックし続けていることがわかったときです。そのような場合は、アクセス コントロール ポリシーの [詳細 (Advanced)] セクションをチェックしてください。

ポリシー順序のベスト プラクティス：

1.) OSI レイヤ 1 ～ 4 情報のみに基づき、ブロックするすべてのトラフィックについて、プレフィルタ ブロック ルールを 1 つまたは複数作成します（注：後述するプラットフォーム固有の考慮事項およびベスト プラクティスを十分考慮してください）

2.) OSI レイヤ 1 ～ 3 情報に基づき、レイヤ 7 インスペクションを回避するすべてのトラフィックについて、プレフィルタ高速パス ルールを 1 つまたは複数作成します（注：後述するプラットフォーム固有の考慮事項およびベスト プラクティスを十分考慮してください）

3.) （プラットフォーム固有）前述のプラットフォームに関する考慮事項において必要な場合は、OSI レイヤ 1 ～ 4 に基づいてブロックはするがオフロードしないすべてのトラフィックについて、1 つまたは複数のアクセス制御ブロック ルールを作成します

4.) （プラットフォーム固有）前述のプラットフォームに関する考慮事項において必要な場合は、OSI レイヤ 1 ～ 4 に基づいて信頼はするがオフロードしないすべてのトラフィックについて、1 つまたは複数のアクセス制御信頼ルールを作成します

© 2018 Cisco Systems, Inc. All rights reserved.

5.) OSI レイヤ 5 以上に基づいて明示的にブロックするすべてのトラフィックについて、1 つまたは複数のアクセス制御ブロック ルールを作成し、ベスト プラクティス 5 で作成したルールの直下に配置します
6.) 対象を絞ったレイヤ 7 インスペクション ポリシーに基づいて許可および検査するすべてのトラフィックについて、1 つまたは複数のアクセス制御許可ルールを作成します
7.) 汎用のレイヤ 7 インスペクション ポリシーで検査するトラフィックについて、1 つまたは複数のアクセス制御許可ルールを作成します

ポリシーの継承：

Firepower システムでは、アクセス コントロール ポリシーおよび侵入ポリシーを継承できます。これらの機能は、多様なアクセス コントロール ポリシーを利用する環境において、ポリシーの運用順序におけるベスト プラクティスに確実に従うときに非常に役立ちます。

多くの場合で最適な方法は、前述したポリシー順序のベスト プラクティスごとに、[アクセス制御ルール (Access Control Rule)] セクション/カテゴリが含まれるアクセス コントロール ポリシーから作成して継承することです。ただし、注意の必要な例外として、プレフィルタ ポリシーがあり、これは継承できません。その他すべてのポリシーの基準となり、ベスト プラクティスのセクションを適用する元となるアクセス コントロール ポリシーを作成することで、その他のユーザが引き続きパフォーマンスと効果を最適化する位置にルールを配置できるようにします。

脅威ポリシーの多様性：

Cisco Firepower Threat Defense には、インスペクション パスとともに動作する検出機能がいくつかあります。これには次が含まれます。

© 2018 Cisco Systems, Inc. All rights reserved.

セキュリティ インテリジェンス（IP ベース）：

アクセス コントロール ポリシー内で設定し、IP アドレス一覧をモニタまたはブロックします。通常は、アクティブな脅威キャンペーンをブラックリストに登録するために使用され、脅威フィード（RSS を介した Talos やサード パーティのフィード、FMC の Threat Intel Director など）によって更新されます。照合は、ハードウェア アクセラレーション ACL の直後に発生するため、全面的に信頼できる具体的な IP アドレスをグローバルにホワイトリスト登録する場にもなります。ただし、ホワイトリスト登録した場合、その IP は将来の脅威シナリオから除外されることがあるので注意してください。

セキュリティ インテリジェンス (URL)：

脅威ベースの URL モニタリングは、トラフィック正規化の後に実行されます（ネットワーク分析ポリシー プリプロセッサで設定）。このコンポーネントは、Cisco Talos が提供する URL、ローカルで設定された URL オブジェクト（FMC 内の [オブジェクト (Objects)] ページで設定）、またはサードパーティ フィード（FMC で Threat Intel Director からフィードされるもの）に基づいてトラフィックをブロック（またはホワイトリスト化）します。この機能はアクセス制御ルールで発生する URL 照合と異なることに注意してください。アクセス コントロール ポリシーによる URL フィルタリングは、コンテンツ分類およびリスク軽減フィルタであると言えます。これは、このエンジンによってブロックされる URL は、インスペクション パスを下へたどって、さらに検出が開始されないということでもあります。

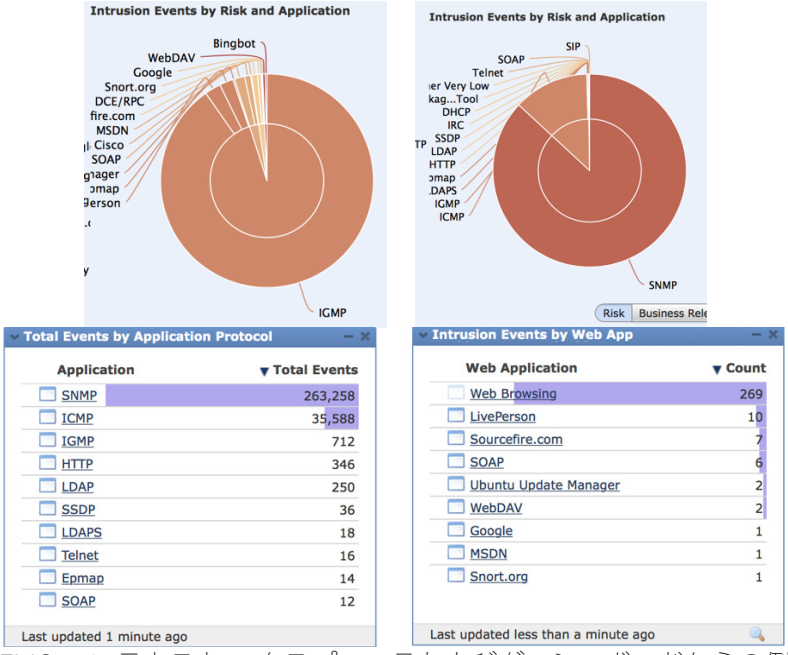
セキュリティ インテリジェンス (DNS)：

IP や URL によるセキュリティ インテリジェンス モニタと同様に、Cisco Talos、ローカルで設定されたオブジェクト、またはサードパーティ フィードによるデータで有効化される、脅威に焦点を当てたエンジンです。このコンポーネントは、DNS リクエストを脅威フィードと照合します。ほぼすべての接続リクエストがドメイン解決を必要とするため、脅威が実装された可能性のあるセッションを開始させないようにすることで、多くの場合で追加の処理をさらに削減するための方法になります。

© 2018 Cisco Systems, Inc. All rights reserved.

アプリケーションの検出：

アプリケーションは、実際には脅威検出コンポーネントではありませんが、リスクの軽減に取り掛かる手段になります。注意深いアナリストは、IPS ファイルおよびマルウェア イベントに関連付けられているアプリケーション セッションを定期的にレビューするでしょう。アプリケーションが脅威の条件と深く関連付けられている場合は、そのようなアプリケーションを全面的にブロックする価値があるかもしれません。



（FMC コンテキスト エクスプローラおよびダッシュボードからの例）

Firepower Threat Defense の OpenApp ID 機能も、検出およびトラフィック制御をさらに強化するメカニズムを提供します。使用例によっては、カスタム アプリケーションの照合が含まれたり、さらには以後のインスペクションに含めたり除外したりする FQDN に基づくアプリケーションの作成が含まれたりする可能性があります。

アプリケーション検出、ホスト プロファイリング、およびパッシブ ユーザ識別はすべて、ネットワーク検出ポリシー内で有効です。

© 2018 Cisco Systems, Inc. All rights reserved.

マルウェアおよびファイルの検出：

この機能はマルウェアおよびファイル ポリシーで設定し、セッションが照合アクセス制御ルールに合格すると、対応する IPS ポリシーがアクセス制御ルールで設定されている場合はその IPS ポリシーに渡されるまでに処理されます。この機能には、ファイル制御とマルウェア検出/ブロッキングという 2 つの重要なコンポーネントがあります。ファイル検出に必要な処理や時間は、マルウェア検出よりも大幅に少なくてすみます。管理者は、ファイル ブロッキングを使用して不要なファイル タイプがネットワーク境界を通過しないようにすることで、リスク軽減とパフォーマンス向上を実現し、可能な場合はアクセス制御ルール スタックの高位で実行させることができます。

ファイル検出とマルウェア検出の両方において、管理者はトラフィック ストリームでファイルを検査できるように検討しなければなりません。たとえば、（アプリケーションによる）SSL または SSH トラフィックに対して「許可」するアクセス制御ルールは、ユーザがファイル ポリシーを有効にすることを許可しません。しかし、ポート TCP/port 22 トラフィックに対する同様のルールが有効な場合、ファイル ポリシーを有効にできますが、トラフィックが合格することを実際に検査できない場合があります。

侵入防御：

Snort® IPS エンジン上に構築される、ディープパケット インスペクション エンジンに基づくルールです。IPS ルールは、Cisco Talos から提供されますが、オープン ソースの Snort® ルール言語で記述されたサードパーティ ルールを含めることもできます。管理者は、Cisco Talos から提供されるデフォルト ポリシーのなかから選択し、そのポリシー上に構築することも、環境に合わせてポリシーをカスタマイズすることもできます。

IPS 変数の考慮事項：

各 IPS ルールでは、少なくとも 2 つの変数 $HOME_NET および $EXTERNAL_NET を使用します。これらの変数を使用すると、境界を通過する脅威に関して、IPS の方向性を得ることができます。変数の設定内容は、IPS ルールにマッピングされる可能性のあるセッション数に影響を及ぼすため、確認できるイベントの数やパフォーマンスの程度に多少なりとも影響します。

このことを理解すれば、変数を調整して a)（検査するフローを少なくすることで）イベント数を減らすことも、または b) 網に引っ掛かった侵害の可能性がある条件を示すこともできます。[オブジェクト管理 (Object Management)] ページで変数セットを変更したり独自に作成したりすることができます。左側の一覧から [変数セット (Variable Sets)] を探してください。

© 2018 Cisco Systems, Inc. All rights reserved.

$HOME_NET のデフォルトは、通常は IPv4 プライベート IP スペースです。パブリック IP アドレスを使用している場合、IPS は、ユーザがそのアドレスを $HOME_NET 変数に含めようとしていると判断することがあります。初期の実装コンサルタントがそう助言している可能性が非常にあります。

$EXTERNAL_NET は、通常、ほとんどのカスタム サイトで 2 つの状態のいずれかに設定されています。「!$HOME_NET」（「!」文字は変数や検索クエリ内で「否定」条件として使用される）または「any」です。さまざまな AC ルールに対して設定する内容によって、結果が変化する可能性があります。

脆弱性に対する攻撃をモニタする IPS ルールのほとんどは、$EXTERNAL_NET -> $HOME_NET のように記述されます。これは、次の条件を意味します。

IPS ルールの設定	$External_NET	→	$HOME_NET	脆弱性がエクスプロイトされたとき
変数設定	! $HOME_NET	→	<内部 IP スペース>	
攻撃 1	送信元：Ext_IP	→	宛先：Int_IP	IPS は検査する
攻撃 2	送信元：Int_IP	→	宛先：Int_IP	IPS は検査しない
攻撃 3	送信元：Int_IP	→	宛先：Ext_IP	IPS は検査しない

攻撃 2 は内部でエクスプロイトされたアセットが別の内部アセットを攻撃している可能性があることに注意してください。これは、WannaCry のような脅威で見られました。攻撃 3 は、ネットワーク内にある侵害されたアセットが今度は外部アセットを攻撃しているシナリオが考えられます（気付かずにボットネットに参加しているモバイルユーザなど）。攻撃 3 が検出されたら、それは侵入の痕跡であり、見つける価値があったということです。

「簡単な」解決法は、両方の変数を「any」にすることです。しかしこの場合は、IPS エンジンに不要な需要が発生し、必要以上にイベントが生成される可能性があります。

Talos から提供される侵入の痕跡ルールは、記述が異なります。すでに侵害されている内部デバイスによる動作を探し、外部の攻撃者にアクセスを試みるため、$HOME_NET à $EXTERNAL_NET のように記述されています。この記述は、これらのルールが使用されるほとんどすべての個所で、発生する条件そのものです。つまり、内部アセット同士、または外部アセットから内部アセットへの検出は発生しないということです。このようなルールでは、$External_NET を「! $HOME_NET」にすることをお勧めします。

© 2018 Cisco Systems, Inc. All rights reserved.

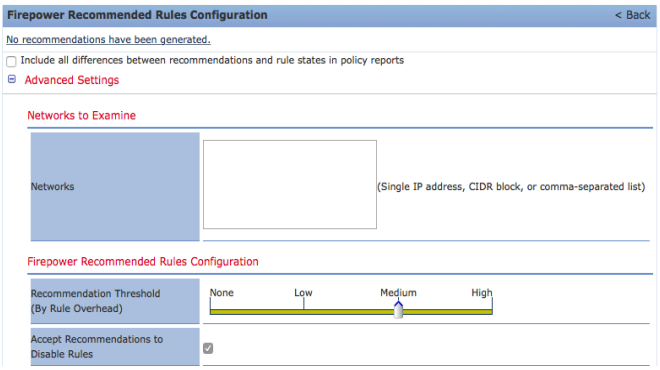
必要に応じて、アクセス制御ルール内の検出をさまざまな変数に基づいて改善できます。インターネットとの間の内部ユーザ トラフィックの場合は、$EXTERNAL_NET を「Not $HOME_NET」に設定できます。内部同士のトラフィックを制御するアクセス ルールの場合は、変数の $External_NET を「any」または内部アドレス空間に設定できます。AC ポリシー ルールでこれらの点に留意すると、IPS ポリシーをますます隙のないものにして、すでに侵害されているデバイスを捕捉でき、ノイズを減らせる可能性もあります。

IPS 変数をレビューする理由：

これらすべてが共有されるため、イベント分析ロジックと組み合わせて、検出条件と方向性に関する組み込みの思想の両方を考慮できます。特定の検出ポイントにおける変数条件を理解しておくと、Firepower Management Center 内の影響分析を利用するときは特に、イベント分析をより効率的に優先順位付けするのに役立ちます。変数の利用方法は、アクセス制御の構成およびローカルの脅威検出の関心事項に基づいてください。

Firepower 推奨の考慮事項：

Firepower Management Center (FMC) には、ネットワーク内のホスト上に存在する可能性のある潜在的脆弱性に一致する IPS ルールを FTD 管理者に推奨する機能があります。この機能の最適化にあたっては、3 つの重要なコンポーネントを考慮してください。



- [検証するネットワーク (Networks to Examine)] では、ホスト脆弱性のマッピングのための IPS ルールと考えられる IP アドレスを選択します。複数の IPS ポリシーが使用されている場合、または IPS ポリシーが特定のトラフィック条件に組み込まれている場合、このコンポーネント内で使用している CIDR のみが、特定の IPS ポリシーでモニタしているトラフィック内で実際に観察されるホストの IP アドレスに沿っていることを確認してください。
- [推奨しきい値 (Recommendation Threshold)] は、選択すべき IPS ルールを Firepower Recommendations に通知します。IPS ルールは、パフォーマンスへの影響が [低 (Low)]、[中 (Medium)]、[高 (High)] として分類されます。[低 (Low)] を選択すると、パフォーマンスの影響が低いルールのみが推奨されます。[高 (High)] を選択すると、脆弱性マッピングで一致するすべてのルールが含まれます。これは IPS ルールの優先度に基づくものではないことに注意してください（IPS ルールの優先度にも [低 (Low)]、[中 (Medium)]、[高 (High)] というラベルが付いています）。

© 2018 Cisco Systems, Inc. All rights reserved.

- [Accept Recommendation to Disable Rules（ルールを無効化するための推奨を受け入れる）] では、ネットワーク内のホストの潜在的脆弱性にマッピングされない IPS ルールが無効になるため、IPS ポリシー内で有効になる IPS ルールを大幅に減らすことができます。あまり予期されない副作用としては、Firepower システム内の IPS ルールの多くは脆弱性マッピングを含まないため、その項目がチェックされるときに無効になっています。たとえば、[侵入の痕跡 (Indication of Compromise)] 大項目内の IPS には、CVE または脆弱性リファレンスがまったくと言っていいほどありません。このような検出もその他の検出も、すでに侵害されているホスト、潜在的なポリシー違反、またはネットワーク内で明白なその他のリスク要因の検索を利用しています。

  これを最適化する方法は 2 つあり、多くの組織では両方を使用しています。1 つ目は、内部間の検出条件用です。ユーザはこのアクションを無効にすることも、IPS ポリシー内に IPS ポリシー階層を作成して特定のポリシー考慮事項を有効にすることもできます。

  もう 1 つは、外部とつながるトラフィックでこの項目をオフのままにすることです。侵入の痕跡（および同様のルール）はほとんどが $HOME_NET から $EXTERNAL_NET（つまり内部から外部）のトラフィック パターンに基づくため、この項目をオフのままにすることで、侵入の痕跡に関するシスコの推奨事項が自動的に無効にならないことが保証されます。

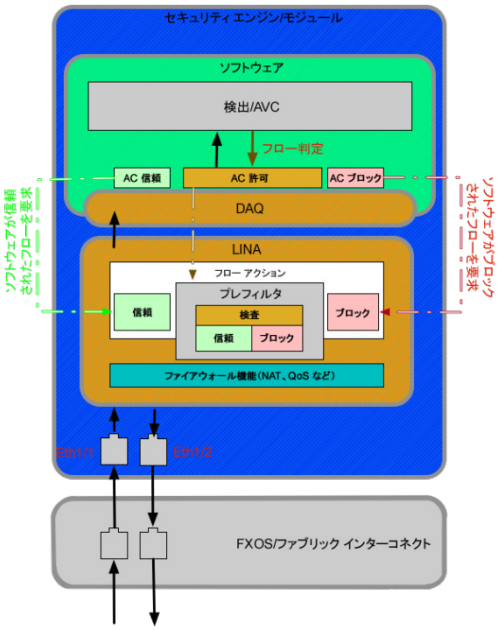
  境界 IPS ポリシー内でこの項目をオンのままにした場合、IPS ポリシー設定エンジン内で検索フィルタ metadata:" impact_flag red" を使用して検索することにより、このようなルールのほとんどを特定できます。

アーキテクチャにおける考慮事項：

利用しているアーキテクチャによって、アクセス コントロール ポリシーの最適な運用順序の設計に影響があります。アーキテクチャごとに、プレフィルタ高速パス トラフィックは、ASIC にオフロードされるかどうか、およびレイヤ 7 インスペクションとリソースを共有するプロセスによって提供されるかどうかが異なります。アクセス制御の運用順序におけるベスト プラクティスに与える主な影響は、プレフィルタ高速パスで処理されるトラフィック、およびアクセス コントロール ポリシーで信頼とマークされるトラフィックに関係します。一般的に使用される 3 つの FTD アーキテクチャ、およびそのプラットフォーム固有の考慮事項とベスト プラクティスについて以下に示します。

© 2018 Cisco Systems, Inc. All rights reserved.

NG 4100/9300：



特別なプラットフォームの考慮事項：

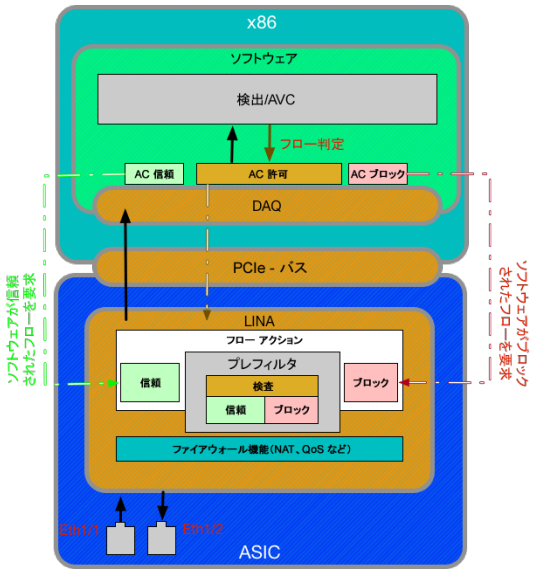
- プレフィルタ高速パス ルールは、フローをオフロード（ASIC に送信）でき、そのようにします。警告：存続期間の短いフロー（DNS など）には使用しないでください。初期の高速パス セッションを確立するコストが計算上高くなります。
- 従来のファイアウォール機能とレイヤ 7 インスペクションは、同じ計算リソースを共有します。一方が過剰に利用すると、もう一方に影響を及ぼすおそれがあります。
- LACP およびレイヤ 2 は FXOS によって処理され、Chassis Manager で管理されます。

© 2018 Cisco Systems, Inc. All rights reserved.

プラットフォーム固有のベスト プラクティス：

- 存続期間の長いフローのうち、レイヤ 7 インスペクションを回避する必要があるもののみをプレフィルタ高速パス処理してください。このようなフローには、バックアップ、データベース レプリケーションなど、単一接続上で大量のデータを送信するものが該当します。
- 存続期間の短いトラフィック（DNS など）は、そのトラフィック速度が ASIC セッションの作成による影響を受けることがあるため、プレフィルタ高速パス処理しないでください。このトラフィックは、アクセス コントロール ポリシーで信頼とマークされる必要があります（セキュリティ インテリジェンスが有効であることが前提）。

NG 2100：



特別なプラットフォームの考慮事項：

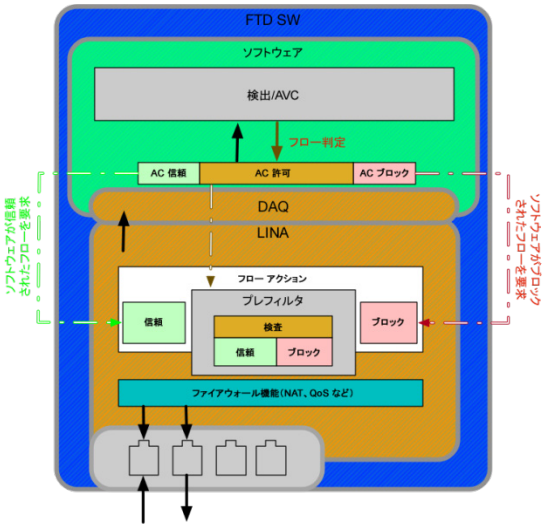
- プレフィルタ高速パス ルールは、フローがオフロード（ASIC に送信）<u>されません</u>。LINA プロセスによって処理され、LINA プロセスを実行中の ASIC で発生します。
- 従来のファイアウォール機能とレイヤ 7 インスペクションは、同じ計算リソースを共有<u>しません</u>。

© 2018 Cisco Systems, Inc. All rights reserved.

プラットフォーム固有のベスト プラクティス：

- レイヤ 7 インスペクションを回避し、従来の ASA インスペクションのみを受信するすべてのトラフィックをプレフィルタ高速パス処理してください。こうして処理されるトラフィックは、レイヤ 7 エンジンが処理する可能性のあるトラフィックとしてカウントされません。

vFTD/ASA 5500-X FTD



特別なプラットフォームの考慮事項：

- プレフィルタ高速パス ルールは、フローがオフロード（ASIC に送信）<u>されません</u>。LINA プロセスによって処理されます。
- 従来のファイアウォール機能とレイヤ 7 インスペクションは、同じカーネル上の同じ計算リソースを共有します。これには、LINA プロセスが提供する高速パス フローが含まれます。

プラットフォーム固有のベスト プラクティス：

- レイヤ 7 インスペクションを回避し、従来の ASA インスペクションのみを受信するすべてのトラフィックをプレフィルタ高速パス処理してください。このトラフィックはさらに迅速に処理され、レイヤ 7 検出を回避しますが、レイヤ 7 エンジンと同じプールからのリソースを利用し続けます。

© 2018 Cisco Systems, Inc. All rights reserved.

運用順序に与える影響

これまで説明してきたとおり、プラットフォームに応じて、プレフィルタ ポリシーに含まれるトラフィックに注意を払い、各プラットフォームの強みを活かすトラフィックを選択する必要があります。この情報は、前出の「ポリシー順序のベスト プラクティス」セクションで説明しています。

法的情報：

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

ハード コピーおよびソフト コピーの複製は公式版とみなされません。最新版はオンライン版を参照してください。

シスコは世界各国 200 箇所にオフィスを開設しています。各オフィスの住所、電話番号、FAX 番号は当社の Web サイト (www.cisco.com/go/offices) をご覧ください。

© 2018 Cisco Systems, Inc. All rights reserved.