はじめに

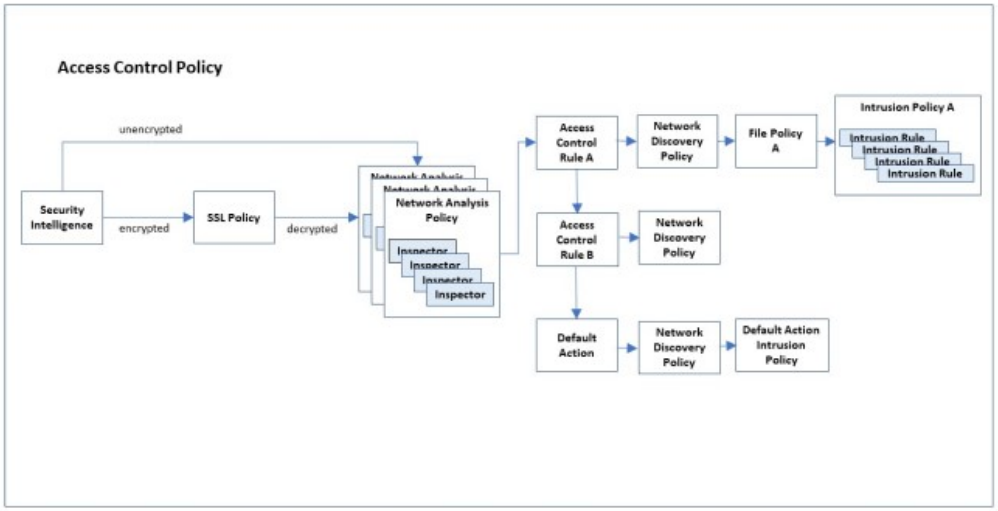
Snort 3 検査について

Snort 侵入防御システム（IPS）はリアルタイムでネットワークトラフィックを分析してパケットを詳細に検査します。Snort は、トラフィックの異常や、ネットワークプローブおよび攻撃を検出してブロックできます。Snort 3 は Snort の最新バージョンです。詳細については、https://snort.org/snort3を参照してください。

Snort は高いパフォーマンスと拡張性を実現するように設計されています。Snort には、インスペクタと呼ばれる設定可能な一連のプラグインが含まれています。Snort インスペクタは、特定のタイプのネットワークプロトコルまたはプローブのトラフィックを検出および分析し、メッセージを正規化してパケット分析を強化し、メッセージに埋め込まれた特定のタイプのファイルを検査できます。ネットワーク分析ポリシー（NAP）で Snort インスペクタを設定し、侵入ポリシーで侵入ルールを有効にします。

アクセス コントロール ポリシー

アクセス コントロール ポリシーは、いくつかの段階でトラフィックを処理します。次の図に、ポリシーの展開の例を示します。このドキュメントで取り上げる要素は、侵入ルールで使用される Snort 3 インスペクタとルールのオプションで、どちらも青色で強調表示されています。



ネットワーク分析ポリシーを使用すると、Snort 3 インスペクタを設定して、トラフィックプロトコルを決定し、データを抽出して正規化できます。複数のネットワーク分析ポリシーを設定でき、それぞれがデータを正規化するために独自に設定された Snort 3 インスペクタのコレクションを使用します。インスペクタは、データストリーム内の異常を検出すると警告を発することができますが、主な目的は、侵入ルール用のデータを準備することです。侵入ポリシーでは、設定した侵入ルールを適用して、回避、侵入、または攻撃の兆候がないかデータを調べます。

ネットワーク分析ポリシー内では、そのプロトコルを処理するインスペクタに固有の設定パラメータを設定することにより、特定のプロトコルを使用してデータの検査動作をカスタマイズできます。たとえば、POP データの検査動作を設定するには、`pop` インスペクタの構成パラメータを設定します。

それらのプロトコルに固有のルールオプションを使用してカスタム侵入ルールを作成することで、一部のプロトコルの侵入ポリシーをカスタマイズすることもできます。

複数のネットワーク分析ポリシーと複数の侵入ポリシーを使用して複雑な設定を確立する場合、システムは最初にデータを処理するネットワーク分析ポリシーを選択します。ネットワーク分析ポリシーで適切なインスペクタを適用して分析を実行した後、そのプロトコルの対応する侵入ポリシーにデータが自動的に渡されることはありません。アクセス コントロール ポリシーは、追加のテストを実行して、どの侵入ポリシーがデータを取得するかを決定します。そのため、アクセス制御、ネットワーク分析、および侵入ポリシーを設定するときは、データが正しいネットワーク分析と侵入ポリシーのペアによって分析されるようにしてください。詳細については、『Cisco Secure Firewall Management Center Snort 3 Configuration Guide』を参照してください。

侵入ルールの更新

Cisco は、Lightweight Security Packages（LSP）形式で侵入ルールの更新を定期的に発行します。これらの更新により、Snort 3 インスペクタの設定パラメータと侵入ルールのオプションのデフォルト値が変更される場合があります。

インスペクタの設定

Secure Firewall Management CenterWeb インターフェイスを介し、インスペクタを有効または無効にしたり、その設定を表示および変更したりできます。Secure Firewall Management CenterWeb インターフェイスは JSON 形式を使用してインスペクタ設定を記述します。詳細については、『Cisco Secure Firewall Management Center Snort 3 Configuration Guide』を参照してください。

インスペクタを使用するには、Management Center Web インターフェイスを介してインスペクタを有効にする必要があります。さらに、サービスインスペクタの場合、`binder` インスペクタでサービスインスペクタのエントリを設定する必要があります。詳細については、バインダインスペクタの概要を参照してください。

Snort 3 インスペクタ リファレンスには、Snort 3 インスペクタのパラメータと組み込みの侵入ルールのオプションのデフォルト設定が反映されています。システムは、LSP の更新、またはシステムで提供される基本のネットワーク アクセス ポリシーに応じて、異なるデフォルトを使用する場合があります。ネットワーク アクセス ポリシーのインスペクタ設定を最も正確に理解するには、Management Center Web インターフェイスに設定を表示します。

Snort 3 インスペクタの概要

Snort 3 のインスペクタは、Snort 2 プリプロセッサと同様に、パケットを分析して正規化するプラグインです。Snort 3 のインスペクタと設定のリストは、Snort 2 のプリプロセッサと設定のリストに直接対応していません。

Snort 3 インスペクタ

- ARP スプーフィングインスペクタ
- バインダインスペクタ
- CIP インスペクタ
- DCE SMB インスペクタ
- DCE TCP インスペクタ
- DNP3 インスペクタ
- FTP クライアントインスペクタ
- FTP サーバーインスペクタ
- GTP 検査インスペクタ
- HTTP 検査インスペクタ
- IEC104 インスペクタ
- IMAP インスペクタ
- MMS インスペクタ

- Modbus インスペクタ
- Normalizer インスペクタ
- POP インスペクタ
- ポートスキャンインスペクタ
- レートフィルタ
- S7CommPlus インスペクタ
- SIP インスペクタ
- SMTP インスペクタ
- SSH インスペクタ
- ストリーム ICMP インスペクタ
- ストリーム IP インスペクタ
- ストリーム TCP インスペクタ
- ストリーム UDP インスペクタ
- Telnet インスペクタ

このドキュメントでは、Snort 3 インスペクタごとに次について説明します。

- インスペクタの目的と機能に関する一般的な情報。
- インスペクタのタイプ：
  - サービス：インターネット サービス プロトコル（HTTP、FTP、TCP、または UDP）で使用されるプロトコルデータユニット（PDU）を分析するインスペクタ。たとえば、`http_inspect`、`ftp_server` などがあります。
  - パッシブ：設定（ `ftp_client`、`ftp_server`）のみを提供するか、他の処理を容易にするインスペクタ（`binder`）。
  - パケット：他のインスペクタが処理を実行する前に生のパケットで処理を実行するインスペクタ。たとえば、`normalizer` などがあります。
  - プローブ：すべての検出が完了した後に、すべてのパケットに対して処理を実行するインスペクタ。たとえば、`port_scan` などがあります。
  - ストリーム：フロートラッキング、インターネットプロトコルの最適化、およびTCPのリアセンブルを実行するインスペクタ。たとえば、`stream_tcp`、`stream_ip` などがあります。
  - 基本モジュール：複数のタイプのトラフィックの検査プロセスをサポートする機能を提供する、設定可能な組み込みの Snort 3 コンポーネント。たとえば、`rate_filter` などがあります。

- 使用法：
  - 検査：ネットワーク分析ポリシー（NAP）内でこれらのインスペクタを設定します。たとえば、`imap`、`ssh` などがあります。
  - グローバル、コンテキスト：これらのインスペクタを一度に設定します。たとえば、`port_scan`、`rate_filter` などがあります。
- インスタンスタイプ：
  - シングルトン：ネットワークアクセスポリシー内の単一のインスタンスに対してこれらのインスペクタを設定します。詳細については、シングルトンインスペクタ （6 ページ）を参照してください。
  - マルチトン：ネットワークアクセスポリシー（NAP）内の複数のインスタンスに対してこれらのインスペクタを設定します。NAP には、ネットワーク、ポート、または VLAN によって区別される複数のインスタンスを含めることができます。各インスタンスは、特定のトラフィックセグメントを処理するように一意に設定されています。詳細については、マルチトンインスペクタ （6 ページ）を参照してください。
- 他のインスペクタが必要：多くのインスペクタは、データストリームを完全に処理するために他のインスペクタに依存しています。あるインスペクタが他のインスペクタの設定を必要とする場合、このドキュメントではそれらの追加インスペクタを識別しています。
- インスペクタを設定するためのベストプラクティス：これらは、各インスペクタに固有の最適なパフォーマンスのための推奨事項です。
- インスペクタの設定パラメータ：Management Center Web インターフェイスで [ポリシー（Policies）] > [アクセス制御（Access Control）] > [ネットワーク分析ポリシー（Network Analysis Policy）] > ポリシー名 > [Snort 3 バージョン（Snort 3 Version）] > インスペクタ名で設定パラメータを設定できます。

（注） インスペクタのパラメータを変更する前に、インスペクタと有効な侵入ルール間の連携動作を理解しておくことをお勧めします。

- ルール：Snort 3 インスペクタはルールを使用してイベントを生成します。組み込みルールには、クラスタイプ、参照、およびその他のメタデータが含まれている場合があります。
- 侵入ルールのオプション：インスペクタによって処理されるデータタイプの侵入ルールのオプションを定義することで、侵入ルールをカスタマイズします。カスタム侵入ルールの管理については、Cisco Secure Firewall Management Center Snort 3 Configuration Guideを参照してください。

（注） カスタム侵入ルールの作成は高度な作業であり、注意して行う必要があります。このドキュメントに記載されていないインスペクタとルールのオプションを使用する必要がある場合があります。このドキュメントに記載されている一部のインスペクタと侵入ルールのオプションを使用するには、Snort のオープンソースドキュメントに記載されているインスペクタとルールのオプションの特定の設定が必要です。一部のルールのオプションは、Snort 高速パターンマッチ機能または検出カーソルの配置に影響を与えます。詳細については、https://www.snort.org/snort3 で入手可能な Snort 3 のオープンソースドキュメントを参照してください。

シングルトンインスペクタ

ネットワーク アクセス ポリシー（NAP）では、シングルトンインスペクタのインスタンスを 1 つだけ使用できます。

- シングルトンインスペクタは、マルチトンインスペクタのように NAP ごとに複数のインスタンスをサポートすることはできません。
- シングルトンインスペクタは、一部の特定のフローには適用されない場合があります。

次に例を示します。

```
{
   "normalizer":{
      "enabled":true,
      "type":"singleton",
      "data":{
         "ip4":{
            "df":true
         }
      }
   }
}
```

マルチトンインスペクタ

ネットワーク アクセス ポリシーでは、必要に応じて設定できるマルチトンインスペクタのインスタンスを 1 つ以上使用できます。マルチトンインスペクタは、ネットワーク、ポート、VLAN などの特定の条件に基づく設定をサポートしています。サポートされている一連の設定でインスタンスが構成されます。マルチトンはデフォルトのインスタンスを提供しますが、特定の条件に基づいて追加のインスタンスを定義できます。トラフィックがカスタマイズされたインスタンスの条件と一致すると、そのインスタンスの設定が適用されます。それ以外の場合は、デフォルトインスタンスの設定が適用されます。デフォルトのインスタンスの名前はインスペクタの名前と同じです。

マルチトンインスペクタの場合、オーバーライドされたインスペクタ設定をアップロードするときは、JSON ファイル内の各インスタンスの一致する `binder` 設定を定義する必要もあります。そのようにしないと、アップロードがエラーになります。新しいインスタンスを作成する

こともできますが、エラーを回避するために、作成するすべての新しいインスタンスに必ず binder 条件を含めてください。

次に例を示します。

- デフォルトのインスタンスが変更されたマルチトンインスペクタは、次のとおりです。

```
{
   "http_inspect":{
      "instances":[
         {
            "name":"http_inspect",
            "data":{
               "response_depth":5000
            }
         }
      ]
   }
}
```

- デフォルトのインスタンスとデフォルトの binder が変更されたマルチトンインスペクタは次のとおりです。

```
{
   "http_inspect":{
      "instances":[
         {
            "name":"http_inspect",
            "data":{
               "response_depth":5000
            }
         }
      ]
   },
   "binder":{
      "rules":[
         {
            "use":{
               "type":"http_inspect"
            },
            "when":{
               "role":"any",
               "ports":"8080",
               "proto":"tcp",
               "service":"http"
            }
         }
      ]
   }
}
```

- カスタムインスタンスとカスタム binder が追加されたマルチトンインスペクタは次のとおりです。

```
{
   "http_inspect":{
      "instances":[
         {
            "name":"http_inspect1",
            "data":{
               "response_depth":5000
            }
         }
```

```
            ]
         },
         "binder":{
            "rules":[
               {
                  "use":{
                     "type":"http_inspect",
                     "name":"http_inspect1"
                  },
                  "when":{
                     "role":"any",
                     "ports":"8080",
                     "proto":"tcp",
                     "service":"http"
                  }
               }
            ]
         }
      }
```

Snort 3 のプロトコルとサービスの識別

binder インスペクタは、すべての Snort サービスインスペクタに影響を与える独自の機能を実行します。binder は、Snort wizard モジュールとともに、ネットワークトラフィックを検査できるストリームまたはサービスインスペクタを決定します。binder インスペクタの設定には、ネットワーク分析ポリシーの別のインスペクタがトラフィックを検査する必要がある場合に定義するポート、ホスト、CIDR、およびサービスが含まれます。

wizard は、マルウェアコマンドチャネルと制御チャネルの検出を可能にする、ポートに依存しないサービス設定をサポートします。

（注） Secure Firewall Management CenterWeb インターフェイスから wizard を設定することはできません。

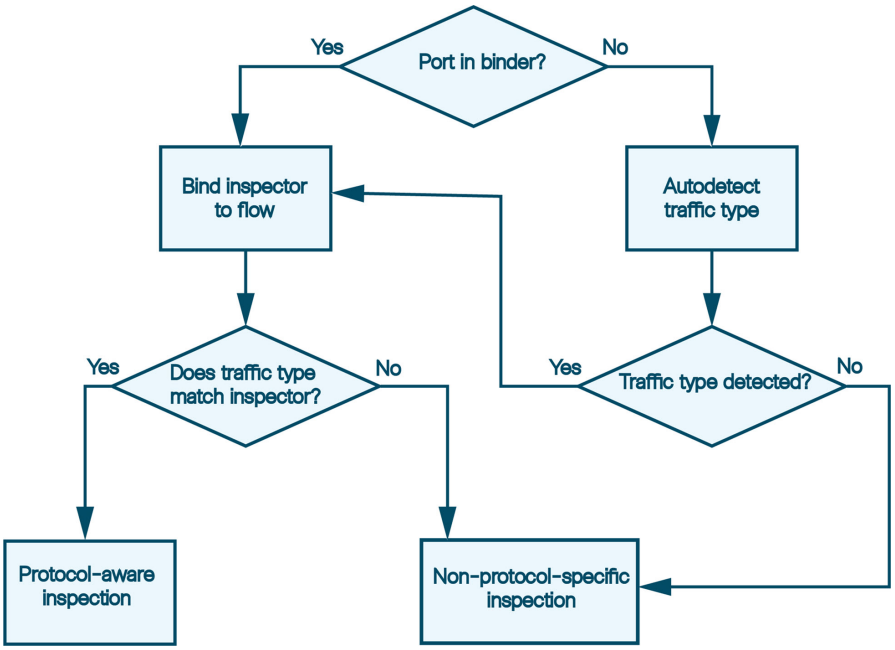
トラフィックがファイアウォールデバイスに到着すると、binder インスペクタは侵入ポリシーを検索し、適用する適切なネットワークアクセスポリシー（NAP）を選択します。NAP 内で、binder はデータフローに使用する適切なストリームとサービスインスペクタを決定します。その後、フローに関連付けられたサービスが変更された場合、NAP は binder を使用して別のサービス インスペクタを選択します。

binder インスペクタの設定には、トラフィックの特性を説明する when パラメータと、それらの特性に一致するトラフィックに適用するインスペクタを指定する use パラメータが含まれています。データフローに適用するインスペクタを決定する場合、binder インスペクタはトラフィックをその when 句に対して上から順に比較し、トラフィックに一致する最初の when 句に対応する use 句を適用します。

特定の binder 条件がデータフローに一致しない場合、wizard はデータフローを分析してサービスを決定します。wizard は binder を呼び出して、そのサービスに適したインスペクタを選択します。サービスを識別できない場合、binder は通常、ストリームインスペクタをフローに

バインドし、システムはペイロードの内容に関係なく、プロトコル固有ではないデータパケットのリアセンブルを実行します。

次の図に、インスペクタがプロトコル固有または非プロトコル固有の検査を実行する方法を示します。サービス検査は、`binder` インスペクタでの `port`、`host`、`service`、および `CIDR` パラメータの設定方法によって異なります。



Management Center Web インターフェイスの NAP の `binder` インスペクタで `use` パラメータと `when` パラメータを定義することでインスペクタの選択基準をカスタマイズできます。`binder` パラメータの詳細については バインダインスペクタの概要を参照してください。Management Center Web インターフェイスをナビゲートしてインスペクタを設定する方法については、Cisco Secure Firewall Management Center Snort 3 Configuration Guideを参照してください。

`binder` を正しく設定しないと、フローのサービスを検出したり、インスペクタをバインドしたりできません。ルールエンジンと自動検出がトラフィックを理解できず、識別できない場合、`binder` インスペクタでポートなどの `when` 基準を設定しても、検査は適用されません。たとえば、`binder` でポート 88 を HTTP ポートとして設定すると、その `binder` は `http_inspect` インスペクタをそのポートのすべてのフローにバインドします。ただし、フローが HTTP ではない場合、ルールエンジンはデータを HTTP として検査せず、代わりにポートベースの検出を実行します。

ネットワーク分析ポリシーでの自動検出と有効化または無効化されたインスペクタ

自動検出の動作は、対象のインスペクタがネットワーク分析ポリシーで有効化されているか無効化されているかによって異なります。対象のインスペクタがネットワーク分析ポリシーで有効になっている場合、自動検出は上記のように機能します。

対象のインスペクタがネットワーク分析ポリシーで無効になっている場合でも、通常、自動検出は引き続きストリームインスペクタ（ストリーム TCP やストリーム UDP など）をフローに

バインドします。ただし、ルールエンジンはサービスの検査も検出も実行しません。TCP フローの場合、ストリーム TCP インスペクタはリアセンブルを実行します。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。