CHAPTER 13

# Guard モジュールによる軽減の分析

この章では、Cisco Anomaly Guard Module（Guard モジュール）による軽減およびゾーンのトラフィックを分析する方法、および設定の問題を識別する方法のガイドラインを示します。また、攻撃のタイプを識別する方法について簡単に説明します。この章は、次の項で構成されています。

# ゾーンのトラフィック パターンの分析

ゾーンの通常のトラフィック レートを前もって知っておくと、ゾーンへの異常なトラフィックを簡単に認識できます。

オンデマンド ゾーンである場合、または最後にラーニング プロセスを実行してからゾーンのトラフィック特性が変わった場合は、現在の攻撃が終了してから Guard モジュールにゾーンのトラフィック パターンをラーニングさせることを強くお勧めします。

ゾーンの現在のトラフィック レートを表示するには、**show rates** コマンドを使用します。詳細については、P.11-4 の「ゾーンのカウンタの表示」を参照してください。

受信トラフィック レートを表示する場合は、次の点に注意してください。

- 受信レートがゼロの場合は、宛先変更の問題が発生していることを示します。詳細については、P.13-3 の「宛先変更の問題」を参照してください。
- 受信レートが正当なトラフィックのレートよりも高い場合は、Guard モジュールによる軽減が機能していることを示します。
  - 正当なトラフィックのレートが、認識しているゾーン トラフィックに比べて高すぎる場合は、P.13-3 の「フロー特性に基づくゾーンへのフローのブロッキング」を参照してください。
  - 正当なトラフィックのレートが、認識しているゾーン トラフィックに比べて低すぎる場合は、P.13-5 の「トラフィック ブロッキング基準の確認」を参照してください。

## 宛先変更の問題

Guard モジュールがパケットをまったく受信しない場合は、宛先変更の問題が発生している可能性があります。宛先変更の問題が発生していると、Guard モジュールは、ゾーンに送信されたトラフィックを受信しません。

宛先変更が正しく設定されていることを確認してください。詳細については、第 5 章「トラフィックの宛先変更の設定」を参照してください。

次のガイドラインを使用します。

- 宛先変更のルートが正しく設定されていることを確認する。詳細については、P.5-9 の「宛先変更ルートの表示」を参照してください。
- ハイジャック VLAN がブロックされないことを確認する。スーパーバイザからハイジャック インターフェイスに ping を実行してください。

## フロー特性に基づくゾーンへのフローのブロッキング

正当なトラフィックのレートが、認識しているゾーン トラフィック特性から判断して高すぎると思われる場合は、Guard モジュールが一部の攻撃トラフィックをブロックしていない可能性があります。この現象は、ラーニング プロセスが実行されなかったオンデマンド ゾーンで発生することがあります。このような場合は、そのゾーンで、オンデマンド ポリシーしきい値が大きすぎる可能性があります。

次の作業を行うことをお勧めします。

- 送信元 IP アドレスに応じてトラフィックを測定するポリシーのしきい値を小さくする。
- 正当なトラフィック レートを確認する。それでも正当なトラフィックのレートが高すぎると思われる場合は、高度かつ大規模なゾンビ攻撃またはクライアント攻撃が発生している可能性があります。このような攻撃は、レートや接続数が通常のフローと変わらない多くのフローで構成されています。このような異常トラフィック フローをブロックするには、フレックスコンテンツ フィルタを設定します。詳細については、P.7-7 の「フレックスコンテンツ フィルタの設定」を参照してください。

ポリシーのしきい値を小さくするには、次の手順を実行します。

**ステップ 1**　ポリシーの現在のしきい値を表示します。関連するゾーン設定モードで次のコマンドを入力します。

```
show policies
```

ポリシーの詳細については、P.8-34 の「ポリシーの表示」を参照してください。

**ステップ 2**　ゾーンのグローバル トラフィックを調べます。次のコマンドを入力します。

```
show policies */*/*/*/global statistics
```

Guard モジュールは、ゾーンに転送されたトラフィック フローの中で、保護ポリシーによって測定された最も高いレートを持ついくつかのトラフィック フローを表示します。サービス タイプおよびトラフィック量がゾーンのトラフィックを表すかどうかを判断します。ポリシーの統計情報の詳細については、P.8-36 の「ポリシーの統計情報の表示」を参照してください。

**ステップ 3**　送信元 IP アドレスによって示される、個々のユーザのトラフィックを調べます。どのポリシーのしきい値が大きく、小さくする必要があるかを判断します。次のコマンドを入力します。

```
show policies */*/*/*/src_ip statistics
```

Guard モジュールは、ゾーンに転送されたトラフィック フローの中で、保護ポリシーによって測定された最も高いレートを持ついくつかのトラフィック フローを表示します。ポリシーの統計情報の詳細については、P.8-36 の「ポリシーの統計情報の表示」を参照してください。

**ステップ 4**　トラフィック量がゾーンのトラフィックを表さない場合は、送信元 IP アドレスのポリシーのしきい値を小さくします。次のコマンドを入力します。

```
policy */*/*/*/src_ip thresh-mult threshold-multiply-factor
```

*threshold-multiply-factor* 引数は、ポリシーのしきい値に掛ける値です。ポリシーのしきい値を小さくするには、1 より小さい数値を入力します。たとえば、しきい値を半分にするには、0.5 と入力します。詳細については、P.8-27 の「係数によるしきい値の乗算」を参照してください。

## トラフィック ブロッキング基準の確認

正当なトラフィックのレートが低すぎると思われる場合は、Guard モジュールが正当なクライアントからゾーンへのアクセスをブロックしている可能性があります。この現象は、ラーニング プロセスがかなり前に実行されたために、現在ではポリシーのしきい値がゾーンのトラフィック パターンに合わなくなってしまった場合に発生することがあります。その結果、ポリシーのしきい値が適切に調整されておらず、小さくなっています。

Guard モジュールのブロッキング基準を確認および変更するには、次の手順を実行します。

**ステップ 1**　Guard　モジュールが正当なクライアントからゾーンへのアクセスをブロックしているのではないかと思われる場合は、Guard モジュールの動的フィルタがこのようなクライアントからのアクセスをブロックしていないかどうか確認します。次のコマンドを入力します。

```
show dynamic-filters [details]
```

動的フィルタの詳細については、P.7-34 の「動的フィルタの表示」を参照してください。動的フィルタでは、動的フィルタが生成される原因となったポリシーの詳細が提供されます。

**ステップ 2**　このようなポリシーの統計情報を表示します。たとえば、送信元 IP アドレスによって示される、個々のユーザのトラフィックを調べます。どのポリシーのしきい値が小さく、大きくする必要があるかを判断します。次のコマンドを入力します。

```
show policies */*/*/*/src_ip statistics
```

Guard モジュールは、ゾーンに転送されたトラフィック フローの中で、保護ポリシーによって測定された最も高いレートを持ついくつかのトラフィック フローを表示します。ポリシーの統計情報の詳細については、P.8-36 の「ポリシーの統計情報の表示」を参照してください。

**ステップ 3**　トラフィック量がゾーンのトラフィックを表さない場合は、しきい値を大きくします。関連するゾーン設定モードで次のコマンドを入力します。

**policy */*/*/*/src_ip thresh-mult** *threshold-multiply-factor*

*threshold-multiply-factor* 引数は、ポリシーのしきい値に掛ける値です。ポリシーのしきい値を大きくするには、1 より大きい数値を入力します。たとえば、しきい値を 2 倍にするには、2 と入力します。詳細については、P.8-27 の「係数によるしきい値の乗算」を参照してください。

**ステップ 4**　動的フィルタのリストを表示します（ステップ 1 を参照してください）。動的フィルタのリストに *drop* アクションを持つ、正当なクライアントの IP アドレスに対する動的フィルタが含まれている場合、その動的フィルタを削除します。次のコマンドを入力します。

**no dynamic-filter** *filter-id*

動的フィルタの詳細については、P.7-31 の「動的フィルタの設定」を参照してください。

**ステップ 5**　Guard モジュールが引き続き特定のポリシーから drop アクションを持つ動的フィルタを生成する場合は、そのポリシーを非アクティブにします。次のコマンドを入力します。

```
state inactive
```

詳細については、P.8-22 の「ポリシーの状態の変更」を参照してください。

**ヒント**　同じポリシー ブランチに属する複数のポリシーが、drop アクションを持つ動的フィルタを生成する場合は、そのポリシー ブランチを非アクティブにすることができます。

**ステップ 6**　ゾーンが正しく機能するために不可欠であると分かっているクライアント IP アドレスが Guard モジュールの保護メカニズムをバイパスするように設定します。このようなクライアントの IP アドレスをバイパス フィルタに追加します。Guard モジュールは、このようなトラフィック フローをゾーンに直接転送します。次のコマンドを入力します。

```
bypass-filter row-num ip-address protocol dest-port fragments-flag
```

詳細については、P.7-21 の「バイパス フィルタの設定」を参照してください。

# 攻撃の軽減の確認

ゾーンに対する攻撃を識別した場合は、Guard モジュールがその攻撃を軽減していることを確認できます。これは、ゾーンのトラフィック パターンを熟知していない場合、またはゾーンがオンデマンド保護中で、Guard モジュールがゾーンのトラフィック パターンをラーニングしなかった場合に特に重要です。

次の作業を行うことができます。

- ゾーンの現在の攻撃レポートを表示する。詳細については、P.13-8 の「ゾーンの現在の攻撃レポートの表示」を参照してください。
- Guard モジュールのフィルタ、カウンタ、および統計情報を表示する。これを行うには、Guard モジュールの動作およびメカニズムを熟知している必要があります。

## ゾーンの現在の攻撃レポートの表示

進行中の攻撃のレポートを表示して、攻撃の特性、および Guard モジュールが攻撃を軽減するために講じた対策を知ることができます。

進行中の攻撃の攻撃レポートを表示するには、**show reports current** コマンドを使用します。詳細については、P.10-14 の「攻撃レポートの表示」を参照してください。

このレポートには、攻撃に関する詳細が記載されます。攻撃の開始日時、ゾーンのトラフィック フローの一般的な分析、ドロップされたパケットおよび返送されたパケットの分析、Guard モジュールがゾーンのトラフィックで検出したトラフィック異常の詳細、ゾーンを保護する（攻撃を軽減する）ために Guard モジュールが実行した処置などの情報が提供されます。詳細については、P.10-2 の「レポートのレイアウトについて」を参照してください。

このレポートには、攻撃の分類に関する詳細が記載されます。DDoS 攻撃は、次のような 2 つの主なクラスに分類されます。

- **帯域幅の枯渇**：正当なトラフィックがゾーンに到達できないようにする不要なトラフィックをゾーンに多量に注入するための攻撃。このような攻撃には、スプーフィングを利用した攻撃や不正な形式のパケットなどがあります。
- **リソースの枯渇**：ゾーンのリソースを使い果たしてしまうための攻撃。

軽減された攻撃のタイプの詳細については、P.10-6 の「Mitigated Attacks」を参照してください。

## Guard モジュールの高度な統計情報の表示

Guard モジュールのフィルタ、カウンタ、および診断情報を表示して、攻撃の特性、および Guard モジュールが攻撃を軽減するために講じた対策を詳細に知ることができます。このような手順を実行するには、Guard モジュールの動作およびメカニズムを熟知している必要があります。

次の情報を表示できます。

- **動的フィルタ**：このフィルタでは、Guard モジュールが攻撃を処理している方法の詳細が提供されます。動的フィルタを表示するには、**show dynamic-filters** コマンドを使用します。詳細については、P.7-34 の「動的フィルタの表示」を参照してください。
- **ユーザ フィルタ**：このフィルタでは、DDoS 攻撃ではないかと思われるトラフィック フローを処理する方法が定義されます。ゾーンの設定には、デフォルトのユーザ フィルタのセットが含まれます。ユーザ フィルタを追加または削除できます。ユーザ フィルタを表示するには、**show** コマンドまたは **show running-config** コマンドを使用します。Guard モジュールは、各ユーザ フィルタで測定された現在のトラフィック レートを表示します。詳細については、P.7-28 の「ユーザ フィルタの表示」を参照してください。
- **ドロップされたパケットに関する統計情報**：この統計情報では、進行中の攻撃のドロップされたパケットの分布を示すリストが提供されます。ドロップされたパケットに関する統計情報を表示するには、**show drop-statistics** コマンドを使用します。詳細については、P.13-10 の「ドロップされたトラフィックの統計情報の表示」を参照してください。
- **ゾーンのレート履歴**：このリストには、Guard モジュールが過去 24 時間に各カウンタで測定したレートが表示されるため、攻撃の展開に関する詳細が分かります。ゾーンのレート履歴を表示するには、**show rates history** コマンドを使用します。詳細については、P.11-4 の「ゾーンのカウンタの表示」を参照してください。
- **ゾーンのカウンタ**：このリストには、Guard モジュールが各カウンタで測定したパケット数が表示されるため、攻撃開始後に Guard モジュールがゾーンのトラフィックを処理した方法を分析できます。詳細については、P.11-4 の「ゾーンのカウンタの表示」を参照してください。

## ドロップされたトラフィックの統計情報の表示

進行中の攻撃のドロップされたパケットの分布を表示できます。Guard モジュールは、保護メカニズムによってドロップされたパケットをレート、パケット、およびビット単位で表示します。

次のコマンドを入力します。

**show drop-statistics**

表 13-1 で、ドロップ統計情報について説明します。

**表 13-1　ドロップ統計情報**

| タイプ | 説明 |
|---|---|
| Total dropped | ドロップされたトラフィックの合計量。 |
| Dynamic filters | 動的フィルタによってドロップされたトラフィックの量。 |
| User filters | ユーザ フィルタによってドロップされたトラフィックの量。 |
| Flex-Content filter | フレックスコンテンツ フィルタによってドロップされたトラフィックの量。 |
| Rate limit | ゾーンのレート リミット保護モジュールによってドロップされたパケットを示します。これらのパケットは、ユーザ フィルタのレート リミット パラメータ、およびゾーンの **rate-limit** コマンドによって定義されます。 |
| Incoming TCP unauthenticated basic | 基本的な TCP スプーフィング防止メカニズムによって認証されなかったためにドロップされたトラフィック。攻撃レポートでは、このようなパケットは Dropped/ Replied Packets テーブル内でスプーフィングされたパケットとしてカウントされます。 |
| Incoming TCP unauthenticated-strong | 強力な TCP スプーフィング防止メカニズムによって認証されなかったためにドロップされたトラフィック。攻撃レポートでは、このようなパケットは Dropped/ Replied Packets テーブル内でスプーフィングされたパケットとしてカウントされます。 |

**表 13-1　ドロップ統計情報（続き）**

| タイプ | 説明 |
|---|---|
| Outgoing TCP unauthenticated | TCP スプーフィング防止メカニズムによって認証されなかったためにドロップされた、ゾーンで開始された接続のトラフィック。攻撃レポートでは、このようなパケットは Dropped/ Replied Packets テーブル内でスプーフィングされたパケットとしてカウントされます。 |
| UDP unauthenticated-basic | 基本的なスプーフィング防止メカニズムによって認証されなかったためにドロップされた UDP トラフィック。攻撃レポートでは、このようなパケットは Dropped/ Replied Packets テーブル内でスプーフィングされたパケットとしてカウントされます。 |
| UDP unauthenticated-strong | 強力なスプーフィング防止メカニズムによって認証されなかったためにドロップされた UDP トラフィック。攻撃レポートでは、このようなパケットは Dropped/ Replied Packets テーブル内でスプーフィングされたパケットとしてカウントされます。 |
| Other protocols unauthenticated | Guard のスプーフィング防止メカニズムによって認証されなかったためにドロップされた、TCP および UDP 以外のトラフィック。攻撃レポートでは、このようなパケットは Dropped/ Replied Packets テーブル内でスプーフィングされたパケットとしてカウントされます。 |
| TCP fragments unauthenticated | Guard のスプーフィング防止メカニズムによって認証されなかったためにドロップされた、断片化された TCP パケット。攻撃レポートでは、このようなパケットは Dropped/ Replied Packets テーブル内でスプーフィングされたパケットとしてカウントされます。 |
| UDP fragments unauthenticated | Guard のスプーフィング防止メカニズムによって認証されなかったためにドロップされた、断片化された UDP パケット。攻撃レポートでは、このようなパケットは Dropped/ Replied Packets テーブル内でスプーフィングされたパケットとしてカウントされます。 |

**表 13-1　ドロップ統計情報（続き）**

| タイプ | 説明 |
|---|---|
| Other protocols fragments unauthenticated | Guard のスプーフィング防止メカニズムによって認証されなかったためにドロップされた、TCP および UDP 以外の断片化されたパケット。攻撃レポートでは、このようなパケットは Dropped/ Replied Packets テーブル内でスプーフィングされたパケットとしてカウントされます。 |
| DNS malformed replies | Guard の保護メカニズムによってドロップされた不正な形式の DNS 応答。攻撃レポートでは、このようなパケットは Dropped/ Replied Packets テーブル内で不正な形式のパケットとしてカウントされます。 |
| DNS spoofed replies | Guard のスプーフィング防止メカニズムによってドロップされた、ゾーンで開始された接続に応答する着信 DNS パケット。攻撃レポートでは、このようなパケットは Dropped/ Replied Packets テーブル内でスプーフィングされたパケットとしてカウントされます。 |
| DNS short queries | Guard の保護メカニズムによってドロップされた短い（不正な形式の）DNS クエリー。攻撃レポートでは、このようなパケットは Dropped/ Replied Packets テーブル内で不正な形式のパケットとしてカウントされます。 |
| NON DNS packets to DNS port | Guard の保護メカニズムによってドロップされた、DNS ポート宛ての非 DNS トラフィック。攻撃レポートでは、このようなパケットは Dropped/ Replied Packets テーブル内で不正な形式のパケットとしてカウントされます。 |
| Bad packets to proxy addresses | Guard の保護メカニズムによってドロップされた、Guard モジュールのプロキシ IP アドレス宛ての不正形式トラフィック。 |
| TCP anti-spoofing mechanisms related pkts | Guard モジュールの TCP スプーフィング防止メカニズムの副次的な動作が原因でドロップされたパケットの数。攻撃レポートでは、このようなパケットは Dropped/ Replied Packets テーブル内で不正な形式のパケットとしてカウントされます。 |

**表 13-1　ドロップ統計情報（続き）**

| タイプ | 説明 |
|---|---|
| DNS anti-spoofing mechanisms related pkts | Guard モジュールの DNS スプーフィング防止メカニズムの副次的な動作が原因でドロップされたパケットの数。攻撃レポートでは、このようなパケットは Dropped/ Replied Packets テーブル内で不正な形式のパケットとしてカウントされます。 |
| Anti-spoofing internal errors | Guard モジュールのスプーフィング防止メカニズムのエラーのためにドロップされたパケットの数。攻撃レポートでは、このようなパケットは Packets テーブルでカウントされます。 |
| Land attack | 送信元 IP アドレスと宛先 IP アドレスが同じであるためにドロップされたパケットの数。攻撃レポートでは、このようなパケットは Dropped/ Replied Packets テーブル内で不正な形式のパケットとしてカウントされます。 |
| Malformed packets | ヘッダーの形式が不正である（ヘッダーのポート、プロトコル、または IP のフィールドがゼロ（0）になっている）ことが原因でドロップされたパケットの数。攻撃レポートでは、このようなパケットは Dropped/ Replied Packets テーブル内で不正な形式のパケットとしてカウントされます。 |

次の例を参考にしてください。

```
user@GUARD-conf-zone-scannet# show drop-statistics
```