CHAPTER 15

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.13-4 の「カウンタを使用したトラフィックの分析」を参照してください。

受信トラフィック レートを表示し、次のガイドラインを考慮してください。

- 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.15-2 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。次のような問題が発生する可能性があります。
  - ゾーンに対する正当なトラフィック　レートが通常のトラフィック状態のゾーン トラフィック レートよりもきわめて高い場合は、P.15-3 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。
  - ゾーンに対する正当なトラフィック　レートが通常のトラフィック状態のゾーン トラフィック レートよりもきわめて低い場合は、P.15-5 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て宛先変更の設定を確認します。

- 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.5-10 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 エンジンからハイジャック 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

ゾーンに対する正当なトラフィック レートが通常のトラフィック状態のゾーン トラフィック レートよりもきわめて高い場合は、Guard モジュールがすべて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。オンデマンド ゾーンなどのゾーンのトラフィック パターンのラーニングを Guard モジュールに許可しなかった場合は、正当なトラフィックの高いレートが発生する可能性があります。Guard モジュールがゾーンのトラフィック パターンを認識しない場合は、特定のゾーンに対するポリシーしきい値が高すぎる可能性があります。

Guard モジュールがゾーンへの不要なフローを転送できないようにするには、次のタスクを実行する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.7-5 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　現在のポリシーしきい値を表示するには、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.8-38 の「ポリシーの表示」を参照してください。

ステップ 2　ゾーン設定モードで次のコマンドを入力して、ゾーンのグローバル トラフィックを調べます。

```
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。ポリシー統計の詳細については、P.8-40 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　ゾーン設定モードで、次のコマンドを入力することにより、送信元 IP アドレスで示される個々のユーザのトラフィックを調べ、小さくする必要のある高いポリシーのしきい値を特定します。

```
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。ポリシー統計の詳細については、P.8-40 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、ゾーン設定モードで次のコマンドを入力して、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。

```
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係数を示します。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.8-29 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。この状態は、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、次のコマンドをゾーン設定モードで入力して、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を確認します。

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

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。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。

ステップ 2　動的フィルタが生成される原因となったポリシーを識別して、これらのポリシーの統計を表示します。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。ゾーン設定モードで次のコマンドを入力することにより、高くする必要が生じた、小さいしきい値のポリシーを判断します。

```
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、ゾーン 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.8-40 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、ゾーン設定モードで次のコマンドを入力して、ポリシーのしきい値を高くします。

```
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係数を示します。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.8-29 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は、ゾーン設定モードで次のコマンドを入力して、その動的フィルタを削除します。

```
no dynamic-filter filter-id
```

動的フィルタの詳細については、P.7-32 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、ポリシー設定モードで次のコマンドを入力して、そのポリシーを非アクティブにします。

```
state inactive
```

詳細については、P.8-23 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、高レベルのポリシー セクション（ポリシー テンプレート セクションやサービス セクションなど）でこれらのポリシーの状態を変更すると、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 モジュールの保護機能をバイパスするように設定します。これによって、Guard モジュールはこれらのトラフィック フローをゾーンに直接転送します。ゾーン設定モードで次のコマンドを入力して、これらのクライアントの IP アドレスでバイパス フィルタを作成します。

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

詳細については、P.7-20 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。このアクションは、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。

攻撃が軽減されていることを確認するには、次のアクションを実行します。

- 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.15-8 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。このアクションを行うには、Guard モジュールの動作および機能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

show reports current コマンドを入力すると、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。詳細については、P.12-14 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.12-2 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（分散型サービス拒絶攻撃）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.12-6 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機能を熟知している必要があります。

- 動的フィルタ：Guard モジュールが攻撃を処理する方法の詳細を提供します。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：DDoS 攻撃であると疑われるトラフィック フローの処理方法を定義します。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 フィルタは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.7-29 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：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を提供します。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.15-10 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.13-4 の「カウンタを使用したトラフィックの分析」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.13-4 の「カウンタを使用したトラフィックの分析」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

設定モードで次のコマンドを入力すると、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。

show drop-statistics

Guard モジュールは、保護機能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。

表 15-1 に、ドロップ統計情報を示します。

表 15-1　ドロップ統計情報

ドロップ統計情報	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	ユーザ フィルタのレート リミット パラメータ、およびドロップされたゾーンの **rate-limit** コマンドによって定義されたパケット。
Incoming TCP unauthenticated basic	TCP の基本的なスプーフィング防止機能で、認証されず、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 Malicious Packets Statistics 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	TCP の強力なスプーフィング防止機能で、認証されず、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 Malicious Packets Statistics 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 15-1　ドロップ統計情報（続き）

ドロップ統計情報	説明
Outgoing TCP unauthenticated	TCP のスプーフィング防止機能で、認証されずにドロップされた、ゾーンから接続が開始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 Malicious Packets Statistics 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機能で、認証されずにドロップされた 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 Malicious Packets Statistics 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	基本的なスプーフィング防止機能で、認証されずにドロップされた 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 Malicious Packets Statistics 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 スプーフィング防止機能で、認証されずにドロップされた 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 Malicious Packets Statistics 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 スプーフィング防止機能で、認証されずにドロップされた TCP 断片化パケット。攻撃レポートでは、このようなパケットは Malicious Packets Statistics 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 スプーフィング防止機能で、認証されずにドロップされた UDP 断片化パケット。攻撃レポートでは、このようなパケットは Malicious Packets Statistics 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 15-1　ドロップ統計情報（続き）

ドロップ統計情報	説明
Other protocols fragments unauthenticated	Guard スプーフィング防止機能で、認証されずにドロップされた TCP および UDP 以外の断片化パケット。攻撃レポートでは、このようなパケットは Malicious Packets Statistics 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 の保護機能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 Malicious Packets Statistics テーブル内の不正形式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機能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 Malicious Packets Statistics 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 の保護機能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 Malicious Packets Statistics テーブル内の不正形式パケットとしてカウントされます。
Non DNS packets to/from DNS port	Guard の保護機能によってドロップされた、DNS ポート宛て、または DNS ポートからの DNS 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 Malicious Packets Statistics テーブル内の不正形式パケットとしてカウントされます。
Bad packets to proxy addresses	Guard の保護機能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。

表 15-1　ドロップ統計情報（続き）

ドロップ統計情報	説明
TCP anti-spoofing mechanisms related pkts	Guard モジュールの TCP スプーフィング防止機能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 Malicious Packets Statistics テーブル内の不正形式パケットとしてカウントされます。
DNS anti-spoofing mechanisms related pkts	Guard モジュールの DNS スプーフィング防止機能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 Malicious Packets Statistics テーブル内の不正形式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機能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。
SIP anti-spoofing features related pkts	Guard モジュールの副次的な動作によりドロップした SIP[1] over UDP パケットの数です。攻撃レポートでは、このようなパケットは Malicious Packets Statistics 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。
SIP malformed packets	不正形式のため、Guard の保護機能によってドロップされた SIP over UDP パケット。攻撃レポートでは、このようなパケットは Malicious Packets Statistics テーブル内の不正形式パケットとしてカウントされます。
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 Malicious Packets Statistics テーブル内の不正形式パケットとしてカウントされます。

表 15-1　ドロップ統計情報（続き）

ドロップ統計情報	説明
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 Malicious Packets Statistics テーブル内の不正形式パケットとしてカウントされます。

1. SIP = Session Initiation Protocol

次の例は、ドロップ統計情報を表示する方法を示しています。

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