攻撃レポート

この章では、Cisco Traffic Anomaly Detector Module（Detector モジュール）が生成する攻撃レポートについて説明します。この章には、次の項があります。

レポートのレイアウトについて

Detector は、攻撃を明確に把握するために役立つ、各ゾーンの攻撃レポートを提供します。攻撃の開始は、Detector が最初の動的フィルタを生成するときで、攻撃の終了は、動的フィルタが使用されなくなり、新しい動的フィルタが追加されなくなったときです。レポートには、攻撃の詳細がセクションに分かれて記載されます。各セクションには、攻撃中のトラフィック フローの異なる面が記載されます。過去の攻撃および進行中の攻撃のレポートを表示できます。また、レポートを FTP サーバまたは セキュア FTP（SFTP）サーバにエクスポートすることもできます。

レポートには、次のセクションがあります。

- General Details
- Attack Statistics
- Detected Anomalies

General Details

攻撃レポートの General Details セクションには、攻撃に関する一般的な情報が記載されます。表 9-1 で、レポートのこのセクションのフィールドについて説明します。

表 9-1　攻撃レポートの General Details セクションのフィールド説明

フィールド	説明
Report ID	レポートの識別番号。
Attack Start	攻撃が開始された日時を表示します。
Attack End	攻撃が終了した日時を表示します。*Attack in progress* は、進行中の攻撃があることを示します。
Attack Duration	攻撃の期間を表示します。

Attack Statistics

Attack Statistics セクションには、受信したトラフィック フローの一般的な分析が記載されます。

Detected Anomalies

攻撃レポートの Detected Anomalies セクションには、Detector 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が記載されます。動的フィルタの作成を必要とするフローは、トラフィック異常として分類されます。これらの異常は頻繁に発生するものではなく、組織的な DDoS 攻撃に変化する可能性があります。Detector は、同じタイプおよび同じフロー パラメータ（送信元 IP アドレスや宛先ポートなど）の異常を 1 つの異常タイプにまとめます。表 9-2 で、検出された異常のさまざまなタイプについて説明します。

表 9-2　検出された異常のタイプ

タイプ	説明
dns (tcp)	攻撃している DNS-TCP プロトコル フロー。
dns (udp)	攻撃している DNS-UDP プロトコル フロー。
fragments	断片化されたトラフィックが異常な量であることが検出されたフロー。
http	異常な HTTP トラフィック フロー。
ip_scan	多くのゾーン宛先 IP アドレスにアクセスしようとした送信元 IP アドレスから開始されたことが検出されたフロー。
other_protocols	攻撃している TCP/UDP 以外のプロトコル フロー。
port_scan	多くのゾーン ポートにアクセスしようとした送信元 IP アドレスから開始されたことが検出されたフロー。
tcp_connections	データを保持している（または保持していない）、異常な数の TCP 同時接続が検出されたフロー。
tcp_incoming	TCP サービスを攻撃していることが検出されたフロー。
tcp_outgoing	ゾーンがクライアントである場合に、ゾーンによって開始された接続に対する SYN-ACK フラッドまたは他のパケット攻撃で構成されていることが検出されたフロー。

表 9-2　検出された異常のタイプ（続き）

タイプ	説明
tcp_ratio	異なるタイプの TCP パケット間（たとえば、SYN パケット対 FIN/RST パケット）の比率が異常であることが検出されたフロー。
udp	攻撃している UDP プロトコル フロー。
unauthenticated_tcp	Detector のスプーフィング防止が認証に成功しなかったことが検出されたフロー。たとえば、ACK フラッド、FIN フラッド、その他の未認証パケットによるフラッドなどです。
user	ユーザ定義によって検出された異常なフロー。
worm_tcp	TCP/IP プロトコルを介したワームの攻撃。

レポート パラメータについて

レポートの異なるセクションには、トラフィック フローの異なる面が記載されます。

表 9-4 で、Attack Statistics のフィールドについて説明します。

表 9-4　Attack Statistics のフィールド説明

フィールド	説明
Total Packets	攻撃パケットの合計数を示します。
Average pps	平均トラフィック レート（pps）を示します。
Average bps	平均トラフィック レート（bps）を示します。
Max. pps	最大トラフィック レート（pps）を示します。
Max. bps	最大トラフィック レート（bps）を示します。

表 9-5 で、Detected Anomalies のフロー統計情報について説明します。

表 9-5　フロー統計情報のフィールド説明

フィールド	説明
ID	検出された異常の識別番号（ID）を示します。
Start time	異常が検出された日時を示します。
Duration	異常の期間（時間、分、秒）を示します。
Type	異常のタイプを指定します。
Triggering rate	ポリシーのしきい値を超過した異常トラフィック レートを示します。
% Threshold	Triggering rate がポリシーのしきい値を上回っているパーセンテージを示します。
Flow	異常なフローを指定します。この特性は、プロトコル番号、送信元 IP アドレス、送信元ポート、宛先 IP アドレス、宛先ポートを含み、トラフィックが断片化されているかどうかを示します。**Any** は、断片化されているトラフィックと断片化されていないトラフィックの両方があることを示します。

任意のパラメータの * という値は、次のいずれかを示します。

- 値が特定されていない。
- 異常のパラメータに対して複数の値が測定された。

任意のパラメータの # という値（数値の前にある）は、そのパラメータに対して測定された値の数を示します。

Detector モジュールは、*notify* という値をフローの説明の右側に表示する場合があります。レポートの任意の行の *notify* という値は、Detector モジュールはその行に記載されているトラフィックのタイプに関する通知を生成するだけで、アクションを実行しないということを示します。

攻撃レポートの表示

特定のゾーンの攻撃レポートのリスト、または特定の攻撃の詳細なレポートを表示するには、**show** コマンドを使用します。次のコマンドを入力します。

show reports [**current** | *report-id*] [**details**]

表 9-6 で、**show reports** コマンドの引数とキーワードについて説明します。

表 9-6　show reports コマンドの引数とキーワード

パラメータ	説明
current	進行中の攻撃。 進行中の攻撃のビット数およびパケット数は表示されません。進行中の攻撃のレポートでは、パケットとビットのフィールドにゼロ（0）という値が表示されます。
report-id	レポートの識別番号。
details	（オプション）フローの詳細を表示します。

たとえば、ゾーンに対するすべての攻撃のリストを表示するには、次のコマンドを入力します。

```
user@DETECTOR-conf-zone-scannet# show reports
```

表 9-7 で、**show reports** コマンド出力のフィールドについて説明します。

表 9-7　show reports コマンド出力のフィールドの説明

フィールド	説明
Report ID	レポートの識別番号。
Attack Start	攻撃が開始された日時。
Attack End	攻撃が終了した日時。*Attack in progress* という値は、進行中の攻撃があることを示します。
Attack Duration	攻撃の期間。

表 9-7　show reports コマンド出力のフィールドの説明（続き）

フィールド	説明
Attack Type	検出された攻撃のタイプ。表示される値は、次のいずれかです。 • **tcp_connections**：データを保持している（または保持していない）、異常な数の TCP 同時接続が検出されたフロー。 • **http**：異常な HTTP トラフィック フロー。 • **tcp_incoming**：TCP サービスを攻撃していることが検出されたフロー。 • **tcp_outgoing**：ゾーンがクライアントである場合に、ゾーンが開始した接続に対する SYN-ACK 攻撃など、クライアントがゾーンであるように見える検出済み攻撃フロー。 • **unauthenticated_tcp**：Detector のスプーフィング防止メカニズムが認証できなかった検出済みフロー。たとえば、ACK フラッド、FIN フラッド、その他の未認証パケットによるフラッドなどです。 • **dns (udp)**：攻撃的な DNS-UDP プロトコル フロー。 • **dns (tcp)**：攻撃的な DNS-TCP プロトコル フロー。 • **udp**：攻撃的な UDP プロトコル フロー。 • **other_protocols**：攻撃している TCP/UDP 以外のプロトコル フロー。 • **fragments**：異常な量の断片化されたトラフィックが検出されたフロー。 • **hybrid**：特性の異なる複数の攻撃で構成された攻撃。 • **ip_scan**：多くのゾーン宛先 IP アドレスにアクセスしようとした送信元 IP アドレスから開始されたことが検出されたフロー。 • **port_scan**：多くのゾーン ポートにアクセスしようとした送信元 IP アドレスから開始されたことが検出されたフロー。 • **user_detected**：ユーザ定義によって検出された異常なフロー。 • **worm_tcp**：TCP/IP プロトコルを介したワームの攻撃。

表 9-7　show reports コマンド出力のフィールドの説明（続き）

フィールド	説明
Malicious Traffic	このフィールドは、Cisco Anomaly Guard Module だけに関連し、Detector モジュールには適用されません。

ゾーンに対する現在の攻撃のレポートを表示するには、次のコマンドを入力します。

```
user@DETECTOR-conf-zone-scannet# show reports current
```

レポートには、次のような出力が表示されます。各セクションの詳細については、P.9-2 の「レポートのレイアウトについて」を参照してください。

```
Attack Start        :   Feb 26 2004 09:58:54
Attack End          :   Attack in progress
Attack Duration     :   00:08:34

Attack Statistics:
             Total      Average    Average      Max pps    Max bps
             Packets    pps        bps
Received     95878      186.53     110977.74    1455.44    914428.24    N/A

Detected Anomalies:
ID      Start Time         Duration   Type              Triggering    %Threshold
                                                        Rate
1       Feb 26 09:58:54    00:08:34   HTTP              997.44        897.44
        Flow: 6 *          *          92.168.100.34  80 no fragments
```

異常が検出されたフローに関する詳細なレポートを表示するには、**details** オプションを使用します。

表 9-8 に、詳細なレポートに含まれている、フローのフィールドの説明を示します。

表 9-8　詳細なレポートのフローのフィールド説明

フィールド	説明
Detected Flow	動的フィルタが生成される原因となったフローを示します。このフローの特性は、プロトコル番号、送信元 IP アドレス、送信元ポート、宛先 IP アドレス、宛先ポートを含み、トラフィックが断片化されているかどうかを示します。**Any** は、断片化されているトラフィックと断片化されていないトラフィックの両方があることを示します。
Action Flow	動的フィルタによって処理されたフローを示します。アクション フローは、検出されたフローよりも範囲が広い可能性があります。たとえば、検出されたフローが特定の送信元 IP アドレスの特定の送信元ポートを示し、アクション フローが特定の送信元 IP アドレスのすべての送信元ポートを示すことがあります。 このフローの特性は、プロトコル番号、送信元 IP アドレス、送信元ポート、宛先 IP アドレス、宛先ポートを含み、トラフィックが断片化されているかどうかを示します。**Any** は、断片化されているトラフィックと断片化されていないトラフィックの両方があることを示します。

攻撃レポートのエクスポート

監視および診断のために、攻撃レポートを FTP または SFTP サーバにエクスポートできます。テキスト形式または Extensible Markup Language（XML）形式で攻撃レポートをエクスポートできます。

この項では、次のトピックについて取り上げます。

攻撃レポートの自動エクスポート

攻撃が終了した時点で攻撃レポートが XML 形式で自動的にエクスポートされるよう、Detector モジュールを設定できます。Detector モジュールは、いずれか 1 つのゾーンのレポートを、そのゾーンに対する攻撃が終了した時点でエクスポートします。XML スキーマについては、このバージョンに付属の xsd ファイルを参照してください。設定モードで、次のいずれかのコマンドを入力します。

- **export reports ftp** *server remote-path* [*login*] [*password*]
- **export reports sftp** *server remote-path login*

（注）　**copy reports** コマンドを入力する前に、Detector モジュールが SFTP 通信に使用する SSH 鍵を設定する必要があります。詳細については、P.4-37 の「SFTP 接続用の鍵の設定」を参照してください。

表 9-9 で、**export reports** コマンドの引数について説明します。

表 9-9　export reports コマンドの引数

パラメータ	説明
ftp	攻撃レポートを FTP サーバにエクスポートします。
sftp	攻撃レポートを SFTP サーバにエクスポートします。
server	サーバの IP アドレス。

表 9-9　export reports コマンドの引数 （続き）

パラメータ	説明
remote-path	ファイルの保存先ディレクトリの完全パス。
login	サーバのログイン名。 *login* 引数は、FTP サーバを定義する場合のオプションです。ログイン名を入力しない場合、FTP サーバは匿名ログインであると想定し、パスワードを要求しません。
password	（オプション）リモート FTP サーバのパスワード。

次の例は、IP アドレス *10.0.0.191* の FTP サーバに対する攻撃が終了したときに、ログイン名 *user1* とパスワード *password1* を使用して、レポートを XML 形式で自動的にエクスポートする方法を示しています。

```
user@DETECTOR-conf# export reports ftp 10.0.0.191 /root/reports user1
password1
```

すべてのゾーンの攻撃レポートのエクスポート

すべてのゾーンの攻撃レポートをテキストまたは XML 形式でエクスポートできます。レポートを FTP または SFTP サーバに手動でコピーするには、**copy reports** コマンドを使用します。

グローバル モードで次のコマンドを入力します。

copy reports [**xml**] [**details**] **ftp** *server full-file-name* [*login*] [*password*]

表 9-10 で、**copy reports** コマンドの引数とキーワードについて説明します。

表 9-10　copy reports コマンドの引数とキーワード

パラメータ	説明
xml	（オプション）レポートを XML 形式でエクスポートします。XML スキーマについては、このバージョンに付属の xsd ファイルを参照してください。デフォルトでは、レポートはテキスト形式でエクスポートされます。 XML 形式のレポートには、すべての詳細が含まれます。**xml** オプションを指定する場合、**details** オプションを指定する必要はありません。
details	（オプション）フロー、および攻撃の送信元 IP アドレスの詳細をエクスポートします。
ftp	攻撃レポートを FTP サーバにエクスポートします。
server	サーバの IP アドレス。
remote-path	サーバによるファイルの保存先ディレクトリの完全パス。
login	サーバのログイン名。 *login* 引数は、FTP サーバを定義する場合のオプションです。ログイン名を入力しない場合、FTP サーバは匿名ログインであると想定し、パスワードを要求しません。
password	（オプション）リモート FTP サーバのパスワード。

次の例は、ログイン名 *user1* とパスワード *password1* を使用して、Detector モジュールによって処理されたすべての攻撃のリストをテキスト形式で IP アドレス *10.0.0.191* の FTP サーバにコピーする方法を示しています。

```
user@DETECTOR# copy reports ftp 10.0.0.191 ADMreports.txt user1
password1
```

ゾーン レポートのエクスポート

特定のゾーンの攻撃レポートを FTP サーバにコピーするには、グローバル モードで次のいずれかのコマンドを入力します。

- **copy zone** *zone-name* **reports** [**current** | *report-id*] [**xml**] [**details**] **ftp** *server full-file-name* [*login*] [*password*]
- **copy zone** *zone-name* **reports** [**current** | *report-id*] [**xml**] [**details**] **sftp** *server full-file-name login*

（注）　**copy reports** コマンドを入力する前に、Detector モジュールが SFTP 通信に使用する SSH 鍵を設定する必要があります。詳細については、P.4-37 の「SFTP 接続用の鍵の設定」を参照してください。

表 9-11 で、**copy zone reports** コマンドの引数とキーワードについて説明します。

表 9-11　copy zone reports コマンドの引数とキーワード

パラメータ	説明
zone-name	既存のゾーンの名前。
current	(オプション)進行中の攻撃のレポートをエクスポートします（該当する場合)。 デフォルトでは、すべてのゾーン レポートをエクスポートします。
report-id	(オプション）既存のレポートの ID。指定した ID 番号を持つレポートが Detector モジュールによってエクスポートされます。ゾーン攻撃レポートの詳細を表示するには、**show zone reports** コマンドを使用します。 デフォルトでは、すべてのゾーン レポートをエクスポートします。

表 9-11　copy zone reports コマンドの引数とキーワード（続き）

パラメータ	説明
xml	（オプション）レポートを XML 形式でエクスポートします。XML スキーマについては、このバージョンに付属の xsd ファイルを参照してください。デフォルトでは、レポートをテキスト形式でエクスポートします。 XML 形式のレポートには、すべての詳細が含まれます。**xml** オプションを指定する場合、**details** オプションを指定する必要はありません。
details	（オプション）フロー、および攻撃の送信元 IP アドレスの詳細をエクスポートします。
ftp	攻撃レポートを FTP サーバにエクスポートします。
sftp	攻撃レポートを SFTP サーバにエクスポートします。
server	サーバの IP アドレス。
remote-path	ファイルの保存先ディレクトリの完全パス。
login	サーバのログイン名。 *login* 引数は、FTP サーバを定義する場合のオプションです。ログイン名を入力しない場合、FTP サーバは匿名ログインであると想定し、パスワードを要求しません。
password	（オプション）リモート FTP サーバのパスワード。

次の例は、ログイン名 *user1* とパスワード *password1* を使用して、ゾーンのすべての攻撃レポートを IP アドレス *10.0.0.191* の FTP サーバにコピーする方法を示しています。

```
user@DETECTOR# copy zone scannet reports ftp 10.0.0.191
ScannetCurrentReport.txt user1 password1
```