攻撃レポート

この章では、Guard が生成する攻撃レポートについて説明します。この章では、次のトピックについて取り上げます。

レポートのレイアウト

Guard 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。攻撃の開始は最初の動的フィルタの生成時で、攻撃の終了は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
- Dropped/ Replied Packets
- Detected Anomalies
- Mitigated Attacks
- Zombies：このセクションは、**show reports details** コマンドおよび **show zombies** コマンドを発行した場合にだけ表示されます。

General Details

攻撃レポートのこのセクションには、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 には、さまざまなパケットのゾーン トラフィック フローの一般的な分析が記載されます。表 9-2 で、パケット タイプについて説明します。

表 9-2　パケット タイプ

タイプ	説明
Received	宛先変更されたトラフィックの合計量を示します。
Forwarded	Guard がゾーンに転送した正当なトラフィックを示します。
Replied	検証の試行で Guard のスプーフィング防止メカニズムおよびゾンビ防止メカニズムが送信元に返送したトラフィックを示します。
Dropped	Guard がドロップしたトラフィックを示します。

Dropped/ Replied Packets

攻撃レポートの Dropped/Replied Packets セクションでは、ドロップされたパケットおよび返送されたパケットが分析されます。レポートでは、パケットがタイプ（スプーフィングまたは形式異常）および処理メカニズム（フィルタ タイプまたはレート リミッタ）によって分類されます。表 9-3 で、ドロップされたパケットのさまざまなタイプについて説明します。

表 9-3　ドロップされたパケットおよび返送されたパケットのタイプ

タイプ	説明
Rate Limiter	ゾーンのレート リミッタおよびユーザ フィルタのレート リミッタによってドロップされたパケット。
Flex Filter	フレックス フィルタによってドロップされたパケット。
User Filters	ユーザ フィルタによってドロップされたパケット。
Dynamic Filters	動的フィルタによってドロップされたパケット。

表 9-3　ドロップされたパケットおよび返送されたパケットのタイプ（続き）

タイプ	説明
Spoofed	Guard によって、スプーフィングされたパケットまたはゾンビが発信したパケットであると識別されたため、ゾーンに転送されなかったパケット。Spoofed パケットは、Replied（返送された）パケットですが、その返送は受信されません。
Malformed	形式異常構造であるため、または Guard のスプーフィング防止メカニズムが原因で、形式異常であると分析されたパケット。

Detected Anomalies

攻撃レポートの Detected Anomalies セクションには、Guard 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。動的フィルタの生成を要求するフローは、異常であると分類されます。このような異常はあまり発生しないか、または体系的な DDoS 攻撃となる可能性があります。Guard 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 9-4 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 9-4　検出された異常のタイプ

タイプ	説明
tcp_connections	データを持つまたは持たない、TCP 同時接続数が異常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。
tcp_incoming	ゾーンがサーバである場合に、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 9-4　検出された異常のタイプ（続き）

タイプ	説明
unauthenticated_tcp	Guard 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、認証されていないパケットの ACK フラッド、FIN フラッド、または他のフラッド。
dns (udp)	攻撃している DNS-UDP プロトコル フロー。
dns (tcp)	攻撃している DNS-TCP プロトコル フロー。
udp	攻撃している 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	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。
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。
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	ユーザ定義によって検出された異常なフロー。

Mitigated Attacks

攻撃レポートの Mitigated Attacks セクションには、Guard がゾーンを保護する（攻撃を軽減する）ために実行した処置が詳細に記載されます。このレポートには、軽減のタイミングおよび軽減された攻撃のタイプの詳細が記載されます。Guard は、使用したメカニズムに応じて軽減のタイプを定義します。このメカニズムは、攻撃のタイプとサブタイプを示します。

たとえば、Guard が syn パケットの攻撃フローに対して基本的なスプーフィング防止メカニズムを使用した場合、軽減された攻撃は **spoofed/tcp_syn_basic** と表示されます。spoofed は攻撃のタイプを示し、tcp_syn_basic はサブタイプを示します。

軽減された攻撃には、次の 5 つのタイプがあります。

- スプーフィング利用
- ゾンビ
- クライアント攻撃
- ユーザ定義
- 形式異常パケット

スプーフィング利用

スプーフィングを利用した攻撃には、スプーフィングされた送信元からの DDoS 攻撃であると識別されるすべてのトラフィック異常が含まれます。表 9-5 で、スプーフィングを利用した攻撃のさまざまなタイプについて説明します。

表 9-5　スプーフィングを利用した攻撃のタイプ

攻撃のタイプ	説明
spoofed/tcp_syn (basic)	基本的なスプーフィング防止メカニズムが認証に成功しなかった syn パケットのフラッド。
spoofed/tcp_syn (strong)	強力なスプーフィング防止メカニズムが認証に成功しなかった syn パケットのフラッド。
spoofed/tcp_syn_ack (basic)	基本的なスプーフィング防止メカニズムが認証に成功しなかった syn_ack パケットのフラッド。
spoofed/tcp_syn_ack (strong)	強力なスプーフィング防止メカニズムが認証に成功しなかった syn_ack パケットのフラッド。
spoofed/tcp_incoming (basic)	基本的なスプーフィング防止メカニズムが認証に成功しなかったトラフィックのフラッド。
spoofed/tcp_incoming (strong)	強力なスプーフィング防止メカニズムが認証に成功しなかったトラフィックのフラッド。
spoofed/tcp_outgoing (strong)	強力なスプーフィング防止メカニズムが認証に成功しなかった、ゾーンで開始された接続に応答する着信トラフィックのフラッド。
spoofed/udp (basic)	基本的なスプーフィング防止メカニズムが認証に成功しなかった UDP トラフィックのフラッド。

表 9-5　スプーフィングを利用した攻撃のタイプ（続き）

攻撃のタイプ	説明
spoofed/udp (strong)	強力なスプーフィング防止メカニズムが認証に成功しなかった UDP トラフィックのフラッド。
spoofed/other_protocols	Guard のスプーフィング防止メカニズムが認証に成功しなかった、TCP および UDP トラフィック以外のフラッド。
spoofed/tcp_fragments	Guard のスプーフィング防止メカニズムが認証に成功しなかった、断片化された TCP パケットのフラッド。
spoofed/udp_fragments	Guard のスプーフィング防止メカニズムが認証に成功しなかった、断片化された UDP パケットのフラッド。
spoofed /other_protocols_fragments	Guard のスプーフィング防止メカニズムが認証に成功しなかった、TCP および UDP 以外の断片化されたパケットのフラッド。
spoofed/dns_queries (strong)	強力なスプーフィング防止メカニズムが認証に成功しなかった DNS クエリー パケットのフラッド。
spoofed/dns_replies (basic)	基本的なスプーフィング防止メカニズムが認証に成功しなかった、ゾーンで開始された接続に応答する着信 DNS パケットのフラッド。
spoofed/dns_replies (strong)	強力なスプーフィング防止メカニズムが認証に成功しなかった、ゾーンで開始された接続に応答する着信 DNS パケットのフラッド。

ゾンビ

ゾンビ攻撃には、ゾンビによって開始された DDos 攻撃であると識別されるトラフィック異常が含まれます。表 9-6 で、ゾンビ攻撃のタイプについて説明します。

表 9-6　ゾンビ攻撃のタイプ

攻撃のタイプ	説明
zombie/http	Guard のゾンビ防止メカニズムが認証に成功しなかった、スプーフィングされていないと識別された多くの送信元からの HTTP トラフィックのフラッド。

クライアント攻撃

クライアント攻撃には、スプーフィングされていないすべてのトラフィック異常が含まれます。表 9-7 で、さまざまなタイプのクライアント攻撃について説明します。

表 9-7　クライアント攻撃のタイプ

攻撃のタイプ	説明
client_attack/tcp_connections	データを持つまたは持たない、TCP 同時接続数が異常であるフロー。
client_attack/http	HTTP トラフィック フローのフラッド。
client_attack/tcp_ incoming	ゾーンがサーバである場合に、TCP サービスを攻撃しているフラッド。
client_attack/tcp_outgoing	ゾーンが開始した認証済み IP 接続からの攻撃フラッド。
client_attack /unauthenticated_tcp	TCP ハンドシェイクを経ていない ACK、FIN、または他のパケットのフラッド、あるいは Guard のスプーフィング防止メカニズムが認証に成功しなかった TCP 接続。
client_attack/dns (udp)	攻撃している DNS-UDP プロトコルのフラッド。
client_attack/dns (tcp)	攻撃している DNS-TCP プロトコルのフラッド。
client_attack/udp	攻撃している UDP プロトコル フローのフラッド。

表 9-7　クライアント攻撃のタイプ（続き）

攻撃のタイプ	説明
client_attack/other_protocols	攻撃している TCP/UDP 以外のプロトコル フローのフラッド。
client_attack/fragments	断片化されたトラフィックのフラッド。
client_attack/user	ユーザ定義の攻撃のフラッド。この攻撃は、ユーザによって追加された動的フィルタによって定義されます。

ユーザ定義

ユーザ定義攻撃には、ユーザ フィルタによって処理されたすべての異常が含まれます。ユーザ フィルタは、デフォルトで機能するか、またはユーザによって設定されます（詳細については、第 7 章「ポリシー テンプレートとポリシーの設定」を参照してください）。表 9-8 で、ユーザ定義攻撃のタイプについて説明します。

表 9-8　ユーザ定義攻撃のタイプ

攻撃のタイプ	説明
user_defined/rate_limit	ゾーンのユーザ フィルタまたはグローバル レート リミッタによってレート制限されたオーバーフロー。
user_defined/user_drop_filters	drop アクションを持つユーザ フィルタによって処理されたフラッド。

形式異常パケット

形式異常パケットには、悪意のある形式異常パケットで構成されると識別されたすべてのトラフィック異常が含まれます。表 9-9 で、さまざまなタイプの形式異常パケットについて説明します。

表 9-9　形式異常パケットのタイプ

攻撃のタイプ	説明
malformed_packets /packets_to_proxy_ip	Guard の プロキシ IP アドレスを攻撃しているフラッド。
malformed_packets /dns_anti_spoofing_algo	Guard の DNS スプーフィング防止メカニズムの動作が原因の形式異常パケットのフラッド。
malformed_packets/dns (queries)	形式異常の DNS パケットのフラッド。
malformed_packets /dns (short_queries)	短い DNS クエリーのフラッド。
malformed_packets/dns (replies)	形式異常の DNS 応答のフラッド。
malformed_packets/src ip = dst ip	送信元および宛先としてゾーンの IP アドレスを持つパケットのフラッド。
malformed_packets /zero_header_field	ヘッダーのフィールドの一部が不正にゼロとなっているパケットのフラッド。

Zombies

ゾンビ攻撃には、ゾンビによって開始された DDoS 攻撃であると識別されたトラフィック異常が含まれます。Guard の攻撃レポートには、現在ゾーンを攻撃しているゾンビを一覧表示するテーブルが表示されます。現在攻撃しているゾンビのリストを表示するには、**show reports details** コマンドおよび **show zombies** コマンドを使用します。

show zombies コマンド出力のフィールドについては、表 9-14 を参照してください。

レポートのパラメータ

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 9-10 で、Attack Statistics および Dropped/ Replied Packets のフィールドについて説明します。

表 9-10　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。
Average pps	平均トラフィック レート（パケット / 秒）。
Average bps	平均トラフィック レート（ビット / 秒）。
Max. pps	最大トラフィック レート（パケット / 秒）。
Max. bps	最大トラフィック レート（ビット / 秒）。
Percentage	受信パケットの合計数に対する、転送されたパケット、返送されたパケット、およびドロップされたパケットのパーセンテージ。

表 9-11 で、Detected Anomalies および Mitigated Attacks のフロー統計情報について説明します。

表 9-11　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	異常または軽減された攻撃のタイプを示します。
Triggering rate	ポリシーのしきい値を超えた異常なトラフィック レートを示します。

表 9-11　フロー統計情報のフィールド説明（続き）

フィールド	説明
% 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	異常なフローおよび軽減された攻撃のフローを示します。この特性は、プロトコル番号、送信元 IP、送信元ポート、宛先 IP、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。

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。このコマンドの構文は、次のとおりです。

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

表 9-12 で、**show reports** コマンドのキーワードと引数について説明します。

表 9-12　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）フローおよび攻撃しているゾンビ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、次のように入力します。

```
admin@GUARD-conf-zone-scannet# show reports
```

レポートには、各攻撃の期間、攻撃の開始日時および終了日時の情報を示す次のような出力が表示されます。

```
Report ID       Attack Start              Attack End               Attack Duration
current         Feb 26 2004 09:58:54      Attack in progress       N/A
4               Feb 25 2004 15:48:25      Feb 25 2004 18:23:46     02:35:21
3               Feb 25 2004 15:38:45      Feb 25 2004 15:48:18     00:09:33
2               Feb 25 2004 15:11:39      Feb 25 2004 15:29:40     00:18:01
1               Feb 25 2004 13:09:10      Feb 25 2004 13:15:28     00:06:18
```

ゾーンに対する現在の攻撃のレポートを表示するには、次のように入力します。

```
admin@GUARD-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」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     Percentage
               Packets     pps         bps
Received       95878       186.53      110977.74   1455.44     914428.24   N/A
Forwarded      53827       104.72      64278.54    1430.85     899196.24   56.14
Replied        1870        3.64        2172.89     23.03       14433.88    1.95
Dropped        40181       78.17       44526.32    96.82       55010.13    41.91


Dropped/Replied Packets:
               Total       Average     Average     Max pps     Max bps     Percentage
               Packets     pps         bps
Rate Limiter   0           0           0           0           0           0
Flex Filter    0           0           0           0           0           0
User Filters   0           0           0           0           0           0
Dynamic        78.07       44473.53    96.82       55010.13    99.84
Filters 40128
Spoofed        12          0.02        11.95       0.15        75.29       0.03
Malformed      53          0.1         52.79       1.56        798.12      0.13


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
```

```
Mitigated Attacks:
ID         Start Time         Duration       Type                    Triggering    %Threshold
                                                                      Rate
1          Feb 26 09:59:40    00:07:59       client_attack/           38            280
                                             tcp_connections
           Flow: 6 (#52)      *              92.168.200.254 80       no fragments
```

検出された異常および軽減された攻撃のフローに関する詳細なレポート、およびゾンビ攻撃のリストを表示するには、**details** オプションを使用します。

表 9-13 に、詳細なレポートに表示されるフローのフィールドのリストを示します。

表 9-13　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	この行には、動的フィルタが生成される原因となったフローが表示されます。
Action Flow	この行には、動的フィルタによって処理されたフローが表示されます。アクション フローは、検出されたフローよりも広範囲であることがあります。たとえば、検出されたフローが特定の送信元 IP 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 のすべての送信元ポートを示すことがあります。

表 9-14 で、ゾンビ攻撃に関する詳細なレポートのフィールドについて説明します。

表 9-14　ゾンビ攻撃に関するテーブルのフィールド説明

フィールド	説明
IP	ゾンビの IP アドレス。
Start Time	ゾンビ接続が初めて識別された日時。
Duration	ゾンビ攻撃の期間。
#Requests	ゾンビによって送信された HTTP get 要求の数。

（注）　ゾンビ攻撃がない場合は、レポートの Zombies という見出しの下に **Report doesn’t exist** と表示されます。

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 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。

（注）　**show running-config** で、ftp サーバのユーザ名とパスワードが表示されます。匿名 ftp アカウントを使用することをお勧めします。

レポートを ftp サーバに手動でコピーするには、**copy** コマンドを使用します。すべてのゾーンの攻撃レポートをコピーすることも、特定のゾーンのレポートをコピーすることもできます。

このコマンドの構文は、次のとおりです。

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

表 9-16 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 9-16　copy reports コマンドのキーワードと引数

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 の詳細をエクスポートします。
server	ftp サーバの IP アドレス。

表 9-16　copy reports コマンドのキーワードと引数（続き）

パラメータ	説明
full-file-name	レポート リストの完全なファイル名。パスを指定しない場合、デフォルトで、ログイン ユーザのホーム ディレクトリが使用されます。
login	（オプション）ftp サーバのログイン名。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。

たとえば、ログイン名 *user1* とパスワード *password1* を使用して、Guard 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には、次のように入力します。

```
admin@GUARD# copy reports ftp 10.0.0.191 Guard-reports.txt user1
password1
```

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 コマンド グループ レベルで次のように入力します。

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

表 9-17 で、**copy zone reports** コマンドのキーワードと引数について説明します。

表 9-17　copy zone reports コマンドのキーワードと引数

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 レポートがエクスポートされます。

表 9-17　copy zone reports コマンドのキーワードと引数 （続き）

パラメータ	説明
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 Guard 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 レポートがエクスポートされます。
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 の詳細をエクスポートします。
server	ftp サーバの IP アドレス。
full-file-name	レポート リストの完全なファイル名。パスを指定しない場合、デフォルトで、ログイン ユーザのホーム ディレクトリが使用されます。
login	（オプション）ftp サーバのログイン名。 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。

たとえば、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には、次のように入力します。

```
admin@GUARD# copy zone scannet reports ftp 10.0.0.191
ScannetCurrentReport.txt user1 password1
```