ファイアウォールの Botnet Traffic Filter ルールの管理

マルウェアとは、知らないうちにホストにインストールされている悪意のあるソフトウェアです。個人情報（パスワード、クレジット カード番号、キー ストローク、または独自データ）の送信などのネットワーク アクティビティを試みるマルウェアは、マルウェアが既知の不正な IP アドレスへの接続を開始したときにボットネット トラフィック フィルタによって検出できます。Botnet Traffic Filter は、悪意のある既知のドメイン名および IP アドレスを含む動的データベースと、着信接続および発信接続とを照合して、疑わしいアクティビティをすべてログに記録します。

また、ブロックアドレスを選択してスタティックブロックリストに追加することで、シスコのダイナミックデータベースを補完できます。ブロックリストに記載すべきでないと考えられるアドレスがシスコのダイナミックデータベースに含まれている場合は、それらのアドレスをスタティック許可リストに手動で入力できます。許可リストのアドレスに関する syslog メッセージは依然として生成されます。ただし、ターゲットになるのはブロック syslog メッセージだけであるため、これは単なる情報提供に過ぎません。内部要件のためにシスコのダイナミックデータベースを使用しない場合は、スタティックブロックリストだけを使用することもできます（ターゲットにするマルウェアサイトをすべて特定できる場合）。

この章は、次のセクションで構成されています。

Botnet Traffic Filter について

Botnet Traffic Filter のアドレス カテゴリ

ボットネット トラフィック フィルタのモニター対象のアドレスは次のとおりです。

- **既知のマルウェア アドレス**：これらのアドレスは、動的データベースおよび静的ブロックリストによって識別されるブロックリストに含まれています。

- **既知の許可アドレス**：これらのアドレスは、許可リストに含まれています。許可されるには、アドレスが、動的データベースによってブロックされ、かつ静的許可リストによって識別される必要があります。
- **あいまいなアドレス**：ブロックリストに記載されていないドメイン名を1つ以上含む複数のドメイン名に関連付けられているアドレス。これらのアドレスは、グレーリストに含まれています。
- **リストに記載されていないアドレス**：どのリストにも記載されていない不明アドレス。

既知アドレスに対する Botnet Traffic Filter のアクション

ボットネット トラフィック フィルタを設定して、疑わしいアクティビティをログに記録できます。必要に応じてボットネット トラフィック フィルタを設定して、疑わしいトラフィックを自動的にブロックすることもできます。

リストに記載されていないアドレスについては、syslog メッセージは生成されません。ただし、ブロックリスト、許可リスト、およびグレイリストに記載されているアドレスについては、タイプ別の syslog メッセージが生成されます。

Botnet Traffic Filter データベース

ボットネット トラフィック フィルタでは、既知のアドレスについて 2 つのデータベースが使用されます。両方のデータベースを使用するか、ダイナミック データベースをディセーブルにしてスタティック データベースだけを使用することができます。このセクションは、次のトピックで構成されています。

- 動的データベースに関する情報
- 静的データベースに関する情報

動的データベースに関する情報

ボットネット トラフィック フィルタでは、Cisco アップデート サーバーからダイナミック データベースの定期アップデートを受け取ることができます。このデータベースには、数千もの既知の不正なドメイン名と IP アドレスが含まれています。

セキュリティ アプライアンスでは動的データベースを次のように使用します。

1. DNS 応答内のドメイン名が動的データベース内の名前と一致した場合、Botnet Traffic Filter はその名前および IP アドレスを DNS 逆ルックアップ キャッシュに追加します。
2. 感染したホストがマルウェア サイトの IP アドレスへの接続を開始すると、セキュリティ アプライアンスは、疑わしいアクティビティについて通知する syslog メッセージを送信します。
3. 場合によっては、IP アドレス自体がダイナミック データベースに入力され、ボットネット トラフィック フィルタは DNS 要求を検査せずに、その IP アドレスへのすべてのトラフィックをログに記録します。

（注） データベースを使用するには、セキュリティ アプライアンスが URL にアクセスできるように、必ずセキュリティ アプライアンス用にドメイン ネーム サーバを設定してください。動的データベースでドメイン名を使用するには、Botnet Traffic Filter のスヌーピングとともに DNS パケット インスペクションをイネーブルにする必要があります。セキュリティ アプライアンスは DNS パケット内を調べて、ドメイン名と関連する IP アドレスを見つけます。

静的データベースに関する情報

不正な名前と見なすドメイン名または IP アドレス（ホストまたはサブネット）をブロックリストに手動で入力できます。許可リストに名前または IP アドレスを入力して、許可リストと動的ブロックリストの両方に表示される名前またはアドレスが syslog メッセージおよびレポートでは許可リストアドレスとしてのみ識別されるようにすることもできます。

これ以外に、Botnet Traffic Filter のスヌーピングとともに DNS パケット インスペクションをイネーブルにする方法もあります。DNS スヌーピングを使用すると、感染したホストが静的データベース上の名前に対して DNS 要求を送信した場合に、セキュリティ アプライアンスは DNS パケット内を調べてドメイン名および関連する IP アドレスを見つけ、その名前および IP アドレスを DNS 逆ルックアップ キャッシュに追加します。

関連項目

- ボットネット トラフィック フィルタの設定のタスク フロー （3 ページ）
- [Botnet Traffic Filter Rules] ページ （12 ページ）

ボットネット トラフィック フィルタの設定のタスク フロー

Botnet Traffic Filter を設定するには、次の手順を実行します。

ステップ 1 DNS サーバの使用をイネーブルにします。

この手順により、セキュリティ アプライアンスで DNS サーバを使用できるようになります。マルチ コンテキスト モードで、コンテキストごとに DNS をイネーブルにします。

詳細については、[DNS] ページを参照してください。

ステップ 2 ダイナミック データベースの使用をイネーブルにする。

この手順により、シスコの更新サーバからデータベースを更新できるようになり、また、セキュリティ アプライアンスでダウンロード済み動的データベースを使用できるようになります。ダウンロードされたデー

タベースのディセーブル化は、マルチ コンテキスト モードでデータベースの使用をコンテキストごとに設定できるようにする場合に有用です。

詳細については、ダイナミック データベースの設定 （5 ページ）を参照してください。

ステップ 3 （任意）スタティック エントリをデータベースに追加する。

この手順では、ブロックまたは許可するドメイン名またはIPアドレスを使用してダイナミックデータベースを補完します。ダイナミック データベースをインターネット経由でダウンロードしない場合は、ダイナミック データベースの代わりにスタティック データベースを使用できます。

詳細については、スタティック データベースへのエントリの追加 （6 ページ）を参照してください。

ステップ 4 DNS スヌーピングをイネーブルにする。

この手順により、DNSパケットのインスペクションがイネーブルになり、（セキュリティアプライアンス用のDNSサーバを使用できない場合は）ドメイン名と動的データベースまたは静的データベース内のドメイン名が比較され、名前および IP アドレスが DNS 逆ルックアップ キャッシュに追加されます。その後、疑わしいアドレスに対して接続が確立されたとき、Botnet Traffic Filter ロギング機能によってこのキャッシュが使用されます。

詳細については、DNS スヌーピングのイネーブル化 （7 ページ）を参照してください。

ステップ 5 ボットネット トラフィック フィルタのトラフィック分類およびアクションをイネーブルにします。

この手順により、Botnet Traffic Filterで、各初期接続パケット内の送信元および宛先IPアドレスを動的データベース、静的データベース、DNS 逆ルックアップ キャッシュ、およびDNS ホスト キャッシュと比較して、一致トラフィックに関する syslog メッセージを送信するか、そのトラフィックをドロップできるようになります。

詳細については、ボットネット トラフィック フィルタのトラフィック分類とアクションのイネーブル化（8 ページ）を参照してください。

ステップ 6 ボットネット アクティビティをモニタおよび軽減します。

デバイスに Botnet Traffic Filter を設定すると、デバイスはボットネット アクティビティを通知する syslog メッセージの生成を開始します。メッセージが適切にログに記録され、必要に応じて通知が送信されるように、デバイス上のsyslog設定を確認する必要があります。悪意のあるトラフィックが識別された場合は、必要なアクションを実行してこのようなトラフィックを停止し、悪意のあるトラフィックを生成している感染コンピュータを浄化する必要があります。

詳細については、次の情報を参照してください。

1. ファイアウォール デバイスでのロギング ポリシーの設定
2. ボットネット アクティビティのモニタリングと軽減
3. ファイアウォール サマリー ボットネット レポートについて

ダイナミック データベースの設定

この手順により、データベースを更新できるようになり、また、セキュリティアプライアンスでダウンロード済み動的データベースを使用できるようになります。

マルチコンテキストモードの場合、すべてのセキュリティコンテキストで使用できるように、システムコンテキストで動的データベースのダウンロードをイネーブルにします。そのあと、コンテキストごとに、動的データベースの使用をイネーブルにするかディセーブルにするかを決定できます。

デフォルトでは、ダイナミックデータベースのダウンロードおよび使用はディセーブルになっています。

関連項目

- [動的ブラックリスト設定（Dynamic Blacklist Configuration）] タブ （13 ページ）
- Botnet Traffic Filter について （1 ページ）
- ボットネット トラフィック フィルタの設定のタスク フロー （3 ページ）
- スタティック データベースへのエントリの追加 （6 ページ）
- DNS スヌーピングのイネーブル化 （7 ページ）
- ボットネット トラフィック フィルタのトラフィック分類とアクションのイネーブル化 （8 ページ）
- [Botnet Traffic Filter Rules] ページ （12 ページ）

はじめる前に

セキュリティ アプライアンスで DNS サーバの使用をイネーブルにします（[DNS] ページを参照）。マルチ コンテキスト モードで、コンテキストごとに DNS をイネーブルにします。

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから **[ファイアウォール（Firewall）] > [ボットネットトラフィックフィルタルール（Botnet Traffic Filter Rules）]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[ファイアウォール（Firewall）] > [ボットネットトラフィックフィルタルール（Botnet Traffic Filter Rules）]** を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

（注） マルチ コンテキスト モードのデバイスの場合、システム コンテキストで動的データベースのダウンロードをイネーブルにし、必要に応じて各セキュリティ コンテキストで動的データベースの使用をイネーブルにします。

[Botnet Traffic Filter Rules] ページ （12 ページ）が開きます。

ステップ 2 [ダイナミックブロックリスト設定（Dynamic Blocklist Configuration）] タブで [サーバーからのダイナミックブロックリストの有効化（Enable Dynamic Blocklist From Server）] を選択して、動的データベースのダウンロードをイネーブルにします。

（注） マルチコンテキストモードの場合、システムコンテキストで動的データベースのダウンロードをイネーブルにします。

この設定により、シスコの更新サーバから動的データベースをダウンロードできるようになります。データベースをセキュリティ アプライアンスにまだインストールしていない場合は、約 2 分後にデータベースがダウンロードされます。セキュリティ アプライアンスが今後の更新を検出するためにサーバをポーリングする頻度（通常は 1 時間おき）が、更新サーバによって決定されます。

ステップ 3 （マルチコンテキストモードだけ）[保存（Save）] をクリックして、システムコンテキストに変更を保存します。次に、Botnet Traffic Filter を設定するコンテキストに移動し、そのコンテキストの [ファイアウォール（Firewall）] > [ボットネット トラフィック フィルタ ルール（Botnet Traffic Filter Rules）] を選択してステップ 4 （6 ページ）に進みます。

ステップ 4 [ダイナミックブロックリスト設定（Dynamic Blocklist Configuration）] タブで [ダイナミックブロックリストの使用（Use Dynamic Blocklist）] を選択して、動的データベースの使用を有効にします。

（注） マルチコンテキストモードの場合、これらの設定はシステム コンテキストでディセーブルになっています。

スタティック データベースへのエントリの追加

スタティックデータベースを使用すると、ブロックまたは許可するドメイン名、IP アドレス、またはネットワークアドレスを使用してダイナミックデータベースを増強できます。詳細については、Botnet Traffic Filter について （1 ページ）を参照してください。

関連項目

- [許可リスト/ブロックリスト（Permitlist/Blocklist）] タブ （19 ページ）
- [デバイス許可リスト（Device Permitlist）] または [デバイスブロックリスト（Device Blocklist）] ダイアログボックス （20 ページ）
- Botnet Traffic Filter について （1 ページ）
- ボットネット トラフィック フィルタの設定のタスク フロー （3 ページ）
- ダイナミック データベースの設定 （5 ページ）
- DNS スヌーピングのイネーブル化 （7 ページ）
- ボットネット トラフィック フィルタのトラフィック分類とアクションのイネーブル化 （8 ページ）
- [Botnet Traffic Filter Rules] ページ （12 ページ）

はじめる前に

- セキュリティ アプライアンスで DNS サーバの使用をイネーブルにします（[DNS] ページを参照）。マルチ コンテキスト モードで、コンテキストごとに DNS をイネーブルにします。

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから **[ファイアウォール（Firewall）] > [ボットネットトラフィックフィルタルール（Botnet Traffic Filter Rules）]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[ファイアウォール（Firewall）] > [ボットネットトラフィックフィルタルール（Botnet Traffic Filter Rules）]** を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

（注） マルチ コンテキスト モードのデバイスの場合、セキュリティ コンテキストで静的データベースを設定します。

これにより、 [Botnet Traffic Filter Rules] ページ （12 ページ）が開きます。

ステップ 2 [許可リスト/ブロックリスト（Permitlist / Blocklist）] タブで、追加するエントリのタイプ（[許可リスト（Permitlist）] または [ブロックリスト（Blocklist）]）に対応した [行の追加（Add Rows）] ボタンをクリックします

[デバイス許可リスト（Device Permitlist）] または [デバイスブロックリスト（Device Blocklist）] ダイアログボックス （20 ページ）が開きます。

ステップ 3 [Domain or IP Address] フィールドに、1 つ以上のドメイン名、IP アドレス、および IP アドレス/ネットマスクを入力します。複数のエントリは、カンマで区切るかまたは別々の行に入力します。タイプごとに最大 1000 のエントリを入力できます。

ステップ 4 [OK] をクリックします。

DNS スヌーピングのイネーブル化

この手順では、DNS パケットのインスペクションとボットネット トラフィック フィルタ スヌーピングをイネーブルにします。DNS パケットのインスペクションとボットネット トラフィック フィルタ スヌーピングでは、ドメイン名がダイナミック データベースまたはスタティック データベースのドメイン名と比較され、ドメイン名と IP アドレスがボットネット トラフィック フィルタの DNS 逆ルックアップ キャッシュに追加されます。その後、疑わしいアドレスに対して接続が確立されたとき、Botnet Traffic Filter ロギング機能によってこのキャッシュが使用されます。

DNS インスペクションのデフォルト設定では、すべてのインターフェイス上のすべての UDP DNS トラフィックが検査され、Botnet Traffic Filter のスヌーピングはディセーブルになります。外部 DNS 要求を送信するインターフェイスでだけ Botnet Traffic Filter のスヌーピングをイネーブルにすることを推奨します。内部 DNS サーバへの送信を含むすべての UDP DNS トラフィックで Botnet Traffic Filter のスヌーピングをイネーブルにすると、セキュリティ アプライアンスに不要な負荷がかかります。

（注） TCP DNS トラフィックはサポートされません。

関連項目

- [Configure DNS] ダイアログボックス
- Botnet Traffic Filter について （1 ページ）
- ボットネット トラフィック フィルタの設定のタスク フロー （3 ページ）
- ダイナミック データベースの設定 （5 ページ）
- スタティック データベースへのエントリの追加 （6 ページ）
- ボットネット トラフィック フィルタのトラフィック分類とアクションのイネーブル化 （8 ページ）
- [Botnet Traffic Filter Rules] ページ （12 ページ）

ステップ 1 最初に、Botnet Traffic Filter を使用してスヌーピングするトラフィックの DNS インスペクションを設定する必要があります。ファイアウォール インスペクション ルールの管理を参照してください。

ステップ 2 新しいインスペクション ルールの定義または既存のインスペクション ルールの編集時に、検査するプロトコルとして [DNS] を選択します。

[Selected Protocol] フィールドの右側にある [Configure] ボタンがアクティブになります。

ステップ 3 [構成] をクリックします。

[Configure DNS] ダイアログボックスが開きます。

ステップ 4 DNS スヌーピングをイネーブルにするには、[動的フィルタスヌーピングを有効化（Enable Dynamic Filter Snooping）] を選択します。

ステップ 5 [OK] をクリックします。

ボットネット トラフィック フィルタのトラフィック分類とアクションのイネーブル化

この手順により、Botnet Traffic Filter で、各初期接続パケット内の送信元および宛先 IP アドレスを動的データベース、静的データベース、DNS 逆ルックアップ キャッシュ、および DNS ホスト キャッシュと比較して、一致トラフィックに関する syslog メッセージを送信できるようになります。また、Botnet Traffic Filter では、一致トラフィックの発生時に接続をドロップすることもできます。特定のインターフェイスに関して、ボットネット トラフィック フィルタリングが適用されるトラフィックを識別するイネーブル化ルールを 1 つだけ指定できます。た

だし、Botnet Traffic Filter によってドロップされるトラフィックを識別する場合は、複数の廃棄ルールを指定できます。

DNS スヌーピングは個別にイネーブルにします（DNS スヌーピングのイネーブル化 （7 ページ）を参照）。一般的に、Botnet Traffic Filter を最大限に利用するには、DNS スヌーピングをイネーブルにする必要がありますが、必要に応じて、Botnet Traffic Filter のロギングだけを単独で使用できます。ダイナミック データベースにDNSスヌーピングが設定されていない場合、ボットネットトラフィックフィルタでは、スタティックデータベースのエントリとダイナミック データベースの IP アドレスだけが使用されます。ダイナミック データベースのドメイン名は使用されません。

[ボットネットトラフィック分類ACLに関する注意事項（ What You Need To Know About Botnet Traffic Classification ACLs）]

イネーブル化ルールおよび廃棄ルールを設定する場合、拡張 ACL ポリシー オブジェクトを指定して、ボットネット トラフィック フィルタリングが適用されるトラフィックを制限することもできます。ACLオブジェクトを指定しなかった場合、すべてのトラフィックに対してフィルタリングが実行されます。このことは、単一の permit IP any any ルールを持つ ACL を指定することと同等です。

フィルタリングが一部のトラフィックで実行されるように ACL を指定する場合は、次の点を考慮してください。

- 許可ルールは、ボットネット トラフィック フィルタリングが適用されるトラフィックを識別します。廃棄ルールの場合、許可エントリは ASA でドロップできるトラフィックを識別します。
- 拒否ルールは、フィルタリングが適用されないトラフィックを識別します。Botnet Traffic Filter は、拒否エントリと一致するトラフィックを無視します。
- 廃棄ルールに選択した ACL は、インターフェイスのイネーブル化ルールに使用されている ACL のサブネットである必要があります。ドロップされるトラフィックについては、ドロップルールの ACL 内に許可ルールがあるだけでなく、トラフィックがイネーブル化ルールの ACL 内にある許可ルールに分類されている必要もあります。これは、イネーブル化ルールで許可されているトラフィックが先にブロック対象として識別されるまで、ドロップルールは考慮されないためです。

インターネットに直接接続されているインターフェイスのすべてのトラフィックに対してボットネット トラフィック フィルタをイネーブルにし、Moderate 以上の重大度のトラフィックのドロップをイネーブルにすることをお勧めします。

関連項目

- [Traffic Classification] タブ （14 ページ）
- BTF イネーブル化ルール エディタ （16 ページ）
- BTF 廃棄ルール エディタ （17 ページ）
- Botnet Traffic Filter について （1 ページ）
- ボットネット トラフィック フィルタの設定のタスク フロー （3 ページ）

- ダイナミック データベースの設定 （5 ページ）
- スタティック データベースへのエントリの追加 （6 ページ）
- DNS スヌーピングのイネーブル化 （7 ページ）
- [Botnet Traffic Filter Rules] ページ （12 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから [ファイアウォール（Firewall）]>[ボットネットトラフィックフィルタルール（Botnet Traffic Filter Rules）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [ファイアウォール（Firewall）]>[ボットネットトラフィックフィルタルール（Botnet Traffic Filter Rules）] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

（注） マルチ コンテキスト モードのデバイスの場合、セキュリティ コンテキストでトラフィック分類を設定します。

[Botnet Traffic Filter Rules] ページ （12 ページ）が開きます。

ステップ 2 指定したトラフィックで Botnet Traffic Filter をイネーブルにするには、次の手順を実行します。

a) [トラフィック分類（Traffic Classification）] タブで、[イネーブル化ルール（Enable Rules）] テーブルの下にある [行の追加（Add Row）] をクリックします。

BTF イネーブル化ルール エディタ （16 ページ）が開きます。

b) [Interfaces] フィールドで、Botnet Traffic Filter をイネーブルにするインターフェイスを指定します。通常は、インターネットに接しているインターフェイスだけをイネーブルにします。インターフェイス セレクタを使用してインターフェイスまたはインターフェイス ロール オブジェクトを選択するには、[選択（Select）] をクリックします（インターフェイス ロール オブジェクトについてを参照）。

All インターフェイス ロール オブジェクトを選択することで（デフォルトで選択されています）、すべてのインターフェイスに適用されるグローバルな分類を設定できます。インターフェイス固有の分類を設定する場合は、そのインターフェイス設定によってグローバル設定が上書きされます。

c) 次のいずれかを実行して、モニタするトラフィックを特定します。

- すべてのトラフィックをモニタするには、ACL フィールドを空白のままにしておきます。
- モニターするトラフィックを指定するには、ACL フィールドの右側にある [選択（Select）] をクリックして、モニターするトラフィックを識別するアクセス制御リストオブジェクトを選択します。たとえば、外部インターフェイス上のポート 80 トラフィックをすべてモニタします。アクセス コントロール リスト オブジェクトの詳細については、アクセス コントロール リスト オブジェクトの作成を参照してください。

（注） イネーブル化ルールはインターフェイスごとに 1 つだけ指定できます。

d) [OK] をクリック

BTF イネーブル化ルール エディタが閉じ、ルールが [Enable Rules] テーブルに追加されます。

ステップ 3 マルウェア トラフィックを自動的にドロップするには、次の手順を実行します。

（注） 自動的にドロップするトラフィックの廃棄ルールを作成する前に、そのトラフィックの Botnet Traffic Filter をイネーブルにする必要があります。

a) [トラフィック分類（Traffic Classification）] タブで、[ドロップルール（Drop Rules）] テーブルの下にある [行の追加（Add Row）] をクリックします。

BTF 廃棄ルール エディタ （17 ページ）が開きます。

b) [Interfaces] フィールドで、トラフィックをドロップするインターフェイスを指定します。そのインターフェイス用のイネーブル化ルールが存在している必要があります。インターフェイスセレクタを使用してインターフェイスまたはインターフェイス ロール オブジェクトを選択するには、[選択（Select）] をクリックします（インターフェイス ロール オブジェクトについてを参照）。

All インターフェイス ロール オブジェクトを選択することで（デフォルトで選択されています）、すべてのインターフェイスに適用されるグローバルな分類を設定できます。インターフェイス固有の分類を設定する場合は、そのインターフェイス設定によってグローバル設定が上書きされます。

c) 次のいずれかを実行して、ドロップするトラフィックを特定します。

- すべてのトラフィックをモニタするには、ACL フィールドを空白のままにしておきます。
- モニターするトラフィックを指定するには、ACL フィールドの右側にある [選択（Select）] をクリックして、モニターするトラフィックを識別するアクセス制御リストオブジェクトを選択します。たとえば、外部インターフェイス上のポート 80 トラフィックをすべてモニタします。アクセス コントロール リスト オブジェクトの詳細については、アクセス コントロール リスト オブジェクトの作成を参照してください。

d) [Threat Level] 領域で、次のいずれかのオプションを選択して、特定の脅威レベルを持つトラフィックをドロップします。デフォルト レベルは、Moderate から Very High までの範囲となります。

（注） デフォルト設定を変更する確固たる理由がない限り、デフォルト設定を使用することを強くお勧めします。

- [Value]：ドロップする脅威レベルを指定します。
- [Range]：脅威レベルの範囲を指定します。

（注） 静的ブロックリストエントリは、常に Very High 脅威レベルに指定されます。

e) [OK] をクリック

BTF 廃棄ルール エディタが閉じ、ルールが [Drop Rules] テーブルに追加されます。

ステップ 4 さらにルールを追加するには、必要に応じて、手順 2 および 3 を繰り返します。ルールの追加が完了したら、[保存（Save）] をクリックして変更を保存します。

ステップ 5 アクション目的でグレーリストのトラフィックをブラックリストのトラフィックとして処理するには、[ダイナミックブラックリスト設定（Dynamic Blacklist Configuration）] タブで [不明なトラフィックをブラック

リストのトラフィックとして処理（Treat Ambiguous traffic as Blacklist）] チェックボックスをオンにします。

このオプションをイネーブルにしないと、グレーリストのトラフィックに廃棄ルールを設定している場合にも、そのトラフィックはドロップされません。

[Botnet Traffic Filter Rules] ページ

[Botnet Traffic Filter Rules] ページを使用すると、ASA セキュリティ デバイスを通過する悪意のあるトラフィックを識別するためのルールを定義できます。

[Botnet Traffic Filter Rules] ページは、次の 3 つのセクションに分かれています。

- [動的ブラックリスト設定（Dynamic Blacklist Configuration）] タブ （13 ページ）
- [Traffic Classification] タブ （14 ページ）
- [許可リスト/ブロックリスト（Permitlist/Blocklist）] タブ （19 ページ）

ナビゲーション パス

[Botnet Traffic Filter Rules] ページにアクセスするには、次のいずれかを実行します。

- （デバイスビュー）デバイスを選択してから、ポリシーセレクタで **[ファイアウォール（Firewall）] > [ボットネットトラフィックフィルタルール（Botnet Traffic Filter Rules）]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[ファイアウォール（Firewall）] > [ボットネットトラフィックフィルタルール（Botnet Traffic Filter Rules）]** を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。
- （マップビュー）デバイスを右クリックし、[ファイアウォールポリシーの編集（Edit Firewall Policies）]>[ボットネットトラフィックフィルタルール（Botnet Traffic Filter Rules）] を選択します。

関連項目

- Botnet Traffic Filter について （1 ページ）
- ボットネット トラフィック フィルタの設定のタスク フロー （3 ページ）
- [動的ブラックリスト設定（Dynamic Blacklist Configuration）] タブ （13 ページ）
- [Traffic Classification] タブ （14 ページ）
- BTF イネーブル化ルール エディタ （16 ページ）
- BTF 廃棄ルール エディタ （17 ページ）
- [許可リスト/ブロックリスト（Permitlist/Blocklist）] タブ （19 ページ）

- [デバイス許可リスト（Device Permitlist）] または [デバイスブロックリスト（Device Blocklist）] ダイアログボックス （20 ページ）
- [Configure DNS] ダイアログボックス

[動的ブラックリスト設定（Dynamic Blacklist Configuration）] タブ

[動的ブラックリスト設定（Dynamic Blacklist Configuration）] タブを使用すると、シスコの更新サーバーからデータベースを更新できるようになり、セキュリティアプライアンスでダウンロード済み動的データベースを使用できるようになります。

ナビゲーション パス

[Botnet Traffic Filter Rules] ページ （12 ページ）から [動的ブラックリスト設定（Dynamic Blacklist Configuration）] タブをクリックします。

関連項目

- ダイナミック データベースの設定 （5 ページ）
- Botnet Traffic Filter について （1 ページ）
- ボットネット トラフィック フィルタの設定のタスク フロー （3 ページ）
- [Botnet Traffic Filter Rules] ページ （12 ページ）
- [Traffic Classification] タブ （14 ページ）
- BTF イネーブル化ルール エディタ （16 ページ）
- BTF 廃棄ルール エディタ （17 ページ）
- [許可リスト/ブロックリスト（Permitlist/Blocklist）] タブ （19 ページ）
- [デバイス許可リスト（Device Permitlist）] または [デバイスブロックリスト（Device Blocklist）] ダイアログボックス （20 ページ）
- [Configure DNS] ダイアログボックス

フィールド リファレンス

表 *1 : [*動的ブラックリスト設定（*Dynamic Blacklist Configuration*）*]* タブ

要素	説明
サーバーからのダイナミックブロックリストの有効化（Enable Dynamic Blacklist From Server）	Cisco アップデート サーバからのダイナミック データベースのダウンロードをイネーブルにします。データベースをセキュリティ アプライアンスにまだインストールしていない場合は、約 2 分後にデータベースがダウンロードされます。セキュリティ アプライアンスが今後の更新を検出するためにサーバをポーリングする頻度（通常は 1 時間おき）が、更新サーバによって決定されます。 （注） デバイスがマルチ コンテキスト モードの場合は、そのデバイスのシステム コンテキストでこのオプションを設定します。
ダイナミックブロックリストを使用（Use Dynamic Blocklist）	Botnet Traffic Filter に対して動的データベースの使用をイネーブルにします。 （注） マルチ コンテキスト モードでは、コンテキストごとにデータベースの使用を設定します。
不明なトラフィックをブラックリストのトラフィックとして処理（Treat Ambiguous traffic as Blacklist）	選択すると、グレーリストのトラフィックは、アクション目的でブロックリストのトラフィックとして処理されます。 このオプションをイネーブルにしないと、グレーリストのトラフィックに廃棄ルールを設定している場合にも、そのトラフィックはドロップされません。

[Traffic Classification] タブ

[Traffic Classification] タブを使用して、デバイスまたは共有ポリシーのトラフィック分類定義を表示または設定し、自動的にドロップされる悪意のあるトラフィックを指定します。トラフィック分類定義（イネーブル化ルール）はACLを伴うインターフェイスまたはインターフェイス ロールで構成され、この ACL によって Botnet Traffic Filter でモニタするトラフィックが識別されます。特定のインターフェイスまたはインターフェイス ロールの設定値を設定できます。All インターフェイス ロール オブジェクトを使用して、ボットネット フィルタリングをグローバルにイネーブルにできます（デフォルトで選択されています）。インターフェイス固有の分類を設定した場合は、そのインターフェイス設定によって、インターフェイス ロールに定義されているすべての設定が上書きされます。

特定のインターフェイスに関して、ボットネット トラフィック フィルタリングが適用されるトラフィックを識別するイネーブル化ルールを 1 つだけ指定できます。ただし、Botnet Traffic Filter によってドロップされるトラフィックを識別する場合は、複数の廃棄ルールを指定できます。

（注） Botnet Traffic Filter を適切に機能させるために、動的フィルタのスヌーピングを設定することを強く推奨します。デバイス ビューでは、Cisco Security Manager によって [Traffic Classification] タブの下部にリンクが表示され、このリンクを使用すると、直接 [Inspection Rules] ページに移動して動的フィルタのスヌーピングをイネーブルにできます。詳細については、DNS スヌーピングのイネーブル化 （7 ページ）を参照してください。

テーブル内のカラムはエントリ設定の概要を示しており、これについてはBTF イネーブル化ルール エディタ （16 ページ）および BTF 廃棄ルール エディタ （17 ページ）で説明します。

トラフィック分類およびアクションを設定するには、次の手順を実行します。

- [行の追加（Add Row）] ボタンをクリックして、インターフェイスまたはインターフェイスロールをテーブルに追加し、BTF イネーブル化ルール エディタ （16 ページ）または BTF 廃棄ルール エディタ （17 ページ）に入力します。
- エントリを選択し、[行の編集（Edit Row）] ボタンをクリックして、既存のエントリを編集します。
- エントリを選択し、[行の削除（Delete Row）] ボタンをクリックして削除します。

ナビゲーション パス

[Botnet Traffic Filter Rules] ページ （12 ページ）で、[トラフィック分類（Traffic Classification）] タブをクリックします。

関連項目

- BTF イネーブル化ルール エディタ （16 ページ）
- BTF 廃棄ルール エディタ （17 ページ）
- ボットネット トラフィック フィルタのトラフィック分類とアクションのイネーブル化 （8 ページ）
- Botnet Traffic Filter について （1 ページ）
- ボットネット トラフィック フィルタの設定のタスク フロー （3 ページ）
- [Botnet Traffic Filter Rules] ページ （12 ページ）
- [動的ブラックリスト設定（Dynamic Blacklist Configuration）] タブ （13 ページ）
- [許可リスト/ブロックリスト（Permitlist/Blocklist）] タブ （19 ページ）
- [デバイス許可リスト（Device Permitlist）] または [デバイスブロックリスト（Device Blocklist）] ダイアログボックス （20 ページ）
- [Configure DNS] ダイアログボックス

BTF イネーブル化ルール エディタ

BTF イネーブル化ルール エディタを使用して、Botnet Traffic Filter をイネーブルにするインターフェイスを指定し、モニタするトラフィックを特定します。イネーブル化ルールはインターフェイスごとに 1 つだけ指定できます。

ナビゲーション パス

BTF イネーブル化ルールエディタにアクセスするには、[トラフィック分類（Traffic Classification）] タブの [イネーブル化ルール（Enable Rules）] テーブルで、作業領域内を右クリックしてから [行の追加（Add Row）] を選択するか、または既存エントリを右クリックして [行の編集（Edit Row）] を選択します。

関連項目

- ボットネット トラフィック フィルタのトラフィック分類とアクションのイネーブル化（8 ページ）
- Botnet Traffic Filter について （1 ページ）
- ボットネット トラフィック フィルタの設定のタスク フロー （3 ページ）
- [Botnet Traffic Filter Rules] ページ （12 ページ）
- [動的ブラックリスト設定（Dynamic Blacklist Configuration）] タブ （13 ページ）
- [Traffic Classification] タブ （14 ページ）
- BTF 廃棄ルール エディタ （17 ページ）
- [許可リスト/ブロックリスト（Permitlist/Blocklist）] タブ （19 ページ）
- [デバイス許可リスト（Device Permitlist）] または [デバイスブロックリスト（Device Blocklist）] ダイアログボックス （20 ページ）
- [Configure DNS] ダイアログボックス

フィールド リファレンス

表 *2 : BTF* イネーブル化ルール エディタ

要素	説明
インターフェイス	Botnet Traffic Filter をイネーブルにするインターフェイスまたはインターフェイス ロール。インターフェイスまたはインターフェイスロールの名前を入力するか、[選択（Select）] をクリックしてリストからインターフェイスまたはインターフェイスロールを選択するか、あるいは新しいロールを作成します。インターフェイスをリストに表示するには、あらかじめ定義しておく必要があります。 All インターフェイス ロール オブジェクトを使用して、ボットネット フィルタリングをグローバルにイネーブルにできます（デフォルトで選択されています）。インターフェイス固有の分類を設定する場合は、そのインターフェイス設定によって、グローバル設定が上書きされます。 インターフェイス ロール オブジェクトは、各デバイスの設定が生成されるときに、実際のインターフェイス名で置き換えられます。インターフェイス ロール オブジェクトについてを参照してください。
ACL	モニタするトラフィックの識別に使用するアクセス リストを指定します。アクセス リストを指定しないと、デフォルトですべてのトラフィックがモニタされます。 モニターするトラフィックを指定するには、ACL フィールドの右側にある [選択（Select）] をクリックして、モニターするトラフィックを識別するアクセス制御リストオブジェクトを選択します。たとえば、外部インターフェイス上のポート 80 トラフィックをすべてモニタします。アクセス コントロール リスト オブジェクトの詳細については、アクセス コントロール リスト オブジェクトの作成を参照してください。

BTF 廃棄ルール エディタ

BTF 廃棄ルール エディタを使用して、自動的にドロップされるマルウェア トラフィックを識別します。インターフェイスごとに複数の廃棄ルールを指定できます。

ナビゲーション パス

BTF ドロップルールエディタにアクセスするには、[トラフィック分類（Traffic Classification）] タブの [ドロップルール（Drop Rules）] テーブルで、作業領域内を右クリックしてから [行の追加（Add Row）] を選択するか、または既存エントリを右クリックして [行の編集（Edit Row）] を選択します。

関連項目

- ボットネット トラフィック フィルタのトラフィック分類とアクションのイネーブル化（8 ページ）

- Botnet Traffic Filter について （1 ページ）
- ボットネット トラフィック フィルタの設定のタスク フロー （3 ページ）
- [Botnet Traffic Filter Rules] ページ （12 ページ）
- [動的ブラックリスト設定（Dynamic Blacklist Configuration）] タブ （13 ページ）
- [Traffic Classification] タブ （14 ページ）
- BTF イネーブル化ルール エディタ （16 ページ）
- [許可リスト/ブロックリスト（Permitlist/Blocklist）] タブ （19 ページ）
- [デバイス許可リスト（Device Permitlist）] または [デバイスブロックリスト（Device Blocklist）] ダイアログボックス （20 ページ）
- [Configure DNS] ダイアログボックス

フィールド リファレンス

表 *3: BTF* 廃棄ルール エディタ

要素	説明
インターフェイス	Botnet Traffic Filter をイネーブルにするインターフェイスまたはインターフェイス ロール。インターフェイスまたはインターフェイスロールの名前を入力するか、[選択（Select）] をクリックしてリストからインターフェイスまたはインターフェイスロールを選択するか、あるいは新しいロールを作成します。インターフェイスをリストに表示するには、あらかじめ定義しておく必要があります。 All インターフェイス ロール オブジェクトを使用して、ボットネット フィルタリングをグローバルにイネーブルにできます（デフォルトで選択されています）。インターフェイス固有の分類を設定する場合は、そのインターフェイス設定によって、グローバル設定が上書きされます。 インターフェイス ロール オブジェクトは、各デバイスの設定が生成されるときに、実際のインターフェイス名で置き換えられます。インターフェイス ロール オブジェクトについてを参照してください。
ACL	モニタするトラフィックの識別に使用するアクセス リストを指定します。アクセス リストを指定しないと、デフォルトですべてのトラフィックがモニタされます。 モニターするトラフィックを指定するには、ACL フィールドの右側にある [選択（Select）] をクリックして、モニターするトラフィックを識別するアクセス制御リストオブジェクトを選択します。たとえば、外部インターフェイス上のポート 80 トラフィックをすべてモニタします。アクセス コントロール リスト オブジェクトの詳細については、アクセス コントロール リスト オブジェクトの作成を参照してください。

要素	説明
脅威レベル	[Threat Level] フィールドは、ドロップされる悪意のあるトラフィックの脅威レベルを特定します。デフォルト レベルは、Moderate から Very High までの範囲となります。 （注） デフォルト設定を変更する確固たる理由がない限り、デフォルト設定を使用することを強くお勧めします。 • [Value]：ドロップする脅威レベルを指定します。 • Very-low • 低い • 中程度 • 高 • Very-high • [Range]：脅威レベルの範囲を指定します。 （注） 静的ブロックリストエントリは、常に Very High 脅威レベルに指定されます。

[許可リスト/ブロックリスト（Permitlist/Blocklist）] タブ

[許可リスト/ブロックリスト（Permitlist/Blocklist）] タブを使用して、デバイスまたは共有ポリシー用の静的データベースのエントリを表示または設定します。[デバイスブロックリスト（Device Blocklist）] には、悪意のあるサイトまたは望ましくないサイトのドメイン名または IP アドレスが含まれます。静的ブロックリストを使用してシスコの動的データベースを補強できます。また、対象とするすべてのマルウェアサイトを特定できる場合は静的ブロックリストだけを使用できます。

[デバイス許可リスト（Device Permitlist）] には、許容可能と認められるサイトのドメイン名または IP アドレスが含まれます。ブロックする必要はないと考えられるアドレスがブロックアドレスとして動的データベースに含まれている場合は、これらのアドレスを手動で静的な許可リストに加えることができます。静的な許可リストのエントリは、静的なブロックリストおよびシスコの動的データベース内のエントリに優先します。許可リストのアドレスに関する syslog メッセージは依然として生成されます。ただし、ターゲットになるのはブロック syslog メッセージだけであるため、これは単なる情報提供に過ぎません。

静的データベースを設定するには、次の手順を実行します。

- [行の追加（Add Row）] ボタンをクリックし、[デバイス許可リスト（Device Permitlist）] または [デバイスブロックリスト（Device Blocklist）] ダイアログボックス （20 ページ）を使用して静的データベースのエントリを定義します。

- エントリを選択し、[行の編集（Edit Row）] ボタンをクリックして、既存のエントリを編集します。

ワンポイント アドバイス

エントリを選択して **F2** キーを押すか、または [デバイス許可リスト（Device Permitlist）] か [デバイスブロックリスト（Device Blocklist）] でエントリをダブルクリックして、その場でエントリを編集します。

- エントリを選択し、[行の削除（Delete Row）] ボタンをクリックして削除します。

ナビゲーション パス

[Botnet Traffic Filter Rules] ページ （12 ページ）から、[許可リスト/ブロックリスト（Permitlist/Blocklist）] タブをクリックします。

関連項目

- スタティック データベースへのエントリの追加 （6 ページ）
- Botnet Traffic Filter について （1 ページ）
- ボットネット トラフィック フィルタの設定のタスク フロー （3 ページ）
- [デバイス許可リスト（Device Permitlist）] または [デバイスブロックリスト（Device Blocklist）] ダイアログボックス （20 ページ）
- [Botnet Traffic Filter Rules] ページ （12 ページ）
- [動的ブラックリスト設定（Dynamic Blacklist Configuration）] タブ （13 ページ）
- [Traffic Classification] タブ （14 ページ）

[デバイス許可リスト（Device Permitlist）] または [デバイスブロックリスト（Device Blocklist）] ダイアログボックス

[デバイス許可リスト（Device Permitlist）] または [デバイスブロックリスト（Device Blocklist）] ダイアログボックスを使用して、許可リスト（安全）またはブロックリスト（悪意）に追加するドメイン名または IP アドレスを手動で定義します。静的ブロックリストを使用してシスコの動的データベースを補強できます。また、対象とするすべてのマルウェアサイトを特定できる場合は静的ブロックリストだけを使用できます。許可リストと動的ブロックリストの両方に表示される名前またはアドレスは、syslog メッセージとレポートでは許可リストアドレスとしてのみ識別されます。

ドメイン名は完全な形式（www.cisco.com など、ホスト名を含む）にしたり、部分的な形式（cisco.com など）にしたりできます。部分的な名前の場合、そのドメイン上のすべての Web サイトホストが、許可リストまたはブロックリストに追加されます。また、ホストの IP アドレスを入力することもできます。カンマまたは改行を使用して、複数のエントリを区切ります。

ナビゲーション パス

[許可リスト/ブロックリスト（Permitlist/Blocklist）] タブ （19 ページ）で、[デバイス許可リスト（Device Permitlist）] または [デバイスブロックリスト（Device Blocklist）] テーブルの下にある [行の追加（Add Rows）] ボタンをクリックするか、またはエントリを選択して [行の編集（Edit Row）] ボタンをクリックします。

関連項目

- スタティック データベースへのエントリの追加 （6 ページ）
- Botnet Traffic Filter について （1 ページ）
- ボットネット トラフィック フィルタの設定のタスク フロー （3 ページ）
- [Botnet Traffic Filter Rules] ページ （12 ページ）
- [動的ブラックリスト設定（Dynamic Blacklist Configuration）] タブ （13 ページ）
- [Traffic Classification] タブ （14 ページ）
- BTF イネーブル化ルール エディタ （16 ページ）
- BTF 廃棄ルール エディタ （17 ページ）
- [許可リスト/ブロックリスト（Permitlist/Blocklist）] タブ （19 ページ）
- [Configure DNS] ダイアログボックス

[デバイス許可リスト（Device Permitlist）] または [デバイスブロックリスト（Device Blocklist）] ダイアログボックス

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。