CHAPTER 25

ボットネット トラフィック フィルタの設定

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。ボットネット トラフィック フィルタは、着信と発信の接続を既知の不正なドメイン名と IP アドレス（*ブラックリスト*）のダイナミック データベースと照合して確認し、疑わしいアクティビティをログに記録したり、疑わしいアクティビティをブロックします。

また、ブラックリスト アドレスを選択してスタティック ブラックリストに追加することで、Cisco ダイナミック データベースを補完できます。ブラ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 Cisco 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 *ホワイトリスト*に手動で入力できます。ホワイトリストにアドレスを入力した場合でも、それら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ラックリスト 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。

（注） 内部要件のために Cisco 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 ブラ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）。

この章では、ボットネット トラフィック フィルタを設定する方法について説明します。この章は、次の項で構成されています。

ボットネット トラフィック フィルタに関する情報

この項では、ボットネット トラフィック フィルタについて説明します。説明する項目は次のとおりです。

ボットネット トラフィック フィルタのアドレス タイプ

ボットネット トラフィック フィルタのモニタ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ラックリストによって識別されるブラ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、ホワイトリストに含まれています。ホワイトリストは、アドレスがダイナミック データベースのブラックリストに記載されており、かつスタティック ホワイトリストで識別される場合に便利です。
- あいまいなアドレス：ブラ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*に記載されます。
- 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。

既知のアドレスに対するボットネット トラフィック フィルタのアクション

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、ブラックリスト、ホワイトリスト、およびグレー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。詳細については、「ボットネット トラフィック フィルタの Syslog メッセージ」（P.25-16）を参照してください。

ボットネット トラフィック フィルタ 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。この項は、次の内容で構成されています。

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。

ASA がダイナミック データベースを使用する方法

ASA は、このダイナミック データベースを次のように使用します。

1. DNS 応答のドメイン名とダイナミック データベースのドメイン名が一致した場合、ボットネット トラフィック フィルタは、このドメイン名と 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した場合、ASA は、疑わしいアクティビティを通知する syslog メッセージを送信します。トラフィックをドロップするように ASA を設定した場合は、必要に応じてトラフィックをドロップします。
3. 場合によっては、IP アドレス自体がダイナミック データベースで提供され、ボットネット トラフィック フィルタが 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たり、ドロップしたりすることがあります。

データベース ファイル

データベース ファイルは、Cisco アップデート サーバからダウンロードされ、実行中のメモリに保存されます。フラッシュ メモリには保存されません。Cisco アップデート サーバ URL にアクセスできるように、ASA で DNS サーバが指定されている必要があります。マルチ コンテキスト モードでは、システムは管理コンテキスト インターフェイスを使用して、すべてのコンテキストのデータベースをダウンロードします。DNS サーバが管理コンテキストで指定されている必要があります。

データベースを削除する必要がある場合は、[Configuration] > [Firewall] > [Botnet Traffic Filter] > [Botnet Database] ペインの [Purge Botnet Database] ボタンを使用してください。この場合、必ず [Configuration] > [Firewall] > [Botnet Traffic Filter] > [Botnet Database] > [Dynamic Database Configuration] 領域の [Use Botnet data dynamically downloaded from updater server] チェックボックスをオフにして、最初にデータベースの使用をディセーブルにしてください。

（注） ダイナミック データベースでドメイン名をフィルタするには、ボットネット トラフィック フィルタ スヌーピングを使用して 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。ASA は、ドメイン名とそれに関連付けられている IP アドレスを DNS パケット内から検出します。

データベース トラフィック タイプ

ダイナミック データベースには、次のタイプのアドレスが含まれます。

- 広告：バナー広告、インタースティシャル広告、リッチ メディア広告、Web サイトのポップアップとポップアンダー、スパイウェアおよびアドウェアを配信するアドバタイジング ネットワーク。これらのネットワークには、広告重視の HTML メールおよび電子メール確認サービスを送信するものがあります。
- データ トラッキング：Web サイトやその他のオンライン要素にトラッキング サービスやメトリック サービスを提供する企業および Web サイトに関連付けられたソース。これらの一部は、小規模なアドバタイズのネットワークを運営します。
- スパイウェア：スパイウェア、アドウェア、グレーウェア、およびその他の潜在的に好ましくないアドバタイジング ソフトウェアを配信するソース。それらの一部は、これらのソフトウェアをインストールするエクスプロイトを実行します。
- マルウェア：さまざまなエクスプロイトを使用して、攻撃対象のコンピュータにアドウェア、スパイウェア、および他のマルウェアを配信するするソース。これらの一部は、プレミアム レート電話番号に偽装発信を行うダイアラーの不正なオンライン ベンダーおよびディストリビュータに関連付けられます。

- 成人向け：成人向けコンテンツ、広告、コンテンツ集約、登録と課金、および年齢認証の Web ホスティングを提供する成人向けのネットワークまたはサービスに関連するソース。これらはアドウェア、スパイウェアおよびダイアラー配信に結び付けられていることがあります。
- ボット ネットワークと脅威ネットワーク：感染したコンピュータを制御する不正なシステム。これらは、脅威ネットワーク上にホストされているシステムかボットネット自体の一部であるシステムのいずれかです。

スタティック 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）をブラックリストに手動で入力できます。スタティック ブラックリスト エントリは、常に Very High 脅威レベルに指定されます。また、ホワイトリストに名前または IP アドレスを入力して、*ダイナミック* ブラックリストとホワイトリストの両方に表示される名前または IP アドレスが、syslog メッセージおよびレポートでホワイトリスト アドレスとしてだけ識別されるようにすることもできます。アドレスがダイナミック ブラックリストに記載されていない場合でも、ホワイトリストに記載されたアドレスの syslog メッセージは表示されます。

スタティック データベースにドメイン名を追加した場合、ASA は、1 分間待機してからそのドメイン名の DNS 要求を送信し、ドメイン名と IP アドレスの組を *DNS ホスト キャッシュ*に追加します（このアクションはバックグラウンド プロセスで、ASA の設定の続行に影響しません）。DNS パケット 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することをお勧めします。次の場合、ASA は、通常の DNS lookup ではなく、ボットネット トラフィック フィルタ スヌーピングを使用してスタティック ブラックリストのドメイン名を解決します。

- ASA DNS サーバが使用できない。
- ASA が通常の DNS 要求を送信する前の 1 分間の待機期間中に接続が開始された。

DNS スヌーピングを使用すると、感染ホストがスタティック データベースに記載されている名前に対する DNS 要求を送信したときに、ASA がドメイン名と関連付けられている IP アドレスを DNS パケット内から検出し、その名前と 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。

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せず、上記の状況のいずれかが発生した場合、このトラフィックは、ボットネット トラフィック フィルタでモニタされません。

DNS 逆ルックアップ キャッシュと DNS ホスト キャッシュに関する情報

DNS スヌーピングがイネーブルになっているダイナミック データベースを使用する場合、エントリは DNS 逆ルックアップ キャッシュに追加されます。スタティック データベースを使用する場合、エントリは DNS ホスト キャッシュに追加されます（DNS スヌーピングがイネーブルになっているスタティック データベースと DNS 逆ルックアップ キャッシュの使用方法については、「スタティック データベースに関する情報」（P.25-4）を参照してください）。

DNS 逆ルックアップ キャッシュと DNS ホスト キャッシュのエントリには、DNS サーバによって提供される time to live（TTL; 存続可能時間）値があります。許容される最大 TTL 値は 1 日（24 時間）です。DNS サーバによって提供された TTL がこれより大きい場合は、TTL が 1 日以下に切り詰められます。

DNS 逆ルックアップ キャッシュの場合、エントリがタイムアウトすると、感染したホストが既知のアドレスへの接続を開始して DNS スヌーピングが発生したときに、ASA がエントリを更新します。

DNS ホスト キャッシュの場合、エントリがタイムアウトすると、ASA がエントリの更新を定期的に要求します。

DNS ホスト キャッシュの場合、ブラックリスト エントリとホワイトリスト エントリの最大数はそれぞれ 1000 です。

表 25-1 に、モデル別の DNS 逆ルックアップ キャッシュの最大エントリ数を示します。

表 25-1　モデル別の DNS 逆ルックアップ キャッシュ エントリ

ASA モデル	最大エントリ
ASA 5505	5000
ASA 5510	10,000
ASA 5520	20,000
ASA 5540	40,000
ASA 5550	40,000
ASA 5580	100,000

ボットネット トラフィック フィルタの動作

図 25-1 に、DNS 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 スヌーピングがイネーブルになっているダイナミック データベースを使用した場合のボットネット トラフィック フィルタの動作を示します。

図 25-1　ダイナミック データベースを使用した場合のボットネット トラフィック フィルタの動作

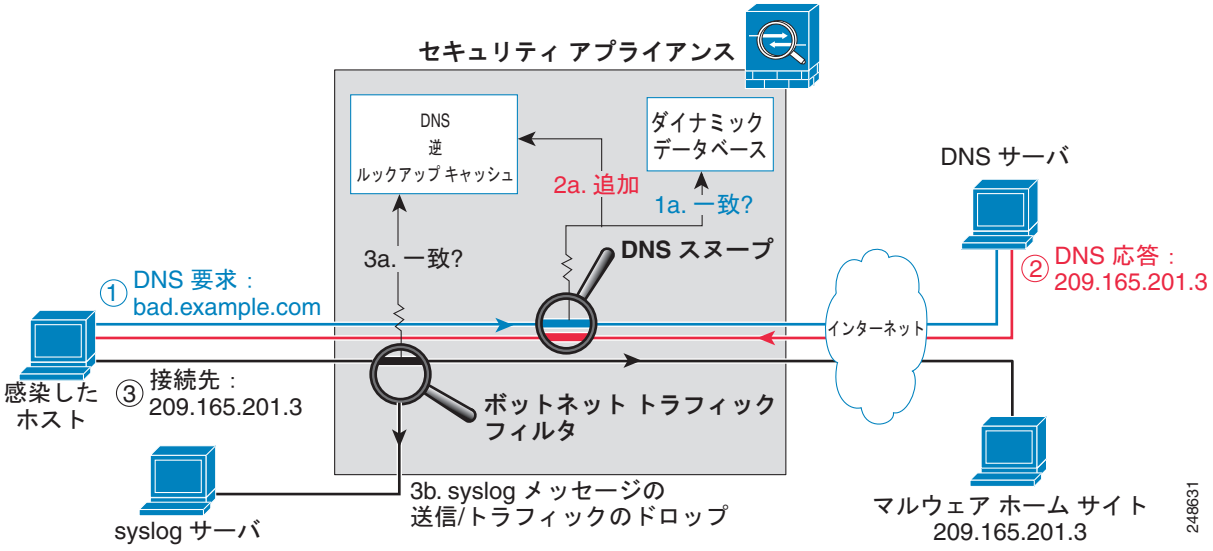
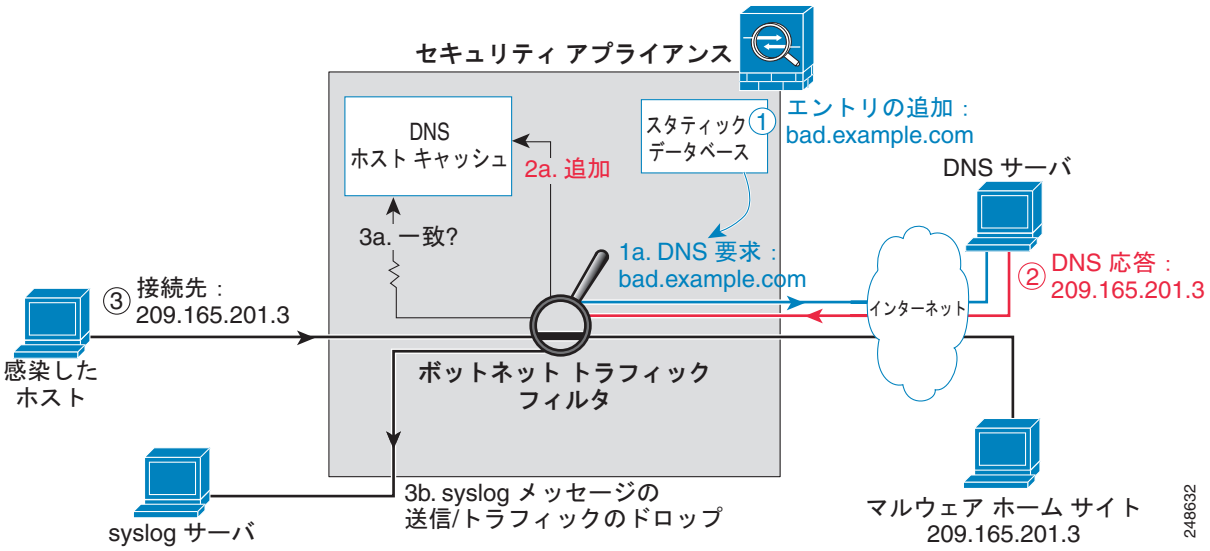


図 25-2 に、スタティック データベースを使用した場合のボットネット トラフィック フィルタの動作を示します。

図 25-2　スタティック データベースを使用した場合のボットネット トラフィック フィルタの動作



ボットネット トラフィック フィルタのライセンス要件

次の表に、この機能のライセンス要件を示します。

モデル	ライセンス要件
すべてのモデル	次のライセンスが必要です。 • ボットネット トラフィック フィルタ ライセンス。 • ダイナミック データベースをダウンロードする高度暗号化（3DES/AES）ライセンス。

ボットネット トラフィック フィルタの前提条件

ダイナミック データベースを使用するには、Cisco アップデート サーバ URL にアクセスできるように、ASA で DNS サーバが指定されている必要があります。マルチ コンテキスト モードでは、システムは管理コンテキスト インターフェイスを使用して、すべてのコンテキストのデータベースをダウンロードします。DNS サーバが管理コンテキストで指定されていることを確認してください。

ガイドラインと制限事項

この項では、この機能のガイドラインと制限事項について説明します。

コンテキスト モードのガイドライン

シングル コンテキスト モードとマルチ コンテキスト モードでサポートされています。

ファイアウォール モードのガイドライン

ルーテッド ファイアウォール モードとトランスペアレント ファイアウォール モードでサポートされています。

フェールオーバーのガイドライン

ステートフル フェールオーバーでは、DNS 逆ルックアップ キャッシュ、DNS ホスト キャッシュ、またはダイナミック データベースの複製はサポートされません。

IPv6 のガイドライン

IPv6 はサポートされません。

その他のガイドラインと制限事項

- TCP DNS トラフィックはサポートされません。
- スタティック データベースには、最大 1000 個のブラックリスト エントリと 1000 個のホワイトリスト エントリを追加できます。
- パケット トレーサはサポートされません。

デフォルト設定

デフォルトでは、ボットネット トラフィック フィルタとダイナミック データベースの使用はディセーブルになっています。

デフォルトでは、DNS インスペクションはイネーブルになっていますが、ボットネット トラフィック フィルタ スヌーピングはディセーブルになっています。

ボットネット トラフィック フィルタの設定

この項は、次の内容で構成されています。

- 「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」（P.25-8）
- 「ダイナミック データベースの設定」（P.25-9）

- 「DNS スヌーピングのイネーブル化」（P.25-11）
- 「スタティック データベースへのエントリの追加」（P.25-10）
- 「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」（P.25-12）
- 「ボット ネット トラフィックの手動ブロック」（P.25-14）
- 「ダイナミック データベースの検索」（P.25-15）

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

ボットネット トラフィック フィルタを設定するには、次の手順を実行します。

ステップ 1　ダイナミック データベースの使用をイネーブルにする。「ダイナミック データベースの設定」（P.25-9）を参照してください。

この手順では、Cisco アップデート サーバからのデータベース アップデートと、ASA によるダウンロードされたダイナミック データベースの使用をイネーブルにします。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。

ステップ 2　（任意）スタティック エントリをデータベースに追加する。「スタティック データベースへのエントリの追加」（P.25-10）を参照してください。

この手順では、ブラックリストまたはホワイトリストに記載するドメイン名または IP アドレスでダイナミック 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。

ステップ 3　DNS スヌーピングをイネーブルにする。「DNS スヌーピングのイネーブル化」（P.25-11）を参照してください。

この手順では、DNS パケットのインスペクションをイネーブルにします。DNS パケットのインスペクションでは、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（ASA 用の DNS サーバが使用できない場合）、ドメイン名と 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。このキャッシュは、疑わしいアドレスへの接続が行われたときにボットネット トラフィック フィルタで使用されます。

ステップ 4　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。「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」（P.25-12）を参照してください。

この手順では、ボットネット トラフィック フィルタをイネーブルにします。ボットネット トラフィック フィルタでは、初期接続の各パケット内の送信元 IP アドレスと宛先 IP アドレスが、ダイナミック データベース、スタティック 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 キャッシュ内の IP アドレスと比較され、一致するトラフィックが見つかった場合は syslog メッセージが送信されるか、すべての一致したトラフィックがドロップされます。

ステップ 5　（任意）syslog メッセージ情報に基づいて、手動でトラフィックをブロックします。「ボット ネット トラフィックの手動ブロック」（P.25-14）を参照してください。

マルウェア トラフィックを自動的にブロックしない場合、トラフィックを拒否するアクセス ルールを設定するか、コマンドライン インターフェイス ツールで **shun** コマンドを使用してホストへのトラフィックとホストからのトラフィックをすべてブロックすることによって、トラフィックを手動でブロックできます。

ダイナミック データベースの設定

この手順では、データベース アップデートと、ASA によるダウンロードされたダイナミック データベースの使用をイネーブルにします。マルチ コンテキスト モードでは、システムは管理コンテキスト インターフェイスを使用して、すべてのコンテキストのデータベースをダウンロードします。コンテキストごとに、データベースを*使用*するように設定できます。

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。

前提条件

[Device Management] > [DNS] > [DNS Client] > [DNS Lookup] 領域で、DNS サーバの ASA の使用をイネーブルにします。マルチ コンテキスト モードでは、システムは管理コンテキスト インターフェイスを使用して、すべてのコンテキストのデータベースをダウンロードします。DNS サーバが管理コンテキストで指定されていることを確認してください。

手順の詳細

ステップ 1　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。

- シングル モードでは、[Configuration] > [Firewall] > [Botnet Traffic Filter] > [Botnet Database] ペインを選択し、[Enable Botnet Updater Client] チェックボックスをオンにします。
- マルチ コンテキスト モードでは、[System execution] スペースで、[Configuration] > [Device Management] > [Botnet Database] ペインを選択し、[Enable Botnet Updater Client] チェックボックスをオンにします。

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。マルチ コンテキスト モードでは、システム実行スペースでこのコマンドを入力します。ASA にデータベースを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適応型セキュリティ アプライアンスにダウンロードされます。アップデート サーバは、将来のアップデートのために ASA がサーバにポーリングする頻度を決定します（通常は 1 時間ごと）。

ステップ 2　（マルチ コンテキスト モードの場合だけ）マルチ コンテキスト モードでは、[Apply] をクリックします。[Device List] でコンテキスト名をダブルクリックして、Botnet Traffic Filter を設定しようとするコンテキストに変更します。

ステップ 3　[Configuration] > [Firewall] > [Botnet Traffic Filter] > [Botnet Database] > [Dynamic Database Configuration] 領域で、[Use Botnet data dynamically downloaded from updater server] チェックボックスをオンにします。

ステップ 4　[Apply] をクリックします。

ステップ 5　（任意）後でデータベースを実行メモリから削除するには、次の手順を実行します。

a.　[Use Botnet data dynamically downloaded from updater server] チェックボックスをオフにしてデータベースの使用をディセーブルにします。

b.　[Apply] をクリックします。

c.　[Purge Botnet Database] をクリックします。

d.　データベースを再度ダウンロードするには、[Use Botnet data dynamically downloaded from updater server] チェックボックスを再度オンにします。

e.　[Apply] をクリックします。

（注）　[Fetch Botnet Database] ボタンは、あくまでもテスト目的のボタンです。このボタンをクリックすると、ダイナミック データベースをダウンロードして検証しますが、実行メモリに保存しません。

[Search Dynamic Database] 領域の詳細については、「ダイナミック データベースの検索」（P.25-15）を参照してください。

次の作業

「スタティック データベースへのエントリの追加」（P.25-10）を参照してください。

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、ブラックリストまたはホワイトリストに記載するドメイン名または IP アドレスでダイナミック データベースを補完できます。スタティック ブラックリスト エントリは、常に Very High 脅威レベルに指定されます。詳細については、「スタティック データベースに関する情報」（P.25-4）を参照してください。

前提条件

- マルチ コンテキスト モードでは、コンテキスト実行スペースでこの手順を実行します。
- [Device Management] > [DNS] > [DNS Client] > [DNS Lookup] 領域で、DNS サーバの ASA の使用をイネーブルにします。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。

手順の詳細

ステップ 1　[Configuration] > [Firewall] > [Botnet Traffic Filter] > [Black List] または [White List] ペインを選択し、[Whitelist] または [Blacklist] の [Add] をクリックします。

[Enter hostname or IP Address] ダイアログボックスが表示されます。

ステップ 2　[Addresses] 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。

コンマ、スペース、行、またはセミコロンで区切られたエントリを複数入力してください。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 3　[OK] をクリックします。

ステップ 4　[Apply] をクリックします。

次の作業

「DNS スヌーピングのイネーブル化」（P.25-11）を参照してください。

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。このキャッシュは、疑わしいアドレスへの接続が行われたときにボットネット トラフィック フィルタで使用されます。

前提条件

- マルチ コンテキスト モードでは、コンテキスト実行スペースでこの手順を実行します。
- 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。モジュラ ポリシー フレームワークを使用した高度な DNS インスペクション オプションの設定の詳細については、「DNS インスペクション」（P.10-1）および第 1 章「サービス ポリシーの設定」を参照してください。

（注） DNS スヌーピングは、[Configuration] > [Firewall] > [Service Policy Rules] > [Rule Actions] > [Protocol Inspection] > [Select DNS Inspect Map] ダイアログボックスでも直接設定できます。この設定を行うには、[Enable Botnet traffic filter DNS snooping] チェックボックスをオンにします。

制限事項

TCP DNS トラフィックはサポートされません。

DNS インスペクションのデフォルト設定と推奨設定

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のすべての UDP DNS トラフィックが検査され、DNS スヌーピングがディセーブルになっています。

DNS スヌーピングは、外部 DNS 要求が送信されるインターフェイスでだけイネーブルにすることを推奨します。すべての UDP DNS トラフィック（内部 DNS サーバへの送信トラフィックを含む）に対して DNS スヌーピングをイネーブルにすると、ASA で不要な負荷が発生します。

たとえば、DNS サーバが外部インターフェイスに存在する場合は、外部インターフェイスのすべての UDP DNS トラフィックに対して DNS インスペクションとスヌーピングをイネーブルにする必要があります。

手順の詳細

ステップ 1　[Configuration] > [Firewall] > [Botnet Traffic Filter] > [DNS Snooping] ペインを選択します。

DNS インスペクションを含むすべての既存のサービス ルールが表に表示されます。

ステップ 2　[DNS Snooping Enabled] カラムで、DNS スヌーピングをイネーブルにするルールごとに、チェックボックスをオンにします。

ステップ 3　[Apply] をクリックします。

次の作業

「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」（P.25-12）を参照してください。

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

この手順では、ボットネット トラフィック フィルタをイネーブルにします。ボットネット トラフィック フィルタでは、初期接続の各パケットの送信元 IP アドレスと宛先 IP アドレスが次の IP アドレスおよびキャッシュと比較されます。

- ダイナミック データベースの IP アドレス
- スタティック データベースの IP アドレス
- DNS 逆ルックアップ キャッシュ（ダイナミック データベースのドメイン名の場合）
- DNS ホスト キャッシュ（スタティック データベースのドメイン名の場合）

アドレスが一致すると、ASA が syslog メッセージを送信します。現在使用可能な追加アクションは、接続のドロップだけです。

前提条件

マルチ コンテキスト モードでは、コンテキスト実行スペースでこの手順を実行します。

推奨設定

DNS スヌーピングは必要ありませんが、ボットネット トラフィック フィルタを最大限に活用するために DNS スヌーピングを設定することをお勧めします（「DNS スヌーピングのイネーブル化」（P.25-11）を参照）。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。

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。

手順の詳細

ステップ 1　[Configuration] > [Firewall] > [Botnet Traffic Filter] > [Traffic Settings] ペインを選択します。

ステップ 2　指定したトラフィックでボットネット トラフィック フィルタをイネーブルにするには、次の手順を実行します。

a. [Traffic Classification] 領域で、ボットネット トラフィック フィルタをイネーブルにする各インターフェイスの [Traffic Classified] チェックボックスをオンにします。

すべてのインターフェイスに適用されるグローバル分類を設定するには、[Global (All Interfaces)] の [Traffic Classified] チェックボックスをオンにします。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。

b. インターフェイスごとに、[ACL Used] ドロップダウン リストから [--ALL TRAFFIC--]（デフォルト）または ASA に設定されている任意のアクセス リストを選択します。

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。

ACL を追加または編集するには、[Manage ACL] をクリックして、ACL マネージャを起動します。詳細については、一般的な操作のコンフィギュレーション ガイドの “Adding ACLs and ACEs” section on page 20-2 を参照してください。

ステップ 3　（任意）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、[Ambiguous Traffic Handling] 領域で、[Treat ambiguous (greylisted) traffic as malicious (blacklisted) traffic] 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、[Blacklisted Traffic Actions] 領域にルールを設定している場合にも、グレーリストのトラフィックはドロップされません。グレイリストの詳細については、「ボットネット トラフィック フィルタのアドレス タイプ」（P.25-2）を参照してください。

ステップ 4　（任意）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。

トラフィックを手動でドロップするには、「ボット ネット トラフィックの手動ブロック」（P.25-14）を参照してください。

a. [Blacklisted Traffic Actions] 領域で、[Add] をクリックします。

[Add Blacklisted Traffic Action] ダイアログボックスが表示されます。

b. [Interface] ドロップダウン リストから、トラフィックをドロップするインターフェイスを選択します。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をイネーブルにしたインターフェイスのみが使用できます。

c. [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。
  - **Very Low**
  - **Low**
  - **Moderate**
  - **High**
  - **Very High**

（注） スタティック ブラックリスト エントリは、常に Very High 脅威レベルに指定されます。

- [Range]：脅威レベルの範囲を指定します。

d. [ACL Used] 領域で、[ACL Used] ドロップダウン リストから [--ALL TRAFFIC--]（デフォルト）または ASA に設定されている任意のアクセス リストを選択します。

（注） ACL が [Traffic Classification] 領域で指定したトラフィックのサブセットであることを確認してください。

ACL を追加または編集するには、[Manage] をクリックして、ACL マネージャを起動します。詳細については、一般的な操作のコンフィギュレーション ガイドの “Adding ACLs and ACEs” section on page 20-2 を参照してください。

e. [OK] をクリックします。

[Traffic Settings] ペインに戻ります。

f. 所定のインターフェイスに追加ルールを適用する場合は、ステップ a ～ e を繰り返します。

所定のインターフェイスに対する複数のルールで、重複トラフィックを指定しないでください。ルール照合順を完全に制御することはできないので、重複トラフィックは、照合されたコマンドを把握できないことになります。たとえば、所定のインターフェイスに対して [--ALL TRAFFIC--] に一致するルールとアクセス リストを使用するコマンドの両方を指定しないでください。この場合、トラフィックは ACL でコマンドに一致しない可能性があります。同様に、ACL で複数のコマンドを指定する場合、各 ACL が一意であり、ネットワークが重ならないことを確認します。

ステップ 5　[Apply] をクリックします。

ボット ネット トラフィックの手動ブロック

マルウェア トラフィックを自動的にブロックしない場合（「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」（P.25-12）を参照）、トラフィックを拒否するアクセス ルールを設定するか、コマンドライン インターフェイス ツールで **shun** コマンド ツールを使用してホストへのトラフィックとホストからのトラフィックをすべてブロックすることによって、トラフィックを手動でブロックできます。一部のメッセージには、ASDM で自動的にアクセス ルールを設定できます。

たとえば、次のような syslog メッセージが表示されます。

```
ASA-4-338002: Dynamic Filter permitted black listed TCP traffic from inside:10.1.1.45/6798
(209.165.201.1/7890) to outside:209.165.202.129/80 (209.165.202.129/80), destination
209.165.202.129 resolved from dynamic list: bad.example.com
```

その後、次のいずれかのアクションを実行できます。

- アクセス ルールを作成して、トラフィックを拒否する。

  たとえば、上記の syslog メッセージを使用して、10.1.1.45 の感染ホストから 209.165.202.129 のマルウェア サイトへのトラフィックを拒否できます。また、さまざまなブラックリスト アドレスへの多数の接続が存在する場合は、ホスト コンピュータの感染を解決するまで 10.1.1.45 からのトラフィックをすべて拒否する ACL を作成できます。

  次の syslog メッセージの場合、Real Time Log Viewer から逆アクセス ルールを自動的に作成できます。

  – 338001, 338002, 338003, 338004 (blacklist)

  – 338201、338202（グレイリスト）

  アクセス ルールの作成に関する詳細については、一般的な操作のコンフィギュレーション ガイドの Chapter 39, “Configuring Logging,” と第 6 章「アクセス ルールの設定」を参照してください。

（注） ボットネット トラフィック フィルタの syslog メッセージから逆アクセス ルールを作成し、インターフェイスに他のアクセス ルールが適用されていない場合は、すべてのトラフィックを不用意にブロックしてしまうことがあります。通常、アクセス ルールがない場合、セキュリティの高いインターフェイスからセキュリティの低いインターフェイスへのトラフィックはすべて許可されます。しかし、アクセス ルールを適用すると、明示的に許可したトラフィック以外のトラフィックはすべて拒否されます。逆アクセス ルールは拒否ルールであるため、必ず、インターフェイスの結果のアクセス ポリシーを編集して、他のトラ

フィックを許可してください。

ACL では、将来の接続がすべてブロックされます。アクティブな現在の接続をブロックするには、**clear conn** コマンドを入力します。たとえば、syslog メッセージに記載されている接続だけを消去するには、**clear conn address 10.1.1.45 address 209.165.202.129** コマンドを入力します。詳細については、コマンド リファレンスを参照してください。

- 感染したホストを排除する。

  感染したホストを排除すると、そのホストからの接続がすべてブロックされます。そのため、特定の宛先アドレスおよびポートへの接続をブロックする場合は、ACL を使用する必要があります。ホストを排除するには、[Tools] > [Command Line Interface] で次のコマンドを入力します。将来の接続をブロックすると同時に現在の接続をドロップするには、宛先アドレス、送信元ポート、宛先ポート、およびオプションのプロトコルを入力します。

  shun *src_ip* [*dst_ip src_port dest_port* [*protocol*]]

  たとえば、10.1.1.45 からの将来の接続をブロックし、syslog メッセージに示されたマルウェア サイトへの現在の接続をドロップするには、次のように入力します。

  shun 10.1.1.45 209.165.202.129 6798 80

感染を解決したら、ACL を削除するか、排除を無効にしてください。排除を無効にするには、**no shun** *src_ip* を入力します。

ダイナミック データベースの検索

ドメイン名または IP アドレスがダイナミック データベースに含まれているかどうかを確認する場合は、データベースから文字列を検索することができます。

手順の詳細

ステップ 1　次の手順で [Search Dynamic Database] 領域にアクセスします。

- シングル モードで、あるいはコンテキスト内で、[Configuration] > [Firewall] > [Botnet Traffic Filter] > [Botnet Database Update] ペインを選択します。
- マルチ コンテキスト モードでは、[System execution] スペースで [Configuration] > [Device Management] > [Botnet Database Update] ペインを選択します。

ステップ 2　[Search string] フィールドに、少なくとも 3 文字以上の文字列を入力し、[Find Now] をクリックします。

最初の 2 つの一致が示されます。一致する項目を絞り込むために詳細な検索条件を指定するには、より長い文字列を入力します。

ステップ 3　表示された一致および検索文字列をクリアするには、[Clear] をクリックするか、新規の文字列を入力して [Find Now] をクリックすると、表示が更新されます。

ボットネット トラフィック フィルタのモニタリング

既知のアドレスがボットネット トラフィック フィルタによって分類されると、syslog メッセージが生成されます。ASA でコマンドを入力して、ボットネット トラフィック フィルタの統計情報やその他のパラメータをモニタすることもできます。この項は、次の内容で構成されています。

ボットネット トラフィック フィルタの Syslog メッセージ

ボットネット トラフィック フィルタでは、338*nnn* という番号が付いた詳細な syslog メッセージが生成されます。メッセージでは、着信接続と発信接続、ブラックリスト アドレス、ホワイトリスト アドレス、またはグレーリスト アドレス、およびその他の多数の変数が区別されます （グレーリストには、ブラ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が含まれています）。

syslog メッセージの詳細については、syslog メッセージ ガイドを参照してください。

次の syslog メッセージの場合、Real Time Log Viewer から逆アクセス ルールを自動的に作成できます。

- 338001, 338002, 338003, 338004 (blacklist)
- 338201、338202（グレイリスト）

一般的な操作のコンフィギュレーション ガイドの Chapter 39, “Configuring Logging,” を参照してください。

ボットネット トラフィック フィルタ モニタ用のペイン

Botnet Traffic Filter を監視するには、次のペインを確認してください。

コマンド	目的
[Home] > [Firewall Dashboard]	[Top Botnet Traffic Filter Hits] を示します。これには、マルウェア サイト、ポート、および感染しているホストの上位 10 件に関するレポートが表示されます。このレポートはデータのスナップショットで、統計情報の収集開始以降の上位 10 項目に一致しない場合があります。IP アドレスを右クリックすると、whois ツールが起動してボットネット サイトの詳細が表示されます。 • [Top Malware Sites]：上位のマルウェア サイトを示します。 • [Top Malware Ports]：上位のマルウェア ポートを示します。 • [Top Infected Hosts]：上位の感染しているホストを示します。
[Monitoring] > [Botnet Traffic Filter] > [Statistics]	ホワイトリスト、ブラックリスト、グレーリストとして分類される接続の数、およびドロップされた接続の数を示します。（グレイリストには、ブラ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が含まれています）[Details] ボタンを押すと、分類されたか、ドロップされたパケットの数を脅威レベルごとに示します。

コマンド	目的
[Monitoring] > [Botnet Traffic Filter] > [Real-time Reports]	上位 10 個のモニタ対象のマルウェア サイト、ポート、および感染ホストのレポートを生成します。上位 10 個のマルウェア サイトのレポートには、ドロップされた接続数、各サイトの脅威レベルとカテゴリが含まれます。このレポートはデータのスナップショットで、統計情報の収集開始以降の上位 10 項目に一致しない場合があります。 サイト IP アドレスを右クリックすると、whois ツールが起動してマルウェア サイトの詳細が表示されます。レポートは、PDF ファイルとして保存できます。
[Monitoring] > [Botnet Traffic Filter] > [Infected Hosts]	感染ホストに関するレポートを生成します。これらのレポートには、感染ホストの詳細な履歴が含まれ、感染ホスト、閲覧したマルウェア サイト、およびマルウェア ポートを示します。[Maximum Connections] オプションは、20 個の感染ホストおよび最大接続数を表示します。[Latest Activity] オプションは、20 個のホストおよび最新のアクティビティを表示します。[Highest Threat Level] オプションは、highest 脅威レベルのマルウェア サイトに接続した 20 個のホストを表示します。[Subnet] オプションは、指定したサブネット内のホストを最大 20 個表示します。 レポートは、[Current View] または [Whole Buffer] のいずれかで PDF ファイルとして保存できます。[Whole Buffer] オプションでは、バッファに格納されている、感染ホストの情報をすべて表示します。
[Monitoring] > [Botnet Traffic Filter] > [Updater Client]	サーバの IP アドレス、ASA が次にサーバに接続する日時、最後にインストールされたデータベースのバージョンなど、アップデート サーバに関する情報を表示します。
[Monitoring] > [Botnet Traffic Filter] > [DNS Snooping]	ボットネット トラフィック フィルタの DNS スヌーピングの実際の IP アドレスと名前を表示します。この出力には、ブラックリストに一致する名前だけでなく、すべての検査済み DNS データが含まれます。スタティック エントリの DNS データは含まれません。
[Monitoring] > [Botnet Traffic Filter] > [Dynamic Database]	ダイナミック データベースが最後にダウンロードされた日時、データベースのバージョン、データベースに含まれているエントリの数、10 個のサンプル エントリなど、ダイナミック データベースに関する情報を表示します。
[Monitoring] > [Botnet Traffic Filter] > [ASP Table Hits]	高速セキュリティ パスにインストールされているボットネット トラフィック フィルタ ルールを表示します。

関連情報

- syslog サーバを設定するには、一般的な操作のコンフィギュレーション ガイドの Chapter 39, “Configuring Logging,” を参照してください。
- アクセス ルールを使用して接続をブロックする場合については、第 6 章「アクセス ルールの設定」を参照してください。

ボットネット トラフィック フィルタの機能履歴

表 25-2 に、各機能変更と、それが実装されたプラットフォーム リリースを示します。ASDM は、複数のプラットフォーム リリースとの下位互換性があるため、サポートが追加された特定の ASDM リリースは一覧には含まれていません。

表 25-2　ボットネット トラフィック フィルタの機能履歴

機能名	プラットフォーム リリース	機能情報
ボットネット トラフィック フィルタ	8.2(1)	この機能が導入されました。
自動ブロッキングおよびブラックリスト カテゴリと脅威レベルのレポーティング	8.2(2)	ボットネット トラフィック フィルタでは、脅威レベルに基づいた、ブラックリストに記載されているトラフィックの自動ブロッキングがサポートされるようになりました。統計情報およびレポートで、マルウェア サイトのカテゴリおよび脅威レベルも表示できます。 上位ホストに対するレポートの 1 時間タイムアウトが削除され、タイムアウトがなくなりました。 次の画面が導入または変更されました。[Configuration] > [Firewall] > [Botnet Traffic Filter] > [Traffic Settings] および [Monitoring] > [Botnet Traffic Filter] > [Infected Hosts]。