CHAPTER 61

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.61-18）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。データベースを削除する必要がある場合は、代わりに **dynamic-filter database purge** コマンドを使用します。最初に **no dynamic-filter use-database** コマンドを入力して、データベースの使用をディセーブルにしてください。

（注） データベースを使用するには、ASA 用のドメイン ネーム サーバを設定して、適応型セキュリティ アプライアンスが URL にアクセスできるようにしてください。

ダイナミック データベースでドメイン名を使用するには、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（高い脅威レベル）：攻撃対象のコンピュータにアドウェア、スパイウェア、およびその他のマルウェアを配信するさまざまなエクスプロイトを使用するソース。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。
- マルウェア（低い脅威レベル）：誇大広告または悪意のあるアンチスパイウェア、アンチマルウェア、レジストリ クリーニング、システム クリーニング ソフトウェアを配信するソース。

- 成人向け：成人向けのコンテンツ、アドバタイジング、コンテンツ集約、登録と課金、経過時間確認などの Web ホスティングまたはサービスを提供する成人向けネットワーク / サービスに関連付けられたソース。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。
- ボットおよび脅威ネットワーク：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、脅威ネットワークでホストされるシステムか、またはボットネットそのものの一部であるシステムのいずれかです。
- （Conficker）ボットおよび脅威ネットワーク：Conficker ボットネットの指示管理サーバまたはボットネット マスター。
- （ZeusBotnet）ボットおよび脅威ネットワーク：Zeus ボットネットの指示管理サーバまたはボットネット マスター。

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.61-4）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 61-1 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 61-1　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 61-1 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 61-1　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

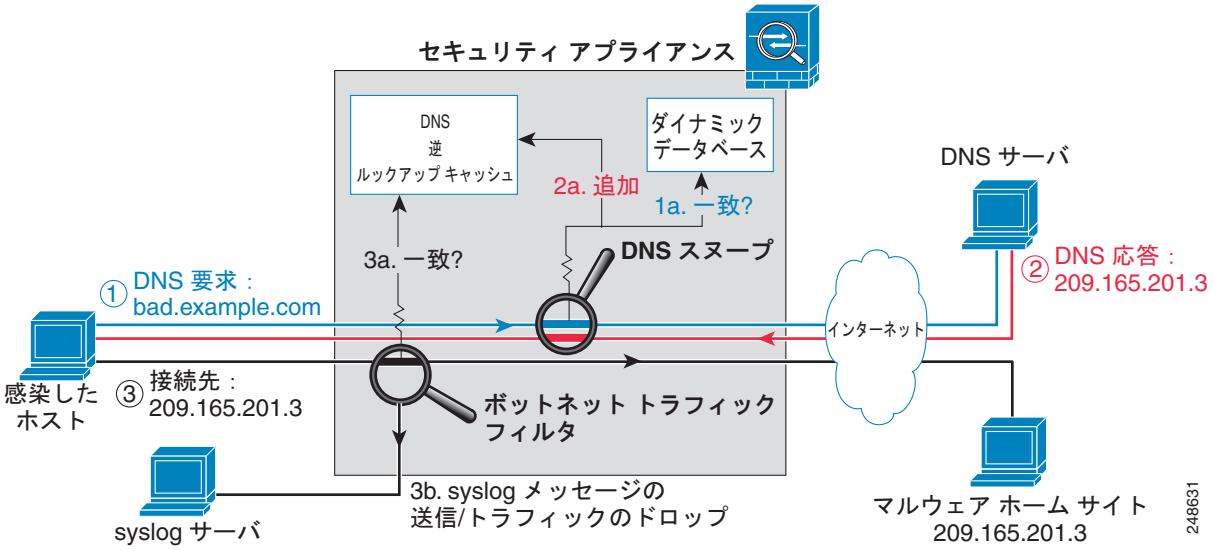
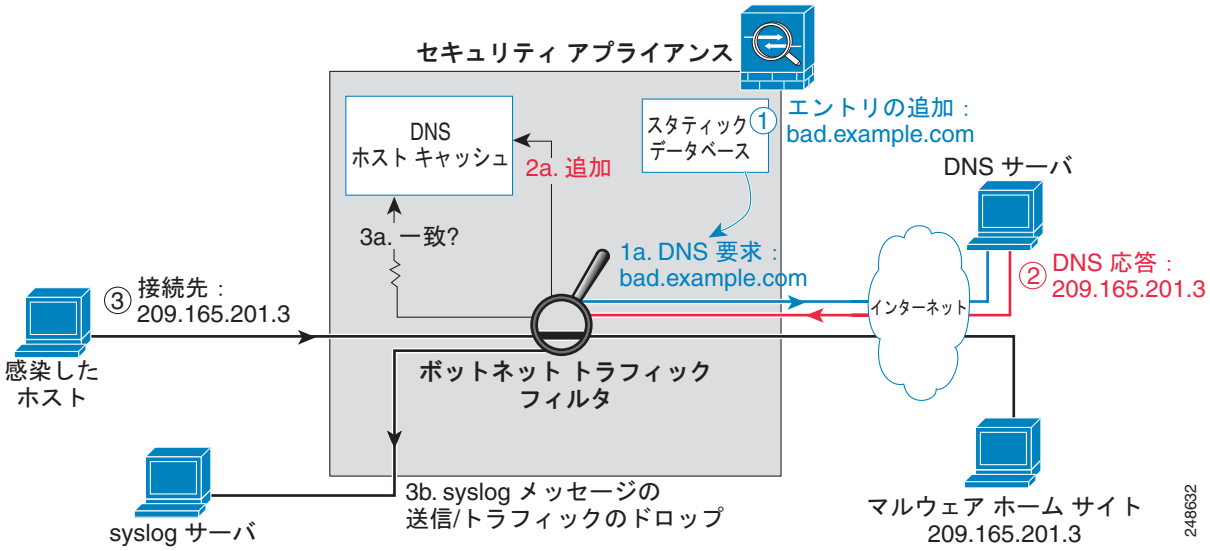


図 61-2 に、スタティック データベースを使用した場合のボットネット トラフィック フィルタの動作を示します。

図 61-2　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。

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

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.61-8）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.61-10）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.61-11）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.61-13）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.61-16）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リストを設定するか、**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。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。

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

「DNS サーバの設定」（P.15-11）の説明に従って、ASA による DNS サーバの使用をイネーブルにします。

手順の詳細

	コマンド	目的
ステップ 1	**dynamic-filter updater-client enable** **例：** `hostname(config)# dynamic-filter updater-client enable`	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。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 モード限定） **changeto context** *context_name* **例：** `hostname# changeto context admin` `hostname/admin#`	コンテキストに切り替えて、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します。
ステップ 3	**dynamic-filter use-database** **例：** `hostname(config)# dynamic-filter use-database`	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、コンテキスト実行スペースでこのコマンドを入力します。

例

次のマルチ モードの例では、ダイナミック データベースのダウンロードと、context1 および context2 でのデータベースの使用をイネーブルにします。

```
hostname(config)# dynamic-filter updater-client enable
hostname(config)# changeto context context1
hostname/context1(config)# dynamic-filter use-database
hostname/context1(config)# changeto context context2
hostname/context2(config)# dynamic-filter use-database
```

次のシングル モードの例では、ダイナミック データベースのダウンロードおよび使用をイネーブルにします。

```
hostname(config)# dynamic-filter updater-client enable
hostname(config)# dynamic-filter use-database
```

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.61-10）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.61-4）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。
- 「DNS サーバの設定」（P.15-11）の説明に従って、ASA による DNS サーバの使用をイネーブルにします。

手順の詳細

	コマンド	目的
ステップ 1	**dynamic-filter blacklist** **例：** `hostname(config)# dynamic-filter blacklist`	ボットネット トラフィック フィルタのブラックリストを編集します。
ステップ 2	次のいずれかまたは両方を入力します。	
	name *domain_name* **例：** `hostname(config-llist)# name bad.example.com`	ブラックリストに名前を追加します。このコマンドを複数回入力して、複数のエントリを追加できます。最大 1000 個のブラックリスト エントリを追加できます。
	address *ip_address mask* **例：** `hostname(config-llist)# address 10.1.1.1 255.255.255.255`	ブラックリストに IP アドレスを追加します。このコマンドを複数回入力して、複数のエントリを追加できます。*mask* には、単一ホストまたはサブネットのマスクを指定できます。
ステップ 3	**dynamic-filter whitelist** **例：** `hostname(config)# dynamic-filter whitelist`	ボットネット トラフィック フィルタのホワイトリストを編集します。
ステップ 4	次のいずれかまたは両方を入力します。	
	name *domain_name* **例：** `hostname(config-llist)# name good.example.com`	ホワイトリストに名前を追加します。このコマンドを複数回入力して、複数のエントリを追加できます。最大 1000 個のホワイトリスト エントリを追加できます。
	address *ip_address mask* **例：** `hostname(config-llist)# address 10.1.1.2 255.255.255.255`	ホワイトリストに IP アドレスを追加します。このコマンドを複数回入力して、複数のエントリを追加できます。*mask* には、単一ホストまたはサブネットのマスクを指定できます。

例

次に、ブラックリストおよびホワイトリストのエントリを作成する例を示します。

```
hostname(config)# dynamic-filter blacklist
hostname(config-llist)# name bad1.example.com
hostname(config-llist)# name bad2.example.com
hostname(config-llist)# address 10.1.1.1 255.255.255.0
hostname(config-llist)# dynamic-filter whitelist
hostname(config-llist)# name good.example.com
hostname(config-llist)# name great.example.com
hostname(config-llist)# name awesome.example.com
hostname(config-llist)# address 10.1.1.2 255.255.255.255
```

次の作業

「DNS スヌーピングのイネーブル化」（P.61-11）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。

次の手順では、DNS インスペクションで使用されるインターフェイス固有のサービス ポリシーを作成します。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.47-1）および第 36 章「モジュラ ポリシー フレームワークを使用したサービス ポリシーの設定」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。

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。この設定の推奨コマンドについては、「例」を参照してください。

手順の詳細

	コマンド	目的
ステップ 1	**class-map** *name* **例：** `hostname(config)# class-map dynamic-filter_snoop_class`	DNS を検査するトラフィックを識別するためのクラス マップを作成します。
ステップ 2	**match** *parameters* **例：** `hostname(config-cmap)# match port udp eq domain`	クラス マップのトラフィックを指定します。使用可能なパラメータの詳細については、「トラフィックの特定（レイヤ 3/4 クラス マップ）」（P.36-12）を参照してください。たとえば、特定のアドレスを送信元または宛先とする DNS トラフィックのアクセス リストを指定したり、すべての UDP DNS トラフィックを指定したりできます。
ステップ 3	**policy-map** *name* **例：** `hostname(config)# policy-map dynamic-filter_snoop_policy`	ポリシー マップを追加または編集し、クラス マップ トラフィックで実行するアクションを設定できるようにします。
ステップ 4	**class** *name* **例：** `hostname(config-pmap)# class dynamic-filter_snoop_class`	ステップ 1 で作成したクラス マップを識別します。
ステップ 5	**inspect dns** [*map_name*] **dynamic-filter-snoop** **例：** `hostname(config-pmap-c)# inspect dns preset_dns_map dynamic-filter-snoop`	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 スヌーピングをイネーブルにします。*map_name* にデフォルトの DNS インスペクション ポリシー マップを使用するには、マップ名に **preset_dns_map** を指定します。DNS インスペクション ポリシー マップの作成の詳細については、「DNS インスペクション」（P.47-1）を参照してください。
ステップ 6	**service-policy** *policymap_name* **interface** *interface_name* **例：** `hostname(config)# service-policy dynamic-filter_snoop_policy interface outside`	インターフェイスでポリシー マップをアクティブにします。インターフェイス固有のポリシーは、グローバル ポリシーより優先されます。各インターフェイスには、ポリシー マップを 1 つだけ適用できます。

例

次の推奨設定では、すべての UDP DNS トラフィックのクラス マップを作成し、デフォルトの DNS インスペクション ポリシー マップを使用して 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 スヌーピングをイネーブルにし、そのポリシー マップを外部インターフェイスに適用します。

```
hostname(config)# class-map dynamic-filter_snoop_class
hostname(config-cmap)# match port udp eq domain
```

```
hostname(config-cmap)# policy-map dynamic-filter_snoop_policy
hostname(config-pmap)# class dynamic-filter_snoop_class
hostname(config-pmap-c)# inspect dns preset_dns_map dynamic-filter-snoop
hostname(config-pmap-c)# service-policy dynamic-filter_snoop_policy interface outside
```

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.61-13）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.61-11）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。この設定用の推奨コマンドについては、「例」を参照してください。

手順の詳細

	コマンド	目的
ステップ 1	（任意） **access-list** *access_list_name* **extended** {**deny** | **permit**} *protocol source_address mask* [*operator port*] *dest_address mask* [*operator port*] **例：** hostname(config)# access-list dynamic-filter_acl extended permit tcp any any eq 80 hostname(config)# access-list dynamic-filter_acl_subset extended permit tcp 10.1.1.0 255.255.255.0 any eq 80	モニタまたはドロップするトラフィックを指定します。モニタ用にアクセス リストを作成しない場合は、デフォルトですべてのトラフィックがモニタされます。アクセス リストを使用して、ドロップするモニタ対象トラフィックのサブセットを指定することもできます。アクセス リストは、モニタ用アクセス リストのサブセットにします。アクセス リストの作成の詳細については、第 20 章「拡張アクセス コントロール リストの追加」を参照してください。
ステップ 2	**dynamic-filter enable** [**interface** *name*] [**classify-list** *access_list*] **例：** hostname(config)# dynamic-filter enable interface outside classify-list dynamic-filter_acl	オプションを設定せずに、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。このコマンドは、すべてのトラフィックをモニタします。 **interface** キーワードを使用して、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することをお勧めします。 **classify-list** キーワードでアクセス リストを指定すると、オプションでモニタ対象を特定のトラフィックに制限できます。 このコマンドは、インターフェイスとグローバル ポリシーごとに 1 回だけ入力できます（**interface** キーワードを指定しない場合）。各インターフェイス コマンドと各グローバル コマンドには、オプションの **classify-list** キーワードがあります。インターフェイス固有のコマンドは、グローバル コマンドより優先されます。

	コマンド	目的
ステップ 3	（任意） **dynamic-filter drop blacklist** [**interface** *name*] [**action-classify-list** *subset_access_list*] [**threat-level** {**eq** *level* | **range** *min max*}] **例：** `hostname(config)# dynamic-filter drop blacklist interface outside action-classify-list dynamic-filter_acl_subset threat-level range moderate very-high`	マルウェア トラフィックを自動的にドロップします。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.61-16）を参照してください。 最初に **dynamic-filter enable** コマンドを設定して、ドロップするすべてのトラフィックをモニタしてください。 インターフェイス ポリシーは、**interface** キーワード、またはグローバル ポリシー（**interface** キーワードを指定しない場合）を使用して設定できます。インターフェイス固有のコマンドは、グローバル コマンドより優先されます。このコマンドは、各インターフェイスおよびグローバル ポリシーに対して複数回入力できます。 **action-classify-list** キーワードは、ドロップするトラフィックをモニタ対象トラフィックのサブセットに制限します。ドロップするトラフィックは、常にモニタ対象トラフィックと等しいか、モニタ対象トラフィックのサブセットです。たとえば、**dynamic-filter enable** コマンドに対してアクセス リストを指定し、このコマンドに対して **action-classify-list** を指定する場合、**dynamic-filter enable** アクセス リストのサブセットになります。 所定のインターフェイス/グローバル ポリシーに対する複数のコマンドで、重複トラフィックを指定しないでください。コマンド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すべてのトラフィックに一致するコマンド（**action-classify-list** キーワードを使用しない）と **action-classify-list** キーワード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、トラフィックと **action-classify-list** キーワードを使用するコマンドとの照合が行われないことがあります。同様に、**action-classify-list** キーワードを使用する複数のコマンドを指定する場合、アクセス リストが固有であり、ネットワークが重複していないことを確認してください。 脅威レベルを設定することによって、ドロップするトラフィックをさらに制限することができます。明示的に脅威レベルを設定しない場合、使用されるレベルは、**threat-level range moderate very-high** です。 **（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。 *level*、*min*、および *max* の各オプションは次のとおりです。 • **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。

	コマンド	目的
ステップ 4	（任意） **dynamic-filter ambiguous-is-black** **例：** hostname(config)# **dynamic-filter ambiguous-is-black**	**dynamic-filter drop blacklist** コマンドを設定すると、このコマンドは、ドロップするために、グレーリストに記載されているトラフィックをブラックリストに記載されているトラフィックとして処理します。このコマンドをイネーブルにしない場合、グレーリストに記載されているトラフィックはドロップされません。グレー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.61-2）を参照してください。

例

次の推奨設定では、外部インターフェイス上のすべてのトラフィックをモニタし、moderate 以上の脅威レベルのすべてのトラフィックをドロップします。

```
hostname(config)# dynamic-filter enable interface outside
hostname(config)# dynamic-filter drop blacklist interface outside
```

一部のトラフィックをモニタ対象から除外する場合は、アクセス リストを使用してトラフィックを制限できます。次に、外部インターフェイス上のポート 80 のトラフィックだけをモニタし、very-high 脅威レベルのトラフィックだけをドロップする例を示します。

```
hostname(config)# access-list dynamic-filter_acl extended permit tcp any any eq 80
hostname(config)# dynamic-filter enable interface outside classify-list dynamic-filter_acl
hostname(config)# dynamic-filter drop blacklist interface outside threat-level eq
very-high
```

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.61-13）を参照）、トラフィックを拒否するアクセス リストを設定するか、**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。

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。

- トラフィックを拒否するアクセスリストを作成する。

  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アクセス リストを作成できます。たとえば、次のコマンドを実行すると、10.1.1.5 から 209.165.202.129 へのトラフィックがすべて拒否されますが、内部インターフェイスのその他のトラフィックはすべて許可されます。

  ```
  hostname(config)# access-list BLOCK_OUT extended deny ip host 10.1.1.45 host
  209.165.202.129
  hostname(config)# access-list BLOCK_OUT extended permit ip any any
  hostname(config)# access-group BLOCK_OUT in interface inside
  ```

アクセス リストの作成の詳細については、第 20 章「拡張アクセス コントロール リストの追加」を参照してください。インターフェイスへのアクセス リストの適用の詳細については、第 42 章「アクセス ルールの設定」を参照してください。

（注） アクセス リストでは、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、アクセス リストを使用する必要があります。ホストを排除するには、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。

  ```
  hostname(config)# 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。

  ```
  hostname(config)# shun 10.1.1.45 209.165.202.129 6798 80
  ```

  排除の詳細については、「不要な接続のブロック」（P.63-2）を参照してください。

感染を解決したら、アクセス リストを削除するか、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

コマンド	目的
dynamic-filter database find *string* **Example:** hostname# dynamic-filter database find	ドメイン名または IP アドレスをダイナミック データベースから検索します。*string* には、ドメイン名または IP アドレスのすべてまたは一部を、3 文字以上の検索文字列で指定できます。一致する項目が複数見つかった場合は、最初の 2 つの項目が表示されます。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。 **（注）** データベース検索では、正規表現はサポートされません。

例

次に、文字列「example.com」で検索する例を示します。この例では、一致する項目が 1 つ見つかります。

```
hostname# dynamic-filter database find bad.example.com
```

```
   bad.example.com
Found 1 matches
```

次に、文字列「bad」で検索する例を示します。この例では、一致する項目が 3 つ以上見つかります。

```
hostname# dynamic-filter database find bad

   bad.example.com
   bad.example.net
Found more than 2 matches, enter a more specific string to find an exact
match
```

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」（P.61-18）
- 「ボットネット トラフィック フィルタ コマンド」（P.61-19）

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。

ボットネット トラフィック フィルタ コマンド

ボットネット トラフィック フィルタをモニタするには、次のいずれかのコマンドを入力します。

コマンド	目的
show dynamic-filter statistics [**interface** *name*] [**detail**]	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）。**detail** キーワードは、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。 統計情報をクリアするには、**clear dynamic-filter statistics** [**interface** *name*] コマンドを入力します。
show dynamic-filter reports top [**malware-sites** | **malware-ports** | **infected-hosts**]	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。 レポート データを消去するには、**clear dynamic-filter reports top** コマンドを入力します。
show dynamic-filter reports infected-hosts {**max-connections** | **latest-active** | **highest-threat** | **subnet** *ip_address netmask* | **all**}	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。**max-connections** キーワードは、20 個の感染ホストおよび最大接続数を表示します。**latest-active** キーワードは、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** キーワードは、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** キーワードは、指定したサブネット内のホストを最大 20 個表示します。**all** キーワードは、バッファに格納された感染ホスト情報をすべて表示します。この表示には、数千ものエントリが含まれることがあります。CLI ではなく、ASDM を使用して PDF を生成できます。 レポート データを消去するには、**clear dynamic-filter reports infected-hosts** コマンドを入力します。
show dynamic-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。
show dynamic-filter dns-snoop [**detail**]	ボットネット トラフィック フィルタの DNS スヌーピングの概要を表示します。**detail** キーワードが指定された場合は、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。 DNS スヌーピング データを消去するには、**clear dynamic-filter dns-snoop** コマンドを入力します。

コマンド	目的
show dynamic-filter data	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。
show asp table dynamic-filter [**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。

例

次に、**show dynamic-filter statistics** コマンドの出力例を示します。

```
hostname# show dynamic-filter statistics
Enabled on interface outside
 Total conns classified 11, ingress 11, egress 0
 Total whitelist classified 0, ingress 0, egress 0
 Total greylist classified 0, dropped 0, ingress 0, egress 0
 Total blacklist classified 11, dropped 5, ingress 11, egress 0
Enabled on interface inside
 Total conns classified 1182, ingress 1182, egress 0
 Total whitelist classified 3, ingress 3, egress 0
 Total greylist classified 0, dropped 0, ingress 0, egress 0
 Total blacklist classified 1179, dropped 1000, ingress 1179, egress 0
```

次に、**show dynamic-filter reports top malware-sites** コマンドの出力例を示します。

```
hostname# show dynamic-filter reports top malware-sites
Site                                    Connections logged dropped Threat Level Category
-------------------------------------------------------------------------------------------
bad1.example.com (10.67.22.34)                          11       0            2      Botnet
bad2.example.com (209.165.200.225)                       8       8            3      Virus
bad1.cisco.example(10.131.36.158)                        6       6            3      Virus
bad2.cisco.example(209.165.201.1)                        2       2            3      Trojan
horrible.example.net(10.232.224.2)                       2       2            3      Botnet
nono.example.org(209.165.202.130)                        1       1            3      Virus

Last clearing of the top sites report: at 13:41:06 UTC Jul 15 2009
```

次に、**show dynamic-filter reports top malware-ports** コマンドの出力例を示します。

```
hostname# show dynamic-filter reports top malware-ports
Port                                        Connections logged
-------------------------------------------------------------------------
tcp 1000                                                   617
tcp 2001                                                   472
tcp 23                                                      22
tcp 1001                                                    19
udp 2000                                                    17
udp 2001                                                    17
tcp 8080                                                     9
tcp 80                                                       3
tcp >8192                                                    2

Last clearing of the top sites report: at 13:41:06 UTC Jul 15 2009
```

次に、**show dynamic-filter reports top infected-hosts** コマンドの出力例を示します。

```
hostname# show dynamic-filter reports top infected-hosts
Host                                        Connections logged
-------------------------------------------------------------------------
10.10.10.51(inside)                                     1190
```

```
10.12.10.10(inside)                                  10
10.10.11.10(inside)                                   5

Last clearing of the top infected-hosts report: at 13:41:06 UTC Jul 15 2009
```

ボットネット トラフィック フィルタの設定例

この項では、シングル コンテキスト モードおよびマルチ コンテキスト モードの推奨設定とその他の可能な設定について説明します。この項は、次の内容で構成されています。

推奨設定例

次のシングル コンテキスト モードの推奨設定例では、ダイナミック データベースのダウンロードおよび使用をイネーブルにします。この設定では、すべての UDP DNS トラフィックのクラス マップを作成し、デフォルトの DNS インスペクション ポリシー マップを使用して 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 スヌーピングをイネーブルにし、そのポリシー マップをインターネットに直接接続されている外部インターフェイスに適用します。

例 61-1　　シングル モードのボットネット トラフィック フィルタの推奨例

```
hostname(config)# dynamic-filter updater-client enable
hostname(config)# dynamic-filter use-database
hostname(config)# class-map dynamic-filter_snoop_class
hostname(config-cmap)# match port udp eq domain
hostname(config-cmap)# policy-map dynamic-filter_snoop_policy
hostname(config-pmap)# class dynamic-filter_snoop_class
hostname(config-pmap-c)# inspect dns preset_dns_map dynamic-filter-snoop
hostname(config-pmap-c)# service-policy dynamic-filter_snoop_policy interface outside
hostname(config)# dynamic-filter enable interface outside
hostname(config)# dynamic-filter drop blacklist interface outside
```

次のマルチ コンテキスト モードの推奨設定例では、2 つのコンテキストでボットネット トラフィック フィルタをイネーブルにします。

例 61-2　　マルチ モードのボットネット トラフィック フィルタの推奨例

```
hostname(config)# dynamic-filter updater-client enable

hostname(config)# changeto context context1

hostname/context1(config)# dynamic-filter use-database
hostname/context1(config)# class-map dynamic-filter_snoop_class
hostname/context1(config-cmap)# match port udp eq domain
hostname/context1(config-cmap)# policy-map dynamic-filter_snoop_policy
hostname/context1(config-pmap)# class dynamic-filter_snoop_class
hostname/context1(config-pmap-c)# inspect dns preset_dns_map dynamic-filter-snoop
hostname/context1(config-pmap-c)# service-policy dynamic-filter_snoop_policy interface
outside
hostname/context1(config)# dynamic-filter enable interface outside
hostname/context1(config)# dynamic-filter drop blacklist interface outside

hostname/context1(config)# changeto context context2
```

```
hostname/context2(config)# dynamic-filter use-database
hostname/context2(config)# class-map dynamic-filter_snoop_class
hostname/context2(config-cmap)# match port udp eq domain
hostname/context2(config-cmap)# policy-map dynamic-filter_snoop_policy
hostname/context2(config-pmap)# class dynamic-filter_snoop_class
hostname/context2(config-pmap-c)# inspect dns preset_dns_map dynamic-filter-snoop
hostname/context2(config-pmap-c)# service-policy dynamic-filter_snoop_policy interface
outside
hostname/context2(config)# dynamic-filter enable interface outside
hostname/context2(config)# dynamic-filter drop blacklist interface outside
```

その他の設定例

次の設定例では、ブラックリストとホワイトリストにスタティック エントリを追加します。次に、外部インターフェイス上のポート 80 のトラフィックをすべてモニタし、ブラックリストに記載されているトラフィックをドロップします。グレーリストに記載されているアドレスも、ブラックリストに記載されているアドレスとして処理します。

```
hostname(config)# dynamic-filter updater-client enable

hostname(config)# changeto context context1

hostname/context1(config)# dynamic-filter use-database
hostname/context1(config)# class-map dynamic-filter_snoop_class
hostname/context1(config-cmap)# match port udp eq domain
hostname/context1(config-cmap)# policy-map dynamic-filter_snoop_policy
hostname/context1(config-pmap)# class dynamic-filter_snoop_class
hostname/context1(config-pmap-c)# inspect dns preset_dns_map dynamic-filter-snoop
hostname/context1(config-pmap-c)# service-policy dynamic-filter_snoop_policy interface
outside
hostname/context1(config-pmap-c)# dynamic-filter blacklist
hostname/context1(config-llist)# name bad1.example.com
hostname/context1(config-llist)# name bad2.example.com
hostname/context1(config-llist)# address 10.1.1.1 255.255.255.0
hostname/context1(config-llist)# dynamic-filter whitelist
hostname/context1(config-llist)# name good.example.com
hostname/context1(config-llist)# name great.example.com
hostname/context1(config-llist)# name awesome.example.com
hostname/context1(config-llist)# address 10.1.1.2 255.255.255.255
hostname/context1(config-llist)# access-list dynamic-filter_acl extended permit tcp any
any eq 80
hostname/context1(config)# dynamic-filter enable interface outside classify-list
dynamic-filter_acl
hostname/context1(config)# dynamic-filter drop blacklist interface outside
hostname/context1(config)# dynamic-filter ambiguous-is-black

hostname/context1(config)# changeto context context2

hostname/context2(config)# dynamic-filter use-database
hostname/context2(config)# class-map dynamic-filter_snoop_class
hostname/context2(config-cmap)# match port udp eq domain
hostname/context2(config-cmap)# policy-map dynamic-filter_snoop_policy
hostname/context2(config-pmap)# class dynamic-filter_snoop_class
hostname/context2(config-pmap-c)# inspect dns preset_dns_map dynamic-filter-snoop
hostname/context2(config-pmap-c)# service-policy dynamic-filter_snoop_policy interface
outside
hostname/context2(config-pmap-c)# dynamic-filter blacklist
hostname/context2(config-llist)# name bad1.example.com
hostname/context2(config-llist)# name bad2.example.com
```

```
hostname/context2(config-llist)# address 10.1.1.1 255.255.255.0
hostname/context2(config-llist)# dynamic-filter whitelist
hostname/context2(config-llist)# name good.example.com
hostname/context2(config-llist)# name great.example.com
hostname/context2(config-llist)# name awesome.example.com
hostname/context2(config-llist)# address 10.1.1.2 255.255.255.255
hostname/context2(config-llist)# access-list dynamic-filter_acl extended permit tcp any
any eq 80
hostname/context2(config)# dynamic-filter enable interface outside classify-list
dynamic-filter_acl
hostname/context2(config)# dynamic-filter drop blacklist interface outside
hostname/context2(config)# dynamic-filter ambiguous-is-black
```

関連情報

- syslog サーバを設定するには、第 81 章「ロギングの設定」を参照してください。
- トラフィックをブロックするアクセス リストを設定するには、第 20 章「拡張アクセス コントロール リストの追加」を参照してください。インターフェイスへのアクセス リストの適用の詳細については、第 42 章「アクセス ルールの設定」を参照してください。
- 接続を排除するには、「不要な接続のブロック」（P.63-2）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 61-2 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。

表 61-2　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。 **dynamic-filter ambiguous-is-black**、**dynamic-filter drop blacklist**、**show dynamic-filter statistics**、**show dynamic-filter reports infected-hosts**、および **show dynamic-filter reports top** コマンドが導入または変更されました。