ESA に関する FAQ： アウトブレイク フィルタ /ウイルス アウトブレイク フィルタ (VOF) に関する FAQ

目次

概要

このドキュメントでは、E メール セキュリティ アプライアンス (ESA) のアウトブレイク フィルタまたはウイルス アウトブレイク フィルタについてよく寄せられる質問 (FAQ) のいくつかについて説明します。

アウトブレイク フィルタとウイルス アウトブレイク フィルタ (VOS) はどのようなものですか

アウトブレイク フィルタは大規模なウイルスの拡散や小規模な非ウイルス性の攻撃 (フィッシング詐欺およびマルウェア配布など) が発生した際にネットワークを保護します。 データが収集され、ソフトウェアの更新が公開されるまで新たなアウトブレイクを検知できない、ほとんどのアンチマルウェア セキュリティ ソフトウェアとは異なり、シスコは感染が拡散したときにデータを収集し、ユーザにこれらのメッセージが到達することを防ぐためにリアルタイムで ESA に更新情報を送信します。

シスコは着信メッセージは、着信メッセージが安全またはアウトブレイクの一部であることを判断するルールを開発するためにグローバル トラフィック パターンを使用します。 アウトブレイクの一部である可能性があるメッセージは、シスコからアップデートされたアウトブレイクの情報または Sophos および McAfee によって発行される新しいアンチウイルス定義に基づいて安全と判断されるまで隔離されます。

小規模な非ウイルス性の攻撃で使用されるメッセージは、正当に見える外見、受信者情報、そし

て短期間だけオンラインに存在し Web セキュリティ サービスが知らないフィッシングおよびマルウェア Web サイトを参照するカスタム URL を使用します。 アウトブレイク フィルタはメッセージの内容を分析し、この種の非ウイルス性の攻撃を検出するために URL リンクを検索します。 アウトブレイク フィルタは Web セキュリティ プロキシによって潜在的に危険な Web サイトへのトラフィックをリダイレクトするために URL を書き換え、ユーザがアクセスしようとしている Web サイトが悪意があるかもしれないことを警告するかまたは Web サイトを完全にブロックします。

ESA で Sophos または McAfee ウイルス対策ソフトウェアを実行していない場合でもアウトブレイク フィルタを使用できますか

シスコでは、ウイルスに対する防御を強化するため、ウイルス アウトブレイク フィルタの他に Sophos または McAfee Anti-Virus を使用することを推奨します。 ただし、VOF は Sophos または McAfee Anti-Virus を有効にしなくても、独立して動作することができます。

アウトブレイク フィルタはどのような状況でメッセージを隔離しますか

メッセージが隔離されるのは、メッセージに含まれている添付ファイルが、現在のアウトブレイク ルールまたはメール管理者が設定したしきい値に一致するかまたはこれらの値を超える場合です。 シスコは、有効な機能キーが含まれている各 ESA に対して最新のアウトブレイク ルールを公開しています。またこれらのアウトブレイク ルールはサポート ポータルでも公開されます。 アウトブレイクの一部である可能性があるメッセージは、シスコからアップデートされたアウトブレイクの情報または Sophos および McAfee によって発行される新しいアンチウイルス定義に基づいて安全と判断されるまで隔離されます。

最新のウイルス アウトブレイクに関する情報は、SenderBase で入手できます。

Cisco Security Intelligence Operations（SIO）Web サイトに、スパム、フィッシング、およびマルウェア配布の試行を含む最新の非ウイルス性の脅威のリストが記載されています。

アウトブレイク隔離がいっぱいになるとどうなりますか

隔離が、割り当てられている最大スペース容量を超えるか、またはメッセージが最大時間設定を超えると、隔離を制限内に維持するため、メッセージが隔離から自動的にプルーニングされます。 メッセージはファーストイン ファーストアウト（FIFO）ベースで削除されます。 つまり、最も古いメッセージが最初に削除されます。 隔離からプルーニングする必要があるメッセージを解放（つまり配信）するか、または削除するように隔離を設定できます。 メッセージを解放する場合は、受信者に対しメッセージが強制的に隔離から解放されたことを通知するテキストをタグとして件名に使用できます。

アウトブレイク隔離から解放されたメッセージは、ウイルス対策モジュールにより再度スキャン

され、ウイルス対策ポリシーに基づいてアクションが実行されます。 このポリシーに基づき、メッセージの配信、削除、またはウイルスに感染した添付ファイルを削除した状態での配信のいずれかの処理が行われます。 アウトブレイク隔離からの解放後の再スキャン中に、ウイルスが検出されることがよくあります。 ESA mail_log またはメッセージ トラッキングを参照して、隔離に示されていた個々のメッセージがウイルスに感染していることが検出されたかどうか、およびそのメッセージが配信されるかどうか、配信される場合はその配信方法を確認できます。

システム隔離がいっぱいになる前に、使用中の隔離が 75% に達した時点でアラートが送信され、さらに 95% に達した時点で別のアラートが送信されます。 アウトブレイク隔離には、特定のウイルス脅威レベル（VTL）に一致するすべてのメッセージを削除または解放できる追加の管理機能があります。 これにより、特定のウイルス脅威に対応するウイルス対策のアップデートを受信した後で、隔離を容易にクリアできます。

アウトブレイク ルールの脅威レベルにはどのような意味がありますか

アウトブレイク フィルタは、0 ~ 5 の脅威レベルで動作します。 脅威レベルは、ウイルス感染発生の可能性を評価します。 ウイルス感染発生リスクに基づき、脅威レベルは疑わしいファイルの隔離に反映されます。 脅威レベルはさまざまな要因に基づいています。このような要因には、ネットワーク トラフィック、疑わしいファイル アクティビティ、ウイルス対策ベンダーから提供される情報、Cisco の Threat Operation Center による分析などがあります。 また、アウトブレイク フィルタではメール管理者がネットワークに対する脅威レベルの影響を増減できます。

レベル	リスク	意味
0	なし	メッセージが脅威であるリスクはありません。
1	低	メッセージが脅威であるリスクは低です。
2	低または中	メッセージが脅威であるリスクは低から中です。 これは疑わしい 脅威です。
3	中間	メッセージが確認されているアウトブレイクの一部であるか、メッセージの内容が脅
4	高	メッセージが大規模アウトブレイクの一部であることが確認されているか、メッセー
5	Extreme	メッセージの内容が、非常に大規模または大規模で、かつ非常に危険なアウトブレイ

ウイルスが発生した場合、どのように警告が通知されますか

SenderBase ネットワークで、特定のメッセージ プロファイル タイプの VTL が引き上げられると、設定されているアラート用電子メール アドレスに送信される電子メール メッセージで、そのことが通知されます。 VTL が、設定されているしきい値を下回ると、別のアラートが送信されます。 このようにして、ウイルスの進行状況をモニタできます。 これらのアラートを確実に受信するには、CLI で **alertconfig** コマンドを使用して、アラートの送信先電子メール アドレスを確認します。

設定を行うかまたは設定を確認するには、次の手順に従います。

- GUI： [Security Services] > [Outbreak Filters] で、[Edit Global Settings...] の下の設定を確認します。
- CLI： **outbreakconfig > setup**

例：

```
> outbreakconfig

Outbreak Filters: Enabled

Choose the operation you want to perform:
- SETUP - Change Outbreak Filters settings.
- CLUSTERSET - Set how the Outbreak Filters are configured in a cluster.
- CLUSTERSHOW - Display how the Outbreak Filters are configured in a cluster.
[]> setup

Outbreak Filters: Enabled
Would you like to use Outbreak Filters? [Y]>

Outbreak Filters enabled.

Outbreak Filter alerts are sent when outbreak rules cross the threshold (go above
or back down below), meaning that new messages of certain types could be quarantined
or will no longer be
quarantined, respectively.

Would you like to receive Outbreak Filter alerts? [N]> y

What is the largest size message Outbreak Filters should scan?
[524288]>

Do you want to use adaptive rules to compute the threat level of messages? [Y]>

Logging of URLs is currently disabled.

Do you wish to enable logging of URL's? [N]> y

Logging of URLs has been enabled.

The Outbreak Filters feature is now globally enabled on the system. You must use the
'policyconfig' command in the CLI or the Email Security Manager in the GUI to enable
Outbreak Filters for the desired Incoming and Outgoing Mail Policies.
```

新しいウイルスの発生が SenderBase により最初に検出され、VTL が引き上げられます。 VTL が設定されている VTL しきい値に一致またはしきい値を超えると、アラートを受信します。 ウイルスが特定および捕捉される時点、および新しいウイルスを識別するためのシグニチャが利用可能になる時点で、Sophos アラートが発行されます。

関連情報

- Cisco 電子メール セキュリティ アプライアンス - エンド ユーザ ガイド
- テクニカル サポートとドキュメント – Cisco Systems