ESA FAQ: Outbreak Filters/Virus Outbreak Filters (VOF) FAQ

Contents

Introduction

This document describes and answers some of the more frequently asked questions regarding Outbreak Filters, or Virus Outbreak Filters (VOF), on the Cisco Email Security Appliance (ESA).

What are Outbreak Filters?

> **Note**: Please be sure that you review the User Guide for the version of AsyncOS for Email Security that you are currently running. Example, User Guide for AsyncOS 13.0 for Cisco Email Security Appliances, Chapter: Outbreak Filters

Outbreak Filters protect your network from large-scale virus outbreaks and smaller, non-viral attacks, such as phishing scams and malware distribution, as they occur. Unlike most anti-malware security software, which cannot detect new outbreaks until data is collected and a software update is published, Cisco gathers data on outbreaks as they spread and sends updated information to your ESA in real-time to prevent these messages from reaching your users.

Cisco uses global traffic patterns to develop rules that determine if an incoming message is safe or part of an outbreak. Messages that may be part of an outbreak are quarantined until they are determined to be safe based on updated outbreak information from Cisco or new anti-virus definitions are published by Sophos and McAfee.

Messages used in small-scale, non-viral attacks use a legitimate-looking design, the recipient's information, and custom URLs that point to phishing and malware websites that have been online only for a short period of time and are unknown to web security services. Outbreak Filters analyze a message's content and search for URL links to detect this type of non-viral attack. Outbreak Filters can rewrite URLs to redirect traffic to potentially harmful websites through a web security proxy, which either warns users that the website they are attempting to access may be malicious

or blocks the website completely.

Can I use Outbreak Filters even if I am not running Sophos or McAfee Anti-Virus on my ESA?

Cisco recommends that you enable Sophos or McAfee Anti-Virus in addition to Outbreak Filters to increase your defense against viral attachments. However, Outbreak Filters can operate independently without requiring Sophos or McAfee Anti-Virus to be enabled.

When does Outbreak Filters quarantine a message?

A message is quarantined when it contains file attachment(s) that meet or exceed the current Outbreak Rules and the thresholds set by mail administrators. Cisco publishes current Outbreak Rules to each ESA that has a valid feature key. Messages that may be part of an outbreak are quarantined until they are determined to be safe based on updated outbreak information from Cisco or new anti-virus definitions are published by Sophos and McAfee.

How are the Outbreak Filter rules written?

Outbreak Rules are published by Cisco Security Intelligence Operations (SIO), a security ecosystem that connects global threat information, reputation-based services, and sophisticated analysis of Cisco security appliances to provide stronger protection with faster response times. By default, your appliance checks for and downloads new outbreak rules every 5 minutes as part of the Service Updates.

SIO consists of three components:

- SenderBase, the world's largest threat monitoring network, and vulnerability database.
- Talos, Cisco's global team of security analysts and automated systems.
- Dynamic updates, real-time updates automatically delivered to appliances as outbreaks occur.

Are there best practices for configuring Outbreak Filters?

Yes. Recommendation for the service level is as follows:

- Enable *Adaptive Rules*
- Set *Maximum Message Size to Scan* to 2M
- Enabled *Web Interaction Tracking*

Configuration at the incoming mail policy level will need to be determined on a per-customer, per-policy basis.

How do I report an incorrect Outbreak Filter rule?

You may report false positive or false negatives in one of two ways:

1. Open a Cisco support case: https://mycase.cloudapps.cisco.com/case

2. Open a reputation ticket with Talos: https://talosintelligence.com/reputation_center/support

Below are the conditions we can refine Outbreak Filtering rules:

- File Extensions
- File Signature (Magic) (Binary signature of the file which indicates its 'true' type)
- URLs
- Filename
- File Size

What happens when the Outbreak quarantine fills up?

When a quarantine exceeds the maximum space allocated to it, or if a message exceeds the maximum time setting, messages are automatically pruned from the quarantine to keep it within limits. Messages are removed on a first-in, first-out (FIFO) basis. In other words, the oldest messages are deleted first. You can configure a quarantine to either release (that is, deliver) or delete a message which must be pruned from a quarantine. If you choose to release messages, you may elect to have the subject line tagged with the text you specify which will alert the recipient that the message was forced out of quarantine.

Following release from the Outbreak quarantine, messages are re-scanned by the anti-virus module, and action is taken according to anti-virus policy. Depending on this policy, a message may be delivered, deleted, or delivered with viral attachments stripped. It is expected that viruses will often be found during re-scan after release from the Outbreak quarantine. The ESA mail_logs or message tracking can be consulted to determine if an individual message that was noted in the quarantine was found to be viral, and if and how it was delivered.

Before a system quarantine fills up, an alert is sent when the quarantine reaches 75% full, and another alert is sent when it reaches 95% full. The Outbreak Quarantine has an additional management feature that allows you to delete or release all messages that match a particular virus threat level (VTL). This allows for easy cleaning of the quarantine after an anti-virus update is received which addresses a particular virus threat.

What is the meaning of the threat level for an Outbreak Rule?

Outbreak Filters act under threat levels between 0 and 5. The threat level rates the likelihood of a viral outbreak. Based on the risk of a viral outbreak, the threat level influences the quarantining of suspicious files. The threat level is based on a number of factors, including but not limited to network traffic, suspicious file activity, input from anti-virus vendors, and analysis by Cisco SIO. In addition, Outbreak Filters allows mail administrators to increase or decrease the impact of threat levels for their networks.

Level	Risk	Meaning
0	None	There is no risk that the message is a threat.
1	Low	The risk that the message is a threat is low.
2	Low/Medium	The risk that the message is a threat is low to medium. It is a “suspected” threat.
3	Medium	Either the message is part of a confirmed outbreak or there is a medium to large risk c content being a threat.
4	High	Either the message is confirmed to be part of a large scale outbreak or its content is v dangerous.

5	Extreme	The message's content is confirmed to part of an outbreak that is either extremely larg scale or large scale and extremely dangerous.

How can I be alerted when an outbreak occurs?

When Outbreak Filters receives new/updates rules to elevate the Quarantine Threat Level for a particular type of message profile, you can be alerted via an email message sent to your configured alert email address. When a threat level falls below your configured threshold, another alert is sent. You can thus monitor the progress of the viral attachment(s). These emails are sent as "Info" emails.

> **Note**: To ensure you will receive these email notifications, verify the email address that alerts are sent to in the CLI using the **alertconfig** command, or the GUI: **System Administration > Alerts**.

To configure, or review configuration

- GUI: Security Services > Outbreak Filters and review the configuration under the **Edit Global Settings...**
- CLI: **outbreakconfig > setup**

Example:

```
> outbreakconfig

NOTICE: This configuration command has not yet been configured for the current cluster mode
(Machine esa2.hc3033-47.iphmx.com).

What would you like to do?
1. Switch modes to edit at mode "Cluster Hosted_Cluster".
2. Start a new, empty configuration at the current mode (Machine esa2.hc3033-47.iphmx.com).
3. Copy settings from another cluster mode to the current mode (Machine esa2.hc3033-
47.iphmx.com).
[1]>

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? [Y]> y

What is the largest size message Outbreak Filters should scan?
[2097152]>
```

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

Logging of URLs is currently enabled.

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

Web Interaction Tracking is currently enabled.

Do you wish to disable Web Interaction Tracking? [N]>

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.
```

Related Information

- **Cisco Email Security Appliance - End-User Guides**
- **Technical Support & Documentation - Cisco Systems**