ESA FAQ ：爆发过滤器/病毒爆发过滤(VOF) FAQ

目录

[简介](#)
[什么是爆发过滤器，或者病毒爆发过滤(VOF) ？](#)
[能否使用爆发过滤器，即使我不运行Sophos或McAfee防病毒在我的ESA ？](#)
[爆发过滤器什么时候检疫消息？](#)
[当爆发检疫得填满，什么发生？](#)
[什么是威胁的含义级为爆发规则？](#)
[当病毒爆发发生时，如何警告？](#)
[相关信息](#)

简介

本文描述并且回答某些关于爆发过滤器或者病毒爆发过滤器的更多常见问题，在电子邮件安全工具(ESA)。

什么是爆发过滤器，或者病毒爆发过滤(VOF) ？

因为他们发生，爆发过滤器保护您的从大规模病毒爆发和更加小，非病毒攻击的网络，例如网络钓鱼诈欺和恶意软件分配。不同于多数反恶意软件security software，不能检测新建的爆发，直到数据收集，并且软件更新发布，思科在爆发的收集数据，当他们传播和在实时发送更新信息对您的ESA防止这些消息到达您的用户。

思科使用全局数据流交通图开发确定的规则传入消息是否作为爆发的安全或部分。可能是爆发的一部分的消息被检疫，直到确定他们是根据更新爆发信息的安全从思科或新建的抗病毒定义由Sophos和McAfee发布。

用于小规模，非病毒攻击的消息使用一合法设计、收件人的信息和指向网络钓鱼和恶意软件网站联机只一段时间里并且是未知对Web安全服务的自定义URL。爆发过滤器分析消息内容并且搜索URL链路检测此种非病毒攻击。爆发过滤器能重写URL重定向流量到潜在有害的网站通过Web安全代理，任一警告用户网站他们尝试访问可能是有恶意的或阻塞网站完全。

能否使用爆发过滤器，即使我不运行Sophos或McAfee防病毒在我的ESA ？

思科建议您使Sophos或McAfee防病毒除病毒爆发过滤器之外增加您的对病毒的防御。然而，VOF能独立地运行，无需要求将启用的Sophos或McAfee防病毒。

爆发过滤器什么时候检疫消息？

消息被检疫，当包含用信件满足或超出当前爆发规则和阈值集管理员的文件附件时。思科发布当前爆发规则对每个ESA有的一个有效功能键和在我们的支持门户。 可能是爆发的一部分的消息被检疫，直到确定他们是根据更新爆发信息的安全从思科或新建的抗病毒定义由Sophos和McAfee发布。

关于当前病毒爆发的信息可以在SenderBase找到

Cisco安全情报交换行动(SIO)网站提供当前非病毒威胁列表，包括垃圾邮件、网络钓鱼和恶意软件分配尝试。

当爆发检疫得填满，什么发生？

当检疫超出最大空间分配到它时，或者，如果消息超出最大时间设置，消息从检疫自动地被修剪适当地保持它。消息删除根据先入先出(FIFO)基本类型。换句话说，以前消息首先删除。您能配置检疫到版本(即请传送)或删除必须从检疫修剪的消息。如果选择发表消息，您可以决定有用您指定将警告收件人的文本标记的标题栏消息是牵强的出于检疫。

从爆发检疫的更低版本，消息由抗病毒模块重新扫描，并且行动根据抗病毒策略采取。根据此策略，消息可能用剥离的病毒附件传送，删除或者传送。预计病毒经常将被找到在重新扫描期间，在从爆发检疫后的版本。ESA mail_logs或消息跟踪可以参见确定一个单个消息在检疫注释是否发现病毒，并且是否，并且它如何传送。

在系统检疫得填满前，警报被发送，当检疫到达75%全双工时，并且另一警报被发送，当到达95%全双工时。爆发检疫有允许您删除或发表所有消息匹配一个特定的病毒威胁级别的一个另外的管理功能(VTL)。这允许检疫的容易清洁，在寻址一个特定的病毒威胁的一次抗病毒更新接收后。

什么是威胁的含义级为爆发规则？

爆发过滤器操作在0和5.之间的威胁级别下。威胁级别对病毒爆发的可能性估计。基于病毒爆发的风险，威胁级别影响检疫可疑文件。威胁级别根据一定数量的要素，包括但不限于网络流量、可疑個、输入从抗病毒供应商和分析由思科的威胁操作中心。 另外，爆发过滤器允许邮件管理员增加或减少威胁级别影响他们的网络的。

级别	里斯克	含义
0	无	没有风险消息是威胁。
1	低	风险消息是威胁低。
2	低/介质	风险消息是威胁是低对介质。它是a ？怀疑？ 威胁。
3	介质	或者消息是被确认的爆发的一部分或有介质对是其的内容巨大的风险威胁。
4	海伊	或者消息被确认是大规模爆发的一部分或其内容是非常危险的。
5	极其	消息？s内容被确认给是二者之一庞大的缩放或大规模和非常危险的一部分的爆发。

当病毒爆发发生时，如何警告？

当SenderBase网络举起消息配置文件时特定类型的VTL，您可以通过电子邮件消息警告传送对您的已配置的提醒的电子邮件地址。当VTL在您的配置的阈值之下时下跌，另一警报被发送。您能因而监控病毒进度。要保证您将收到这些警报，验证电子邮件地址使用**alertconfig**命令，警报被发送对在CLI。

配置或者reivew confirugation

- GUI ：安全服务>爆发过滤器和查看配置在**编辑全局设置下…**
- CLI ： **outbreakconfig >设置**

例如。

```
> 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.
```

新的病毒爆发将由SenderBase首先检测，并且VTL将是高的。 如果VTL满足或超出您的已配置的VTL阈值，您将收到警报。 Sophos警报将跟随，病毒识别并且捕获，并且，当识别签名的新的病毒变得可用。

相关信息

- 思科电子邮件安全工具-最终用户指南
- 技术支持和文档 - Cisco Systems