集中化策略的最佳实践，病毒和爆发检疫设置和迁移从ESA到SMA

目录

简介

以下检疫在Cisco安全管理设备(SMA)可能共同当前集中：

- 防病毒
- 爆发
- 用于捉住的消息的策略检疫：
  消息过滤器内容过滤器数据丢失预防政策

集中这些检疫提供以下好处：

- 管理员能管理从多个电子邮件安全工具(ESA)的被检疫的消息在一个位置。
- 被检疫的消息在防火墙后存储而不是在DMZ，减小安全风险。
- 作为在SMA的标准的备份功能一部分集中化检疫可以备份。

先决条件

- 运行8.1的SMA (SMA用户指南、章节8，集中化策略、病毒和爆发检疫)
- 运行8.0.1的ESA (ESA用户指南、章节27，检疫)
- 防火墙端口7025 /TCP (里里外外)/主机名使用：AsyncOS IP/说明： 帕斯策略、病毒和爆发检疫数据在电子邮件安全工具和安全管理设备之间，当此功能是集中化的

配置

开始与ESA，在现有策略检疫，那里在策略检疫的有源消息：

为了移植这些消息然后取决于在SMA是拥有策略检疫的活动设备，请完成以下方向。

在SMA，请导航对**管理设备>集中式服务>Policy、病毒和爆发检疫**。 如果已经没启用，请点击

Enable (event) ：

选择接口，如果适用，打算处理从ESA的流量到SMA。

Note:检疫波尔特也许更改，但是将需要打开这，如果有到位防火墙/network ACL。

单击 submit。屏幕将刷新显示？启用的服务？消息，如下被看到：

导航对**管理设备>集中式服务> Security伊莱克斯**并且添加ESA通信到SMA ：

单击**添加电子邮件设备**。

Note:您只需要添加SMA将使用与ESA联络的IP地址。 设备名称作为一管理参考仅使用。

请务必**建立连接**和**测试连接**。当建立从SMA的连接后到ESA，管理员用户用户名和密码将是请求的。 这是被添加ESA的管理用户和密码。 基于在什么已经是活跃的与什么被添加，测验的结果可能变化，但是应该类似于：

请务必这时**提交**和**确认更改**在SMA。

此时，如果将再访ESA和尝试配置策略检疫的集中式服务部分，它类似于以下：

在SMA必须仍然完成迁移步骤。返回到SMA并且继续以下部分。

一旦**进行更改**完成，**启动迁移向导？**步骤2将变得激活：

选择**启动迁移向导**并且继续如下：

如果仅一特定的检疫将被移植，请选择**自定义**。在本例中，我们将继续**自动**，将移植ANY/ALL从ESA的策略检疫到SMA。 请注意:您将看到在ESA期间选择的指定的名称添加前面提到，跟随由用于通信的IP地址：

单击**其次**，并且继续：

最后，请单击**提交**，并且提交“成功”通知：

确认您的在SMA的更改。

返回对ESA，请导航对**安全服务>Policy、病毒和爆发检疫**。在SMA的事先需要的步骤当前被认可：

点击Enable (event) ？和请继续：

公告，那此处再用于通信的适当的端口是要注意的。这些**必须**配比和，如果防火墙/network ACL是在使用中的，必须打开为了允许在ESA和SMA之间的适当的迁移。

Note: 如果有策略、病毒和在ESA配置的爆发检疫，检疫和所有他们的消息的迁移开始，当您确认此更改。

Note: 仅一迁移进程可以在任何时间进展中。请勿启用集中化策略、病毒和爆发检疫在别的电

子邮件安全工具，直到上一个迁移完成。

单击**提交**和终于单击**进行**。 信息通知应该是类似的。如果有很大数量的消息已经在本地检疫，这些可能需要时间从ESA处理到SMA ：

再访SMA，并且导航对**管理设备>集中式服务>Policy、病毒和爆发检疫**。 迁移步骤当前将完成：

验证

此时，策略检疫的迁移从ESA到SMA完成。对于最终验证，请检查在SMA的策略检疫：

您应该看到在ESA最初列出的同样消息。选择#在Messages列的超链接，并且验证：

如果查看在ESA的mail_logs，将提交实际消息的迁移：

Note: 注释使用ESA (XX.X.XX.XX X)和SMA (YY.Y.YY.YY Y)之间的通信通过端口7025。

```
Wed Mar  5 02:48:40 2014 Info: New SMTP DCID 2 interface XX.X.XX.XXX address
YY.Y.YY.YYY port 7025
Wed Mar  5 02:48:40 2014 Info: DCID 2 TLS success protocol TLSv1 cipher RC4-SHA
the.cpq.host
Wed Mar  5 02:49:52 2014 Info: New SMTP DCID 3 interface XX.X.XX.XXX address
YY.Y.YY.YYY port 7025
Wed Mar  5 02:49:52 2014 Info: DCID 3 TLS success protocol TLSv1 cipher RC4-SHA
the.cpq.host
Wed Mar  5 02:50:22 2014 Info: New SMTP DCID 4 interface XX.X.XX.XXX address
YY.Y.YY.YYY port 7025
Wed Mar  5 02:50:22 2014 Info: DCID 4 TLS success protocol TLSv1 cipher RC4-SHA
the.cpq.host
Wed Mar  5 02:50:23 2014 Info: New SMTP DCID 5 interface XX.X.XX.XXX address
YY.Y.YY.YYY port 7025
Wed Mar  5 02:50:23 2014 Info: DCID 5 TLS success protocol TLSv1 cipher RC4-SHA
the.cpq.host
Wed Mar  5 02:50:40 2014 Info: New SMTP DCID 6 interface XX.X.XX.XXX address
YY.Y.YY.YYY port 7025
Wed Mar  5 02:50:40 2014 Info: DCID 6 TLS success protocol TLSv1 cipher RC4-SHA
the.cpq.host
Wed Mar  5 02:50:41 2014 Info: New SMTP DCID 7 interface XX.X.XX.XXX address
YY.Y.YY.YYY port 7025
Wed Mar  5 02:50:41 2014 Info: DCID 7 TLS success protocol TLSv1 cipher RC4-SHA
the.cpq.host
Wed Mar  5 02:50:42 2014 Info: New SMTP DCID 8 interface XX.X.XX.XXX address
YY.Y.YY.YYY port 7025
Wed Mar  5 02:50:42 2014 Info: DCID 8 TLS success protocol TLSv1 cipher RC4-SHA
the.cpq.host
Wed Mar  5 02:51:01 2014 Info: New SMTP DCID 9 interface XX.X.XX.XXX address
YY.Y.YY.YYY port 7025
Wed Mar  5 02:51:01 2014 Info: DCID 9 TLS success protocol TLSv1 cipher RC4-SHA
the.cpq.host
Wed Mar  5 02:51:01 2014 Info: CPQ listener cpq_listener starting
Wed Mar  5 02:51:01 2014 Info: New SMTP DCID 10 interface XX.X.XX.XXX address
YY.Y.YY.YYY port 7025
Wed Mar  5 02:51:01 2014 Info: DCID 10 TLS success protocol TLSv1 cipher RC4-SHA
the.cpq.host
Wed Mar  5 02:51:02 2014 Info: New SMTP DCID 11 interface XX.X.XX.XXX address
```

```
YY.Y.YY.YYY port 7025
Wed Mar  5 02:51:02 2014 Info: DCID 11 TLS success protocol TLSv1 cipher RC4-SHA
the.cpq.host
Wed Mar  5 02:51:02 2014 Info: MID 1 enqueued for transfer to centralized quarantine
"Policy" (content filter _policy_q_in_)
Wed Mar  5 02:51:02 2014 Info: MID 1 queued for delivery
Wed Mar  5 02:51:02 2014 Info: New SMTP DCID 12 interface XX.X.XX.XXX address
YY.Y.YY.YYY port 7025
Wed Mar  5 02:51:02 2014 Info: DCID 12 TLS success protocol TLSv1 cipher RC4-SHA
the.cpq.host
Wed Mar  5 02:51:02 2014 Info: Delivery start DCID 12 MID 1 to RID [0] to Centralized
Policy Quarantine
Wed Mar  5 02:51:02 2014 Info: MID 2 enqueued for transfer to centralized quarantine
"Policy" (content filter _policy_q_in_)
Wed Mar  5 02:51:02 2014 Info: MID 2 queued for delivery
Wed Mar  5 02:51:02 2014 Info: MID 3 enqueued for transfer to centralized quarantine
"Policy" (content filter _policy_q_in_)
Wed Mar  5 02:51:02 2014 Info: MID 3 queued for delivery
Wed Mar  5 02:51:02 2014 Info: Message done DCID 12 MID 1 to RID [0] (centralized
policy quarantine)
Wed Mar  5 02:51:02 2014 Info: MID 1 RID [0] Response 'ok:  Message 1 accepted'
Wed Mar  5 02:51:02 2014 Info: Message finished MID 1 done
Wed Mar  5 02:51:02 2014 Info: MID 1 migrated from all quarantines
Wed Mar  5 02:51:02 2014 Info: Delivery start DCID 12 MID 2 to RID [0] to Centralized
Policy Quarantine
Wed Mar  5 02:51:02 2014 Info: New SMTP DCID 13 interface XX.X.XX.XXX address
YY.Y.YY.YYY port 7025
Wed Mar  5 02:51:02 2014 Info: DCID 13 TLS success protocol TLSv1 cipher RC4-SHA
the.cpq.host
Wed Mar  5 02:51:02 2014 Info: New SMTP DCID 14 interface XX.X.XX.XXX address
YY.Y.YY.YYY port 7025
Wed Mar  5 02:51:02 2014 Info: DCID 14 TLS success protocol TLSv1 cipher RC4-SHA
the.cpq.host
Wed Mar  5 02:51:02 2014 Info: Message done DCID 12 MID 2 to RID [0] (centralized
policy quarantine)
Wed Mar  5 02:51:02 2014 Info: MID 2 RID [0] Response 'ok:  Message 2 accepted'
Wed Mar  5 02:51:02 2014 Info: Message finished MID 2 done
Wed Mar  5 02:51:02 2014 Info: MID 2 migrated from all quarantines
Wed Mar  5 02:51:02 2014 Info: Delivery start DCID 12 MID 3 to RID [0] to Centralized
Policy Quarantine
Wed Mar  5 02:51:02 2014 Info: Message done DCID 12 MID 3 to RID [0] (centralized
policy quarantine)
Wed Mar  5 02:51:02 2014 Info: MID 3 RID [0] Response 'ok:  Message 3 accepted'
Wed Mar  5 02:51:02 2014 Info: Message finished MID 3 done
Wed Mar  5 02:51:02 2014 Info: MID 3 migrated from all quarantines
Wed Mar  5 02:51:02 2014 Info: New SMTP DCID 15 interface XX.X.XX.XXX address
YY.Y.YY.YYY port 7025
Wed Mar  5 02:51:02 2014 Info: DCID 15 TLS success protocol TLSv1 cipher RC4-SHA
the.cpq.host
Wed Mar  5 02:51:07 2014 Info: DCID 12 close
```

再访ESA，并且当前提交下列，当查看策略，病毒，爆发检疫时：

验证下一步通过为策略检疫将被捉住的ESA发送一个新的测试消息。查看在ESA的mail_logs，请注意选中项目线路指示转移从ESA到SMA通过7025，指示策略检疫：

```
Wed Mar  5 02:57:47 2014 Info: Start MID 4 ICID 6
Wed Mar  5 02:57:47 2014 Info: MID 4 ICID 6 From: <robsherw.cisco@gmail.com>
Wed Mar  5 02:57:47 2014 Info: MID 4 ICID 6 RID 0 To: <robsherw@cisco.com>
Wed Mar  5 02:57:47 2014 Info: MID 4 Message-ID
'<7642E61C-4BA2-432E-A524-E163EA0B9753@gmail.com>'
Wed Mar  5 02:57:47 2014 Info: MID 4 Subject 'NEW FUNNY'
```

```
Wed Mar  5 02:57:47 2014 Info: MID 4 ready 525 bytes from
<robsherw.cisco@gmail.com>
Wed Mar  5 02:57:47 2014 Info: MID 4 matched all recipients for per-recipient
policy DEFAULT in the inbound table
Wed Mar  5 02:57:47 2014 Info: MID 4 enqueued for transfer to centralized
quarantine "Policy" (content filter _policy_q_in_)
Wed Mar  5 02:57:47 2014 Info: MID 4 queued for delivery
Wed Mar  5 02:57:47 2014 Info: New SMTP DCID 16 interface XX.X.XX.XXX address
YY.Y.YY.YYY port 7025
Wed Mar  5 02:57:47 2014 Info: DCID 16 TLS success protocol TLSv1 cipher RC4-SHA
the.cpq.host
Wed Mar  5 02:57:47 2014 Info: Delivery start DCID 16 MID 4 to RID [0] to Centralized
Policy Quarantine
Wed Mar  5 02:57:47 2014 Info: Message done DCID 16 MID 4 to RID [0] (centralized
policy quarantine)
Wed Mar  5 02:57:47 2014 Info: MID 4 RID [0] Response 'ok:  Message 4 accepted'
Wed Mar  5 02:57:47 2014 Info: Message finished MID 4 done
Wed Mar  5 02:57:52 2014 Info: DCID 16 close
```

再访在SMA的以前被提及的策略检疫，新的测试消息当前是检疫：

相关信息

- 集中策略、病毒和爆发检疫(PVO)的ESA不可能启用
- 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