Оптимальные методы для централизованной политики, вируса и карантинной настройки вспышки и миграции от ESA до SMA

Содержание

Введение

Следующий карантин может теперь быть коллективно централизован на Устройстве менеджмента Cisco Security (SMA):

- Антивирус
- Вспышка
- Карантин политики использовал для сообщений, которые пойманы: Фильтры сообщенияФильтры контентаПолитика предотвращения потери данных

Централизация этого карантина предлагает следующие преимущества:

- Администраторы могут управлять изолированными сообщениями от множественных Устройств безопасности электронной почты (ESA) в одном местоположении.
- Изолированные сообщения хранятся позади межсетевого экрана вместо в DMZ, уменьшая угрозу безопасности.
- Централизованный карантин может быть выполнен резервное копирование как часть стандартных функциональных возможностей резервирования на SMA.

Предварительные условия

- SMA, работающий 8.1 (Руководство пользователя SMA, Глава 8, Централизованная Политика, Вирус и Карантин Вспышки)
- ESA, работающий 8.0.1 (Руководство пользователя ESA, Глава 27, Карантин)
- Межсетевой экран - порт 7025 / TCP (В и) / использование Имени хоста: AsyncOS IPs / Описание: когда эта функция централизована, политика Прохода, вирус, и вспышка изолируют данные между устройствами Безопасности электронной почты и устройством Управления системой безопасности

Настройка

Начиная с ESA, в Карантине существующей политики, в Карантине Политики существуют активные сообщения:

Чтобы переместить эти сообщения и затем полагаться на SMA, чтобы быть активным устройством, владеющим Карантином Политики, завершите следующие направления.

На SMA перейдите к **Устройству менеджмента> Centralized Services> Политика, Вирус и Карантин Вспышки**. Если не включенный уже, нажмите **Enable:**

Выберите интерфейс, если применимо, который предназначен для обработки трафика от ESA до SMA.

> **Примечание:** Карантинный порт может быть изменен, но это должно будет быть открыто, если там будет существовать ACL межсетевого экрана/сети.

Нажмите кнопку Submit (Отправить). Экран обновит для показа ? Сервис включен? сообщение, замеченное ниже:

Перейдите к **Устройству менеджмента>> Security Centralized Services Устройства** и добавьте связь ESA к SMA:

Нажмите Add почтовое устройство.

> **Примечание:** Только необходимо добавить IP-адрес, который SMA будет использовать для передачи с ESA. Название устройства используется только в качестве административной ссылки.

Обязательно **Установите Соединение** и **Тестовое подключение**. После установления соединения от SMA до ESA запросят пользовательское имя администратора и пароль. Это - административный пользователь и пароль ESA, который добавляется. На основе какого уже активно по сравнению с тем, что добавляется, результаты теста могут варьироваться, но должны быть подобны:

Обязательно **Отправьте** и **Передайте Изменения** на этом этапе на SMA.

В это время, если бы необходимо было пересмотреть ESA и попытаться настроить раздел Centralized Services Карантина Политики, это было бы подобно придерживающемуся:

Шаги миграции должны все еще быть выполнены на SMA. Возвратитесь к SMA и продолжите следующий раздел.

Однажды **Изменения Передачи** завершен, **Мастер Миграции Запуска?** из шага 2 станет активным:

Выберите **Launch Migration Wizard** и продолжите следующим образом:

Если только определенный карантин должен быть перемещен, выбрать **Custom**. В данном примере мы продолжим **Автоматический**, который переместит Карантин Политики ANY/ALL от ESA до SMA. Обратите внимание на то, что вы будете видеть, что указанное имя, выбранное во время ESA, добавляет ранее упомянутый, придерживавшийся IP-адресом, используемым в связи:

Нажмите Next и продолжите:

Наконец, нажмите **Submit**, и уведомление "Success" представлено:

Передайте свои изменения на SMA.

Возвращаясь к ESA, перейдите к **Сервисам безопасности> Политика, Вирус и Карантин Вспышки**. Необходимые как условие шаги в SMA теперь распознаны:

Нажать **Enable?**, и продолжите:

Заметьте, это здесь снова, на соответствующий порт, используемый для связи, обращают внимание. Они **должны** совпасть, и если ACL межсетевого экрана/сети используется, должен быть открыт для разрешения надлежащей миграции между ESA и SMA.

> **Примечание:** Если у вас есть политика, вирус, и карантин вспышки, настроенный на ESA, миграции карантина и всех их сообщений, начинается, как только вы передаете это изменение.

> **Примечание:** Только один процесс переноса может произойти в любое время. Не включайте централизованную политику, вирус и карантин вспышки на другом устройстве Безопасности электронной почты, пока предыдущая миграция не будет завершена.

Нажмите **Submit**, и наконец нажмите **Commit**. Информационное уведомление должно быть подобным. Если существует большое число сообщений уже в локальном карантине, они могут занять время для обработки от ESA до SMA:

Пересмотрите SMA и перейдите к **Устройству менеджмента> Centralized Services> Политика, Вирус и Карантин Вспышки**. Шаги миграции будут теперь выполнены:

Проверка

В это время миграция Карантина Политики от ESA до SMA завершена. Для заключительной проверки проверьте Карантин Политики на SMA:

Необходимо видеть те же сообщения, которые были первоначально перечислены на ESA. Выберите # гиперссылку в столбце сообщений и проверьте:

При рассмотрении mail_logs на ESA миграция фактических сообщений будет представлена:

> **Примечание:** Обратите внимание на использование связи между ESA (XX X.XX.XXX) и SMA (YY.Y.YY.YYY) через порт 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
```

Пересмотрите ESA, и ниже приводится теперь представленный при просмотре Политики, Вируса, Карантина Вспышки:

Следующий шаг проверки передает новое тестовое сообщение через ESA, который будет пойман для карантина политики. При рассмотрении mail_logs на ESA, заметьте выделенную линию, указывающую на передачу от ESA до SMA через 7025, указав на Карантин Политики:

```
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
```

Пересмотрите ранее упомянутый Карантин Политики на SMA, новое тестовое сообщение находится теперь в карантине также:

Дополнительные сведения

- Политика Централизации ESA, Вирус и Карантин Вспышки (PVO) не Могут быть Включены
- Устройство безопасности электронной почты Cisco - руководства пользователя
- Cisco Systems – техническая поддержка и документация