Оптимальные методы конфигурации для ESA CES

Содержание

Введение

Этот документ предоставляет сводку рекомендаций для Облачной безопасности электронной почты (CES) Cisco использования администраторов для настройки их Cisco Email Security Appliance (ESA).

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Администрирование ESA, и CLI и администрирование уровня GUI

Используемые компоненты

Сведения в этом документе основываются на оптимальных методах и рекомендациях для клиентов CES и администраторов.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить

потенциальное воздействие всех команд до их использования.

Родственные продукты

Данный документ также может использоваться со следующими версиями программного и аппаратного обеспечения:

- ESA собственные аппаратные средства и виртуальные устройства (параметры), выполняющие любую версию AsyncOS для Безопасности электронной почты

Оптимальные методы конфигурации для ESA CES

> % Warning: Любые изменения к конфигурации (конфигурациям) на основе оптимальных методов как предусмотрено в этом документе должны быть рассмотрены и поняты до фиксации ваших изменений конфигурации в производственной среде. Консультируйтесь со своим Системным инженером CES или Командой по работе с корпоративными заказчиками до изменения конфигурацию этого, вы не делаете 100% понимают или имеют комфорт с при управлении.

Сервисы безопасности

Защита от спама IronPort (IPBы)

- Всегда просматривайте 1.5 МБ и Никогда не просматривайте 2 МБ

Фильтрация URL-адресов

- Включите классификацию URL и репутацию
- Включите веб-отслеживание взаимодействия

Обнаружение Graymail

- Включите и Максимальный размер сообщений 1 МБ

Фильтры вспышки

- Включите Адаптивные Правила, размер Просмотра Max 1 МБ
- Включите веб-отслеживание взаимодействия

Усовершенствованная вредоносная защита

- Включите дополнительные типы файла после активации опции

Отслеживание сообщений

- Включите Отклоненную Регистрацию Соединения (при необходимости)

Администрирование системы

Пользователи

- Политика set password

- Если возможные рычаги Протокол LDAP для аутентификации

Регистрационные подписки

- Включите журналы истории конфигурации
- Включите журналы фильтрации URL-адресов
- Регистрируйте дополнительный заголовок 'от'

Уровень CLI изменения

Веб-фильтрация URL-адресов SDS безопасности

- **websecurityadvancedconfig**

```
Do you want to disable DNS lookups? [N]> y

Enter the maximum number of URLs that should be scanned:
[100]> 20

Enter the threshold value for outstanding requests:
[50]> 5

Enter the default time-to-live value (seconds):
[30]> 600

Do you want to rewrite all URLs with secure proxy URLs? [Y]> n
```

Регистрация URL

- Фильтрация URL-адресов включения ESA и оптимальные методы
- **outbreakconfig**

```
Logging of URLs is currently disabled.

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

Logging of URLs has been enabled.
```

Фильтр антиспуфинга

- Подделанное почтовое обнаружение (FED) с безопасностью электронной почты Cisco

Фильтр штамповки заголовка

- запишите и включите фильтр следующего сообщения:

```
Logging of URLs is currently disabled.

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

Logging of URLs has been enabled.
```

Таблица доступа к хосту

Additional Sender Groups

- Руководство пользователя ESA: создание Sender Group для обработки сообщений SKIP_SBRS – Разместите выше для источников ту репутацию пропускаSPOOF_ALLOW – Часть спуфинга фильтраПАРТНЕР – Для TLS Принудительные соединения

В предопределенной группе отправителя SUSPECTLIST

- Руководство пользователя ESA: проверка отправителя: хост включите "Очки SBRS ни на Одном"Дополнительно, позвольте "Соединиться, поиск записи PTR хоста отказывает из-за временной Ошибки DNS"

Агрессивная выборка HAT

- BLACKLIST [-10 к-2] ПОЛИТИКА: ЗАБЛОКИРОВАННЫЙ
- SUSPECTLIST [-2 к-1] ПОЛИТИКА: HEAVYTHROTTLED
- GRAYLIST [-1 к 2 и NONE] ПОЛИТИКА: LIGHTTHROTTLED
- ПОЛИТИКА ACCEPTLIST [2 TO 10]: ACCEPTED

Примечание: Вышеупомянутые примеры HAT показывают дополнительно настроенную Почтовую Политику Потока. Для полной информации относительно MFP, см. Руководство пользователя соответствующей версии AsyncOS для Безопасности электронной почты, работающей на вашем ESA. Пример, AsyncOS 10.0: Таблица доступа к хосту (HAT), Sender Groups и Почтовая Политика Потока

Почтовая политика потока (параметры политики по умолчанию)

Настройки безопасности

- Transport Layer Security (TLS) набора к предпочтительному
- Включите Систему политик отправителя (SPF)
- Включите DomainKeys определенную почту (DKIM)
- Включите основанную на домене проверку подлинности сообщений, создание отчетов и соответствие (DMARC) проверка и передайте составные отчёты об отзыве

Примечание: DMARC требует, чтобы дополнительная настройка настроила. Для полной информации относительно DMARC, см. Руководство пользователя соответствующей версии AsyncOS для Безопасности электронной почты, работающей на вашем ESA. Пример, AsyncOS 10.0: Проверка DMARC

Политика входящей почты

Пороги для защиты от спама

- Пороги нужно покинуть в порогах по умолчанию. Модификация выигрыша могла привести к увеличению ошибочного допуска.

Антивирус

- Сканирование сообщения: Просмотр для Вирусов только
- Неподдающиеся сканированию сообщения, Вирус Зараженные сообщения: набор "Архивное Исходное сообщение" к Нет

AMP

- Добавьте, что "AMP" для Подчинения Предварительно ожидает для Неподдающегося сканированию, отключает "Архивное сообщение"

Graymail

- Сканирование включило для каждого Вердикта, Предварительно ожидайте Предмет и Поставьте
- Добавьте x-заголовок для Объемной электронной почты, заголовок = "X-BulkMail", значение = "Истинный"

Фильтры вспышки

- Уровень угрозы по умолчанию равняется 3, отрегулируйте согласно своим требованиям безопасности Если уровень угрозы для сообщения будет равняться или будет превышать этот порог, то сообщение будет передаваться Карантину Вспышки. (1=lowest угроза, 5=highest угроза)
- Включите модификацию сообщения. URL перезаписи для сообщения без знака
- Смените Тему, предварительно ожидают к: [Возможное Мошенничество $threat_category]

Политика исходящей почты

Антивирус

- Сканирование сообщения
- Просмотр для Вирусов толькоснятие Включает X-заголовок с результатами сканирования AV в сообщении
- Для всех сообщений: Усовершенствованный> Другое Уведомление, включите "Другим" и включайте admin/SOC контактный электронный адрес

Карантин политики

Предварительно создайте следующий Карантин:

- Несоответствующий входящий
- Несоответствующий исходящий
- URL, злонамеренный входящий
- URL, злонамеренный исходящий
- Подозрительный спуфинг
- Вредоносное ПО

Другие параметры настройки

Словари

- Включите / Профанация Анализа и Сексуальный Словарь Сроков
- Создайте подделанный почтовый словарь с исполнительными названиями
- Создайте Словарь для ограниченных или других ключевых слов

Целевые средства управления

- Включите TLS для назначения по умолчанию
- Более низкие пороги набора для доменов веб-почты
- Ограничьте свою собственную исходящую почту с целевыми параметрами настройки контроля

Фильтры контента

> **Примечание:** Для полной информации относительно фильтров контента, см. Руководство пользователя соответствующей версии AsyncOS для Безопасности электронной почты, работающей на вашем ESA. Пример, AsyncOS 10.0: Фильтры контента

Несоответствующий фильтр контента

- Профанация условий OR Сексуальное соответствие словаря, передайте копию к Несоответствующему карантину

URL злонамеренный фильтр контента репутации

- Передайте копию к Злонамеренному URL (-10 к-6) для изоляции

Фильтр контента Категории URL с ними выбранными

- Взрослый, порнография, жестокое обращение с детьми, играя на деньги
- Передайте копию к Несоответствующему карантину

Подделанное почтовое обнаружение

- Словарь по имени "Executives_FED"
- FED () порог 90 Карантина копия

Макрос Включил фильтр контента Документов

- если одно или более прикреплений содержат Макрос
- Дополнительное условие-> Из Недоверяемого диапазона SBRS
- Передайте копию для изоляции

Прикрепляемая защита

- если защищены одно или более прикреплений
- Дополнительное условие-> Из Недоверяемого диапазона SBRS
- Передайте копию для изоляции

Дополнительные сведения

- BRKSEC-2131 - Безопасность электронной почты Cisco: оптимальные методы и точно настраивающий (Лас-Вегас 2016 года)
- BRKSEC-2131 - Безопасность электронной почты для непочтовых людей (Сан-Диего 2015 года)
- BRKSEC-3770 - (DMARC) - не являются phish: глубокое погружение в почтовые способы аутентификации (Сан-Франциско 2014 года)
- Лицензионное соглашение с конечным пользователем CES
- Описание услуг CES
- Cisco облачные сроки Universal
- Cisco Systems – техническая поддержка и документация