Как настроить сеть Cisco Web Security Appliance и RSA DLP для взаимодействия?

Содержание

Вопрос:

Как настроить сеть Cisco Web Security Appliance и RSA DLP для взаимодействия?

Обзор:

Этот документ предоставляет дополнительные сведения вне руководства пользователя Cisco WSA AsyncOS и Сети DLP RSA 7.0.2 Руководства по развертыванию, чтобы помочь клиентам взаимодействовать эти два продукта.

Описание продукта:

Cisco Web Security Appliance (WSA) является устойчивым, безопасным, эффективным устройством, которое защищает корпоративные сети против находящихся на web вредоносных и шпионящих программ, которые могут поставить под угрозу корпоративную безопасность и представить интеллектуальную собственность. Веб-Устройство безопасности предоставляет глубокий контроль содержимого приложения путем предложения услуги веба - прокси для стандартных протоколов связи, таких как HTTP, HTTPS и FTP.

Комплект DLP RSA включает комплексное решение по предотвращению потери данных, которое позволяет клиентам обнаружить и защитить уязвимые данные на предприятии путем усиления общей политики через инфраструктуру, чтобы обнаружить и защитить уязвимые данные в центре обработки данных в сети, и в оконечных точках. Комплект DLP включает следующие компоненты:

- **Центр обработки данных DLP RSA**. Центр обработки данных DLP помогает вам определять местоположение уязвимых данных независимо от того, где это находится в центре обработки данных, на файловых системах, базах данных, почтовых системах и больших средах SAN/NAS.
- **Сеть DLP RSA**. Сетевые мониторы DLP и принуждают передачу уязвимых данных в сети, такой как электронная почта и веб - трафик.
- **Оконечная точка DLP RSA**. Оконечная точка DLP помогает вам обнаруживать, контролировать и управлять уязвимыми данными на оконечных точках, таких как портативные ПК и рабочие столы.

Cisco WSA имеет способность взаимодействовать с Сетью DLP RSA.

Сеть DLP RSA включает следующие компоненты:

- **Сетевой контроллер**. Основное устройство, которое поддерживает информацию о политике передачи содержания и конфиденциальных данных. Сетевой контроллер управляет и обновляет управляемые устройства с политикой и определением деликатного характера наряду с любыми изменениями к их конфигурации после начальной конфигурации.
- **Управляемые устройства**. Эти устройства помогают передаче сети Сетевого монитора DLP и сообщают или перехватывают передачу:
  Датчики. Установленный в границах сети, Датчики пассивно контролируют трафик, оставляя сеть или пересекая границы сети, анализируя его для присутствия деликатного характера. Датчик является внеполосным решением; это может только отследить и сообщить нарушения политики.**Перехватчики**. Также установленный в границах сети, Перехватчики позволяют вам внедрять изоляцию и/или отклонение электронной почты (SMTP) трафик, который несет деликатный характер. Перехватчик является встроенным сетевым прокси и поэтому может заблокировать уязвимые данные от отъезда предприятия.**Серверы ICAP**. Устройства сервера специального назначения, которые позволяют вам внедрять мониторинг или блокирование HTTP, HTTPS или деликатного характера несущего трафика FTP. Сервер ICAP работает с прокси-сервером (настроенный как клиент ICAP), чтобы контролировать или заблокировать уязвимые данные от отъезда предприятия

Cisco WSA взаимодействует с Сетью DLP RSA Сервер ICAP.

Известные ограничения

Cisco WSA Внешняя интеграция DLP с Сетью DLP RSA поддерживает следующие действия: Позвольте и Блок. Это еще не поддерживает, "Модифицируют / Удаляют Содержание" (также названный Редакцией) действие.

Требования к продукту для совместимости

Совместимость Cisco WSA и Сеть DLP RSA была протестирована и проверена с моделями продукта и версиями программного обеспечения в следующей таблице. Функционально говорить эту интеграцию может работать с изменениями к модели и программному обеспечению, следующая таблица представляет протестированное единственное, проверенное, и поддержала комбинации. Строго рекомендуется использовать последнюю поддерживаемую версию обоих продуктов.

Продукт	Версия программного обеспечения
Cisco Web Security Appliance (WSA)	Версии AsyncOS 6.3 и выше
Сеть DLP RSA	7.0.2

Внешняя функция DLP

Используя Внешнюю функцию DLP Cisco WSA, можно передать все или определенный исходящий HTTP, HTTPS и трафик FTP от WSA до Сети DLP. Весь трафик передан с помощью Интернет-протокола адаптации контроля (ICAP).

Архитектура

Руководство Развертывания сети DLP RSA показывает следующую архитектуру общего назначения для взаимодействующей Сети DLP RSA с прокси-сервером. Эта архитектура не является определенной для WSA, но применяется к любому прокси, который взаимодействует с Сетью DLP RSA.

Рисунок 1: Развертываемая архитектура для сети DLP RSA и Cisco Web Security Appliance

Настройка Cisco Web Security Appliance

1. Определите внешнюю систему DLP на WSA, который работает с Сетью DLP сервер ICAP. Для инструкций посмотрите подключенную выборку от Руководства пользователя WSA "Инструкции по Руководству пользователя, Определяющие Внешние Системы DLP".

2. Создайте одну или более Внешней политики DLP, которая определяет, которые торгуют WSA, передает к Сети DLP для сканирования содержания с помощью ниже шагов:

- Под **GUI> веб-Менеджер безопасности> Внешняя политика DLP> Добавляет Политику**
- Щелкните по ссылке под столбцом ***Destinations*** для группы политик, которую вы хотите настроить
- Под 'Редактируют Целевые Параметры настройки' раздел, выбирают? Определить Назначения, Просматривающие Пользовательские настройки? из выпадающего меню
- Мы можем тогда настроить политику, чтобы 'Просмотреть все загрузки' или просмотреть загрузки на определенные домены/узлы, заданные в пользовательских категориях URL

Настройка сеть DLP RSA

Этот документ предполагает, что Сетевой контроллер DLP RSA, Сервер ICAP и Диспетчер предприятия были установлены и настроены.

1. Используйте Диспетчера предприятия DLP RSA для настройки Сетевого Сервера ICAP. Для подробных инструкций при устанавливании вашей Сети DLP сервер ICAP обратитесь к Руководству Развертывания сети DLP RSA. Основные параметры, которые необходимо задать на странице Конфигурации сервера ICAP: Имя хоста или IP-адрес Сервера ICAP.В **Общем** разделе **Параметров настройки** страницы конфигурации введите следующую информацию: Период времени в секундах, после которых сервер, как считают, испытал таймаут в поле **Server Timeout in**

Seconds.Выберите один из следующих как ответ **На Server Timeout**:**Открытый сбой**. Выберите эту опцию, если вы хотите позволить передачу после server timeout.**Закрытый сбой**. Выберите эту опцию, если вы хотите заблокировать передачу после server timeout.

2. Используйте Диспетчера предприятия DLP RSA для создания один или несколько сетевая специфичная политика, чтобы контролировать и заблокировать сетевой трафик, который несет деликатный характер. Для подробных инструкций для создания политики DLP обратитесь к Руководству Пользователя сети DLP RSA или справке Предприятия Manageronline. Основные шаги для выполнения являются придерживающимся: От библиотеки enable шаблона политики по крайней мере одна политика, которая целесообразна для вашей среды и содержания, которое вы будете контролировать.В той политике установите DLP Сетевые специфичные правила нарушения политики, которые задают действия, которые Сетевой продукт выполнит автоматически, когда события (нарушения политики) будут иметь место. Установите правило обнаружения политики для обнаружения всех протоколов. Заставьте действие политики "контролировать и блокироваться".

Дополнительно мы можем использовать Диспетчера предприятия RSA для настройки Сетевого уведомления, которое передается пользователю, когда происходят нарушения политики. Это уведомление передается Сетью DLP как замена для исходного трафика.

Протестируйте настройку

1. Настройте свой браузер для направления исходящего потока данных от браузера для движения непосредственно в прокси WSA.

   Например, при использовании браузера Mozilla Firefox сделайте придерживающееся: В браузере FireFox выберите **Tools> Options**. Диалоговое окно Options появляется.Нажмите вкладку **Network**, затем нажмите **Settings**. Диалоговое окно Настроек соединения появляется.Установите флажок **Manual Proxy Configuration**, затем введите IP-адрес или имя хоста прокси-сервера WSA в поле **HTTP Proxy** и номере порта 3128 (по умолчанию).**Нажмите OK**, затем **OK** снова для сохранения новых настроек.
2. Попытайтесь загрузить некоторое содержание, которое вы знаете, находится в нарушении Сетевой политики DLP, которую вы ранее включили.
3. Необходимо видеть Сетевое сообщение сброса ICAP в браузере.
4. Используйте 'Диспетчера предприятия' для просмотра получающегося события и инцидента, которые были созданы в результате этого нарушения политики.

Устранение неисправностей

1. При настройке внешнего сервера DLP на веб-Устройстве безопасности для Сети DLP RSA используйте следующие значения:

   Адрес сервера: IP-адрес или имя хоста Сети DLP RSA сервер ICAPПорт: порт TCP использовал обращаться к Серверу сети DLP RSA , как правило, **1344**Сервисный Формат ссылки: **icap://*<hostname_or_ipaddress>*/srv_conalarm**Пример: icap://dlp. пример.

com/srv_conalarm

2. Активируйте опцию получения трафика WSA для получения трафика между прокси WSA и Сетевым сервером ICAP. Это полезно при диагностировании проблем с подключением. Чтобы сделать это, сделайте придерживающееся:

   На GUI WSA перейдите **к Поддержке и Меню справки** в правой верхней части интерфейса пользователя. Выберите **Packet Capture** из меню, затем нажмите кнопку **Edit Settings**. Окно настроек Перехвата Редактирования появляется.

   В разделе Фильтров **Захвата пакета** экрана введите IP-адрес Сетевого сервера ICAP в поле **Server IP**.**Нажмите кнопку Submit, чтобы сохранить изменения.**
3. Используйте следующее пользовательское поле в журналах доступа WSA (Под ***GUI> Администрирование системы> Регистрационные Подписки> accesslog***) для получения дополнительных сведений:
   %Xp: Внешний вердикт сканирования сервера DLP (0 = никакое соответствие на сервере ICAP; 1 = соответствие политики против сервера ICAP и '-(дефис)' = Никакое сканирование не инициировалось внешним сервером DLP),

[Инструкции по руководству пользователя, определяющие внешние системы DLP.]

_