Содержание

[Введение](#)
[Установите пользовательскую политику DLP для обнаружения отформатированных и бесформатных номеров социального страхования](#)
[Создайте пользовательскую политику](#)
[Создайте классификатор](#)
[Установите параметры настройки степеней серьезности ошибки](#)
[Установите масштаб степеней серьезности ошибки](#)
[Отправьте и передайте изменения](#)
[Последние шаги](#)
[Дополнительные сведения](#)

Введение

Этот документ описывает, как установить пользовательскую политику DLP для обнаружения и отформатированных и восстановленных после форматирования Номеров социального страхования (SSN) на Cisco Email Security Appliance (ESA).

Установите пользовательскую политику DLP для обнаружения отформатированных и бесформатных номеров социального страхования

Дизайном механизм сканирования DLP только обнаруживает отформатированные Номера социального страхования. Это происходит из-за высокого уровня ошибочных допусков, вызванных 9-разрядными номерами, содержавшимися в данных, используемых различными отраслями. Например, Номера маршрутизации ABA Банка являются 9 цифрами и инициировали бы при сканировании для бесформатного Номера социального страхования. Как таковой рекомендуется избежать просматривать для бесформатных Номеров социального страхования, пока строго не требуется вашей организацией. Если требуется, что ваша организация просматривает для бесформатных Номеров социального страхования, можно создать пользовательскую политику DLP путем выполнения действий, предоставленных в решении ниже.

AsyncOS предоставляет возможность создавать вашу собственную политику с нуля с помощью классификаторов, разработанных RSA или организацией. Когда предопределенные шаблоны политики не встречают исключительные требования вашей сетевой среды, эту опцию считают усовершенствованной и нужно использовать только в редких случаях.

Создайте пользовательскую политику

1. От GUI: **Почтовая Политика> Менеджер Политики DLP**.
2. Нажмите **Add DLP Policy...** кнопка.
3. Выберите **Custom Policy** внизу экрана и **нажмите Add** рядом с Пользовательской Политикой.
4. Введите имя политики DLP . Пример: *SSN пользовательская политика*.

Создайте классификатор

Создание пользовательских классификаторов дает вам большую гибкость по просмотренным критериям в механизме DLP. Мы будем использовать это в наших интересах для сканирования и для отформатированного SSN и для восстановленного после форматирования SSN.

1. От Содержания, Совпадающего с выпадающим Классификатором, выберите **Create a Classifier** и нажмите **кнопку Add** .
2. Введите содержание, совпадающее с именем классификатора . Пример: *SSN все форматы.*
3. Под разделом Правил, набор выпадающее от Слов или Фраз к **Объекту**.
4. Выберите объект: **Номер социального страхования US, Отформатированный**.
5. **Нажмите Add правило**.
6. Снова выберите **Entity**.
7. Выберите объект: **Номер социального страхования US, Бесформатный**.
8. **Нажмите кнопку Submit (Отправить).**

Установите параметры настройки степеней серьезности ошибки

Следующие параметры настройки являются хорошей отправной точкой, однако они - просто рекомендация для помощи вам и могут потребовать некоторой калибровки или параметров настройки альтернативной конфигурации на основе ваших организационных потребностей.

- **Параметры настройки критической степени серьезности**
  Действие, примененное к сообщения: **карантин**
  Включите шифрование (проверенный)
  Правило шифрования: **Всегда используйте шифрование сообщения**
  Профиль шифрования (выбирают ваш настроенный профиль шифрования от выпадающего),
  Предмет зашифрованного сообщения: **$subject**
- **Параметры настройки высокого уровня важности**
  Действие, примененное к сообщения: **поставить**
  Включите шифрование (проверенный)
  Правило шифрования: **Всегда используйте шифрование сообщения**
  Профиль шифрования (выбирают ваш настроенный профиль шифрования от выпадающего),
  Предмет зашифрованного сообщения: **$subject**
- **Параметры настройки средней степени серьезности**
  Действие, примененное к сообщения: *поставить*

Включите шифрование (проверенный)
Правило шифрования: **Только используйте шифрование сообщения, если отказывает TLS**
Профиль шифрования (выбирают ваш настроенный профиль шифрования от выпадающего),
Предмет зашифрованного сообщения: **$subject**

- **Параметры настройки низкой степени серьезности**
  Действие, примененное к сообщения: **поставить**
  Включите шифрование (неконтролируемый)

Установите масштаб степеней серьезности ошибки

Снова, следующие параметры настройки являются хорошей отправной точкой, однако они - просто рекомендация для помощи вам и могут потребовать некоторой калибровки или параметров настройки альтернативной конфигурации на основе ваших организационных потребностей.

1. Направо от схемы масштаба степеней серьезности ошибки нажмите **Edit Scale**.
2. Двигайте первый маркер, пока НЕ ПРОИГНОРИРУЮТ = 0.
3. Двигайте второй маркер до НИЗКИЙ = 1 - 9.
4. Двигайте третий маркер до MEDIUM = 10 - 50.
5. Двигайте четвертый маркер до ВЫСОКИЙ = 60 - 89.
6. Если вы установили, это правильно, ВАЖНЫЙ будет автоматически установлено 90 - 100.
7. Нажмите **Done** по окончании.

Отправьте и передайте изменения

Для завершения создания этой политики нажмите **кнопку отправки** . Нажмите кнопку **Commit Changes** в верхнем правом углу GUI. Вы будете взяты на экран Uncommitted Changes, нажать **Commit Changes**. Необходимо видеть**, что Никакие изменения не ожидают** в верхнем правом углу GUI в случае успеха.

Последние шаги

Необходимо будет теперь включить политику DLP по Политике Исходящей почты под **Почтовой Политикой-> Политика Исходящей почты**. Для тестирования за пределами производства можно создать пользовательскую исходящую политику с собой, определял как отправителя, и включите политику DLP по этой тестовой политике.

Дополнительные сведения

- Устройство безопасности электронной почты Cisco - руководства пользователя
- Cisco Systems – техническая поддержка и документация