ESA испытывает сильный удар (NDR) Storm

Содержание

Введение

Этот документ описывает проблему, с которой встречаются, где ваш Email Security Appliance (ESA) испытывает шторм сильного удара и предлагает решение проблемы.

Общие сведения

Шторм сильного удара является побочным эффектом joe задания или обратным рассеянием почтового спама.

Джо Джоб

joe задание является атакой спама, которая использует поддельные данные отправителя и цели бросить тень на репутацию очевидного отправителя и/или побудить получателей принимать меры против очевидного отправителя.

Обратное рассеяние

Обратное рассеяние является побочным эффектом почтового спама, вирусов, и собирает червей, где почтовые серверы, которые получают спам и другие почтовые возвращенные сообщения передачи к невиновной стороне. Это происходит, потому что отправитель конверта исходного сообщения подделан для содержания адреса электронной почты жертвы. Так как эти сообщения не требовались получателями, существенно подобны друг другу и переданы в объемных количествах, они квалифицируют как незапрашиваемая объемная электронная почта или спам. Также, системы, которые генерируют почтовое обратное рассеяние, могут стать перечисленными на различных Черных списках Системы доменных имен (DNSBLs) и быть в нарушении Условий предоставления услуг интернет-провайдеров.

Проблема

Ваш ESA испытывает шторм сильного удара, где существует наводнение сообщений, введенных в ESA. Количество входящего соединения пронзает во время такой атаки. Устройство могло бы разработать резервную копию workqueue. Чтобы проверить, подвергается ли устройство такой атаке, grep, почта регистрирует для почты **От** адреса. Сильные удары (Неотчеты о доставке - NDR) имеют пустую почту конверта **От** адреса.

```
ironport.com> grep -e "From:" mail_logs
Mon Oct 20 14:40:55 2008 Info: MID 10 ICID 19 From: <>
Mon Oct 20 14:40:55 2008 Info: MID 11 ICID 19 From: <>
Mon Oct 20 14:40:55 2008 Info: MID 12 ICID 19 From: <>
```

Устройство, которое подвергается шторму сильного удара, будет иметь большинство сообщений с почтой конверта **От** адреса' **<>**'.

Решение

Существует много опций для управления штормом сильного удара.

Проверка сильного удара

Для борьбы с этими неверно направленными атаками сильного удара AsyncOS включает Проверку Сильного удара Cisco. Когда включено, эта функция помечает адрес Отправителя Конверта для сообщений, передаваемых через ESA. Получатель Конверта для любого возвращенного сообщения, полученного ESA, тогда проверен для присутствия этой метки. Когда легитимные возвращенные сообщения получены, метка, которая была добавлена к адресу Отправителя Конверта, удалена, и сильный удар отправлен получателю. Возвращенные сообщения, которые не содержат метку, могут быть обработаны отдельно.

AsyncOS рассматривает сильные удары как почту с пустой почтой **От** адреса (**<>**).

Сообщения, которые являются от адресов таким как mailer-daemon@example.com или postmaster@example.com, не считает сильными ударами система и не подвергаются Проверке Сильного удара.

Настройте ключи маркировки адреса проверки сильного удара

Адрес Проверки Сильного удара, Помечающий распечатку Ключей, показывает ваш текущий ключ и любые неочищенные ключи, которые вы использовали в прошлом. Для добавления нового ключа выполните эти шаги:

1. На странице **Mail Policies> Bounce Verification** нажмите **New Key**.
2. Введите текстовую строку и нажмите **Submit**.
3. Передайте свои изменения.

Удаление ключей

Если вы выбираете правило для удаления от ниспадающего меню и нажимаете **Purge,** можно удалить старые ключи маркировки адреса**.**

Настройте параметры настройки проверки сильного удара Cisco

Параметры настройки проверки сильного удара определяют, какие меры принять, когда получен недопустимый сильный удар.

- Выберите **Mail Policies> Bounce Verification**.
- **Нажмите кнопку Edit Settings (Изменить настройки).**
- Выберите, отклонить ли недопустимые сильные удары или добавить пользовательский заголовок к сообщению. Если вы хотите добавить заголовок, введите имя заголовка и значение.
- Дополнительно, включите умные исключения. Эта установка позволяет сообщениям входящей почты и возвращенным сообщениям, генерируемым внутренними серверами RADIUS быть автоматически освобожденными от обработки проверки сильного удара (даже когда одиночный слушатель используется для обеих входящей и исходящей почты).
- Отправьте и передайте свои изменения.

Настройте проверку сильного удара Cisco с CLI

Можно использовать **bvconfig** и **destconfig** команды в CLI для настройки проверки сильного удара. Эти команды обсуждены в справочном руководстве по интерфейсу CLI Cisco AsyncOS.

Проверка сильного удара Cisco и конфигурация кластера

Проверка сильного удара работает в конфигурации кластера, пока оба устройства Cisco используют тот же "ключ сильного удара". При использовании того же ключа любая система должна быть в состоянии принять легитимный bounceback. Модифицированная метка/ключ заголовка не является определенной для каждого устройства Cisco.

Почтовый фильтр

Если вы не можете использовать Проверку Сильного удара, потому что вы используете отдельные устройства для получения и доставки, можно установить фильтр сообщения, чтобы к групповым сообщениям, которые имеют пустую почту **От** адреса.

Почтовый блок

Так как эти возвращенные сообщения будут, скорее всего, иметь несуществующий адрес получателя конверта, можно заблокировать недопустимые адреса через проверку получателя Протокола LDAP диалога, чтобы помочь понижать влияние таких сообщений.