

Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Как вы анализируете неустойчивые проблемы доставки почты на ESA?](#)

Введение

Этот документ описывает, как проанализировать неустойчивые проблемы доставки почты на Cisco Email Security Appliance (ESA).

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- ESA Cisco
- AsyncOS

Используемые компоненты

Сведения в этом документе основываются на всех версиях AsyncOS.

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.

Как вы анализируете неустойчивые проблемы доставки почты на ESA?

Можно использовать Инъекционные Журналы Отладки для отслеживания всего диалога Протокола SMTP между ESA и входящим подключением к серверу. Каждая линия в Инъекционных Журналах Отладки выделяет данные, которые переданы и получены во

время диалога SMTP.

Выполните эти шаги для включения Инжекционных Журналов Отладки с GUI:

1. Перейдите к **Администрированию системы > Регистрационные Подписки на GUI**.
2. Выберите **подписку журнала Add....**
3. В поле Log Type выберите **Injection Debug Logs** и введите соответствующие данные.

Вот некоторые важные факторы при вводе Инжекционных Журналов Отладки data:

- Адреса CIDR, такие как **10.1.1.0/24**, разрешены.
- Диапазоны IP-адресов, такой как **10.1.1.10-20**, разрешены.
- IP-подсети, такой как **10.2.3**, разрешены.
- Имена хоста и подстановочные знаки, такие как **сгм. пример. com**, разрешены (но не **example.com**).
- Подстановочные знаки должны быть выражены как **example.com** (без звездочки).
- При отслеживании входящей электронной почты имя хоста должно совпасть с хостом отправителя.
- При отслеживании исходящей электронной почты имя хоста должно совпасть с названием (названиями) внутреннего хоста.
- Количество сеансов SMTP должно быть между один и 25.

Выполните эти шаги для включения Инжекционных Журналов Отладки с CLI:

1. Введите **logconfig> новая** команда в CLI.
2. Выберите **Injection Debug Logs**.
3. Введите имя для журнала, такого как **debugging_example**.
4. Введите имя хоста, IP-адрес или блок IP-адресов, для которых вы хотите сделать запись инжекционной отладочной информации, такой как **mail1. пример. com**.
5. Введите номер сеансов SMTP, которых вы хотите сделать запись для этого домена. Гарантируйте, что значение между один и 25.
6. Введите метод, который вы хотите использовать для получения журналов, таких как **Опрос FTP**.

7. Введите имя файла. При необходимости можно использовать имя файла по умолчанию.

8. Выберите настройки по умолчанию, которые остаются.

Когда ESA принимает почту от сервера, данный пример показывает Инжекционные Журналы Отладки.

Примечание: Инжекционные Журналы Отладки и Доменные Журналы Отладки подобны mail_logs, таким образом, можно использовать **grep** и **хвостовые команды**.

```
Sent to '10.251.21.203': '220 ironportappliance ESMTTP\r\n'
Rcvd from '10.251.21.203': 'EHLO outgoing.example.com\r\n'
Sent to '10.251.21.203': '250-nibbles.run\r\n250-8BITMIME\r\n250
SIZE 104857600\r\n'
Rcvd from '10.251.21.203': 'MAIL FROM:<jsmith@example.com>\r\n'
Sent to '10.251.21.203': '250 sender <jsmith@example.com> ok\r\n'
Rcvd from '10.251.21.203': 'RCPT TO:<test@example.org>\r\n'
Sent to '10.251.21.203': '250 recipient <test@example.org>ok\r\n'
Rcvd from '10.251.21.203': 'DATA\r\n'
Sent to '10.251.21.203': '354 go ahead\r\n'
Rcvd from '10.251.21.203': 'To: "test@example.org" <test@example.org>
\r\nSubject: 12:14pm - test\r\nFrom: Hotel_Users <jsmith@example.com>
\r\nContent-Type: text/plain; format=flowed; delp=yes;
charset=iso-8859-15\r\nMIME-Version: 1.0\r\nContent-Transfer-Encoding:
7bit\r\nDate: Tue, 09 Jan 2007 12:14:35 -0800\r\nMessage-ID:
<op.tlwk6lvgwomlp4@outgoing.example.com>\r\nUser-Agent: Opera Mail/9.10
(Win32)\r\n\r\ntest\r\n'
Rcvd from '10.251.21.203': '\r\n.\r\n'
Sent to '10.251.21.203': '250 ok: Message 270 accepted\r\n'
Rcvd from '10.251.21.203': 'QUIT\r\n'
Sent to '10.251.21.203': '221 nibbles.run\r\n'
```