Содержание

Введение

Этот документ описывает, как решить неустойчивые проблемы и прерванные соединения во время получения и доставки почты.

Предварительные условия

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Обмен через закрытый Интернет (PIX) Cisco или версия 7.x Устройства адаптивной защиты (ASA) и выше
- Cisco Email Security Appliance (ESA)

Общие сведения

Шлюзы электронной почты ESA Cisco являются по сути почтовыми межсетевыми экранами. Это инвертирует потребность в восходящем межсетевом экране, таком как PIX Cisco или ASA, для осмотра почтового трафика к и от ESA. Предложено отключить опции Контроля приложения Расширенной версии простого протокола передачи электронной почты (ESMTP) на межсетевом экране для любых адресов узла устройства безопасности. По умолчанию контроль протокола ESMTP включен для всех соединений, которые проходят через межсетевые экраны Cisco. Это означает, что все команды, выполненные между почтовыми шлюзами через порт TCP 25, а также отдельные заголовки сообщения, проанализированы для соблюдения строго спецификаций Запроса на комментарий (RFC), которые включают 821 RFC, 1123, и 1870. Существуют определенные значения по умолчанию для максимального числа получателей и размеров сообщения, которые могли бы вызвать проблемы с доставкой к и от вашего ESA. Эти определенные настройки по умолчанию конфигурации выделены здесь (взятый от Средства поиска команд Command Lookup Tool Cisco).

Команда inspect esmtp включает функциональность, ранее предоставленную командой **smtp**

устройства, и предоставляет дополнительную поддержку для некоторых команд ESMTP. Контроль приложения ESMTP добавляет поддержку восьми команд ESMTP, включая AUTH, ЭХЛО, ETRN, СПРАВКА, SAML, ПЕРЕДАЕТ, SOML и VRFY. Наряду с поддержкой семи RFC 821 команда (ДАННЫЕ, HELO, ПОЧТА, NOOP, УШЛА, RCPT, RSET), устройство безопасности поддерживает в общей сложности 15 команд SMTP. Другие команды ESMTP, такие как ATRN, STARTLS, ONEX, VERB, РАЗДЕЛЕНИЕ НА БЛОКИ и частные расширения и не поддерживаются. Неподдерживаемые команды преобразованы в Xs, которые отклонены внутренним сервером. Это приводит к сообщению, такому как 500 неизвестных Команд: XXX. От неполных команд сбрасывают.

Команда inspect esmtp изменяет символы в сообщении SMTP сервера к звездочкам за исключением "2", "0", "0" символы. Возврат каретки (CR) и символы (LF) перевода строки проигнорированы. С включенной проверкой SMTP сеанс, используемый для интерактивного SMTP, ждет допустимой команды, и межсетевой экран esmtp механизм состояний поддерживает корректные состояния для сеанса, если не наблюдаются эти правила:

- Команды SMTP должны составить по крайней мере четыре символа в длине.
- Команды SMTP должны быть завершены с возвратом каретки и переводом строки.
- Команды SMTP должны ждать ответа прежде, чем выполнить следующий ответ.

Сервер SMTP отвечает на запросы клиента с числовыми кодами ответа и дополнительными человекочитаемыми строками. Контроль приложения SMTP управляет и уменьшает команды, которые пользователь может использовать, а также сообщения, что возвращается сервер. Проверка SMTP выполняет три основных задачи:

- Ограничивает запросы SMTP семью основными командами SMTP и восемью расширенными командами.
- Контролирует последовательность отклика команды SMTP.
- Генерирует след аудита. Когда недопустимый символ, встроенный в почтовый адрес, заменен, Запись журнала аудита 108002 генерируется. Для получения дополнительной информации посмотрите RFC 821.

Проверка SMTP контролирует последовательность команды и ответа для следующих аномальных подписей:

- Усеченные команды.
- Неправильное завершение команды (не завершенный с <CR> <LR>).
- . Если Интерфейс PHY для PCI Express (КАНАЛ), которым подпись найдена в качестве параметра к ПОЧТЕ от или RCPT для управления, сеанс закрыт, это не конфигурируемо пользователем.
- Неожиданный переход сервером SMTP.
- Для неизвестных команд устройство безопасности изменяет все символы в пакете к X. В этом случае сервер будет генерировать код ошибки клиенту. Из-за изменения в пакете контрольная сумма TCP должна быть повторно вычислена или отрегулирована.
- Потоковое редактирование TCP.

Выходные данные show service-policy осматривают ESMTP, предоставляет инспекционные значения по умолчанию и их соответствующие действия.

```
Global policy:
Service-policy: global_policy
Class-map: inspection_default
Inspect: esmtp _default_esmtp_map, packet 104468, drop 0, reset-drop 0
mask-banner, count 639 obfuscate the SMTP banner greeting
```

```
match cmd line length gt 512 deny all SMTP commands (and close connection)
drop-connection log, packet 0
match cmd RCPT count gt 100 drop all messages (and connection) with more
than 100 recipients
drop-connection log, packet 0
match body line length gt 998 log all messages with lines > 998 chars
log, packet 0
match header line length gt 998 drop all messages (and connection)
with headers > 998 chars
drop-connection log, packet 41
match sender-address length gt 320 drop all messages (and connection) with
envelope sender > 320 bytes
drop-connection log, packet 0
match MIME filename length gt 255 drop all messages (and connection) with
MIME attachment filenames > 255 bytes
drop-connection log, packet 0
match ehlo-reply-parameter others obfuscate extended commands not explicitly
noted in the RFCs (such as STARTTLS)
mask, packet 2555
```

Проблема

Иногда, сообщения будут не в состоянии быть правильно переданными или полученными ESA Cisco. Один или больше этих сообщений замечены в устройстве ESA Cisco mail_logs:

- Передайте прерванный MID XXX
- Получение прерванного ICID 21916 проиграло
- ICID 21916 близко
- Ошибка подключения: DCID: XXX domain:example.com IP: 10.1.2.3 порта: 25 подробных данных: [Ошибка 60]
  Операция вызвала таймаут интерфейса: 10.10.10.1 причин: ошибка сети

Решение

Некоторые из этих настроек по умолчанию могли повлиять на вещи как предоставление зашифрованных сообщений Transport Layer Security (TLS), кампании списка рассылки и устранение проблем. Лучшая политика могла бы сделать, чтобы вы использовали межсетевой экран для осмотра всего остающегося почтового трафика, который сначала не проходит через устройство безопасности при освобождении всего трафика, который имеет. Данный пример иллюстрирует, как настроить конфигурацию по умолчанию (обращенный внимание ранее) для освобождения Контроля приложения ESMTP для одиночного адреса узла безопасности.

Можно определить весь трафик к и от внутреннего адреса ESA Cisco для ссылки в class-map Модульной системы политик (MPF):

```
Global policy:
Service-policy: global_policy
Class-map: inspection_default
Inspect: esmtp _default_esmtp_map, packet 104468, drop 0, reset-drop 0
mask-banner, count 639 obfuscate the SMTP banner greeting
match cmd line length gt 512 deny all SMTP commands (and close connection)
```

```
drop-connection log, packet 0
match cmd RCPT count gt 100 drop all messages (and connection) with more
than 100 recipients
drop-connection log, packet 0
match body line length gt 998 log all messages with lines > 998 chars
log, packet 0
match header line length gt 998 drop all messages (and connection)
with headers > 998 chars
drop-connection log, packet 41
match sender-address length gt 320 drop all messages (and connection) with
envelope sender > 320 bytes
drop-connection log, packet 0
match MIME filename length gt 255 drop all messages (and connection) with
MIME attachment filenames > 255 bytes
drop-connection log, packet 0
match ehlo-reply-parameter others obfuscate extended commands not explicitly
noted in the RFCs (such as STARTTLS)
mask, packet 2555
```

Это создает новый class-map, чтобы в частности совпасть или выбрать трафик, который будет рассматриваться по-другому:

```
Global policy:
Service-policy: global_policy
Class-map: inspection_default
Inspect: esmtp _default_esmtp_map, packet 104468, drop 0, reset-drop 0
mask-banner, count 639 obfuscate the SMTP banner greeting
match cmd line length gt 512 deny all SMTP commands (and close connection)
drop-connection log, packet 0
match cmd RCPT count gt 100 drop all messages (and connection) with more
than 100 recipients
drop-connection log, packet 0
match body line length gt 998 log all messages with lines > 998 chars
log, packet 0
match header line length gt 998 drop all messages (and connection)
with headers > 998 chars
drop-connection log, packet 41
match sender-address length gt 320 drop all messages (and connection) with
envelope sender > 320 bytes
drop-connection log, packet 0
match MIME filename length gt 255 drop all messages (and connection) with
MIME attachment filenames > 255 bytes
drop-connection log, packet 0
match ehlo-reply-parameter others obfuscate extended commands not explicitly
noted in the RFCs (such as STARTTLS)
mask, packet 2555
```

Этот раздел связывает новый class-map Cisco и отключает опции контроля протокола ESMTP:

```
Global policy:
Service-policy: global_policy
Class-map: inspection_default
Inspect: esmtp _default_esmtp_map, packet 104468, drop 0, reset-drop 0
mask-banner, count 639 obfuscate the SMTP banner greeting
match cmd line length gt 512 deny all SMTP commands (and close connection)
drop-connection log, packet 0
match cmd RCPT count gt 100 drop all messages (and connection) with more
than 100 recipients
drop-connection log, packet 0
match body line length gt 998 log all messages with lines > 998 chars
log, packet 0
match header line length gt 998 drop all messages (and connection)
with headers > 998 chars
```

```
drop-connection log, packet 41
match sender-address length gt 320 drop all messages (and connection) with
envelope sender > 320 bytes
drop-connection log, packet 0
match MIME filename length gt 255 drop all messages (and connection) with
MIME attachment filenames > 255 bytes
drop-connection log, packet 0
match ehlo-reply-parameter others obfuscate extended commands not explicitly
noted in the RFCs (such as STARTTLS)
mask, packet 2555
```

Также обратите внимание на оператор переадресации, который может помочь управлять количеством поступления и полуоткрытых (начальных) соединений с адресом. Это полезно для борьбы с атаками "отказ в обслуживании" (DoS), но может вмешаться в скорости доставки.

Формат для запаздывания параметров команд NAT и STATIC... [tcp (max_conns)] [max_embryonic].
Данный пример задает пределы 50 общих TCP - подключений и 100 полуоткрытых или попыток неустановившегося соединения:

```
Global policy:
Service-policy: global_policy
Class-map: inspection_default
Inspect: esmtp _default_esmtp_map, packet 104468, drop 0, reset-drop 0
mask-banner, count 639 obfuscate the SMTP banner greeting
match cmd line length gt 512 deny all SMTP commands (and close connection)
drop-connection log, packet 0
match cmd RCPT count gt 100 drop all messages (and connection) with more
than 100 recipients
drop-connection log, packet 0
match body line length gt 998 log all messages with lines > 998 chars
log, packet 0
match header line length gt 998 drop all messages (and connection)
with headers > 998 chars
drop-connection log, packet 41
match sender-address length gt 320 drop all messages (and connection) with
envelope sender > 320 bytes
drop-connection log, packet 0
match MIME filename length gt 255 drop all messages (and connection) with
MIME attachment filenames > 255 bytes
drop-connection log, packet 0
match ehlo-reply-parameter others obfuscate extended commands not explicitly
noted in the RFCs (such as STARTTLS)
mask, packet 2555
```