



ID документа: 118735

Обновлено: 10 февраля 2015

Внесенный встроенным самоконтролем Sumit, специалистом службы технической поддержки Cisco.



[PDF загрузки](#)



[Печать](#)

[\[+\] Feedback](#)

Родственные продукты

- [Безопасность](#)
- [Cisco Catalyst 6500 Series Firewall Services Module](#)

Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Общие сведения](#)

[Проблема](#)

[Условия](#)

[Проверка](#)

[Решение](#)

[Дополнительные сведения](#)

[Связанные обсуждения Сообщества Cisco Support](#)

Введение

Этот документ описывает определенную проблему с неустойчивыми отбрасываниями трафика на Модуле Сервисов межсетевых экранов (FWSM) после обновления программного обеспечения к Выпуску 4.1.11 или позже.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Сведения в этом документе основываются на FWSM с Выпуском ПО 4.1 (11) или позже.

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.

Общие сведения

Согласно поведению FWSM, если вы используете TCP в качестве транспортного протокола регистрации для передачи сообщений к серверу системного журнала, он запрещает новые соединения как измерения безопасности, если FWSM неспособен достигнуть сервера системного журнала. Можно использовать команду **разрешения-hostdown на регистрацию** для удаления этого ограничения.

Проблема

Существует неустойчивая проблема отбрасывания трафика на FWSM после обновления к Выпуску 4.1.11 или позже. FWSM начинает запрещать все новые соединения.

Самое значимое отбрасывание трафика для Протокола ICMP, так как каждый Эхо-запрос протокола ICMP рассматривается как новое соединение. Подключение восстановлено, как только TCP - подключение к серверу системного журнала успешен.

Для Выпуска 4.1.11 FWSM или позже, если на основе TCP сервер системного журнала не достижим даже с политикой "разрешения-hostdown", FWSM запрещает все новые соединения. "Функция" разрешения-hostdown на регистрацию больше не работает после обновления FWSM к Выпуску 4.1.11 или позже.

FWSM продолжает повторно соединяться с сервером системного журнала TCP каждую минуту, пока временной сервер не подключен. Таким образом, одиночное квитирование TCP - подключения результаты отказа в простое минимальной одной минуты для всех **новых соединений**, потому что FWSM пытается связаться с сервером системного журнала TCP снова, только после одной минуты.

Условия

- FWSM выполняет Выпуск 4.1.11 или позже.
- FWSM должен быть в одном режиме.
- Сервер системного журнала TCP должен быть недостижимым от FWSM.

Проверка

Для определения этого поведения проверьте медленный путь (NP3) статистика. Если на основе TCP сервер системного журнала не достижим, даже с политикой "разрешения-hostdown", Запрещение Ведет (Состояние Коннектикута) встречные увеличения.

```
pri/act# show clock
09:31:55.070 GMT Thu May 15 2014
```

```
pri/act# show np3 stats | ex : 0
<<NP 3 stats>>
Discard Statistics
-----
```

```
Egress Discards : 34412
ACL Denied Packets : 157
Rev Route Lkup Fail : 202
Self Route Packets : 40
Deny Conns (Conn State): 34013 <-----Counter to monitor
```

```
pri/act# show clock
09:32:06.020 GMT Thu May 15 2014
```

```
pri/act# show np3 stats | ex : 0
<<NP 3 stats>>
Discard Statistics
-----
```

```
Egress Discards : 46634
ACL Denied Packets : 157
Rev Route Lkup Fail : 202
Self Route Packets : 40
Deny Conns (Conn State): 46235 <-----Counter seen increasing
```

Решение

Дефект был подан для отслеживания этой проблемы, но это не будет исправлено, так как FWSM достиг конца даты Релиза сопровождающего ПО.

[Окончание продаж и уведомление об окончании срока службы для модулей сервисов межсетевого экрана](#)

Для устранения этой проблемы измените конфигурацию сервера регистрации на транспорт UDP.

```
pri/act# show clock
09:31:55.070 GMT Thu May 15 2014
```

```
pri/act# show np3 stats | ex : 0
<<NP 3 stats>>
Discard Statistics
-----
```

```
Egress Discards : 34412
ACL Denied Packets : 157
Rev Route Lkup Fail : 202
Self Route Packets : 40
Deny Conns (Conn State): 34013 <-----Counter to monitor
```

```
pri/act# show clock
09:32:06.020 GMT Thu May 15 2014
```

```
pri/act# show np3 stats | ex : 0
<<NP 3 stats>>
Discard Statistics
-----
Egress Discards : 46634
ACL Denied Packets : 157
Rev Route Lkup Fail : 202
Self Route Packets : 40
Deny Conns (Conn State): 46235 <-----Counter seen increasing
```

Дополнительные сведения

- [Справочник по командам: регистрация разрешения-hostdown](#)
- [Справочник по командам: logging host #.#.#.#](#)
- [Cisco Systems – техническая поддержка и документация](#)

Действительно ли этот документ был полезен? [Да](#) [Нет](#)

Спасибо за ваш отзыв.

[Адресовать вопрос техподдержке \(требуется контракт сервиса Cisco.🔒\)](#)

Связанные обсуждения Сообщества Cisco Support

[Сообщество Cisco Support](#) является форумом для вас, чтобы спросить и ответить на вопросы, общие предложения, и сотрудничать с вашими узлами.

См. [Cisco Technical Tips Conventions](#) для получения информации об условных обозначениях, используемых в этом документе.

Обновлено: 10 февраля 2015

ID документа: 118735