Решите общие проблемы GETVPN

Содержание

Введение

Этот документ описывает, какие отладки собрать для большей части общей Группы Зашифрованная Транспортная VPN (GETVPN) выполняет.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- GETVPN
- Использование сервера системного журнала

Используемые компоненты

Настоящий документ не имеет жесткой привязки к каким-либо конкретным версиям программного обеспечения и оборудования.

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 - средства устранения проблем GETVPN

GETVPN предоставляет обширный набор средств устранения проблем для упрощения процесса устранения неполадок. Важно понять, какое из этих программных средств доступно, и когда они являются соответствующими каждой задаче по устранению проблем. При устранении проблем это всегда - хорошая идея запуститься с наименее навязчивых методов, так, чтобы негативно не влияли на производственную среду. Для помощи тому процессу этот раздел описывает некоторые обычно используемые доступные программные средства:

Средства отладки уровня управления

Команды "show"

Команды показа обычно используются для показа операций во время выполнения в среде GETVPN.

Системные журналы

GETVPN имеет расширенный набор сообщений системного журнала для значительных событий протокола и состояний ошибки. Это должно всегда быть первым местом для взгляда перед выполнением любых отладок.

Трассировка события домена группы интерпретации (GDOI)

Эта опция была добавлена в Версии 15.1 (3) T. Трассировка события предлагает легкому весу, постоянному отслеживанию для значительных событий GDOI и ошибок. Существует также отслеживание выходного пути с обратной трассировкой, включенной для условий исключений.

Условные отладки GDOI

Эта опция была добавлена в Версии 15.1 (3) T. Это позволяет фильтруемые отладки для данного устройства на основе адреса партнера (peer) и должно всегда использоваться, если это возможно, особенно на Сервере ключей.

Крипто-глобальный и отладки GDOI

Это все различные отладки GETVPM. Admin должны проявить осмотрительность при отладке в крупномасштабных средах. С отладками GDOI пять уровней отладки предоставлены для дальнейшей глубины детализации отладки:

```
GM1#debug crypto gdoi gm rekey ?
all-levels All levels
detail Detail level
error Error level
event Event level
packet Packet level
terse Terse level
```

Уровень	Что вы получите

отладки	
Ошибка	Состояния ошибки
Краткий	Важные сообщения пользователю и проблемам протокола
Событие	Изменения состояния и события те, которые передают и получают, повторно вводят
Подробность	Самая подробная информация о сообщении отладки
Пакет	Включает дамп подробных сведений о пакете
Все	Все вышеупомянутые

Средства отладки плоскости данных

Вот некоторые средства отладки плоскости данных:

- Списки доступа
- Учет приоритета IP-трафика
- Netflow
- Счетчики интерфейса
- Крипто-счетчики
- Технология CEF IP глобальные и счетчики сбросов на функцию
- Встроенная функция захвата пакетов (EPC)
- Отладки Плоскости данных (пакет IP и отладки CEF)

Устранение неполадок

Подготовка к средству регистрации и другие оптимальные методы

Прежде чем вы начнете устранять неполадки, гарантировать подготовку средства регистрации, как описано здесь. Некоторые оптимальные методы также перечислены здесь:

- Проверьте количество свободной памяти маршрутизатора и настройте **отладку буферированной регистрации** к большому значению (10 МБ или больше если возможный).

- Отключите регистрацию к консоли, монитору и серверам системного журнала.

- Получите содержание буфера журнала с **командой show log** через определенные промежутки времени, каждые 20 минут к часу, для предотвращения регистрационной потери, подлежащей выплате буферизовать повторное использование.

- Что бы ни случилось, введите **команду show tech** от Элементов группы, на которые влияют (GMS) и Серверы ключей (KSs), и исследуйте выходные данные **команды show ip route** в глобальном и каждой Виртуальной маршрутизации и Передаче включенный (VRF), если кто-либо требуется.

- Используйте Протокол NTP для синхронизации часов между всеми устройствами, которые отлажены. Включите миллисекунду (msec) метки времени и для отладки и для сообщений журнала:
```
GM1#debug crypto gdoi gm rekey ?
all-levels All levels
detail Detail level
error Error level
event Event level
packet Packet level
terse Terse level
```

- Удостоверьтесь, что к выходным данным команды show добавляют метку времени.
```
Router#terminal exec prompt timestamp
```

- Когда вы собираете выходные данные команды show для событий уровня управления или счетчиков плоскости данных, всегда собираете несколько повторений тех же выходных данных.

Установление IKE устранения неполадок

Когда процесс регистрации сначала начинается, GMS и KSs выполняют согласование о Сеансах Протокола IKE для защиты трафика GDOI.

- На GM проверьте, что успешно установлен IKE:
```
gm1#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst src state conn-id status
172.16.1.9 172.16.1.1 GDOI_REKEY 1068 ACTIVE
172.16.1.1 172.16.1.9 GDOI_IDLE 1067 ACTIVE
```
Примечание: Состояние GDOI_IDLE, которое является ядром регистрации, испытывает таймаут быстро и исчезает, потому что это не необходимо больше после начальной регистрации.

- На KS необходимо видеть:
```
ks1#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst src state conn-id status
172.16.1.1 172.16.1.9 GDOI_IDLE 1001 ACTIVE
```
Примечание: Повторно вводить сеанс только появляется при необходимости на KS.

Выполните эти шаги, если вы не достигаете того состояния:

- Для понимания о причине сбоя проверьте выходные данные от этой команды: `router# show crypto isakmp statistics`

- Если предыдущий шаг не полезен, можно получить понимание на уровне протокола при включении обычных отладок IKE: `router# debug crypto isakmp`**Примечания:**
  * Даже при том, что IKE используется, он не используется на обычном порту UDP/500, а скорее на UDP/848.
  * При обнаружении с проблемой на этом уровне предоставьте отладки и для KS и для GM, на который влияют.

- Из-за зависимости от вздохов Ривест-Шамир-Адлемена (RSA) для группы повторно вводит, KS **нужно** было настроить ключ RSA, и это должно иметь то же название как то, заданное в конфигурации группы.

  Для проверки этого введите эту команду:

  ```
  ks1# show crypto key mypubkey rsa
  ```

Устраните неполадки начальной регистрации

На GM, для проверки состояния регистрации, исследуют выходные данные этой команды:

```
gm1# show crypto gdoi | i Registration status
Registration status  : Registered
gm1#
```

Если выходные данные указывают на что-нибудь кроме **Зарегистрированного**, введите эти команды:

На GMS:

- Завершите работу крипто-поддерживающих интерфейсов.
  Внимание. : Ожидается, что включают управлению при нестандартном подключении.

- Включите эти отладки:
  ```
  gm1# debug crypto gdoi infra packet
  gm1# debug crypto gdoi gm packet
  ```

- Включите отладки на стороне KS (см. следующий раздел).

- Когда отладки KS являются готовыми, незакрытыми крипто-поддерживающими интерфейсами и ждут регистрации (чтобы ускорить процесс, выполнить **команду clear crypto gdoi** на GM).

На KSs:

- Проверьте, что присутствие RSA включает KS:
  ```
  ks1# show crypto key mypubkey rsa
  ```

- Включите эти отладки:
  ```
  ks1# debug crypto gdoi infra packet
  ks1# debug crypto gdoi ks packet
  ```

Решите связанные с политикой проблемы

Проблема политики происходит ДО регистрации (Отнесенный к близкой к сбою политике)

Эта проблема только влияет на GMS, поэтому соберите эти выходные данные от GM:

```
gm1# show crypto ruleset
```

> **Примечание:** В Cisco IOS XE?, эти выходные данные всегда пусты начиная с классификации пакетов в не сделанный в программном обеспечении.

Выходные данные **команды show tech** от устройства, на которое влияют, предоставляют остаток необходимой информации.

Проблема политики Происходит Пострегистрация и Принадлежит Глобальной политике, которая Выдвинута

Обычно существует два способа, которыми проявляет эта проблема:

- KS не может выдвинуть политику к GM.
- Существует частичное приложение политики среди GMS.

Чтобы помочь решать любую проблему, выполните эти шаги:

1. На GM, на который влияют соберите эти выходные данные:
   ```
   gm1# show crypto gdoi acl
   gm1# show crypto ruleset
   ```

2. Включите эти отладки на GM:
   ```
   gm1# debug crypto gdoi infra packet
   gm1# debug crypto gdoi gm acls packet
   ```

3. На KS, к который регистры GM, на которые влияют, соберите эти выходные данные:
   ```
   ks1# show crypto gdoi ks members
   ks1# show crypto gdoi ks policy
   ```

   > **Примечание:** Для определения, с каким KS GM соединяется, введите команду **группы show crypto gdoi**.

4. На том же KS включите эти отладки:
   ```
   ks1# debug crypto gdoi infra packet
   ks1# debug crypto gdoi ks acls packet
   ```

5. Вынудите GM зарегистрироваться в этой команде на GM:
   ```
   clear crypto gdoi
   ```

Проблема политики происходит пострегистрация и принадлежит слиянию глобальной политики и локальных замен

Эта проблема обычно проявляет себя в форме сообщений, которые указывают, что зашифрованный пакет был получен, для которого локальная политика указывает, что это, как предполагается, не зашифровано и наоборот. Все данные, запрошенные в предыдущем разделе и выходных данных **команды show tech**, требуются в этом случае.

Устранение неполадок повторно вводит проблемы

На GMS:

- Соберите эти отладки:
```
gm1# debug crypto gdoi infra packet
gm1# debug crypto gdoi gm packet
gm1# debug crypto gdoi gm rekey packet
```

- Введите эту команду, чтобы проверить, что GM все еще имеет Сопоставление безопасности (SA) IKE типа GDOI_REKEY:
```
gm1# show crypto isakmp sa
```

На KSs:

- Соберите выходные данные **команды show crypto key mypubkey rsa** от **EACH** KS. Ключи, как ожидают, будут **идентичны**.

- Введите эти отладки для просмотра то, что происходит на KS:
```
ks1# debug crypto gdoi infra packet
ks1# debug crypto gdoi ks packet
ks1# debug crypto gdoi ks rekey packet
```

Устраните неполадки Синхронизируемого антивоспроизведения (TBAR)

Функция TBAR требует хронометража через группы, и поэтому требует, чтобы постоянно повторно синхронизировались псевдотаймеры GMS. Это выполнено во время, повторно вводят или каждые два часа, какой бы ни на первом месте.

> **Примечание:** Все выходные данные и отладки должны быть собраны в то же время и от GMS и от KS так, чтобы они могли быть коррелированы соответственно.

Для исследования проблем, которые происходят на этом уровне, собирают эти выходные данные.

- На GMS:
  ```
  gm1# show crypto gdoi
  gm1# show crypto gdoi replay
  ```

- На KS:
  ```
  ks1# show crypto gdoi ks members
  ks1# show crypto gdoi ks replay
  ```

Для исследования хронометража TBAR большим количеством динамического способа включите эти отладки:

- На GM:
  ```
  gm1# debug crypto gdoi gm rekey packet
  gm1# debug crypto gdoi replay packet (verbosity might need to be lowered)
  ```

- На KS:
  ```
  ks1# debug crypto gdoi ks rekey packet
  ks1# debug crypto gdoi replay packet (verbosity might need to be lowered)
  ```

С Версии IOS 15.2 (3) T Cisoc была добавлена способность сделать запись ошибок TBAR, который упрощает определять эти ошибки. На GM используйте эту команду, чтобы проверить, существуют ли какие-либо ошибки TBAR:

```
R103-GM#show crypto gdoi gm replay
Anti-replay Information For Group GETVPN:
 Timebased Replay:
   Replay Value            : 512.11 secs
   Input Packets           : 0       Output Packets          : 0
   Input Error Packets   : 0       Output Error Packets  : 0
   Time Sync Error     : 0       Max time delta       : 0.00secs

TBAR Error History (sampled at 10pak/min):
   No TBAR errors detected
```

Для получения дополнительной информации о том, как решить проблемы TBAR, обратитесь ко Времени Базирующийся Сбой Антивоспроизведения.

Устраните неполадки резервирования KS

Кооператив (COOP) устанавливает сеанс IKE для защиты interKSs связи, таким образом, методика поиска и устранения проблем, ранее описанная для установления IKE , применима здесь также.

СПЕЦИФИЧНОЕ ДЛЯ COOP устранение проблем включает выходные проверки этой команды на всем включенном KSs:

```
ks# show crypto gdoi ks coop
```

> **Примечание:** Наиболее распространенная ошибка, сделанная с развертываниями COOP KSs, состоит в том, чтобы забыть импортировать тот же ключ RSA (и частный и общий) для группы на всем KSs. Это вызывает проблемы во время, повторно вводит. Чтобы проверить и сравнить открытые ключи среди KSs, сравнивает выходные данные **команды show crypto key mypubkey rsa** от каждого KS.

Если устранение проблем на уровне протокола требуется, включите эту отладку на всем включенном KSs:

```
ks# debug crypto gdoi ks coop packet
```

Часто задаваемые вопросы

Почему вы видите, что это сообщение об ошибках "% Устанавливает отклоненного rekey authentication"?

Вы видите это сообщение об ошибках при настройке KS после того, как добавлена эта линия:

```
ks# debug crypto gdoi ks coop packet
```

Причина для этого сообщения об ошибках обычно в том состоит, потому что не существует маркированный GETVPN_KEYS ключа. Для решения проблемы этого создайте ключ с корректной меткой с помощью команды:

```
ks# debug crypto gdoi ks coop packet
```

> **Примечание:** Добавьте экспортное ключевое слово в конце, если это - развертывания COOP, и затем импортируйте тот же ключ в другом KS

Может маршрутизатор, настроенный, поскольку KS для одной группы GETVPN также функционируют как GM для той же группы?

Нет. Все развертывания GETVPN требуют специализированного KS, который не может участвовать как GM для тех же групп. Эта функция не поддерживается, потому что, добавляя функциональность GM к KS со всеми возможными взаимодействиями как шифрование, маршрутизация, QoS, и т.д., не оптимально для состояния этого решающего сетевого устройства. Это должно быть доступный в любом случае для всех развертываний GETVPN для работы.

Дополнительные сведения

- Группа зашифрованная транспортная VPN (VPN GET) - Cisco Systems
- Cisco Systems – техническая поддержка и документация