Руководство устранения неполадок GETVPN

Содержание

Введение

Этот документ предназначен для представления структурированной методики устранения проблем и полезных инструментов, чтобы помочь определять и изолировать Группу Зашифрованная Транспортная VPN (GETVPN) проблемы и предоставлять возможные решения.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- GETVPN
  [Официальное руководство по конфигурации GETVPN](#)
  [Официальное руководство по проектированию и вводу в эксплуатацию 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.

Методика устранения проблем GETVPN

Как с большей частью устранения проблем проблем сложной технологии, ключ должен быть в состоянии изолировать проблему к определенной функции, подсистеме или компоненту. Решение GETVPN состоит из многих компонентов функции в частности:

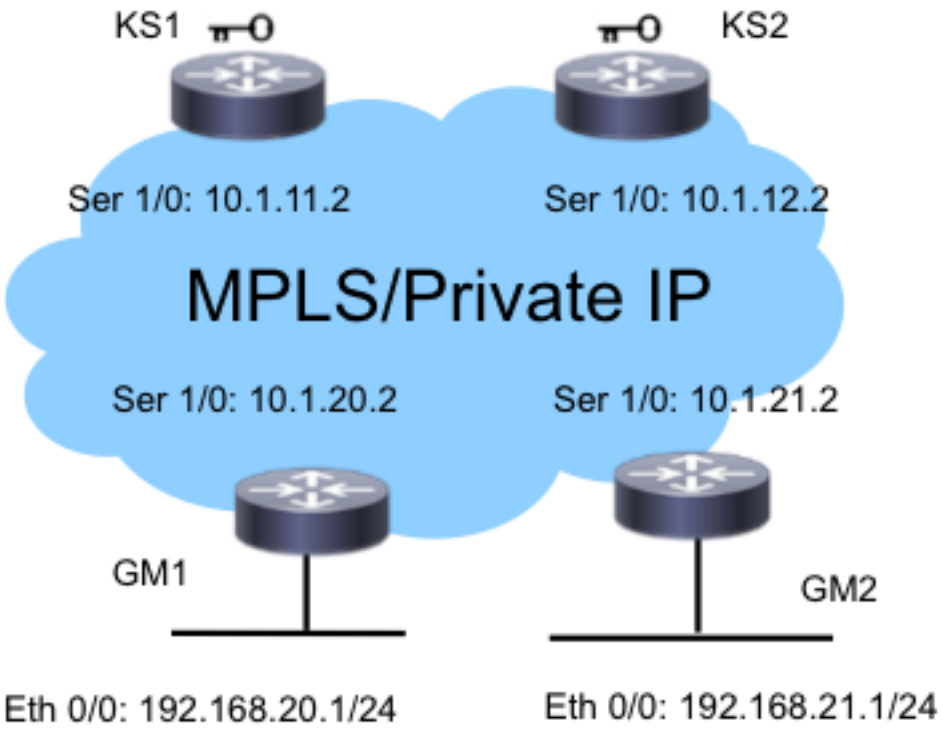
- Протокол IKE - Используемый между Элементом группы (GM) и Сервером ключей (KS), и среди Совместного Протокола (COOP) KSs, чтобы аутентифицировать и защитить Уровень управления.
- Домен группы интерпретации (GDOI) - Протокол использовал для KS, чтобы распределить ключи группы и предоставить ключевой сервис те, которые повторно вводят ко всему GMS.
- COOP - Протокол использовал для KSs, чтобы связаться друг с другом и обеспечить избыточность.

- Сохранение заголовка - IPsec в Туннельном режиме, который сохраняет заголовок пакета исходных данных для доставки сквозного трафика.
- Время базирующееся антивоспроизведение (TBAR) - механизм обнаружения Воспроизведения используется в среде ключа группы.

Это также 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. Ключ к этому структурированному устранению проблем должен быть в состоянии сломать проблему или к контролю или к проблеме плоскости данных. Можно сделать это, если вы придерживаетесь протокола или потока данных и используете различные программные средства, представленные здесь для установки контрольных точек их.

Ссылочная топология

Эта топология GETVPN и схема адресации используются всюду по остатку этой документации по устранению проблем.



Ссылочные конфигурации

- KS1

```
crypto gdoi group G1
identity number 3333
server local
rekey authenmypubkeyrsa get
rekey transport unicast
sa ipsec 1
profile gdoi-p
match address ipv4ENCPOL
```

```
address ipv4 10.1.11.2
redundancy
local priority 10
peer address ipv4 10.1.12.2
```

- GM1

```
crypto gdoi group G1
identity number 3333
server address ipv4 10.1.11.2
server address ipv4 10.1.12.2
!
crypto map gm_map 10 gdoi
set group G1
!
interface Serial1/0
crypto map gm_map
```

Примечание: KS2 и конфигурации GM2 не включены здесь для краткости.

Терминология

- **KS** - Сервер ключей
- **GM** - Элемент группы
- **COOP** - Совместный протокол
- **TBAR** - Время базирующееся антивоспроизведение
- **KEK** - ключ шифрования
- **TEK** - ключ шифрования трафика

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 GMS, на который влияют, и 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:
```
service timestamps debug datetime msec
service timestamps log datetime msec
```

- 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.

Решите проблемы уровня управления GETVPN

Уровень управления означает все события протокола, которые вели до политики и создания Сопоставления безопасности (SA) на GM так, чтобы они были готовы зашифровать и дешифровать трафик плоскости данных. Некоторые ключевые контрольные точки в уровне управления GETVPN:

Уровень управления отлаживая оптимальные методы

Эти оптимальные методы устранения проблем не GETVPN определенный; они применяются к почти любой отладке уровня управления. Важно применить эти оптимальные методы для обеспечения большей части эффективного устранения проблем:

- Выключите вход через консоль и используйте буфер журнала или системный журнал для сбора отладок.
- Используйте NTP для синхронизации синхронизаций маршрутизатора на всех устройствах, которые отлажены.
- Включите msec, устанавливающий метку времени для отладки и сообщений журнала:
  `service timestamp debug datetime msec`
  `service timestamp log datetime msec`
- Удостоверьтесь, что к выходным данным команды show добавляют метку времени так, чтобы они могли быть коррелированы с выходными данными отладки:
  `terminal exec prompt timestamp`
- Используйте условную отладку в среде масштаба, если это возможно.

Средства устранения проблем уровня управления GETVPN

Команды показа GETVPN

Как правило это выходные данные команды, которые необходимо собрать для почти всех проблем GETVPN.

KS

```
show crypto gdoi
show crypto gdoi ks coop
show crypto gdoi ks members
show crypto gdoi ks rekey
show crypto gdoi ks policy
```

GM

```
show crypto eli
show crypto isakmp sa
show crypto gdoi
show crypto gdoi gm
show crypto gdoi gm rekey
```

Сообщения системного журнала GETVPN

GETVPN предоставляет обширный набор сообщений системного журнала для значительных событий протокола и состояний ошибки. Системный журнал должен всегда быть первым местом для взгляда при выполнении устранения проблем GETVPN.

Общие сообщения системного журнала KS

	Пояснение
COOP_CONFIG_MISMATCH	Конфигурации между первичным ключом сервер серверного и вторич ключа не соответствуют.
COOP_KS_ELECTION	Локальный сервер ключей ввел процесс голосования в группу.
COOP_KS_REACH	Достижимость между настроенными совместными серверами ключей восстановлена.
COOP_KS_TRANS_TO_PRI	**Локальный сервер ключей, перешедший к основной роли от того, чтоб быть дополнительным сервером в группе.**
COOP_KS_UNAUTH	Санкционированный удаленный сервер пытался связаться с локальны сервером ключей в группе, которую можно было считать враждебным событием.
COOP_KS_UNREACH	**Достижимость между настроенными совместными серверами ключей потеряна, который можно было считать враждебным событием.**
KS_GM_REVOKED	Во время повторно вводят протокол, неавторизованный участник пыта присоединиться к группе, которую можно было считать враждебным событием.
KS_SEND_MCAST_REKEY	**Передача групповой адресации повторно вводит.**
KS_SEND_UNICAST_REKEY	**Передача индивидуальной рассылки повторно вводит.**
KS_UNAUTHORIZED	Во время протокола регистрации GDOI неавторизованный участник пытался присоединиться к группе, которую можно было считать враждебным событием.
UNAUTHORIZED_IPADDR	Запрос регистрации был отброшен, потому что запрашивающее устройство не авторизовалось присоединиться к группе.

Общие сообщения системного журнала GM

	Пояснение
GM_CLEAR_REGISTER	**Команда clear crypto gdoi** была выполнена участником локальной гру
GM_CM_ATTACH	Криптокарта была подключена для участника локальной группы.
GM_CM_DETACH	Криптокарта была отсоединена для участника & локальной группы
GM_RE_REGISTER	**Контекст безопасности IPSec, созданный для одной группы, возможн истекся или очищен. Потребность повторно регистрировать к сервер ключей.**
GM_RECV_REKEY	**Повторно введите полученный.**
GM_REGS_COMPL	**Завершенная регистрация.**
GM_REKEY_TRANS_2_MULTI	Элемент группы перешел от использования индивидуальной рассыл повторно вводят механизм к использованию механизма групповой адресации.
GM_REKEY_TRANS_2_UNI	Элемент группы перешел от использования групповой адресации, повторно вводят механизм к использованию механизма индивидуаль

	рассылки.
PSEUDO_TIME_LARGE	Элемент группы получил псевдовремя со значением, которое являет основном другим с его собственного псевдовремени.
REPLAY_FAILED	Элемент группы или сервер ключей отказали антипроверку воспроизведения.

Примечание: Сообщения, выделенные в красном, являются наиболее распространенными или значительными сообщениями, замеченными в среде GETVPN.

Крипто-глобальный и отладки GDOI

Отладки GETVPN разделены:

1. Сначала устройством, на котором вы устраняете неполадки. `F340.06.15-2900-18#debug cry gdoi ?`
```
all-features All features in GDOI
condition    GDOI Conditional Debugging
gm           Group Member
ks           Key Server
```
2. Второй типом ошибки вы устраняете неполадки. `GM1#debug cry gdoi gm ?`
```
all-features   All Group Member features
infrastructure GM Infrastructure
registration   GM messages related to registration
rekey          GM messagese related to Re-Key
replay         Anti Replay
```
3. Треть уровнем отладки, которая должна быть включена. В Версии 15.1 (3) T и позже, все отладки функции GDOI были стандартизированы для имения этих уровней отладки. Это было разработано, чтобы помочь устранять неполадки крупномасштабных сред GETVPN с достаточной глубиной детализации отладки. При отладке проблем GETVPN важно использовать соответствующий уровень отладки. Как правило запустите с самого низкого уровня отладки, который является уровнем ошибки, и увеличьте глубину детализации отладки при необходимости. `GM1#debug cry gdoi gm all-features ?`
```
all-levels All levels
detail     Detail level
error      Error level
event      Event level
packet     Packet level
terse      Terse level
```

Условная отладка GDOI

В Cisco IOS® Version 15.1 (3) T и позже, была добавлена условная отладка GDOI, чтобы помочь устранять неполадки GETVPN в крупномасштабной среде. Таким образом, весь Протокол ISAKMP и отладки GDOI могут теперь быть инициированы с условным фильтром на основе группы или IP - адреса адресуемого точки. Для большинства проблем GETVPN хорошо включить и ISAKMP и отладки GDOI с соответствующим условным фильтром, так как GDOI отлаживает, только показывают GDOI-специфичные операции. Для использования ISAKMP и условных отладок GDOI, выполните эти два простых шага:

1. Установите условный фильтр.
2. Включите соответствующий ISAKMP и GDOI, как обычно.

Пример:

```
KS1# debug crypto gdoi condition peer add ipv4 10.1.20.2
% GDOI Debug Condition added.

KS1#
KS1# show crypto gdoi debug-condition
GDOI Conditional Filters:
Peer Address 10.1.20.2
Unmatched NOT set

KS1#debug crypto gdoi ks registration all-levels
GDOI Key Server Registration Debug level: (Packet, Detail, Event, Terse, Error)
```

> **Примечание:** И с ISAKMP и с условными отладками GDOI, для ловли сообщений отладки, которые не могли бы иметь условной информации о фильтре, например IP-адрес в пути отладки, может быть включен **несопоставленный** флаг. Однако это должно использоваться с осторожностью, потому что это может произвести большое количество отладочной информации.

Трассировки события GDOI

Это было добавлено 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. Трассировки события могут предоставить большую информацию об истории события GETVPN, чем традиционные системные журналы.

Трассировки события GDOI разрешены по умолчанию и могут быть получены из буфера трассировки с командой **ровной трассировки show monitor**.

```
GM1#show monitor event-trace gdoi ?
all Show all the traces in current buffer
back Show trace from this far back in the past
clock Show trace from a specific clock time/date
coop GDOI COOP Event Traces
exit GDOI Exit Traces
from-boot Show trace from this many seconds after booting
infra GDOI INFRA Event Traces
latest Show latest trace events since last display
merged Show entries in all event traces sorted by time
registration GDOI Registration event Traces
rekey GDOI Rekey event Traces

GM1#show monitor event-trace gdoi rekey all
*Nov 6 15:55:16.117: GDOI_REKEY_EVENT: ACK_SENT: From 10.1.12.2 to 10.1.13.2
with seq no 1 for the group G1
*Nov 6 15:55:16.117: GDOI_REKEY_EVENT: REKEY_RCVD: From 10.1.12.2 to 10.1.13.2
with seq no 1 for the group G1
*Nov 6 16:11:01.125: GDOI_REKEY_EVENT: ACK_SENT: From 10.1.12.2 to 10.1.13.2
with seq no 1 for the group G1
*Nov 6 16:11:01.125: GDOI_REKEY_EVENT: REKEY_RCVD: From 10.1.12.2 to 10.1.13.2
with seq no 1 for the group G1
```

Выходная трассировка пути предоставляет подробные сведения о выходном пути, который является исключением и состояниями ошибки с опцией обратной трассировки, включенной по умолчанию. Обратная трассировка может тогда использоваться для декодирования точной кодовой последовательности, которая привела к выходному состоянию тракта. Используйте **подробную** опцию для получения обратной трассировки из буфера

трассировки:

```
GM1#show monitor event-trace gdoi exit all detail
*Nov 6 15:15:25.611: NULL_VALUE_FOUND:Invalid GROUP Name
-Traceback= 0xCA51318z 0xCA1F4DBz 0xC9B2707z 0xCA1ED4Ez 0x97EB018z
0x97EA960z 0x97E8D62z 0x97F3706z 0x97F3361z 0xA02684Ez
*Nov 6 15:15:25.611: MAP_NOT_APPLIED_IN_ANY_INTERFACE:
-Traceback= 0xCA51318z 0xCA46718z 0xCA1EF79z 0x97EB018z 0x97EA960z
0x97E8D62z 0x97F3706z 0x97F3361z 0xA02684Ez 0xA01FD52z
*Nov 6 15:15:25.650: NULL_VALUE_FOUND:NULL Parameters passed idb or ipaddress
when idb ipaddress is changed
-Traceback= 0xCA51318z 0xCA22430z 0xA09A8DCz 0xA09D8F6z 0xA0F280Fz
0xBA1D1F4z 0xBA1CACCz 0xBA1C881z 0xBA1C5BBz 0xA0F494Az
```

Размер буфера трассировки по умолчанию является 512 записями, и это не могло бы быть достаточно, если проблема неустойчива. Для увеличения этого размера записи трассировки по умолчанию параметры конфигурации трассировки события могут быть изменены как показанный здесь:

```
GM1#show monitor event-trace gdoi rekey parameters
Trace has 512 entries
Stacktrace is disabled by default

GM1#
GM1#config t
Enter configuration commands, one per line. End with CNTL/Z.
GM1(config)#monitor event-trace gdoi rekey size ?
<1-1000000> Number of entries in trace
```

Контрольные точки уровня управления GETVPN и общие проблемы

Вот некоторые проблемы плоскости обычного управления для GETVPN. Для повторения Уровень управления определен, поскольку все компоненты функции GETVPN потребовали для включения dataplane шифрования и расшифровки на GMS. На высоком уровне это требует успешной регистрации GM, политики безопасности и загрузки/установки SA, и последующий KEK/TEK повторно вводит.

Настройка COOP и создание политики

Чтобы проверить и проверить, что KS успешно создал политику безопасности и связанный KEK/TEK, войдите:

```
KS1#show crypto gdoi ks policy
Key Server Policy:
For group G1 (handle: 2147483650) server 10.1.11.2 (handle: 2147483650):

For group G1 (handle: 2147483650) server 10.1.12.2 (handle: 2147483651):

# of teks : 1 Seq num : 10
KEK POLICY (transport type : Unicast)
spi : 0x18864836BA888BCD1126671EEAFEB4C7
management alg : disabled encrypt alg : 3DES
crypto iv length : 8 key size : 24
orig life(sec): 1200 remaining life(sec): 528
sig hash algorithm : enabled sig key length : 162
sig size : 128
sig key name : key1

TEK POLICY (encaps : ENCAPS_TUNNEL)
spi : 0x91E3985A
```

```
access-list : ENCPOL
transform : esp-null esp-sha-hmac
alg key size : 0 sig key size : 20
orig life(sec) : 900 remaining life(sec) : 796
tek life(sec) : 2203 elapsed time(sec) : 1407
override life (sec): 0 antireplay window size: 4

Replay Value 442843.29 secs
```

Когда существует другая политика, настроенная между основным и вторичным KSs, одна типичная проблема с настройкой политики KS. Это может привести к непредсказуемому поведению KS, и об этой ошибке сообщат:

```
KS1#show crypto gdoi ks policy
Key Server Policy:
For group G1 (handle: 2147483650) server 10.1.11.2 (handle: 2147483650):

For group G1 (handle: 2147483650) server 10.1.12.2 (handle: 2147483651):

# of teks : 1 Seq num : 10
KEK POLICY (transport type : Unicast)
spi : 0x18864836BA888BCD1126671EEAFEB4C7
management alg : disabled encrypt alg : 3DES
crypto iv length : 8 key size : 24
orig life(sec): 1200 remaining life(sec): 528
sig hash algorithm : enabled sig key length : 162
sig size : 128
sig key name : key1

TEK POLICY (encaps : ENCAPS_TUNNEL)
spi : 0x91E3985A
access-list : ENCPOL
transform : esp-null esp-sha-hmac
alg key size : 0 sig key size : 20
orig life(sec) : 900 remaining life(sec) : 796
tek life(sec) : 2203 elapsed time(sec) : 1407
override life (sec): 0 antireplay window size: 4

Replay Value 442843.29 secs
```

В настоящее время между основным и вторичным KSs нет никакого синхронизования автоматической конфигурации, таким образом, они должны быть вручную исправлены.

Поскольку COOP является важным (и почти всегда обязательный) конфигурация для GETVPN, это является ключевым, чтобы удостовериться, что COOP работает правильно и COOP, роли KS корректны:

```
KS1#show crypto gdoi ks coop
Crypto Gdoi Group Name :G1
Group handle: 2147483650, Local Key Server handle: 2147483650

Local Address: 10.1.11.2
Local Priority: 200
 Local KS Role: Primary   , Local KS Status: Alive
Local KS version: 1.0.4
Primary Timers:
Primary Refresh Policy Time: 20
Remaining Time: 10
Antireplay Sequence Number: 40

Peer Sessions:
Session 1:
Server handle: 2147483651
```

```
Peer Address: 10.1.12.2
Peer Version: 1.0.4
Peer Priority: 100
Peer KS Role: Secondary , Peer KS Status: Alive
Antireplay Sequence Number: 0

IKE status: Established
Counters:
Ann msgs sent: 31
Ann msgs sent with reply request: 2
Ann msgs recv: 64
Ann msgs recv with reply request: 1
Packet sent drops: 7
Packet Recv drops: 0
Total bytes sent: 20887
Total bytes recv: 40244
```

В функциональной настройке COOP должен наблюдаться этот поток протокола:

Exchange IKE> ANN с приоритетами COOP, которыми обмениваются> Выборы COOP> ANN от основного до вторичного KS (политика, база данных GM и ключи)

Когда COOP не работает правильно, или если существует разделение COOP, такое как множественный KSs становятся основным KS, эти отладки должны быть собраны для устранения проблем:

```
debug crypto isakmp
debug crypto gdoi ks coop all-levels
show crypto isakmp sa
show crypto gdoi ks coop
```

Настройка IKE

Успешный обмен IKE требуется для GETVPN для обеспечения управляющего канал для последующей политики и загрузки SA. В конце успешного обмена IKE создана эта IKE SA:

```
GM1#show crypto isa sa
IPv4 Crypto ISAKMP SA
dst src state conn-id status
10.1.13.2 10.1.11.2 GDOI_REKEY        1075 ACTIVE
10.1.11.2 10.1.13.2 GDOI_IDLE         1074 ACTIVE

IPv6 Crypto ISAKMP SA

GM1#
```

> **Примечание:** Как только начальный обмен IKE завершает, последующая политика и ключи будут **выдвинуты** от KS до GM с использованием GDOI_REKEY SA. Таким образом, существует, не повторно вводят для GDOI_REKEY SA, когда они истекают; когда их сроки службы истекают, они исчезают. Однако должна всегда быть GDOI_REKEY SA на GM для него для получения, повторно вводит.

Обмен IKE для GETVPN не отличается от IKE, используемого в традиционных Туннелях IPSec "точка-точка", таким образом, метод устранения проблем остается тем же. Эти отладки должны быть собраны для решения проблем аутентификации IKE:

```
debug crypto isakmp
debug crypto isakmp error
debug crypto isakmp detail (hidden command, if detailed isakmp exchange information
is needed)
```

debug crypto isakmp packet (hidden command, if packet level isakmp information is needed)

Регистрация, загрузка политики и установка SA

Как только аутентификация IKE успешно выполняется, регистры GM с KS. Эти сообщения системного журнала, как ожидают, будут замечены, когда это произойдет правильно:

```
%GDOI-5-GM_REKEY_TRANS_2_UNI: Group G1 transitioned to Unicast Rekey.
%GDOI-5-SA_KEK_UPDATED: SA KEK was updated
%GDOI-5-SA_TEK_UPDATED: SA TEK was updated
%GDOI-5-GM_REGS_COMPL: Registration to KS 10.1.12.2 complete for group G1 using
address 10.1.13.2
%GDOI-5-GM_INSTALL_POLICIES_SUCCESS: SUCCESS: Installation of Reg/Rekey policies
from KS 10.1.12.2 for group G1 & gm identity 10.1.13.2
```

Политика и ключи могут быть проверены с этой командой:

```
GM1#show crypto gdoi
GROUP INFORMATION

Group Name : G1
Group Identity : 3333
Crypto Path : ipv4
Key Management Path : ipv4
Rekeys received : 1
IPSec SA Direction : Both

Group Server list : 10.1.11.2
10.1.12.2

Group member : 10.1.13.2 vrf: None
Version : 1.0.4
Registration status : Registered
Registered with : 10.1.12.2
Re-registers in       : 139 sec
Succeeded registration: 1
Attempted registration: 1
Last rekey from : 10.1.11.2
Last rekey seq num : 0
Unicast rekey received: 1
Rekey ACKs sent : 1
Rekey Rcvd(hh:mm:ss)  : 00:05:20
allowable rekey cipher: any
allowable rekey hash : any
allowable transformtag: any ESP

Rekeys cumulative
Total received : 1
After latest register : 1
Rekey Acks sents : 1

ACL Downloaded From KS 10.1.11.2:
access-list deny icmp any any
access-list deny eigrp any any
access-list deny ip any 224.0.0.0 0.255.255.255
access-list deny ip 224.0.0.0 0.255.255.255 any
access-list deny udp any port = 848 any port = 848
access-list permit ip any any

KEK POLICY:
Rekey Transport Type : Unicast
Lifetime (secs) : 878
Encrypt Algorithm : 3DES
```

```
Key Size : 192
Sig Hash Algorithm : HMAC_AUTH_SHA
Sig Key Length (bits) : 1024

TEK POLICY for the current KS-Policy ACEs Downloaded:
Serial1/0:
IPsec SA:
spi: 0x8BF147EF(2347845615)
transform: esp-3des esp-sha-hmac
sa timing:remaining key lifetime (sec): (200)
Anti-Replay(Time Based) : 4 sec interval


GM1#
GM1#
GM1#show crypto ipsec sa

interface: Serial1/0
Crypto map tag: gm1map, local addr 10.1.13.2

protected vrf: (none)
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
current_peer 0.0.0.0 port 848
PERMIT, flags={}
#pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 10.1.13.2, remote crypto endpt.: 0.0.0.0
path mtu 1500, ip mtu 1500, ip mtu idb Serial1/0
current outbound spi: 0x0(0)
PFS (Y/N): N, DH group: none

local crypto endpt.: 10.1.13.2, remote crypto endpt.: 0.0.0.0
path mtu 1500, ip mtu 1500, ip mtu idb Serial1/0
current outbound spi: 0x8BF147EF(2347845615)
PFS (Y/N): N, DH group: none

inbound esp sas:
spi: 0x8BF147EF(2347845615)
transform: esp-3des esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 1, flow_id: SW:1, sibling_flags 80000040, crypto map: gm1map
sa timing: remaining key lifetime (sec): (192)
Kilobyte Volume Rekey has been disabled
IV size: 8 bytes
replay detection support: Y replay window size: 4
Status: ACTIVE(ACTIVE)

inbound ah sas:

inbound pcp sas:

outbound esp sas:
spi: 0x8BF147EF(2347845615)
transform: esp-3des esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 2, flow_id: SW:2, sibling_flags 80000040, crypto map: gm1map
sa timing: remaining key lifetime (sec): (192)
Kilobyte Volume Rekey has been disabled
```

```
IV size: 8 bytes
replay detection support: Y replay window size: 4
Status: ACTIVE(ACTIVE)

outbound ah sas:

outbound pcp sas:
GM1#
```

Примечание: С GETVPN входящие и исходящие SA используют тот же SPI.

С регистрацией GETVPN и типом установки политики проблем, эти отладки необходимы для устранения проблем:

```
debug crypto isakmp (KS and GM)
debug crypto gdoi ks registration all-levels (KS)
debug crypto gdoi gm registration all-level (GM)
debug crypto engine (GM only)
show crypto eli detail (multiple iterations on GM)
```

Примечание: Дополнительные отладки могут требоваться в зависимости от результата этих выходных данных.

Так как регистрация GETVPN, как правило, сразу происходит после повторной загрузки GM этот сценарий EEM мог бы быть полезным для сбора этих отладок:

```
debug crypto isakmp (KS and GM)
debug crypto gdoi ks registration all-levels (KS)
debug crypto gdoi gm registration all-level (GM)
debug crypto engine (GM only)
show crypto eli detail (multiple iterations on GM)
```

Повторно ввести

Однажды GMS зарегистрированы к KS, и сеть GETVPN должным образом установлена, основной KS ответственен за передачу, повторно вводят сообщения ко всему GMS, зарегистрированному к нему. Повторно вводить сообщения используются для синхронизации всей политики, ключей, и псевдовремена на GMS. Повторно вводить сообщения могут быть переданы через индивидуальную рассылку или метод групповой адресации.

Когда повторно вводить сообщение передается, это сообщение системного журнала замечено на KS:

```
debug crypto isakmp (KS and GM)
debug crypto gdoi ks registration all-levels (KS)
debug crypto gdoi gm registration all-level (GM)
debug crypto engine (GM only)
show crypto eli detail (multiple iterations on GM)
```

На GMS это - системный журнал, который замечен, когда это получает повторно введение:

```
debug crypto isakmp (KS and GM)
debug crypto gdoi ks registration all-levels (KS)
debug crypto gdoi gm registration all-level (GM)
debug crypto engine (GM only)
show crypto eli detail (multiple iterations on GM)
```

Требование открытых и секретных ключей криптосистемы RSA для повторно вводит на KS

Повторно введите функциональность, требует, чтобы присутствие RSA включило KS. KS предоставляет открытый ключ Открытых и секретных ключей криптосистемы RSA к GM через этот безопасный канал во время регистрации. KS тогда подписывает сообщения GDOI, передаваемые GM с секретным ключом RSA в информационном наполнении SIG GDOI. GM получает сообщения GDOI и использует общедоступный ключ RSA для проверки сообщения. Сообщения между KS и GM зашифрованы с KEK, который также распределен GM во время регистрации. Как только регистрация завершена, последующий повторно вводит, зашифрованы с KEK и подписаны с секретным ключом RSA.

Если ключ RSA не является никаким подарком на KS во время регистрации GM, это сообщение появляется на системном журнале:

```
debug crypto isakmp (KS and GM)
debug crypto gdoi ks registration all-levels (KS)
debug crypto gdoi gm registration all-level (GM)
debug crypto engine (GM only)
show crypto eli detail (multiple iterations on GM)
```

Когда ключи не присутствуют на KS, регистры GM впервые, но следующее повторно вводят сбои от KS. В конечном счете существующие ключи на GM истекают, и это повторно регистрирует снова.

```
debug crypto isakmp (KS and GM)
debug crypto gdoi ks registration all-levels (KS)
debug crypto gdoi gm registration all-level (GM)
debug crypto engine (GM only)
show crypto eli detail (multiple iterations on GM)
```

Так как Открытые и секретные ключи криптосистемы RSA используются для подписания повторно вводить сообщений, они MUST быть тем же между основным и всем вторичным KSs. Это гарантирует, что во время основного сбоя KS, повторно введение передаваемого вторичным KS (новый основной KS) может все еще быть должным образом проверено GMS. Когда это генерирует Открытые и секретные ключи криптосистемы RSA на основном KS, пара ключей должна быть создана с экспортной опцией так, чтобы они могли быть экспортированы в весь вторичный KSs для соответствия этому требованию.

Повторно введите устранение проблем

KEK/TEK повторно вводит сбой, одна из наиболее распространенных проблем GETVPN, с которыми встречаются в клиентских развертываниях. Устранение проблем повторно вводит проблемы, должен выполнить повторно вводить действия, как выделено здесь:

1. Повторно введение становилось передаваемым KS?

   Это может быть проверено observion %GDOI-5-KS_SEND_UNICAST_REKEY сообщения системного журнала или более точно с этой командой:

```
KS1#show crypto gdoi ks rekey
Group G1 (Unicast)
Number of Rekeys sent               : 341
Number of Rekeys retransmitted      : 0
KEK rekey lifetime (sec) : 1200
Remaining lifetime (sec) : 894
Retransmit period : 10
Number of retransmissions : 5
IPSec SA 1 lifetime (sec) : 900
Remaining lifetime (sec) : 405
```

Количество повторно вводит ретранслируемый, показательно из, повторно вводят пакеты подтверждения, не полученные KS, и поэтому возможный повторно вводят проблемы. Следует иметь в виду, что GDOI повторно вводят UDP использования как ненадежный механизм переноса, таким образом, некоторые повторно вводят отбрасывания, мог бы ожидаться в зависимости от надежности сети базовой передачи, но тенденция увеличиться повторно вводит повторные передачи, должен всегда исследоваться.

Более подробный на GM повторно вводят статистику, может также быть получен. Это, как правило, - первое место для поиска потенциала, повторно вводят проблемы.

```
KS1#show crypto gdoi ks members

Group Member Information :

Number of rekeys sent for group G1 : 346

Group Member ID : 10.1.14.2 GM Version: 1.0.4
Group ID : 3333
Group Name : G1
Key Server ID : 10.1.11.2
 Rekeys sent       : 346
Rekeys retries : 0
Rekey Acks Rcvd : 346
Rekey Acks missed : 0

Sent seq num : 2 1 2 1
Rcvd seq num : 2 1 2 1

Group Member ID : 10.1.13.2 GM Version: 1.0.4
Group ID : 3333
Group Name : G1
Key Server ID : 10.1.12.2
 Rekeys sent       : 340
Rekeys retries : 0
Rekey Acks Rcvd : 340
Rekey Acks missed : 0

Sent seq num : 2 1 2 1
Rcvd seq num : 2 1 2 1
```

2. Повторно вводить пакеты отправлены в сети базовой инфраструктуры?

   Стандартное Устранение проблем связанных с IP вдоль повторно вводить пути переадресации должно придерживаться, чтобы гарантировать, что повторно вводить пакеты не отброшены в транзитной сети между KS и GM. Некоторые общие средства устранения проблем, используемые здесь, являются Списками контроля доступа ввода/вывода (ACL), Netflow и захват пакета в транзитной сети.

3. Повторно вводить пакеты достигают, процесс GDOI для повторно вводят обработку?

   Проверьте, что GM повторно вводит статистику:

```
GM1#show crypto gdoi gm rekey
Group G1 (Unicast)
Number of Rekeys received (cumulative) : 340
Number of Rekeys received after registration : 340
```

```
Number of Rekey Acks sent : 340
```

4. Повторно вводить пакет подтверждения возвращаются к KS?

   Придерживайтесь Шагов 1 - 3 для отслеживания повторно вводить пакета подтверждения от GM назад к KS.

Muticast повторно вводят

Групповая адресация повторно вводит, отличается от индивидуальной рассылки, повторно вводят в этих аспектах:

- Так как групповая адресация используется для переноса, они повторно вводят пакеты от KS до GMS, KS не должен реплицировать повторно вводить пакеты сам. KS только передает одну копию повторно вводить пакета, и они реплицированы в поддерживающую групповую адресацию сеть.
- Нет никакого механизма подтверждения для групповой адресации, повторно вводят, поэтому если бы GM не должен был получать повторно вводить пакет, KS не знал бы о нем, и поэтому никогда не будет удалять GM из своей базы данных GM. И потому что нет никакого подтверждения, KS будет всегда повторно передавать повторно вводить пакеты на основе повторно вводить конфигурацию повторной передачи.

Обычно замеченная групповая адресация повторно вводит проблему, когда повторно введение не получено на GM. Могло быть много возможных причин для этого, таких как:

- Проблема доставки пакетов в многоадресной инфраструктуре маршрутизации
- Сквозная многоадресная маршрутизация не включена в сети

Первый шаг для решения проблемы с групповой адресацией повторно вводит, должен видеть, повторно вводят ли, работает, когда коммутировано от групповой адресации до метода индивидуальной рассылки.

Как только вы определяете это, проблема является определенной для групповой адресации, повторно вводят, проверяют, что KS передает повторно введение к заданному адресу групповой адресации.

```
GM1#show crypto gdoi gm rekey
Group G1 (Unicast)
Number of Rekeys received (cumulative) : 340
Number of Rekeys received after registration : 340
Number of Rekey Acks sent : 340
```

Протестируйте подключение групповой адресации между KS и GM с запросом протокола управляющих сообщений интернета (ICMP) к адресу групповой адресации. Весь GMS, которые являются частью группы многоадресной рассылки, должен ответить на эхо-запрос. Гарантируйте, что ICMP исключен из политики шифрования KS для этого теста.

```
KS1#ping 226.1.1.1

Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 226.1.1.1, timeout is 2 seconds:

Reply to request 0 from 10.1.21.2, 44 ms
```

Если эхо - тест (ping test) групповой адресации отказывает, то переданное в многоадресном режиме устранение проблем должно быть выполнено, который является за пределами области этого документа.

Проверка реле уровня управления

Признак

Когда клиенты обновляют свой GM к новой ПО Cisco IOS версии, они могли бы испытать KEK, повторно вводят сбои с этим сообщением, наблюдаемым в системном журнале:

```
KS1#ping 226.1.1.1

Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 226.1.1.1, timeout is 2 seconds:

Reply to request 0 from 10.1.21.2, 44 ms
```

Это поведение вызвано проблемой совместимости, начатой с антипроверки воспроизведения, которая добавлена для сообщений уровня управления. В частности KS, который выполняет более старый код, перезагрузит KEK, повторно вводят порядковый номер к 1, и это будет отброшено GM, который выполняет новый код, когда это интерпретирует это, поскольку воспроизводимый повторно вводит пакет. Для получения дополнительной информации посмотрите идентификатор ошибки Cisco CSCta05809 (GETVPN: уровень управления GETVPN, разумный для воспроизведения), и Ограничения конфигурации GETVPN.

Общие сведения

С GETVPN сообщения Уровня управления могут нести критичную по времени информацию для предоставления контролируемого по времени сервиса антипроверки воспроизведения. Поэтому эти сообщения требуют защиты Антиответ сами для обеспечения времени accruracy. Эти сообщения:

- **Повторно введите сообщения** от KS до GM
- **Сообщения уведомления COOP** между KSs

Когда TBAR включен, как часть этой реализации защиты Антиответ, проверки порядкового номера были добавлены для защиты воспроизводимых сообщений, а также псевдопроверки времени.

Решение

Для решения этого вопроса и GM и KS должны быть обновлены к версиям Cisco IOS после функции проверки воспроизведения Уровня управления. С новым ПО Cisco IOS кодом KS не перезагружает порядковый номер назад к 1 для KEK, повторно вводят, но вместо этого это продолжает использовать текущий порядковый номер и только перезагружает порядковый номер для TEK, повторно вводит.

Эти версии Cisco IOS имеют функции Проверки воспроизведения:

- 12.4 (15) T10
- 12.4 (22) T3
- 12.4 (24) T2
- 15.0 (1) M и позже

Другие связанные проблемы воспроизведения

- Сбой из-за COOP к сообщениям ANN, отказывающим проверку воспроизведения (идентификатор ошибки Cisco CSCtc52655)

Плоскость управления отладкой воспроизводит сбои

Для других сбоев Воспроизведения Уровня управления соберите эту информацию и удостоверьтесь, что времена синхронизируются между KS и GM.

- Системный журнал и от GM и от KS
- Отладки ISAKMP
- Отладки GDOI (повторно вводят и воспроизводят), и от KS и от GM

Проблемы фрагментации пакета уровня управления

С GETVPN Фрагментация пакета Уровня управления является общей проблемой, и это может проявить себя в одном из этих двух сценариев, когда пакеты Уровня управления являются достаточно большими, что они потребуют Фрагментации ip:

- GETVPN пакеты Объявления COOP
- GETVPN повторно вводят пакеты

Пакеты объявления COOP

Пакеты Объявления COOP несут информацию о базе данных GM, и таким образом могут стать большими в больших развертываниях GETVPN. От прошлого опыта сеть GETVPN, которая состоит из 1500 + GMS, произведет пакеты Объявления, больше, чем 18024 байта, который является размером Огромного буфера Cisco IOS по умолчанию. Когда это происходит, KS не в состоянии выделять буфер, достаточно большой для передачи пакетов ANN с этой ошибкой:

```
KS1#ping 226.1.1.1

Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 226.1.1.1, timeout is 2 seconds:

Reply to request 0 from 10.1.21.2, 44 ms
```

Для исправления этого условия эта настройка буфера рекомендуется:

```
KS1#ping 226.1.1.1

Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 226.1.1.1, timeout is 2 seconds:

Reply to request 0 from 10.1.21.2, 44 ms
```

Повторно введите пакеты

GETVPN повторно вводят пакеты, может также превысить типичного IP 1500 года размер Maximum Transition Unit (MTU), когда политика шифрования является крупной, такой как политика, которая состоит из 8 + линии Записей управления доступом (ACE) в ACL шифрования.

Проблема фрагментации и идентификация

В обоих из предыдущих сценариев GETVPN должен быть в состоянии должным образом передать и получить фрагментированные пакеты UDP для COOP, или GDOI повторно вводят для работы должным образом. Фрагментация ip может быть проблемой в некоторых сетевых средах. Например, сеть, которая состоит из плоскости переадресации Равноценного много пути (ECMP) и некоторых устройств в плоскости переадресации, требует действительной повторной сборки фрагментированных пакетов IP, таких как Действительная повторная сборка фрагментации (VFR).

Для определения проблемы проверьте ошибки повторной сборки на устройстве, где подозревается, что должным образом не получен фрагментированный UDP 848 пакетов:

```
KS1#show ip traffic | section Frags
Frags: 10 reassembled, 3 timeouts, 0 couldn't reassemble
0 fragmented, 0 fragments, 0 couldn't fragment
```

Если тайм-ауты пересборки продолжают инкрементно увеличиваться, используйте **команду debug ip error**, чтобы подтвердить, является ли отбрасывание частью ПОВТОРНО ВВОДИТЬ/COOP потока пакетов. После того, как подтвержденное, обычное устранение проблем IP - переадресации должно быть выполнено для изоляции точного устройства в плоскости переадресации, которая, возможно, отбросила пакеты. Некоторые обычно используемые программные средства включают:

- Захват пакета
- Статистика перенаправления трафика
- Статистика характеристики безопасности (Межсетевой экран, IPS)
- Статистика VFR

Проблемы совместимости GDOI

Различные проблемы совместимости были найдены с GETVPN за эти годы, и важно заметить версии Cisco IOS Release между KS и GM и среди KSs для проблем совместимости.

Другие известные проблемы совместимости GETVPN:

- Проверка реле уровня управления
- KEK GETVPN повторно вводит изменение поведения
- Идентификатор ошибки Cisco CSCub42920 - GETVPN: KS не в состоянии проверять хэш в, повторно вводят ACK от предыдущих версий GM
- Идентификатор ошибки Cisco CSCuw48400 (GetVPN GM, неспособный зарегистрироваться или повторно ввести сбои - хэш сигнала> SHA-1 по умолчанию)

Процедура обновления IOS GETVPN

Когда обновление Кода Cisco IOS должно быть выполнено в среде GETVPN, эта процедура обновления Cisco IOS должна быть выполнена:

1. Обновите вторичный KS сначала и ждите до COOP завершены выборы KS.
2. Повторите Step1 для всего вторичного KSs.
3. Обновите основной KS.
4. GMS обновления.

Решите проблемы плоскости данных GETVPN

По сравнению с проблемами Уровня управления проблемы плоскости данных GETVPN являются проблемами, где GM имеет политику и ключи для выполнения dataplane шифрования и расшифровки, но по некоторым причинам не работает поток сквозного трафика. Большинство проблем dataplane для GETVPN касается передачи IPsec общего назначения и не GETVPN определенный. Таким образом, большая часть подхода к устранению проблем, описанного здесь, применяется к IPsec общего назначения dataplane проблемы также.

С проблемами шифрования (оба Основанных на группе или попарных туннеля), важно устранять проблему и изолировать проблему к отдельному маршруту канала передачи данных. В частности подход к устранению проблем, описанный здесь, предназначен, чтобы помочь вам отвечать на эти вопросы:

- Какое устройство является преступником - маршрутизатор дешифрования или маршрутизатор шифрования?
- В котором направлении проблема происходит - вход или выход?

Средства устранения проблем плоскости данных GETVPN

IPsec dataplane устранение проблем очень отличается от этого для Уровня управления. С dataplane обычно нет никаких отладок, которые можно выполнить, или по крайней мере работать безопасно в производственной среде. Таким образом, устранение проблем полагается в большой степени на другие счетчики и статистику трафика, которая может помочь отслеживать пакет вдоль пути переадресации. Идея состоит в том, чтобы быть в состоянии разработать ряд контрольных точек, чтобы помочь изолировать, где пакеты могли бы быть отброшены как показано здесь:

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)

Контрольные точки в канале передачи данных в предыдущем образе могут быть проверены с этими программными средствами:

Шифрование GM

- Входной интерфейс LAN (локальной сети)
  Ввод для ACL
  Входной netflow
  Встроенный захват пакета
  Входной учет приоритетов

- Ядро шифрования
  show crypto ipsec sa
  подробность show crypto ipsec sa
  статистика акселератора show crypto engine

- Выходной Интерфейс WAN
  Выходной netflow
  Встроенный захват пакета
  Выходной учет приоритетов

Дешифрование GM

- Входной Интерфейс WAN
  Ввод для ACL
  Входной netflow
  Встроенный захват пакета
  Входной учет приоритетов

- Ядро шифрования
  show crypto ipsec sa
  подробность show crypto ipsec sa
  статистика акселератора show crypto engine

- Выходной интерфейс LAN (локальной сети)
  Выходной netflow
  Встроенный захват пакета

Адрес возврата придерживается того же трафика. Следующие разделы имеют некоторые примеры этих dataplane программных средств в использовании.

В отличие от стандарта Счетчики

В отличие от стандарта счетчики на маршрутизаторе основываются на потоке IPsec. К сожалению, это не работает хорошо с GETVPN, так как GETVPN, как правило, развертывает политику шифрования "permit ip any any", которая шифрует все. Таким образом, если проблема только происходит для некоторых потоков и не всех, эти счетчики может быть несколько трудно использовать, чтобы правильно оценить, если пакеты зашифрованы или дешифрованы, когда существует достаточно значительного фонового трафика, который работает.

```
GM1#show crypto ipsec sa | in encrypt|decrypt
#pkts encaps: 100, #pkts encrypt: 100, #pkts digest: 100
#pkts decaps: 100, #pkts decrypt: 100, #pkts verify: 100
```

Netflow

Netflow может использоваться для мониторинга и входа и выходного трафика на обоих GMS. Обратите внимание с политикой **permit ip any any** GETVPN, enrypted трафик будет агрегатом и не предоставляет на сведения о потоках. На сведения о потоках должен будет тогда быть собран с маркировкой DSCP/приоритетов, описанной позже.

В данном примере netflow для 100 эхо-запросов количества от хоста позади GM1 к хосту позади GM2 показывают на различных контрольных точках.

Шифрование GM

Конфигурация Netflow:

```
interface Ethernet0/0
description LAN
ip address 192.168.13.1 255.255.255.0
ip flow ingress
ip pim sparse-dense-mode
!
interface Serial1/0
description WAN interface
ip address 10.1.13.2 255.255.255.252
ip flow egress
ip pim sparse-dense-mode
crypto map gm1map
```

Выходные данные Netflow:

```
GM1#show ip cache flow | be SrcIf
SrcIf SrcIPaddress DstIf DstIPaddress Pr SrcP DstP Pkts
Et0/0 192.168.13.2 Se1/0* 192.168.14.2 32 8DE1 6523   100
Et0/0 192.168.13.2 Se1/0 192.168.14.2 01 0000 0800   100
GM1#
```

> **Примечание:** В предыдущих выходных данных, * обозначает выходной трафик. Первая линия показывает выходной зашифрованный поток данных (с протоколом 0x32 = ESP) из интерфейса глобальной сети (WAN) и второго входного трафика ICMP линии, поражающего интерфейс LAN (локальной сети).

Дешифрование GM

!--- конфигурацию:

```
interface Ethernet0/0
description LAN interface
ip address 192.168.14.1 255.255.255.0
ip flow egress
ip pim sparse-dense-mode
!
interface Serial1/0
description WAN interface
ip address 10.1.14.2 255.255.255.252
ip flow ingress
ip pim sparse-dense-mode
crypto map gm1map
```

Выходные данные Netflow:

```
GM2#show ip cache flow | be SrcIf
SrcIf SrcIPaddress DstIf DstIPaddress Pr SrcP DstP Pkts
Se1/0 192.168.13.2 Et0/0 192.168.14.2 32 8DE1 6523   100
```

```
Se1/0 192.168.13.2 Et0/0* 192.168.14.2 01 0000 0800   100
GM2#
```

Маркирующие Приоритеты DSCP/IP

Проблема с устренением проблемы шифрования состоит в том, что, как только пакет зашифрован, вы теряете видимость в информационное наполнение, которое является тем, что шифрование, как предполагается, делает, и это мешает отслеживать пакет для определенного IP flow. Существует два способа обратиться к этому ограничению когда дело доходит до устренения проблемы IPsec:

- NULL ESP использования как IPsec преобразовывает. IPsec все еще выполняет ESP инкапсуляцию, но никакое шифрование не применено к информационному наполнению, таким образом, они видимы в захвате пакета.
- Маркируйте IP flow с уникальной Кодовой точкой дифференцированных сервисов (DSCP) / приоритеты, отмечающие на основе их характеристик L3/L4.

NULL ESP требует изменений на обеих оконечных точках туннеля, и часто не позволяется на основе политики безопасности клиента. Поэтому Cisco, как правило, рекомендует использование DSCP/приоритетов, отмечающего вместо этого.

Справочная таблица DSCP/Приоритетов

ToS (hex)	ToS (Десятичное число)	Приоритет IP	DSCP	Двоичные файлы
0xE0	224	7 управлений сетью	56 CS7	11100000
0xC0	192	6 межсетевого контроля	48 CS6	11000000
0xB8	184	5 Важных	46 EF	10111000
0xA0	160		40 CS5	10100000
0x88	136	4 высших приоритета	34 AF41	10001000
0x80	128		32 CS4	10000000
0x68	104	3 Флэша	26 AF31	01101000
0x60	96		24 CS3	01100000
0x48	72	2 Непосредственных	18 AF21	01001000
0x40	64		16 CS2	01000000
0x20	32	1 Приоритет	8 CS1	00100000
0x00	0	0 Подпрограмм	0 Dflt	00000000

Пакеты Марка с DSCP/Приоритетами

Эти методы, как правило, используются для маркировки пакетов определенными маркировками DSCP/Приоритетов.

PBR

```
interface Ethernet1/0
ip policy route-map mark
!
access-list 150 permit ip host 172.16.1.2 host 172.16.254.2
!
route-map mark permit 10
match ip address 150
set ip precedence flash-override
```

MQC

```
class-map match-all my_flow
```

```
match access-group 150
!
policy-map marking
class my_flow
set ip precedence 4
!
interface Ethernet1/0
service-policy input marking
```

Эхо-запрос маршрутизатора

```
GM1-host#ping ip
Target IP address: 192.168.14.2
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface:
Type of service [0]: 136
...
<snip>
```

> **Примечание:** Это всегда - хорошая идея контролировать поток обычного трафика и профиль DSCP/приоритетов перед применением маркировки так, чтобы отмеченный трафик был уникален.

Маркированные пакеты монитора

Учет приоритета IP-трафика

```
interface Ethernet0/0
ip address 192.168.1.2 255.255.255.0
ip accounting precedence input
middle_router#show interface precedence
Ethernet0/0
Input
Precedence 4: 100 packets, 17400 bytes
```

Интерфейсный ACL

```
middle_router#show access-list 144
Extended IP access list 144
10 permit ip any any precedence routine
20 permit ip any any precedence priority
30 permit ip any any precedence immediate
40 permit ip any any precedence flash
50 permit ip any any precedence flash-override (100 matches)
60 permit ip any any precedence critical
70 permit ip any any precedence internet (1 match)
80 permit ip any any precedence network
```

Встроенный захват пакета

Встроенная функция захвата пакетов (EPC) является полезным инструментом для получения пакетов в уровне интерфейса, чтобы определить, если пакет достиг определенного устройства. Помните, что EPC работает хорошо для трафика открытого текста, но это может быть проблема, когда зашифрованы захваченные пакеты. Поэтому способы как маркировка DSCP/приоритетов, обсужденные ранее или другие символы IP, такие как длина пакета IP, должны использоваться вместе с EPC для создания устранения проблем более эффективным.

Трассировка пакетов Cisco IOS XE

Это - полезная возможность для отслеживания пути переадресации функции на всех платформах, которые выполняют Cisco IOS XE, такой как CSR1000v, ASR1000 и ISR4451-X.

Общие проблемы плоскости данных GETVPN

Устранение проблем IPsec dataplane для GETVPN главным образом не отличается от устранения проблем традиционного IPsec "точка-точка" dataplane проблемы за двумя исключениями из-за этих уникальных dataplane свойств GETVPN.

Время базирующийся сбой антивоспроизведения

В сети GETVPN сбоев TBAR может часто быть трудно устранить неполадки, так как больше нет попарных туннелей. Для устранения проблем сбоев TBAR GETVPN выполните эти шаги:

1. Определите, какой пакет отброшен из-за сбоя TBAR, и впоследствии определите шифрование GM.

   До Версии 15.3 (2) T системный журнал сбоя TBAR не распечатал адрес источника отказавшего пакета, таким образом, это делает очень трудным определить, какой пакет отказал. Это было значительно улучшено в Версии 15.3 (2) T и позже, где Cisco IOS распечатывает это:

```
middle_router#show access-list 144
Extended IP access list 144
10 permit ip any any precedence routine
20 permit ip any any precedence priority
30 permit ip any any precedence immediate
40 permit ip any any precedence flash
50 permit ip any any precedence flash-override (100 matches)
60 permit ip any any precedence critical
70 permit ip any any precedence internet (1 match)
80 permit ip any any precedence network
```

   История TBAR была также внедрена в этой версии:

```
GM2#show crypto gdoi gm replay
Anti-replay Information For Group G1:
Timebased Replay:
Replay Value : 621388.66 secs
Input Packets : 0 Output Packets : 0
Input Error Packets : 2 Output Error Packets : 0
Time Sync Error : 0 Max time delta : 0.00 secs


TBAR Error History (sampled at 10pak/min):
19:29:32.081 EST Wed Nov 13 2013: src=192.168.13.2; my_pst=620051.84 secs;
peer_pst=619767.09 secs; win=4
```

   Примечание: Усовершенствования, упомянутые ранее, были с тех пор внедрены в Cisco IOS XE идентификатором ошибки Cisco CSCun49335 и в Cisco IOS идентификатором ошибки Cisco CSCub91811.
   Для версий Cisco IOS, которые не имели этой функции, **debug crypto gdoi gm подробность воспроизведения** может также предоставить эту информацию, невзирая

на то, что эта отладка распечатывает информацию о TBAR для всего трафика (не, только пакеты понизились из-за сбоя TBAR), таким образом, не могло бы быть выполнимо работать в производственной среде.

```
GM2#show crypto gdoi gm replay
Anti-replay Information For Group G1:
Timebased Replay:
Replay Value : 621388.66 secs
Input Packets : 0 Output Packets : 0
Input Error Packets : 2 Output Error Packets : 0
Time Sync Error : 0 Max time delta : 0.00 secs


TBAR Error History (sampled at 10pak/min):
19:29:32.081 EST Wed Nov 13 2013: src=192.168.13.2; my_pst=620051.84 secs;
peer_pst=619767.09 secs; win=4
```

2. Как только источник пакета определен, должна существовать возможность для обнаружения шифрования GM. Затем псевдометка времени и на шифровании и на дешифровании GMS должна быть проверена для любого потенциального дрейфа псевдовремени. Лучший способ сделать это должно было бы синхронизировать и GMS и KS к NTP и периодически собирать псевдоинформацию о времени со ссылочными системными часами на всех них, чтобы определить, вызвана ли проблема расфазировкой тактовых сигналов на GMS.

GM1

```
GM1#show crypto gdoi gm replay
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is hardware calendar, *21:06:26.469 EST Wed Nov 13 2013

Anti-replay Information For Group G1:
Timebased Replay:
Replay Value              : 625866.26 secs
Input Packets : 0 Output Packets : 0
Input Error Packets : 0 Output Error Packets : 0
Time Sync Error : 0 Max time delta : 0.00 secs
```

GM2

```
GM2#show crypto gdoi gm replay
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is hardware calendar, *21:06:26.743 EST Wed Nov 13 2013

Anti-replay Information For Group G1:
Timebased Replay:
Replay Value              : 625866.51 secs
Input Packets : 4 Output Packets : 4
Input Error Packets : 2 Output Error Packets : 0
Time Sync Error : 0 Max time delta : 0.00 secs
```

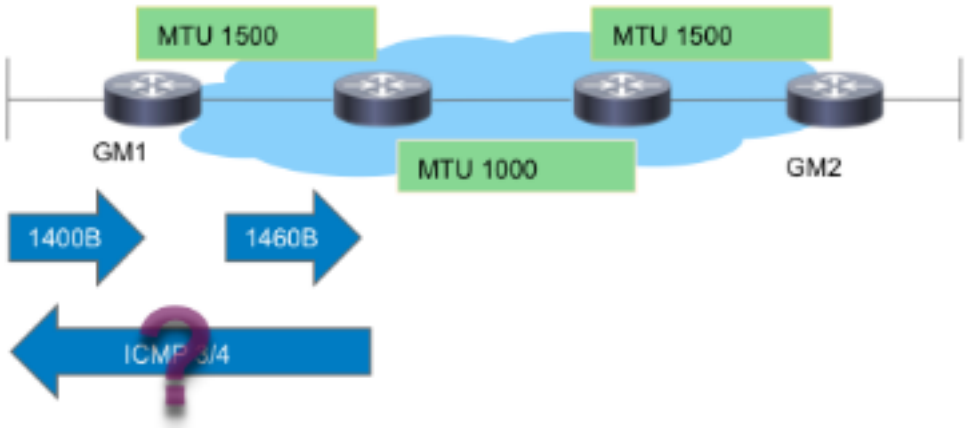
В предыдущем примере, если псевдовремя (как обозначено Значением Воспроизведения) существенно отличается между GMS, когда выходные данные перехвачены с тем же ссылочным временем, тогда проблема может быть приписана расфазировке тактовых сигналов.

Примечание: На маршрутизаторе Cisco Aggregated Services платформа серии 1000, из-за архитектуры платформы, канал передачи данных на процессоре Quantum Flow (QFP) фактически обращается к настенным часам для подсчета псевдосигналов времени. Когда стенное время синхронизации изменяется из-за синхронизования NTP,

это создало проблемы с TBAR. Эта проблема задокументирована с идентификатором ошибки Cisco CSCum37911.

PMTUD и сохранение заголовка GETVPN

С GETVPN Обнаружение MTU-маршрута (PMTUD) не работает между шифрованием и дешифрованием GMS, и большие пакеты с битом "Не фрагментировать" (DF) устанавливают, может быть помещен в черный список. Причина, что это не работает, происходит из-за Сохранения Заголовка GETVPN, где источник данных / адреса назначения (DA) сохранен в заголовке инкапсуляции ESP. Это изображено в этом образе:



Поскольку образ показывает, PMTUD ломается с GETVPN с этим потоком:

1. Большой пакет данных поступает в шифрование GM1.
2. Пакет ESP постшифрования передан из GM1 и отправлен к назначению.
3. Если будет транзитное соединение с IP MTU 1400 байтов, то пакет ESP будет отброшен, и ICMP 3/4 пакет, который слишком большое сообщение будет передаваться к источнику пакетов, который является источником пакета данных.
4. Пакет ICMP3/4 или отброшен из-за ICMP, не исключенного из политики шифрования GETVPN, или понизился конечным хостом, так как это ничего не знает о пакете ESP (не прошедшее поверку подлинности информационное наполнение).

Таким образом, PMTUD не работает с GETVPN сегодня. Для обхождения этой проблемы Cisco рекомендует эти шаги:

1. Внедрите "ip tcp adjust-mss" для сокращения оловянного заказа о размера сегмента пакета TCP, принимают издержки шифрования и MTU минимального пути в транзитной сети.
2. Очистите бит DF в пакете данных, поскольку они поступают в шифрование GM во избежание PMTUD.

IPsec общего назначения проблемы Dataplane

Большая часть IPsec dataplane устранение проблем походит на устраняющие неполадки традиционные Туннели IPSec "точка-точка". Одна из общих проблем является %CRYPTO-4-RECVD_PKT_MAC_ERR. Посмотрите Системный журнал "%CRYPTO-4-RECVD_PKT_MAC_ERR": сообщение об ошибках с Потерей Эхо-запроса По Устранению проблем Туннеля IPSec для большего количества подробных данных устранения проблем.

Типичные ошибки

Это сообщение может генерироваться, когда Пакет ipsec получен, который не совпадает с SPI в SADB. Посмотрите идентификатор ошибки Cisco CSCtd47420 - GETVPN - CRYPTO-4-RECVD_PKT_NOT_IPSEC сообщил для PKT, не совпадающего с потоком. Пример:

```
GM2#show crypto gdoi gm replay
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is hardware calendar, *21:06:26.743 EST Wed Nov 13 2013

Anti-replay Information For Group G1:
Timebased Replay:
Replay Value              : 625866.51 secs
Input Packets : 4 Output Packets : 4
Input Error Packets : 2 Output Error Packets : 0
Time Sync Error : 0 Max time delta : 0.00 secs
```

Это сообщение должно быть %CRYPTO-4-RECVD_PKT_INV_SPI, который является тем, о чем сообщают для традиционного IPsec, а также на некоторых аппаратных платформах, таких как ASR. Эта косметическая проблема была исправлена идентификатором ошибки Cisco CSCup80547: Ошибка в создании отчетов о CRYPTO-4-RECVD_PKT_NOT_IPSEC для pak ESP.

> **Примечание:** Эти сообщения могут иногда появляться из-за другого дефекта GETVPN CSCup34371: GETVPN GM останавливает decrytping трафик после TEK, повторно вводят.

В этом случае GM не может дешифровать трафик GETVPN, невзирая на то, что он имеет допустимый контекст безопасности IPSec в SADB (повторно вводимый SA). Проблема исчезает, как только SA истекает и удален из SADB. Эта проблема вызывает значительный простой, потому что TEK повторно вводит, выполнен заранее. Например, простой может составить 22 минуты в случае срока действия TEK 7200 секунд. См. описание дефекта для точного условия, которое нужно соблюдать для обнаружения с этим дефектом.

Устраните неполадки GETVPN на Платформах который Cisco IOS XE Выполнения

Команды для устранения неполадок

Платформы, которые выполняют Cisco IOS XE, имеют определяемые платформой реализации, и часто требуют определяемой платформой отладки для проблем GETVPN. Вот список команд, как правило, используемых для устранения проблем GETVPN на этих платформах:

show crypto eli все

статистика политики IPSec программного обеспечения show platform

ipsec программного обеспечения show platform fp активные материально-технические ресурсы

show platform hardware qfp активный ipsec функции spd все

show platform hardware qfp активная статистика понижается ясный

show platform hardware qfp активное ясное отбрасывание данных ipsec функции

show crypto ipsec sa

show crypto gdoi

покажите крипто-внутренний ipsec

debug crypto ipsec

ошибка debug crypto ipsec

состояния debug crypto ipsec

сообщение debug crypto ipsec

req hw debug crypto ipsec

debug crypto gdoi gm инфра подробность

debug crypto gdoi gm повторно вводит подробность

Общие проблемы ASR1000

Сбой установки политики IPsec (непрерывная перерегистрация)

Если ядро шифрования не поддерживает политику IPsec или полученный алгоритм, ASR1000 GM мог бы продолжить регистрироваться к Серверу ключей. Например, на Структуре с двухслойным пассивирующим покрытием из оксида и нитрида кремния базировал платформы ASR (такие как ASR1002), Комплект-B или политика SHA2 не поддерживаются, и это может вызвать непрерывные перерегистрационные признаки.

Общие Проблемы Миграции/Обновления

Ограничение ASR1000 TBAR

На платформе ASR1000 идентификатор ошибки Cisco, который исправляют CSCum37911, представил ограничение на эту платформу, где не поддерживается время TBAR меньше чем 20 секунд. Посмотрите Ограничения для GETVPN на XE IOS.

Этот дефект усовершенствования был открыт для снимания этого ограничения, идентификатор ошибки Cisco CSCuq25476 - ASR1k должен поддержать размер окна TBAR GETVPN меньше чем 20 секунд.

Обновление: Это ограничение было с тех пор снято с исправлением для идентификатора ошибки Cisco CSCur57558, и это больше не ограничение в XE3.10.5, XE3.13.2 и коде следующих версий.

Также обратите внимание для GM, который работает на платформах Cisco IOS XE (ASR1k

или ISR4k), это настоятельно рекомендовано это, устройство выполняет версию с исправлением для этой проблемы, если включен TBAR; идентификатор ошибки Cisco CSCut91647 - GETVPN на XE IOS: GM неправильно отбрасывает пакеты из-за сбоя TBAR.

Проблема классификации ISR4x00

Регрессия была найдена на платформе ISR4x00, где проигнорирована запрещать политика. Для получения дополнительной информации посмотрите идентификатор ошибки Cisco CSCut14355 - GETVPN - ISR4300 GM игнорирует, запрещают политику.

Дополнительные сведения

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