КОД БЕЗОПАСНОСТИ

Аппаратно-программный комплекс шифрования

Континент

Версия 3.7

Рекомендации по эксплуатации

Редакция 1.2

Почтовый адрес:	**115127, Россия, Москва, а/я 66** **ООО "Код Безопасности"**
Телефон:	**8 495 982-30-20**
E-mail:	**info@securitycode.ru**
Web:	**https://www.securitycode.ru**

Оглавление

Список сокращений

КК	Криптографический коммутатор
КТ	Контрольная точка
КШ	Криптографический шлюз
ПУ ЦУС	Программа управления ЦУС
ЦУС	Центр управления сетью криптографических шлюзов
IP	Internet Protocol
MSS	Maximum Segment Size
MTU	Maximum Transmission Unit
NAT	Network Address Translation
STUN	Session Traversal Utilities for NAT
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VPN	Виртуальная частная сеть

Введение

Рекомендации предназначены для администраторов изделия "Аппаратно-программный комплекс шифрования "Континент". Версия 3.7" (далее — комплекс). В них содержатся дополнительные сведения по эксплуатации комплекса.

Сайт в интернете. Информация о продуктах компании "Код Безопасности" представлена на сайте https://www.securitycode.ru/products/.

Служба технической поддержки. Связаться со службой технической поддержки можно по телефону 8 800 505-30-20 или по электронной почте support@securitycode.ru.

Учебные курсы. Освоить аппаратные и программные продукты компании "Код Безопасности" можно в авторизованных учебных центрах. Перечень учебных центров и условия обучения представлены на сайте компании https://www.securitycode.ru/company/education/training-courses/. Связаться с представителем компании по вопросам организации обучения можно по электронной почте education@securitycode.ru.

Начало взаимодействия КШ и ЦУС

Взаимодействие КШ и ЦУС происходит следующим образом (см. Рис. 1):

1. КШ стартует и каждые 20 секунд отправляет в ЦУС UDP-пакеты с порта 5100 на порт 5101 (keep-alive).
2. ЦУС проверяет имитовставку полученных UDP-пакетов:
   - если ключи управления не совпадают, ЦУС отвечать не будет, и каждые 20 секунд в журнале появляется запись "Ошибка имитовставки <№ КШ>";
   - если ключи управления совпадают, ЦУС отвечает с порта 5101 на порт 5100. После перезагрузки ЦУС и КШ идентификатор UDP-сессии не совпадет.
3. Далее происходит TCP-согласование UDP-сессии:
   - если UDP-сессия согласована, в ПУ ЦУС КШ отображается со статусом "включен" и управляется ЦУС;
   - если UDP-сессия не согласована, в ПУ ЦУС КШ отображается со статусом "выключен" или со статусом "включен" с зеленой стрелкой. В таком случае КШ не выполняет команды ЦУС, которые передаются через TCP-трафик.

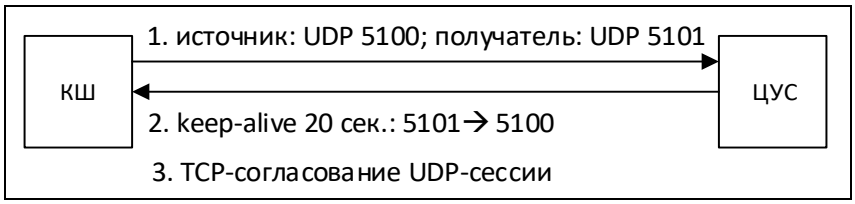

Рис. 1 Взаимодействие КШ и ЦУС

Построение VPN-туннелей с помощью STUN

В процессе существования VPN-туннелей между КШ (настроены связи) каждый КШ с периодом 10 секунд асинхронно отправляет на адреса партнеров тестовые туннельные пакеты. Ответы на эти пакеты не ожидаются. Пакеты отправляются с учетом созданных классов трафика и их настроек.

В ЦУС реализован механизм STUN, который управляет настройками шифратора КШ. А именно — транслирует партнерам по связям те адреса/порты КШ, которые зафиксированы в настройках STUN-сервера. Настройки могут быть:

- динамическими — IP-адреса, с которых КШ подключился к ЦУС;
- статическими — заданными администратором вручную.

Внимание! КШ также могут изменить настройки шифраторов друг друга. Это происходит в случае, если КШ получил туннельные пакеты с IP-адреса и порта "парного" КШ, которые не совпадают с полученными от ЦУС.

На Рис. 2 показан вариант построения VPN-туннеля, когда у каждого КШ несколько внешних интерфейсов (внешних каналов), например, с номерами 0, 1, 2. Если эти интерфейсы расположены в разных, непересекающихся по маршрутизации каналах, то построить VPN-туннель между КШ возможно только с помощью дополнительных настроек маршрутизации (динамической, статической, в том числе с использованием Multi-WAN) и внесения статических записей в STUN-сервер.

Причина в том, что КШ может подключиться к ЦУС только по одному из каналов. Задать приоритет и определить заранее, по какому каналу произойдет подключение к ЦУС при работоспособности всех каналов, невозможно.

Примечание. Для построения туннеля по конкретному IP-адресу (с использованием статической записи в STUN) должен совпасть и IP-адрес, и порт. Для этого можно локально в ЦУС для каждого КШ, находящегося за NAT, добавить его IP-адрес в формате "<ID>:<IP-адрес>", а порт КШ должен соответствовать классам трафика.

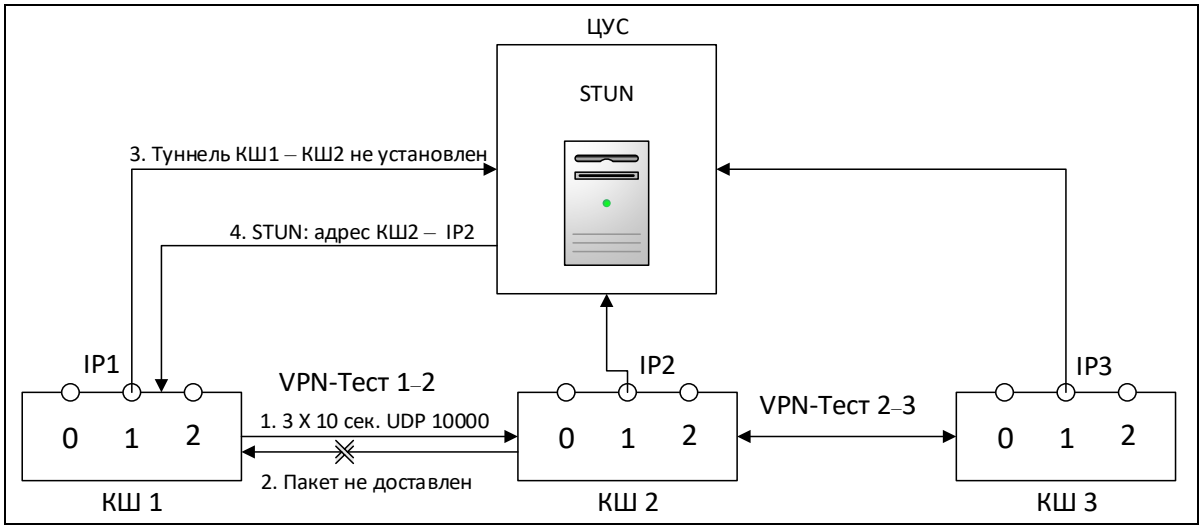

Рис. 2 Построение VPN-туннеля с помощью STUN

В начале создания связи ЦУС отправляет на каждый КШ адреса с младших по номеру интерфейсов (адреса нулевых интерфейсов или младших по номеру VLAN-интерфейсов).

В процессе работы STUN-сервер ЦУС отправляет на каждый КШ адреса интерфейсов, с которых КШ подключились к ЦУС (динамические записи STUN-сервера) или адреса из статических записей STUN-сервера.

Для построения туннеля КШ отправляют тестовые пакеты друг другу раз в 10 секунд (каждый КШ посылает пакеты на своем ключе) асинхронно по тем адресам, которые были получены от ЦУС.

В общем случае интерфейсы КШ с ЦУС должны присутствовать во всех каналах.

Ниже приведены сценарии построения VPN-туннелей с помощью STUN-сервера.

Сценарий 1

Исходные данные:

- Инфраструктура VPN — топология "звезда".
- Два непересекающихся по маршрутизации канала связи — интернет и "частная" IP-адресация.
- Оба канала — уровень L3.
- Существует приоритет "частного" канала.
- Адреса всех КШ (включая ЦУС) — реальные (NAT не применяется).

В данном случае на КШ центрального офиса и ЦУС целесообразно настроить статическую маршрутизацию со шлюзом по умолчанию в интернет. Пулам адресов "частного" канала задать маршруты в "частный" канал. На КШ филиалов — настроить Multi-WAN с приоритетом в "частный" канал.

КШ центрального офиса может подключиться к ЦУС по любому из каналов с одинаковой вероятностью, поэтому в STUN-сервер ЦУС может быть помещен любой из внешних адресов КШ. Допустим, это будет "интернет" IP-адрес КШ центрального офиса, тогда:

1. При создании связей (если внешний IP-адрес КШ установлен на младший по номеру интерфейс) и дальнейшей работе ЦУС будет отправлять на КШ филиалов "интернет" IP-адрес КШ центрального офиса, который попал в STUN-сервер.
2. КШ филиалов отправляют пакеты (с интервалом 10 секунд) на КШ центрального офиса по приоритетному "частному" каналу.
3. КШ центрального офиса (примерно в течение 30 секунд) не получает от КШ филиалов пакеты (так как они отправляют их на "интернет" IP-адрес, но в "частный" канал).
4. КШ центрального офиса отправляет в ЦУС сообщение, что туннель между КШ центрального офиса и КШ филиала не построен.

5. STUN считывает IP-адрес КШ филиала (с которого КШ подключился к ЦУС из "частной" сети) и отправляет его на КШ центрального офиса.
6. КШ центрального офиса отправляет тестовые туннельные пакеты согласно маршрутизации, в "частную" сеть со своего частного адреса.
7. Они достигают КШ филиала и тот перенастраивает свой шифратор на "частный" адрес КШ центрального офиса и начинает отправлять пакеты на новый адрес.
8. После этого восстанавливается работоспособность VPN-туннеля.
9. В случае если происходит отказ канала в филиале, маршрутизация перестраивается на интернет-канал и далее события происходят следующим образом:
   - VPN-туннель перестанет работать.
   - КШ филиала подключится к ЦУС со своего "интернет" IP-адреса.
   - "Интернет" IP-адрес КШ филиала запишется в STUN-сервер и ЦУС передаст его на КШ центрального офиса.
   - КШ центрального офиса начнет посылать тестовые туннельные пакеты на "интернет" IP-адрес КШ филиала.
   - КШ филиала после получения пакетов перенастроит свой шифратор.
   - Работоспособность VPN-туннеля восстановится.
10. В случае если КШ центрального офиса изначально подключится к ЦУС по "частному" адресу, в STUN-сервер ЦУС будет помещен этот адрес. И тогда VPN-соединения будут устанавливаться без потери времени.

Сценарий 2

Рассмотрим сценарий 1 с некоторым изменением сетевой архитектуры.

Пусть один (или более) КШ филиала выходит в интернет из-за Hide NAT. В этом случае настроек Multi-WAN на стороне филиалов недостаточно.

Проблема будет в следующем: когда создадутся условия **п. 10** сценария 1, то при событиях, указанных в **п. 9**, туннель не установится. КШ филиала подключится к ЦУС через интернет-канал, ЦУС будет его видеть, но его настройки в шифратор КШ центрального офиса не отправит, так как он "спрятан" за Hide NAT и доступа к нему из интернета не будет. В результате туннель не установится из-за некорректных настроек шифраторов обоих КШ. Необходимо, чтобы настройки были корректны хотя бы у одного КШ.

Выход из данной ситуации — поместить внешний IP-адрес КШ центрального офиса в STUN-сервер ЦУС **статически**, используя локальное меню ЦУС.

В этом случае, администратор ЦУС создаст ситуацию по **п. 1** сценария 1 на постоянной основе. Это позволит строиться VPN-соединениям в любом случае.

Сценарий 3

Рассмотрим сценарий 2 с условием, что ЦУС и КШ центрального офиса находятся за Static NAT. При этом ЦУС и КШ центрального офиса будут взаимодействовать только по внутренним "частным" адресам.

До создания конфигурационных файлов всех КШ — для их взаимодействия с ЦУС — необходимо добавить альтернативный адрес в настройках ЦУС, соответствующий адресу NAT для ЦУС.

Как и в предыдущем сценарии, необходимо поместить внешний IP-адрес КШ центрального офиса в STUN-сервер ЦУС **статически**, используя локальное меню ЦУС.

Сценарий 4

Рассмотрим сценарий 1 при условии необходимости построения VPN-структуры с топологией Full-Mesh.

Для реализации данного решения необходимо применить настройки динамической маршрутизации на всех КШ и ЦУС.

Для получения примеров настройки КШ в описанных условиях обращайтесь в техническую поддержку компании "Код Безопасности".

Сценарий 5

Если в рассматриваемом сценарии один из каналов имеет уровень L2 и он не основной (резервный), то при установлении VPN-соединения по данному каналу оно будет существовать и не переключится на другой канал. Причина в том, что туннель будет всегда работоспособен независимо от правил маршрутизации.

Сценарий 6

Если оба КШ, между которыми необходимо настроить VPN-соединение, находятся за Hide NAT, то в этом случае VPN-туннель никогда не установится. Необходимо настроить хотя бы для одного КШ Static NAT.

Настройки VPN

Настройки VPN КШ — адрес и порт 10000 (для класса трафика по умолчанию). Эти настройки ЦУС берет из STUN. Когда ЦУС принимает пакеты от КШ, то анализирует адрес, порт источника и определяет тип NAT:

- если порт источника 10000, он неизменный, а адрес источника совпадает с адресом на интерфейсе, то NAT не настроен;
- если порт и адрес изменились (но не меняются для разных пакетов; КШ для этого отправляет сразу два тестовых пакета в STUN по портам UDP 5106 и 5107), то настроен Static NAT;
- если меняются и порты в динамике, и адрес, то настроен Hide NAT.

В случае, когда VPN-туннель не установлен, в описании задач КШ отображается команда "Динамическое обновление параметров парной связи". Это значит, что ЦУС отправляет на КШ настройки из STUN — адрес, порт и т. д. Данная команда имеет отношение только к адресации и портам (не имеет отношения к ключам шифрования).

Смена ключей парной связи

Ключи парной связи могут меняться автоматически или по команде администратора.

Срок действия ключей определяется временным интервалом или количеством зашифрованного и расшифрованного трафика. Срок действия ключей парной связи контролируется КШ:

1. Срок действия ключей парной связи — не более 12 месяцев. Как только администратор установил новую парную связь или ЦУС автоматически сгенерировал новый ключ парной связи, начинает работать счетчик на 11 месяцев (чтобы была возможность заранее поменять ключи парной связи). В момент истечения счетчика на 11 месяцев КШ запросит у ЦУС новый ключ:
   - если ЦУС включен, сгенерируется новый ключ;
   - если ЦУС выключен в момент истечения счетчика, новый ключ не сгенерируется. Через месяц (когда пройдет 12 месяцев) VPN-трафик заблокируется.
2. Срок действия ключей парной связи закончится после выполнения шифрования $2^{32}*70$ пакетов, то есть 70 циклов по 2^{32} пакетов.

   Примечание. Каждый пакет нумеруется и шифруется своим ключом шифрования, который зависит от номера пакета.

   До начала шифрования пакетов с использованием новых ключей парной связи счетчик max_counter_low равен 70. После выполнения шифрования $2^{32}*70$ пакетов счетчик max_counter_high станет равным 0 и КШ запросит у ЦУС новый ключ:
   - если ЦУС включен, сгенерируется новый ключ и шифрование пакетов продолжится на нем;
   - если ЦУС выключен, новый ключ не сгенерируется и шифрование пакетов прекратится.

Настройки параметров шифратора

Распределение пакетов между ядрами с учетом соединений

Каждая сессия КШ или КК шифруется либо на одном ядре, либо все ядра участвуют в шифровании пакетов этой сессии. Распределение по нескольким ядрам происходит на основании L3-хэш или L2-хэш, которые считаются от сокета (L3/L4-хэш) или от MAC-адреса (L2-хэш).

Данная настройка в локальном меню имеет два режима:

- Разрешение распределения пакетов с учетом соединений — будет задействовано только одно ядро: пакеты обрабатываются последовательно.

  На КШ по умолчанию разрешено распределение пакетов с учетом соединений, то есть в КШ все пакеты одного соединения шифруются одним ядром (и ответные пакеты шифруются этим же ядром). Если запретить распределение, то один пакет будет шифроваться одним ядром, другой — другим ядром и т. д.

- Запрет распределения пакетов с учетом соединений — будут задействованы все ядра: пакеты обрабатываются асинхронно, повышается общая производительность, но понижается качество одной сессии.

  На КК по умолчанию запрещено распределение пакетов с учетом соединений, что приводит к переупорядочиванию пакетов из-за асинхронной работы. Пакеты обрабатываются асинхронно, в результате чего пакеты, которые должны прийти по порядку, приходят в другом порядке. Следовательно, качество TCP-соединения ухудшается и снижается скорость передачи данных.

Важно настраивать этот параметр под свою схему.

Настройку "Разрешение/запрет распределения пакетов с учетом соединений" можно проверить в технологическом отчете по значению параметра:

- net.inet.ipcrypt.l3_hash=1 — разрешено на КШ (по умолчанию);
- net.inet.ipcrypt.l3_hash=0 — запрещено на КШ;
- net.inet.ipcrypt.l2_hash=1 — разрешено на КК;
- net.inet.ipcrypt.l2_hash=2 — разрешено на КК при установке определнных патчей на 3.7.7 и 3.9.0 в отношении L3/L4;
- net.inet.ipcrypt.l2_hash=0 — запрещено на КК (по умолчанию).

Фрагментация пакетов при работе устройства

При шифровании КК порождается фрагментированный трафик. В результате на входе пакет 1500 Байт, а на выходе два шифрованных пакета (для КК overhead — не менее 70 Б). Поэтому рекомендуется до поступления пакетов на порт коммутации КК уменьшать их MTU.

КШ в общем случае сам автоматически согласовывает MTU с внутренними ресурсами до значения 1448. Изменять настройки по умолчанию в данном случае не требуется.

Начиная с версии 3.7.7.752 (КК) для TCP-сессии возможно устанавливать значение MSS, за счет чего будет регулироваться MTU:

- на КШ значение MSS рекомендовано устанавливать не более 1408 Б (MSS=1500 Б-20 Б (TCP-заголовок)-20 Б (IP-заголовок)-52 Б (overhead));
- на КК — не более 1390 Б (MSS=1500 Б-20 Б (TCP-заголовок)-20 Б (IP-заголовок)-70 Б (overhead)).

Контрольные точки для Multi-WAN

В настройках Multi-WAN указываются два внешних интерфейса, выбирается режим "Обеспечение отказоустойчивости канала связи (Failover)", задается КТ для каждого интерфейса.

Диагностика канала связи — это тестирование доступности контрольной точки. Рекомендуется контрольную точку выбирать в канале связи (или, например, "парного" КШ).

Если КТ доступны, устанавливается маршрут по умолчанию для этого интерфейса КШ (0.0.0.0/0 — адрес шлюза):

- если КТ 1 доступна, маршрут по умолчанию станет 10.1.1.1;
- если КТ 2 доступна, маршрут по умолчанию станет 10.2.2.1 (см. Рис. 3);
- если обе КТ недоступны, маршрут по умолчанию может измениться на 127.0.0.1 и канал связи перестанет работать.

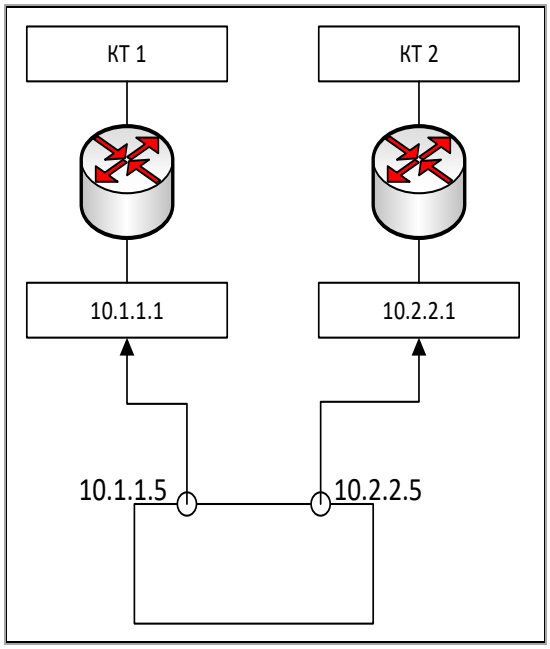

Рис. 3 Маршруты по умолчанию

Рекомендуется прописать статический маршрут в таблице маршрутизации или не задавать КТ для одного из каналов (если их два или три), тогда маршрут по умолчанию на КШ останется актуальным.

Примечание. Маршрут по умолчанию не влияет на туннели, которые установились вне маршрута по умолчанию. Если КШ имеет L2-канал и на нем установился туннель (по MAC-адресам), то этот туннель не разорвется до тех пор, пока существует L2-канал (даже если он не приоритетный и низкоскоростной). Маршрутизация не повлияет на этот туннель.

Переключение КШ в кластере

Среднее время переключения между основным и резервным КШ — 0,5-1 сек. Каждые полсекунды оцениваются интерфейсы.

Балл выключенного состояния внешнего интерфейса — 100, внутреннего интерфейса — 1.

Баллы всех выключенных внешних интерфейсов — 2000, всех внутренних — 1000.

Соответственно, если происходит отказ одного внешнего интерфейса, то прибавляется 100 баллов к исходному состоянию. Если отказ внутреннего — прибавляется 1 балл. Если произошел отказ всех интерфейсов, то прибавляется 2000 и 1000 баллов для внешних и внутренних интерфейсов соответственно.

Чем больше баллов, тем "хуже" состояние модуля.

Ниже приведены сценарии переключений между двумя КШ в кластере.

Сценарий 1

КШ 1 — основной, КШ 2 — резервный. У каждого КШ два внутренних и два внешних интерфейса. На КШ 1 отключается один внешний интерфейс (плюс 100 баллов), на КШ 2 отключается один внутренний интерфейс (плюс 1 балл). Теперь КШ 1 стал резервным, а КШ 2 — основным.

Сценарий 2

Дополнительно к сценарию 1 на КШ 1 отключается внутренний интерфейс (стало 100+1), на КШ 2 отключается внутренний интерфейс (стало 1000 баллов). Теперь КШ 1 станет основным, КШ 2 — резервным, так как на КШ 2 отключены оба внутренних интерфейса.