Код безопасности
ГК «Информзащита»

Аппаратно-программный комплекс шифрования

Континент
Версия 3.5

Руководство администратора

Тестирование каналов связи



© Компания "Код Безопасности", 2010. Все права защищены.

Все авторские права на эксплуатационную документацию защищены.

Этот документ входит в комплект поставки изделия. На него распространяются все условия лицензионного соглашения. Без специального письменного разрешения компании "Код Безопасности" этот документ или его часть в печатном или электронном виде не могут быть подвергнуты копированию и передаче третьим лицам с коммерческой целью.

Информация, содержащаяся в этом документе, может быть изменена разработчиком без специального уведомления, что не является нарушением обязательств по отношению к пользователю со стороны компании "Код Безопасности".

Почтовый адрес:	**127018, г. Москва, ул. Сущевский вал, дом 47, стр. 2, помещение №1**
Телефон:	**(495) 980-23-45**
Факс:	**(495) 980-23-45**
e-mail:	**info@securitycode.ru**
Web:	**http://www.securitycode.ru**

Версия: 3.5 Последнее обновление: 29-04-10

Оглавление

Введение **4**

Общие сведения **5**

Подготовка к тестированию **5**

Тестирование с помощью программы PortCheck **6**

Тестирование канала связи АП–СД в программе ChannelChecker **7**

Приложение **8**

Взаимодействующие компоненты комплекса 8

Тестовые сообщения программы PortCheck 9

Протоколы и порты 10

Документация **11**

Введение

Данное руководство предназначено для администратора изделия "Аппаратно-программный комплекс шифрования "Континент" (далее — комплекс "Континент", АПКШ "Континент", Комплекс). В руководстве приводится общий порядок применения сервисных программ PortCheck и ChannelChecker.

Приступая к изучению данного руководства, необходимо предварительно ознакомиться с документами [1] и [2].

Условные обозначения

В данном руководстве для выделения некоторых элементов текста используется ряд условных обозначений. Особо важная и дополнительная информация отмечена пиктограммами на полях:



- Так обозначается дополнительная информация.
- Такой пиктограммой выделяется важная информация, которую необходимо принять во внимание.

Другие источники информации

Сайт в Интернете. Если у вас есть доступ в Интернет, вы можете посетить сайт компании "Код Безопасности" (http://www.securitycode.ru/) или связаться с представителями компании по электронной почте (support@securitycode.ru и hotline@infosec.ru).

Учебные курсы. Освоить аппаратные и программные продукты компании "Код Безопасности" можно на курсах Учебного центра "Информзащита". Перечень курсов и условия обучения представлены на сайте http://www.itsecurity.ru/. Связаться с представителем учебного центра можно по электронной почте (edu@infosec.ru).

Общие сведения

Организация виртуальных частных сетей (Virtual Private Network — VPN) предусматривает объединение территориально распределенных локальных вычислительных сетей (сегментов VPN) и отдельных компьютеров предприятия в единую защищенную сеть с использованием общедоступных сетей обмена данными. В связи с этим в VPN широко применяются стандартные протоколы IP, TCP и UDP. Для идентификации отдельных потоков данных, порождаемых взаимодействием различных процессов (программ), в протоколах TCP и UDP используются идентификаторы портов. Для обеспечения уникального адреса каждого процесса идентификатор используемого им порта объединяется с IP-адресом компьютера. В результате получается сокет (socket — разъем), являющийся уникальным в объединенных локальных сетях. Соединение в сети полностью идентифицируется парой сокетов взаимодействующих процессов.

Основным назначением Комплекса является защита информации, передаваемой между сегментами VPN по общедоступным сетям связи, а также защита сегментов VPN от проникновения извне. Выполнение данных задач предусматривает взаимодействие между процессами (программами) различных компонентов Комплекса.

Для передачи зашифрованного трафика между компонентами Комплекса используется IP-протокол с номером 250. Передача служебных пакетов осуществляется по протоколам и портам, перечисленным на стр. 10. На пути трафика, передаваемого между компонентами Комплекса (абонентским пунктом и сервером доступа или между программой управления и сервером доступа и т. д.) могут находиться межсетевые экраны или другое оборудование, осуществляющее фильтрацию IP-пакетов. В этом случае для данных устройств необходимо установить настройки, разрешающие прохождение зашифрованного трафика и служебных пакетов Комплекса.

Программа PortCheck разработана для тестирования установленных правил фильтрации межсетевых экранов, находящихся на пути зашифрованного и служебного трафика между компонентами Комплекса. Данная сервисная программа имитирует взаимодействие процессов (программ) различных компонентов Комплекса и проверяет возможность обмена данными между ними. Результаты проверки отображаются в окне программы.



С помощью программы PortCheck тестируется взаимодействие между абонентским пунктом (АП —версии ниже 3.2) и сервером доступа (СД), а также взаимодействие между центром управления сетью (ЦУС) и криптошлюзом (КШ — версий 2 и 3). Для тестирования взаимодействия между АП (версии 3.2 и выше) и СД используется программа ChannelChecker.

Подготовка к тестированию

Перед проведением тестирования каналов связи между сегментами VPN, в которых устанавливаются (или уже установлены) компоненты Комплекса, необходимо выполнить подготовительные действия.

Для подготовки к тестированию:

1. В сегментах VPN определите компьютеры, которые будут имитировать компоненты Комплекса.



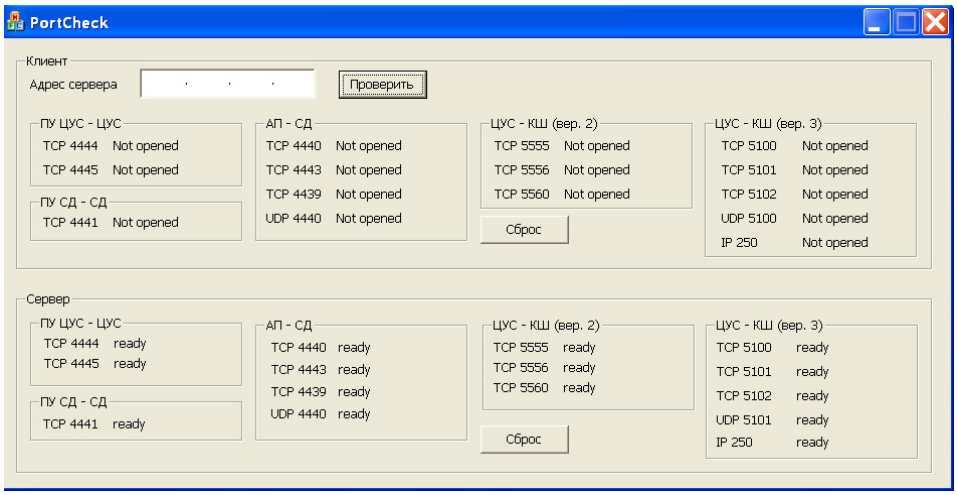
Программы PortCheck и ChannelChecker предназначены для работы на компьютерах, функционирующих под управлением Windows 2000 Professional (SP4) или Windows XP Professional (SP2).

2. Имитирующим компьютерам установите IP-адреса, предусмотренные для компонентов Комплекса.
3. С установочного диска скопируйте файлы PortCheck.exe и ChannelChecker.exe на компьютеры, имитирующие соответствующие компоненты Комплекса.

Тестирование с помощью программы PortCheck

Для проведения тестирования:

1. На компьютерах, имитирующих компоненты Комплекса, запустите программу PortCheck. На экране отобразится стартовое окно программы:



Поскольку взаимодействие между компонентами Комплекса организовано по технологии "клиент-сервер", стартовое окно программы содержит поле для ввода адреса компьютера, имитирующего сервер, а также две однотипные группы полей "Клиент" и "Сервер". В этих группах отображаются сообщения программы о стадии и результатах проверки возможности прохождения IP-пакетов для каждого используемого протокола и порта (сокета). Перечень сообщений программы приведен на стр. 9.

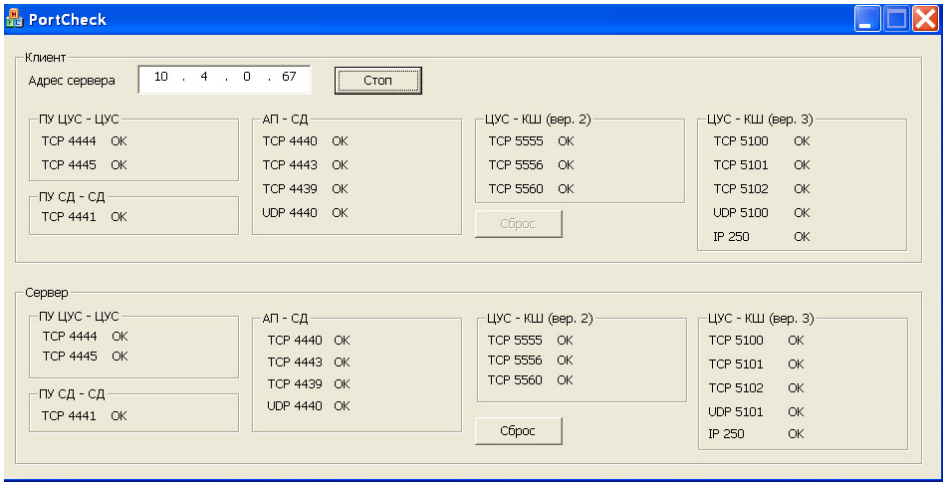
2. На компьютере, выполняющем функцию клиента в тестируемой паре взаимодействующих сегментов VPN, в поле "Адрес сервера" введите IP-адрес сервера.



При проведении тестирования программа PortCheck, установленная на компьютере, имитирующем сервер, работает в автоматическом режиме.

3. Нажмите кнопку "Проверить".

Программа осуществит проверку поддержки в используемом канале связи протокола IP 250. Кроме этого, последовательно организует соединение и осуществит проверку возможности обмена данными между компонентами Комплекса. Результаты тестирования отображаются в окне программы обоих компьютеров, имитирующих взаимодействующие сегменты VPN, справа от наименования каждого используемого протокола и порта (см. рисунок ниже). Описание принятых обозначений взаимодействующих компонентов Комплекса приводится на стр. 8.



4. Для остановки процесса тестирования нажмите кнопку "Стоп". Для продолжения нажмите кнопку "Проверить".
5. Для тестирования взаимодействия с другим сегментом VPN нажмите кнопку "Сброс" в клиентской и серверной группе полей для удаления предыдущих результатов. В поле "Адрес сервера" введите IP-адрес другого компонента Комплекса, выполняющего функцию сервера, и нажмите кнопку "Проверить".

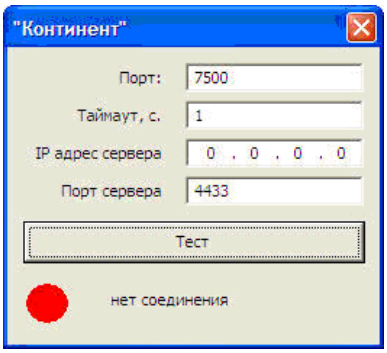
Тестирование канала связи АП–СД в программе ChannelChecker

Программа ChannelChecker используется для тестирования взаимодействия между абонентским пунктом (версии 3.2 и выше) и сервером доступа. Программа имитирует работу абонентского пункта, реализуя установку и разрыв PPP-соединения.

Для проведения тестирования:

1. На компьютере, имитирующем АП, запустите программу ChannelChecker.exe.

   На экране отобразится стартовое окно программы:



2. В поле "Порт" укажите UDP-порт АП, через который программа проверки будет взаимодействовать с сервером доступа.
3. В поле "Тайм-аут" укажите отрезок времени (в секундах), в течение которого ожидается ответ от сервера доступа.
4. В поле "IP-адрес сервера" укажите адрес сервера доступа, взаимодействие с которым тестируется.
5. В поле "Порт сервера" укажите UDP-порт СД, через который программа проверки будет взаимодействовать с сервером доступа.
6. Нажмите кнопку "Тест" для начала процесса тестирования.
7. Результат тестирования отобразится в окне сообщения:
   - в случае если соединение между АП и СД было успешно установлено, появится сообщение "Проверка успешно завершена";
   - в случае если за указанный в поле "Тайм-аут" отрезок времени ответ от СД не получен, появится сообщение "Тайм-аут истек".

Приложение

Взаимодействующие компоненты комплекса

Обозначение	Описание
ПУ ЦУС — ЦУС	Программа управления ЦУС — Центр управления сетью
АП — СД	Абонентский пункт — Сервер доступа
ЦУС — КШ (вер. 2)	Центр управления сетью — Криптографический шлюз (АПКШ "Континент" 2.00.76 и более ранние версии)
ЦУС — КШ (вер. 3)	Центр управления сетью — Криптографический шлюз (АПКШ "Континент" 3.00.28 и более поздние версии)

Тестовые сообщения программы PortCheck

Результаты тестирования отображаются в виде сообщений для каждого протокола, используемого Комплексом.

Сообщение	Описание
	IP (серверная часть):
ready	Серверная часть готова
got message	Сообщение получено
OK	OK
address/protocol busy	Адрес или протокол заняты
internal error	Внутренняя ошибка
send failed	Ошибка отсылки
need admin rights	Для проверки требуются права Администратора
	IP (клиентская часть):
not probed	Проверка не проводилась
data sent	Данные отосланы
OK	OK
internal error	Внутренняя ошибка
send failed	Ошибка отсылки
receive failed	Ошибка получения
interrupted	Процесс проверки прерван
timed out	Тайм-аут истек
protocol not available	Протокол недоступен
need admin rights	Для проверки требуются права Администратора
	TCP (серверная часть)
ready	Порт готов к установлению соединения
connected	Соединение установлено
got message	Сообщение получено
OK	OK
port busy	Порт занят
internal error	Внутренняя ошибка
	TCP (клиентская часть)
not connected	Соединение не установлено (проверка не началась)
connected	Соединение установлено
data sent	Данные отосланы
OK	OK
connection failed	Соединение установить не удалось
send failed	Ошибка отсылки
receive failed	Ошибка получения
interrupted	Процесс проверки прерван
internal error	Внутренняя ошибка
	UDP (серверная часть)
ready	Привязаны к порту
got message	Сообщение получено
OK	OK
port busy	Порт занят
internal error	Внутренняя ошибка
send failed	Ошибка отсылки
	UDP (клиентская часть)
not probed	Проверка не проводилась
data sent	Данные отосланы
OK	OK
internal error	Внутренняя ошибка
send failed	Ошибка отсылки
receive failed	Ошибка получения
interrupted	Процесс проверки прерван
timed out	Тайм-аут истек
remote port closed	Порт сервера закрыт

Протоколы и порты

В данном разделе представлены сведения о протоколах и портах, используемых для связи между компонентами комплекса.

Если на пути зашифрованного трафика находятся межсетевые экраны или другое оборудование, осуществляющее фильтрацию IP-пакетов, необходимо создать для них правила, разрешающие прохождение служебных пакетов комплекса "Континент" по протоколам и портам, указанным в таблице.

Протокол/порт	Назначение	Источник/получатель	Примечание
TCP/4431	Управление Сервером доступа	Программа управления Сервером доступа / Сервер доступа	АПКШ "Континент" 3.2.21 и более поздние версии
TCP/4444	Передача сообщений от Программы управления ЦУС к ЦУС и обмен сообщениями между ЦУС и Агентом ЦУС	Программа управления ЦУС / ЦУС; Агент ЦУС и СД / ЦУС; ЦУС / Агент ЦУС и СД	
TCP/4445	Передача обновлений ПО от Программы управления ЦУС к ЦУС и обмен сообщениями между Программой управления ЦУС и Агентом ЦУС	Программа управления ЦУС / ЦУС; Программа управления ЦУС / Агент ЦУС и СД; Агент ЦУС и СД / Программа управления ЦУС	АПКШ "Континент" 3.1.18 и более поздние версии
TCP/4446	Аутентификация хостов в защищенном сегменте сети	Компьютер с установленной программой "Клиент аутентификации хоста" / КШ	
TCP/5100	Передача сообщений от ЦУС к КШ и обмен сообщениями между КШ в кластере	ЦУС / КШ; Основной КШ / Резервный КШ; Резервный КШ / Основной КШ	АПКШ "Континент" 3.0 и более поздние версии
TCP/5101	Передача сообщений от КШ к ЦУС	КШ / ЦУС	АПКШ "Континент" 3.0 и более поздние версии
TCP/5102	Передача файлов от ЦУС к КШ	ЦУС / КШ	АПКШ "Континент" 3.0 и более поздние версии
UDP/5101	Передача сообщений от КШ к ЦУС	КШ (исходящий порт 5100) / ЦУС	АПКШ "Континент" 3.0 и более поздние версии
UDP/5557	Передача сообщений об активности между КШ в кластере	Основной КШ / Резервный КШ; Резервный КШ / Основной КШ	АПКШ "Континент" 3.0 и более поздние версии
UDP/4433	Обмен сообщениями между сервером доступа и абонентским пунктом	Сервер доступа / Абонентский пункт	Номер порта по умолчанию; изменяется в программе управления сервером доступа. АПКШ "Континент" 3.2.21 и более поздние версии
UDP/7500	Обмен сообщениями между сервером доступа и абонентским пунктом	Абонентский пункт / Сервер доступа	Номер порта по умолчанию; изменяется в настройках виртуального адаптера Continent 3 PPP Adapter. АПКШ "Континент" 3.2.21 и более поздние версии
UDP/10000	Передача зашифрованного трафика	КШ / КШ, КШ / ЦУС	АПКШ "Континент" 3.5
IP-250	Передача зашифрованного трафика между КШ, принадлежащими одной сети	КШ / КШ, КШ / ЦУС	АПКШ "Континент" 3.4 и более ранние версии
	Передача зашифрованного трафика между КШ, принадлежащими разным сетям	КШ / КШ	Независимо от версии

Документация

1	Аппаратно-программный комплекс шифрования "Континент". Централизованное управление комплексом. Руководство администратора
2	Аппаратно-программный комплекс шифрования "Континент". Локальное управление криптографическим шлюзом. Руководство администратора
3	Аппаратно-программный комплекс шифрования "Континент". Аудит. Руководство администратора
4	Аппаратно-программный комплекс шифрования "Континент". Сервер доступа. Руководство администратора
5	Аппаратно-программный комплекс шифрования "Континент". Программа мониторинга КШ. Руководство пользователя
6	Аппаратно-программный комплекс шифрования "Континент". Тестирование каналов связи. Руководство администратора
7	Аппаратно-программный комплекс шифрования "Континент". Обновление программного обеспечения. Руководство администратора
8	Средство криптографической защиты информации "Континент-АП". Межсетевой экран. Руководство администратора
9	Средство криптографической защиты информации "Континент-АП". Абонентский пункт. Руководство пользователя
10	Аппаратно-программный комплекс шифрования "Континент". Аутентификация хоста. Руководство администратора

Примечание. Набор документов, входящих в комплект поставки, может отличаться от указанного списка.