КОД БЕЗОПАСНОСТИ

Средство защиты информации

Secret Net Studio

Мандатное управление доступом для сетевого трафика

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

ПО	Программное обеспечение
ПРД	Правила разграничения доступа
ГОСТ	Черновик ГОСТ Р Защита информации. Управление потоками информации в информационной системе. Форматы обмена метками конфиденциальности
Формат ГОСТ	Формат меток, определенный в ГОСТ (IP-опция 130)
SA	Security Association – соединение, которое представляет собой согласованную политику или способ обработки данных, обмен которыми предполагается между двумя устройствами сообщающихся сторон
Защищаемый компьютер	Компьютер с защищаемым сетевым трафиком

Введение

Данное руководство предназначено для администраторов изделия "Средство защиты информации Secret Net Studio" (далее — Secret Net Studio). В нем содержатся сведения о маркировке сетевого трафика с помощью утилиты ScAuthSrvConfig.exe.

Условные обозначения

В руководстве для выделения некоторых элементов текста используется ряд условных обозначений.

Внутренние ссылки обычно содержат указание на номер страницы с нужными сведениями.

Важная и дополнительная информация оформлена в виде примечаний. Степень важности содержащихся в них сведений отображают пиктограммы на полях.

- Так обозначается дополнительная информация, которая может содержать примеры, ссылки на другие документы или другие части этого руководства.
- Такой пиктограммой выделяется важная информация, которую необходимо принять во внимание.
- Эта пиктограмма сопровождает информацию предостерегающего характера.

Исключения. Примечания могут и не сопровождаться пиктограммами. А на полях, помимо пиктограмм примечаний, могут быть приведены и другие графические элементы, например, изображения кнопок, действия с которыми упомянуты в тексте расположенного рядом абзаца.

Другие источники информации

Сайт в Интернете. Вы можете посетить сайт компании "Код Безопасности" (https://www.securitycode.ru/) или связаться с представителями компании 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).

Общие сведения

Мандатное управление доступом для сетевого трафика поддерживается в Secret Net Studio, начиная с версии 8.4.

Требования к программному обеспечению

Для использования механизма мандатного управления доступом необходимо установить следующие компоненты Secret Net Studio на стороне сервера:

- Secret Net Studio – Сервер безопасности;
- Secret Net Studio – Центр управления.

На стороне клиента необходимо установить ПО Secret Net Studio под управлением сервера безопасности с установленными компонентами:

- Базовая защита;
- Полномочное управление доступом;
- Персональный межсетевой экран;
- Авторизация сетевых соединений.

Подробные сведения об установке ПО Secret Net Studio содержатся в документе "Средство защиты информации Secret Net Studio. Руководство администратора. Установка, обновление, удаление".

Внимание!

- Функция маркировки сетевого трафика работает только если включен компонент "Авторизация сетевых соединений" (см. документ "Средство защиты информации Secret Net Studio. Руководство администратора. Настройка и эксплуатация. Сетевая защита");
- Маркировка сетевых пакетов осуществляется только для TCP- и UDP-соединений.

Маркировка сетевого трафика

Режимы маркировки

В Secret Net Studio 8.5 реализовано четыре режима маркировки трафика:

- Режим 1 – режим маркировки IP-опцией 130. Применяется для маркировки исходящего сетевого трафика на удаленные компьютеры, если на них не установлено ПО Secret Net Studio. В этом режиме сетевые пакеты маркируются в соответствии с форматом ГОСТ (см. стр.7);

  Примечание.

  - В режиме 1 маркировка пакетов осуществляется только для исходящих соединений, устанавливаемых от имени пользователя, вошедшего в систему на удаленном компьютере, на котором не установлен клиент Secret Net Studio.
  - Если удаленный компьютер без установленного на нем Secret Net Studio работает под управлением ОС Windows, в режиме 1 ОС Windows не будет принимать сетевой трафик, промаркированный IP-опцией 130 в соответствии с ГОСТ. Чтобы маркированный сетевой трафик не отбрасывался ОС, необходимо использовать специальный режим маркировки "gost-win-compat", в котором IP-опция 130 по формату совместима с ГОСТ, но имеет такой размер, который ОС Windows считает допустимым (см. стр.15).

- Режим 2 – режим маркировки, который используется для связи с компьютерами, на которых установлены компоненты Secret Net Studio "Персональный межсетевой экран" и "Авторизация сетевых соединений". В этом режиме текущий уровень доступа пользователя хранится в билете (ticket) Kerberos и передается один раз перед установкой сетевого соединения при создании ассоциации SA. Сетевой трафик при этом подписывается, а не маркируется (см. стр.9);
- Режим 3 – режим аналогичен режиму 2, но сетевой трафик между компьютерами не подписывается, а маркируется в соответствии с форматом ГОСТ (см. стр.10);
- Режим 4 – режим приема маркированного сетевого трафика от компьютеров без установленного Secret Net Studio. При работе этого режима ожидается, что сетевые пакеты, исходящие от удаленного компьютера, маркируются в соответствии с форматом ГОСТ (см. стр.11).

Режим 1

Данный режим используется в случае, если нужно маркировать исходящий сетевой трафик метками в формате ГОСТ с компьютеров, на которых установлено ПО Secret Net Studio на компьютеры без установленного на них ПО Secret Net Studio.

При отправке сетевых пакетов на удаленный компьютер srv1, компьютер client1 маркирует пакеты меткой с уровнем допуска текущего пользователя Secret Net Studio в формате ГОСТ (см. рис.1).

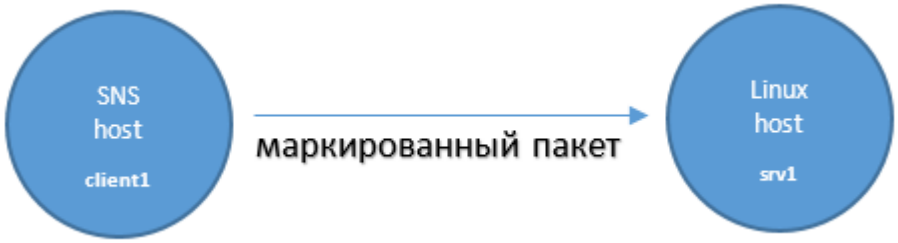


Рис. 1. Отправка сетевых пакетов в режиме 1.

При получении ответного сетевого трафика от удаленного компьютера srv1, компьютер client1 проверяет наличие маркировки (если нужно) и соответствие уровня допуска уровню текущего пользователя Secret Net Studio (см. рис.2).

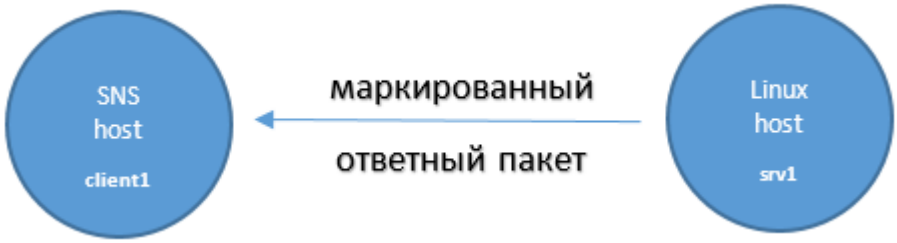


Рис. 2. Получение сетевых пакетов в режиме 1.

Чтобы настроить маркировку сетевого трафика в режиме 1:

1. Включите контроль потоков (см. стр.19).
2. Выполните настройку максимального уровня допуска пользователя (см. стр.19).
3. Для дальнейшей настройки параметров удаленного компьютера, входящий сетевой трафик на который будет маркироваться, запустите утилиту ScAuthSrvConfig.exe (подробное описание команд утилиты см. на стр.13).
4. Используя команду "add pc" утилиты ScAuthSrvConfig.exe, добавьте компьютер с защищаемым сетевым трафиком (далее – защищаемый компьютер) без клиента Secret Net Studio и с IP-адресами, заданными вручную.

   Пример

   ```
   add pc srv1 192.168.243.107 /agentless 1
   ```

   Будет добавлен компьютер с именем "srv1" и IP-адресом 192.168.243.107.
5. Настройте параметры защищаемого компьютера с помощью команды "set computer_policy" утилиты ScAuthSrvConfig.exe.

   Пример 1

   ```
   set cp srv1 /addrs_policy manual
   /auth_rule_gen_skip_everyone 0
   ```

   Будет настроено использование статических IP-адресов и разрешена генерация правил аутентификации для группы everyone.

   Пример 2

   ```
   set cp srv1 /mark_type to-host /mark_mode gost
   ```

   Будет включена маркировка сетевого трафика на данный компьютер с использованием меток в формате ГОСТ. Команда /mark_type to-host означает, что сетевая защита ожидает, что в обратную сторону сетевой трафик маркироваться не будет.

4 Добавьте разрешающее правило разграничения доступа для всех портов. На основе этого правила будет сгенерировано правило аутентификации.

   Пример

   ```
   add nr srv1 /at allow /direction in /local_ports *
   /groups everyone
   ```

В течение 5-7 минут настройки будут разосланы на все компьютеры, на которых установлены компоненты сетевой защиты. После этого исходящий сетевой трафик пользователей будет содержать метки конфиденциальности, соответствующие уровню конфиденциальности их сеанса (см. рис.3).

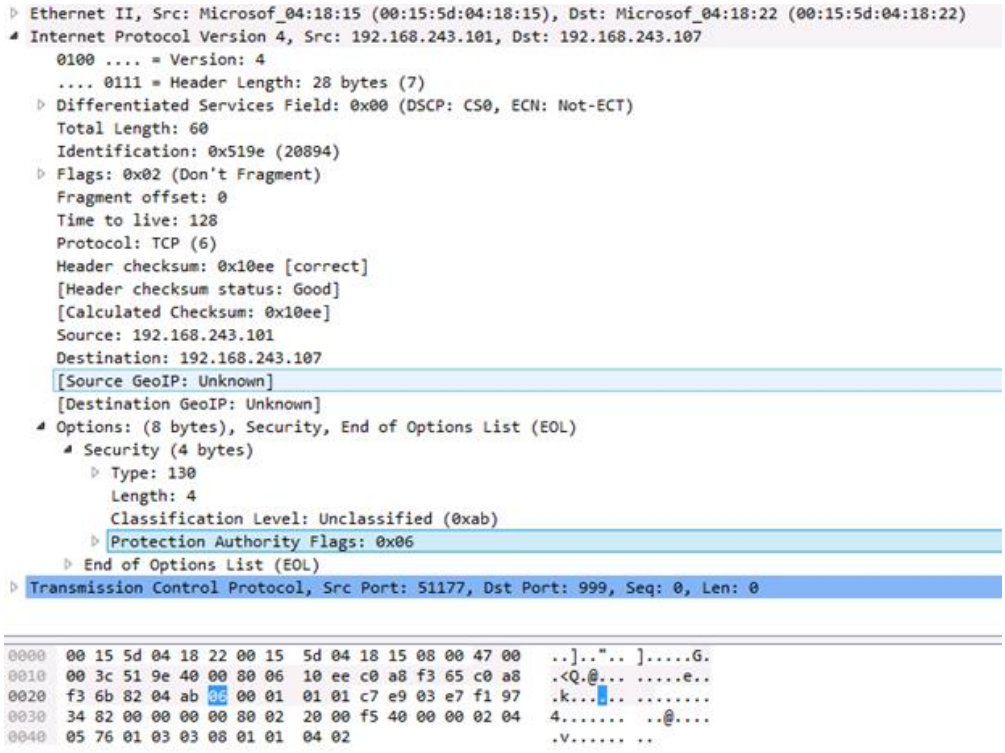


Рис. 3. TCP-пакет, промаркированный меткой с уровнем доступа 3 "Совершенно секретно".

Режим 2

Данный режим используется в случае, если нужно настроить маркировку сетевого трафика в формате ГОСТ между двумя компьютерами, на которых установлено ПО Secret Net Studio.

При установке сетевого соединения параметры подписи пакетов предварительно согласовываются с помощью ассоциации безопасности (SA). Также при этом передается уровень допуска текущего пользователя Secret Net Studio (см. рис.4).

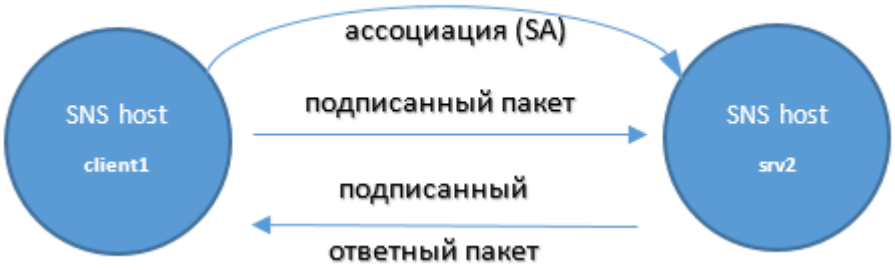


Рис. 4. Передача сетевого трафика в режиме 2.

В этом режиме работы используется обычный для Secret Net Studio режим авторизации сетевых соединений и подписи сетевого трафика.

Чтобы настроить маркировку сетевого трафика в режиме 2:

1. Включите контроль потоков (см. стр.19).
2. Выполните настройку максимального уровня допуска пользователя (см. стр.19).
3. Для дальнейшей настройки запустите утилиту ScAuthSrvConfig.exe (подробное описание команд утилиты см. на стр.13).

4. Создайте ПРД с заданным уровнем конфиденциальности. Уровень конфиденциальности соединения пользователя необходимо получить из токена пользователя, который находится в ассоциации, устанавливаемой перед соединением.

   Пример

   ```
   add nr srv2 /at deny /local_ports 999 /mandatory_level "0"
   ```

   Будет добавлено правило, запрещающее входящий неконфиденциальный сетевой трафик на порт 999 компьютера srv2.

   Значение параметра "mandatory_level" указывается в следующем формате: * | [= | < | <= | > | >=]<уровень>.

   Например, параметр может принимать значения:

   - "*" – уровень конфиденциальности пользователя может быть любым. Параметр принимает это значение по умолчанию;
   - "3" – уровень конфиденциальности пользователя должен быть равен 3;
   - "=0" – уровень конфиденциальности пользователя должен быть равен 0;
   - "<3" – уровень конфиденциальности пользователя должен быть меньше 3;
   - "<=2" – уровень конфиденциальности пользователя должен быть меньше либо равен 2;
   - ">0" – уровень конфиденциальности пользователя должен быть больше 0;
   - ">=2" – уровень конфиденциальности пользователя должен быть больше либо равен 2.

Если после настройки режима пользователь, обладающий неконфиденциальным уровнем допуска, обратиться к порту 999 компьютера srv2, ему будет отказано в доступе. Пользователь, имеющий уровень допуска, отличный от неконфиденциального, получит доступ к этому порту.

Режим 3

Данный режим используется в случае, если нужно настроить маркировку сетевого трафика в формате ГОСТ между двумя компьютерами, на которых установлено ПО Secret Net Studio.

При установке сетевого соединения параметры маркировки предварительно согласовываются с помощью SA (см. рис. 5).

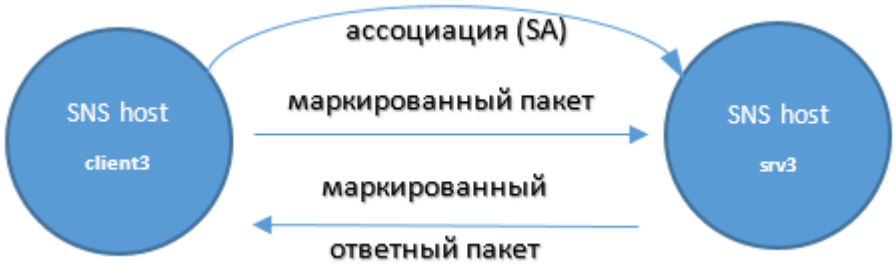


Рис. 5. Передача сетевого трафика в режиме 3.

Примечание.

- Не поддерживается одновременное выполнение маркировки и подписи/шифрования сетевого трафика. При включении маркировки пакетов с помощью утилиты ScAuthSrvConfig.exe будут сброшены параметры подписи/шифрования.
- ПРД получают информацию об уровне пользователя не из сетевого трафика, а из токена удаленного пользователя (который создается при установке сетевого соединения).

Чтобы настроить маркировку сетевого трафика в режиме 3:

1. Включите контроль потоков (см. стр.19).
2. Выполните настройку максимального уровня допуска пользователя (см. стр.19).
3. Для дальнейшей настройки запустите утилиту ScAuthSrvConfig.exe (подробное описание команд утилиты см. на стр.13).
4. Настройте для компьютера, входящий сетевой трафик которого должен быть промаркирован, политику аутентификации, которая требует обязательной маркировки сетевого трафика.

   Пример

   ```
   set cp srv3 /mark_type both /mark_mode gost
   ```

   Будет настроена политика аутентификации для компьютера с именем srv3 с указанием необходимости маркировки трафика по ГОСТ в обоих направлениях.
5. Создайте ПРД с указанием сетевых портов, сетевой трафик к которым необходимо маркировать. На основе этих ПРД будет сгенерировано правило аутентификации, с помощью которого все удаленные компьютеры с установленным ПО Secret Net Studio будут понимать, что требуется маркировка сетевого трафика, отправляемого на этот компьютер.

   Пример

   ```
   add nr srv3 /at deny /direction in /local_ports 999
   /groups everyone

   add nr srv3 /at allow /direction in /local_ports 999
   /groups everyone /mandatory_level ">=1"
   ```

   Будут добавлены запрещающее и разрешающее доступ правила для порта 999 и протоколов TCP, UDP.

   Примечание. Если в правиле не будет указан параметр "mandatory_level" и в панели управления Secret Net Studio не будет включен параметр "Включить защиту соединений", то правило аутентификации не будет сгенерировано. Маркировка в этом случае работать не будет.

Теперь если пользователь компьютера из текущего домена безопасности будет устанавливать сетевое подключение на указанный в правилах порт, сетевые пакеты этого соединения будут маркироваться в формате ГОСТ в обоих направлениях.

Пример

Команда для создания TCP-соединения с компьютером srv3:

```
telnet srv3 999
```

Режим 4

Данный режим используется в случае, если нужно настроить маркировку входящего сетевого трафика в формате ГОСТ с компьютеров, на которых не установлено ПО Secret Net Studio на компьютеры с установленным ПО Secret Net Studio.

При получении маркированных пакетов агент сетевой защиты запоминает максимальный уровень допуска и снимает маркировку (см. рис. 6).

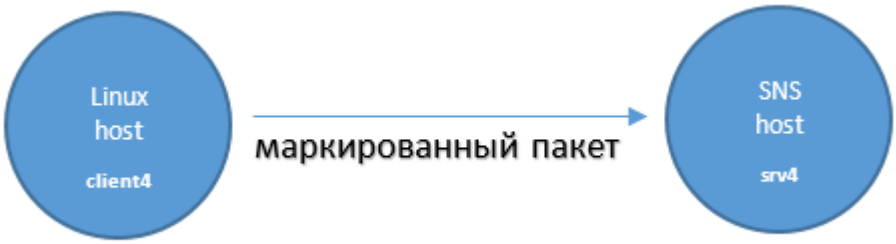


Рис. 6. Получение сетевых пакетов в режиме 4.

Компьютер маркирует ответный пакет полученным ранее уровнем допуска (см. рис. 7).

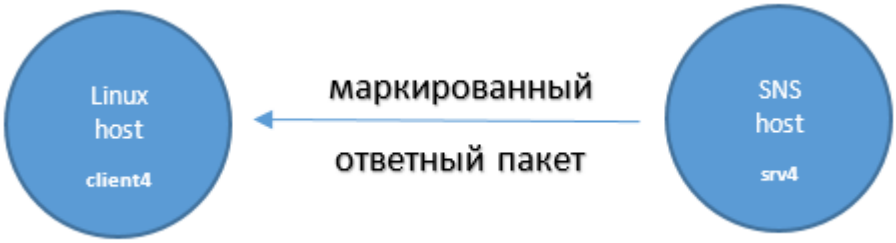


Рис. 7. Отправка сетевых пакетов в режиме 4.

Чтобы настроить маркировку сетевого трафика в режиме 4:

1. Запустите утилиту ScAuthSrvConfig.exe (подробное описание команд утилиты см. на стр.13).
2. Включите опцию отслеживания соединений для компьютера, входящий сетевой трафик которого должен быть промаркирован (и который должен маркировать ответный сетевой трафик).

   Пример

   ```
   set cp srv4 /conntrack_mode enabled
   ```

3. Добавьте защищаемый компьютер, от которого должен приниматься маркированный сетевой трафик.

   Пример

   ```
   add pc client4 192.168.243.107 /agentless 1
   ```

   Будет добавлен защищаемый компьютер с именем client4 без клиента Secret Net Studio с IP-адресами, заданными вручную.
4. Настройте политику маркировки пакетов так, чтобы IP-адреса компьютера указывались вручную и разрешите генерацию правил аутентификации для группы everyone.

   Пример

   ```
   set cp client4 /addrs_policy manual
   /auth_rule_gen_skip_everyone 0
   ```

5. Включите маркировку сетевого трафика для данного компьютера с использованием меток в формате ГОСТ.

   Пример

   ```
   set cp client4 /mark_type both /mark_mode gost
   ```

6. Добавьте правило, разрешающее доступ ко всем портам. На основе этого ПРД будет сгенерировано правило аутентификации.

   Пример

   ```
   add nr client4 /at allow /direction in /local_ports *
   /groups everyone
   ```

   Теперь, если пользователь с компьютера client4 установит сетевое соединение с компьютером srv4, сетевые пакеты этого соединения будут маркироваться в формате ГОСТ в обоих направлениях. Ответный сетевой трафик компьютера srv4 будет промаркирован меткой с таким же уровнем, с каким был промаркирован исходящий сетевой трафик компьютера client4.

Утилита ScAuthSrvConfig.exe

Утилита ScAuthSrvConfig.exe располагается на сервере безопасности в папке установки, по умолчанию — Secret Net Studio\Server\Authentication Server\.

Запустите утилиту, используя команду:

```
ScAuthSrvConfig.exe <domain> [/a|admin <value>]
```

где:

- **domain** — домен безопасности;
- **/a|admin <value>** — имя администратора домена.

Пример

```
ScAuthSrvConfig.exe SP.LOC /admin administrator
```

Будет выполнено подключение к серверу авторизации, расположенному в домене SP.LOC, с помощью учетной записи администратора домена.

После запуска утилита переходит в режим командной строки. Для просмотра списка доступных команд используйте команду <?>.

Примечание. Помощь по работе любой команды можно получить, запустив команду с параметром [/?], или (в некоторых случаях) запустив команду без параметров.

Настройка параметров защищаемого компьютера

Добавление защищаемого компьютера

Для добавления компьютера в список защищаемых выполните команду:

```
add pc <protected_computer> [IP_address] [/forcecreate
] [/description <value>] [/agentless 0|1]
```

где:

- **protected_computer** — имя компьютера;
- **IP-address** — IP-адрес компьютера;
- **/forcecreate** — создать учетную запись Kerberos, если она не существует;
- **/agentless <value>** — флаг клиента Secret Net Studio. Может принимать значения:
  - **0** – если на защищаемом компьютере установлен клиент Secret Net Studio;
  - **1** – если на защищаемом компьютере не установлен клиент Secret Net Studio.

Пример

```
add pc testcomp1 192.168.243.107 /agentless 1
```

Будет добавлен защищаемый компьютер с именем testcomp1 и IP-адресом 192.168.243.107 без клиента Secret Net Studio.

Редактирование списка IP-адресов защищаемого компьютера

Для изменения списка IP-адресов защищаемого компьютера выполните команду:

```
modify pc <protected_computer> [/addaddress|aa <value>]
[/removeaddress|ra <value>] [/agentless 0|1]]
```

где:

- **/addaddress|aa <value>** — добавить IP-адрес компьютера;
- **/removeaddress|ra <value>** — удалить IP-адрес компьютера;

Пример

```
modify pc testcomp1 /addaddress 192.168.243.127
```

Будет добавлен IP-адрес 192.168.243.127 защищаемого компьютера testcomp1.

Просмотр параметров защищаемого компьютера

Просмотреть информацию о защищаемом компьютере можно с помощью команды:

```
show pc <protected_computer>
```

Пример

```
show pc testcomp1
```

Просмотр списка защищаемых компьютеров

Чтобы просмотреть список защищаемых компьютеров, выполните команду:

```
show pcs <name_mask>
```

где **name_mask** — маска имени компьютеров.

Пример 1

```
show pcs
```

Будет выведена информация обо всех защищаемых компьютерах.

Пример 2

```
show pcs t*
```

Будет выведена информация о защищаемых компьютерах, имена которых начинаются с символа "t".

Удаление защищаемого компьютера

Чтобы удалить защищаемый компьютер из списка, выполните команду:

```
delete pc <protected_computer>
```

Пример

```
delete pc testcomp1
```

Компьютер с именем testcomp1 будет удален из списка защищаемых объектов.

Управление политиками аутентификации защищаемого компьютера

Настройка политик аутентификации

Для настройки политик защищаемого компьютера выполните команду:

```
set computer_policy(cp) <protected_computer>
[/mark_type <value>] [/mark_mode <value>]
[/addrs_policy <value>] [/auth_rule_gen_skip_everyone
<value>]
```

Описание команд представлено в следующей таблице.

Команда	Описание
/mark type <value>	Направление сетевого трафика, для которого выполняется маркировка. Может принимать значения: • **off** – маркировка пакетов выключена; • **to-host** – включена маркировка пакетов, направляемых в сторону защищаемого компьютера; • **from-host** – включено снятие маркировки пакетов, направляемых от защищаемого компьютера; • **both** – включены обе функции: маркировка пакетов в сторону защищаемого компьютера и снятие маркировки пакетов от защищаемого компьютера
/mark_mode <value>	Режим маркировки пакетов. Может принимать значения: • **gost** – режим ГОСТ; • **gost-win-compat** – режим ГОСТ, совместимый с ОС Windows
/addr_policy <value>	Политика получения адресов компьютера. Может принимать значения: • **auto** – IP-адреса компьютера будут получены из информации, присланной клиентом Secret Net Studio; • **resolve** – IP-адреса компьютера периодически определяются на каждом клиенте Secret Net Studio; • **manual** – IP-адреса задаются вручную
/auth_rule_gen_skip_ everyone <value>	Настройка генерации правил аутентификации для группы everyone. Может принимать значения: • **0** – разрешить генерацию правил аутентификации для группы everyone • **1** – не создавать правила аутентификации для группы everyone;

Примечание. Другие возможные значения параметров команды set computer_policy(cp) можно просмотреть с помощью команды <?>.

Пример 1

```
set cp testcomp1 /mark_type both /mark_mode gost
```

Будет настроена политика маркировки пакетов на защищаемом компьютере с именем testcomp1.

Пример 2

```
set cp testcomp1 /addrs_policy manual
```

Будет настроено использование статических IP-адресов для защищаемого компьютера testcomp1.

Пример 3

```
set cp testcomp1 /auth_rule_gen_skip_everyone 0
```

Будет разрешена генерация правил аутентификации для группы everyone.

Просмотр настроенных политик защищаемого компьютера

Просмотреть текущие настройки политик для защищаемого компьютера можно с помощью команды:

```
show computer_policy(cp) <protected_computer>
```

Управление правилами разграничения доступа

Управление правилами разграничения доступа осуществляется с помощью следующих команд:

- add normal_rule(nr) – добавление правила;
- modify normal_rule(nr) – редактирование правила;
- delete normal_rule(nr) – удаление правила;
- show normal_rule(nr) – отображение параметров правила;
- show normal_rules(nrs) – отображение всех правил для компьютера.

Ниже описана процедура добавления ПРД. Остальные команды имеют аналогичные параметры.

Добавление правила

Для добавления нового правила разграничения доступа выполните следующую команду:

```
add normal_rule(nr) <protected_computer> [/order
<value>] [/at allow|deny] [/direction in|out] [/proto
<value>] [/remote_addrs <value>] [/remote_ports
<value>] [/local_addrs <value>] [/local_ports <value>]
[/principals <value>] [/groups <value>] [/extsubjects
<value>] [/rest_proc_sids <value>] [/sid]
[/mandatory_level <value>] [/audit 1|0] [/enable 1|0]
[/schedule <value>] [/action <value>] [/act_folder
<value>] [/act_start_type system|console|all-
interactive|any-interactive] [/act_token_type
system|user|user-elevated] [/action_beep 1|0]
[/adapters_to_include <value>] [/adapters_to_exclude
<value>] [/adapters_match incl-excl|all-excl+incl]
[/reply_on_reject 1|0] [/protect_out_channel 1|0]
[/filter <value>] [/include_processes <value>]
[/exclude_processes <value>] [/network_service|ns
<value>]
```

Описание команд представлено в следующей таблице.

Команда	Описание
/order <value>	Порядковый номер правила. Может быть целым числом или принимать значения: • **f** – первое правило; • **l** – последнее правило
/at <value>	Тип доступа. Может принимать значения: • **allow** – доступ разрешен; • **deny** – доступ запрещен
/direction <value>	Направление правила. Может принимать значения: • **in** – входящее направление; • **out** – исходящее направление
/proto<value>	Номер протокола транспортного уровня
/remote_addrs <value>	IP-адреса, диапазон IP-адресов или маска подсети удаленного компьютера
/remote_ports <value>	Порты удаленного компьютера

Команда	Описание
/local_addrs <value>	IP-адреса, диапазон IP-адресов или маска подсети локального компьютера
/local_ports <value>	Порт локального компьютера
/principals <value>	Учетные записи пользователей или компьютеров
/groups <value>	Группы Secret Net Studio. Может принимать значения: • **everyone;** • **anonymous;** • **authenticated;** • **computers;** • **users**
/extsubjects <value>	Идентификаторы (SID) Active Directory для внешних субъектов
/rest_proc_sids <value>	Допустимые субъекты безопасности процесса (идентификаторы (SID) пользователей)
/sid	Флаг, указывающий на то, что параметры "groups" и "extsubjects" являются идентификаторами групп, а не именами
/mandatory_level <value>	Мандатный уровень. Значение параметра указывается в следующем формате: * | [= | < | <= | > | >=]<уровень>. Например, параметр может принимать значения: • "*" – уровень конфиденциальности пользователя может быть любым. Параметр принимает это значение по умолчанию; • "3" – уровень конфиденциальности пользователя должен быть равен 3; • "=0" – уровень конфиденциальности пользователя должен быть равен 0; • "<3" – уровень конфиденциальности пользователя должен быть меньше 3; • "<=2" – уровень конфиденциальности пользователя должен быть меньше либо равен 2; • ">0" – уровень конфиденциальности пользователя должен быть больше 0; • ">=2" – уровень конфиденциальности пользователя должен быть больше либо равен 2
/audit <value>	Настройки аудита. Может принимать значения: • **1** – аудит включен; • **0** – аудит выключен
/enable <value>	Активация правила. Может принимать значения: • **1** – правило включено; • **0** – правило выключено
/schedule <value>	Расписание работы правил
/action <value>	Команда, выполняемая при срабатывании правила. Если значение не задано, команда не выполняется
/act_folder <value>	Рабочая папка
/act_start_type <value>	Выбор сессии для запуска команды. Может принимать значения: • **system** – системная сессия (sessionId=0). Является значением по умолчанию; • **console** – локальная консоль; • **all-interactive** – интерактивные сессии всех пользователей
/act_token_type <value>	Выбор пользователя для запуска команды. Действует только для интерактивных сессий. Может принимать значения: • **system** – системный токен; • **user** – обычный токен пользователя; • **user-elevated** – токен пользователя с максимальными привилегиями

Команда	Описание
/action_beep <value>	Активация звукового оповещения администратора. Может принимать значения: • **1** – звуковое оповещение включено; • **0** – звуковое оповещение выключено
/adapters_to_include <value>	Список идентификаторов (GUID) сетевых адаптеров, к которым применимо правило
/adapters_to_exclude <value>	Список идентификаторов (GUID) сетевых адаптеров, к которым правило неприменимо
/adapters_match <value>	Настройки применения правила к сетевым адаптерам. Может принимать значения: • **incl-excl** – действовать на <adapters-to-include> адаптеры, исключая <adapters-to-exclude> адаптеры; • **all-excl+incl** – действовать на все адаптеры, включая <adapters-to-include>, исключая <adapters-to-exclude> адаптеры
/reply_on_reject <value>	При срабатывании запрещающих правил доступа (deny), посылать RST-ответ по протоколам ICMP/TCP. Может принимать значения: • **1** –включено; • **0** –выключено
/protect_out_channel <value>	Флаг "Требовать защищенное соединение" в настройках правила (для исходящего направления). Может принимать значения: • **1** – защита включена; • **0** – защита выключена
/filter <value>	Фильтр содержимого пакетов
/include_processes <value>	Список процессов, к которым применимо правило
/exclude_processes <value>	Список процессов, к которым правило не применимо
/network_service <value>	Имя шаблона сетевого сервиса для создания правила

Приложение

Настройка полномочного управления доступом

Чтобы при входе в систему пользователь мог выбрать текущий уровень конфиденциальности отличный от уровня "неконфиденциально" выполните настройку полномочного управления доступом.

Для настройки полномочного управления доступом необходимо включить контроль потоков и настроить максимальный уровень допуска пользователя.

Включение контроля потоков

Для включения контроля потоков:

1. В программе управления Secret Net Studio откройте панель "Компьютеры" и выберите объект, для которого необходимо настроить параметры. Вызовите для него контекстное меню и активируйте в нем команду "Свойства".
2. Перейдите на вкладку "Настройки" и нажмите при необходимости кнопку "Загрузить настройки", затем в разделе "Политики" выберите элемент "Полномочное управление доступом".

   В правой части экрана появится область настройки выбранных параметров.
3. Для параметра "Режим работы" установите отметку в поле "Контроль потоков включен" и нажмите кнопку "Применить" в нижней части вкладки "Настройки".

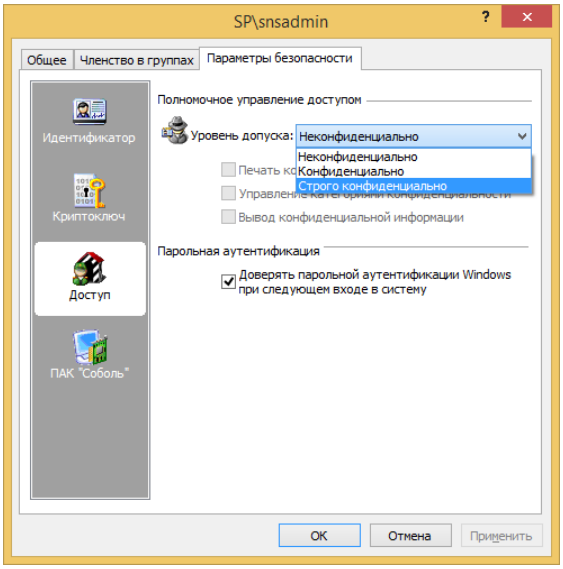
Пояснение. Чтобы настроить название уровней конфиденциальности, выберите параметр "Названия уровней конфиденциальности", наведите указатель на нужную категорию и дважды нажмите левую кнопку мыши. Это может понадобиться, например, чтобы привести категории в соответствие с примерами уровней конфиденциальности, приведенными в ГОСТ для меток конфиденциальности:

- 0 – Не секретно;
- 1 – ДСП;
- 2 – Секретно;
- 3 – Совершенно секретно.

Настройка максимального уровня допуска

Для настройки максимального уровня допуска пользователя:

1. На любом компьютере, на котором установлено ПО Secret Net Studio, запустите программу "Управление пользователями" с помощью учетной записи пользователя, у которой есть права на администрирование Secret Net Studio (по умолчанию группа "Domain Admins").
2. Наведите указатель на нужного пользователя и нажмите правую кнопку мыши, в контекстном меню выберите пункт "Свойства". Откроется диалог настройки параметров пользователя.



3. Для параметра "Уровень допуска" выберите значение "Строго конфиденциально" и нажмите кнопку "ОК". Уровень допуска пользователя будет изменен и при следующем входе пользователя в систему на экране появится диалог выбора уровня конфиденциальности для текущего сеанса.