

ООО «С-Терра СиЭсПи»  
124498, г. Москва, Зеленоград, Георгиевский проспект,  
дом 5, помещение I, комната 33  
Телефон: +7 (499) 940 9061  
Факс: +7 (499) 940 9061  
Эл.почта: [information@s-terra.com](mailto:information@s-terra.com)  
Сайт: <http://www.s-terra.com>



## **Программный комплекс CSP VPN Gate. Версия 3.11**

### **Руководство администратора**

### **Cisco-like команды**

РЛКЕ.00005-02 90 03

18.04.2012

# Содержание

<b>Cisco-like команды .....</b>	<b>5</b>
Консоль ввода команд, родственных Cisco Systems.....	5
Запуск консоли	6
Удаленная настройка по SSH	8
Интерфейс пользователя	9
Специальные команды редактирования	11
Команды, родственные Cisco Systems	13
Команды входа в режимы настроек.....	14
configure terminal	14
enable	15
Команды выхода из режимов настроек .....	16
end	16
exit (EXEC)	17
exit (global)	18
disable	19
Команды вывода информации (информационные команды) .....	20
show version	20
show version csp	22
show privilege	23
show load-message	24
show running-config	25
show terminal	26
show ip route	27
show crypto isakmp policy	31
Команды настройки терминала.....	32
terminal width	32
terminal length	33
Команды вызова системных команд и системные команды.....	34
run	34
ping	36
Команды создания пользователей, назначения паролей, уровня привилегий.....	37
enable password	37
enable secret	39
username password	41
username secret	44

---

Команды настройки протоколирования событий.....	47
logging	47
logging facility	49
logging trap	50
logging on	51
Команды настройки SNMP-сервера .....	52
snmp-server community	52
snmp-server location	54
snmp-server contact	55
snmp-server host	56
snmp-server enable traps	57
snmp-server trap-source	58
Команды для назначения имени хоста и имени домена.....	59
hostname	59
ip domain name	60
Команды для работы с таблицей маршрутизации .....	61
ip route	61
Команды для работы с сертификатами .....	63
crypto pki trustpoint	63
crypto pki certificate chain	68
crypto identity	72
Команды для работы с предопределенным ключом .....	75
crypto isakmp key	75
ip host	77
Команды создания и редактирования списков доступа .....	79
ip access-list	79
ip access-list resequence	92
access-list (standard)	93
access-list (extended)	94
Команды создания IKE политики .....	95
crypto isakmp policy	95
crypto isakmp peer	102
crypto isakmp identity	105
crypto isakmp keepalive	106
crypto ipsec security-association lifetime	107
Команды формирования набора преобразований IPsec .....	108
crypto ipsec transform-set	108
Команды для работы с IKECFG пулом .....	111

---

ip local pool	111
crypto isakmp client configuration address-pool local	113
crypto map client configuration address	114
crypto dynamic-map client configuration address	115
Команды создания и редактирования криптографических карт.....	116
crypto map (global IPsec)	116
crypto dynamic-map	130
Команды настройки сетевых интерфейсов.....	132
interface	132
crypto ipsec df-bit (global)	143
Игнорируемые команды .....	144

# Cisco-like команды

---

## Консоль ввода команд, родственных Cisco Systems

Консоль (Command Line Interface) предназначена для ввода команд, аналогичных командам Cisco IOS (далее – cisco-like команды). Интерфейс командной строки CSP VPN Gate предоставляет возможность создавать политику безопасности более гибкую, чем это может сделать Router MC.

Для работы консоли необходимы файлы:

в директории /opt/VPNagent/bin:

- cs\_console – исполняемый файл
- cmd.xml – XML-база поддерживаемых команд
- cs\_conv.ini – ресурсный файл настроек консоли и конвертора (может редактироваться пользователем)
- cs\_cons\_reg.ini – ресурсный файл внутренних настроек консоли и конвертора (автоматически редактируется при запуске консоли)

в директории /opt/VPNagent/lib:

- libs\_csconfig.so – библиотека обработчика конфигурации
- libs\_csconverter.so – библиотека конвертора.

Консоль разделяется на три основных модуля:

**Командный интерпретатор** – обеспечивает прием и синтаксический разбор команд.

**Обработчик конфигурации** – формирует и обрабатывает внутреннюю модель Cisco-like конфигурации. Передает сформированную конфигурацию для конвертирования в Native-конфигурацию.

**Конвертор** – преобразует Cisco-like конфигурацию в формат Native-конфигурации. Подробно конвертор описан в документе [«Приложение»](#) в разделе «Конвертор».

## Запуск консоли

CLI консоль автоматически запускается при входе в систему пользователем “cscons” (для него программа cs\_console прописана как default shell). Кроме того, пользователи, обладающие административными привилегиями (например, “root”), могут запускать консоль непосредственно из shell операционной системы по мере необходимости. Запуск производится вызовом команды **cs\_console**, находящейся в каталоге **/opt/VPNagent/bin/**.

**Примечание:** Для работы консоли обязательно должен быть запущен сервис vpnsvc. Не останавливайте сервисы vpnagent при работающей консоли, иначе она окажется неработоспособной.

Дополнительные ключи командной строки:

- **nolog** – сообщения о состоянии команды выводятся в `stdout` и не выводятся в лог (по умолчанию – выводятся в лог).

При запуске для процесса cs\_console выставляется значение переменной окружения PATH:

```
/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin
```

Изменить значение переменной окружения PATH можно в файле `cs_conv.ini` (секция [env]), который расположен в каталоге `/opt/VPNagent/bin`. Подробное описание смотрите в документе «[Приложение](#)» в разделе «Управление конвертором с помощью INI-файла».

### Синхронизация

При старте консоли происходит синхронизация описания CA-сертификатов в базе локальных настроек и Cisco-like конфигурации (команда `trustpoint`):

1. если в Cisco-like конфигурации присутствует сертификат, который отсутствует в базе локальных настроек (например, сертификат, удаленный с помощью команды `cert_mgr remove`), то этот сертификат автоматически удаляется из Cisco-like конфигурации с выдачей сообщения в лог. Если этот сертификат был последним в `trustpoint`, этот `trustpoint` автоматически удаляется
2. если в базе локальных настроек присутствует сертификат, который отсутствует в Cisco-like конфигурации, то этот сертификат добавляется в Cisco-like конфигурацию командой `trustpoint` с именем `s-terra_technological_trustpoint`. Если этот `trustpoint` отсутствует, он создается автоматически.

Также при старте консоли происходит синхронизация описания `preshaed` ключей в базе локальных настроек и Cisco-like конфигурации:

1. если в Cisco-like конфигурации присутствует ключ, который отсутствует в базе локальных настроек (например, ключ, удаленный с помощью команды `key_mgr remove`), то этот ключ автоматически удаляется из Cisco-like конфигурации с выдачей сообщения в лог
2. если значение ключа, указанного в Cisco-like конфигурации, поменялось в базе локальных настроек, то значение ключа также меняется и в Cisco-like конфигурации.

Все команды консоли описаны в разделе «[Команды, родственные Cisco Systems](#)».

При запуске утилиты **cs\_console** возможны ошибки, которые выдаются на консоль:

Таблица 1

Текст сообщения	Пояснение
ERROR: vpnsvc daemon is not running, cs_console will exit now!  Press ENTER to continue	Ошибка: сервис vpnsvc не запущен. cs_console сейчас завершит работу.  Для продолжения нажмите ENTER...  (сообщение возникает, если во время работы cs_console был остановлен сервис vpnsvc)

ERROR: Could not initialize module manager. Press ENTER to exit	Ошибка: не удалось инициализировать module manager. Для выхода нажмите ENTER... (скорее всего, обозначает, что Продукт неправильно установлен или испорчен)
ERROR: Could not establish connection with daemon. Press ENTER to exit	Ошибка: не удалось установить связь с сервисом. Для выхода нажмите ENTER... (наиболее вероятная причина – попытка запуска cs_console при остановленном сервисе)
ERROR: Could not initialize resources. Press ENTER to exit	Ошибка: не удалось проинициализировать ресурсы. Для выхода нажмите ENTER... (скорее всего, обозначает, что Продукт неправильно установлен или испорчен)
ERROR: Could not initialize interfaces. Press ENTER to exit	Ошибка: не удалось проинициализировать интерфейсы. Для выхода нажмите ENTER...
ERROR: Invalid XML file. Press ENTER to exit...	Ошибка: неверный формат XML-файла. Для выхода нажмите ENTER...
ERROR: Unable to get super-user privileges. Press ENTER to exit...	Ошибка: невозможно получать права суперпользователя. Для выхода нажмите ENTER...
ERROR: Internal error. Press ENTER to exit...	Ошибка: внутренняя ошибка. Для выхода нажмите ENTER...
Password required, but none set	Для входа в привилегированный режим требуется пароль, но он не задан в конфигурации.

### **Загрузка начальной конфигурации**

Если при загрузке начальной конфигурации в какой-то из команд произошла ошибка:

- если для данной ошибки доступно специфическое сообщение (которое может быть выведено в случае подобной ошибки при ручном вводе команды), то это сообщение выдается на консоль
- на консоль выдается сообщение:  
Warning: Command "<cmd>" processing failed
- в лог выдается сообщение:  
Command "<command\_line>", processed with status FAIL
- команда игнорируется.

## Удаленная настройка по SSH

Создание локальной политики безопасности для шлюза CSP VPN Gate 3.11 можно осуществить удаленно при помощи консоли по протоколу SSH1 или SSH2.

Настройку шлюза проводите под защитой IPsec. Для этой цели после инсталляции CSP VPN Gate рекомендуется загрузить начальную конфигурацию, которая позволит в дальнейшем создать *защищенный канал* для удаленной настройки шлюза. Создание начальной конфигурации описано в разделе «Построение VPN туннеля между шлюзом безопасности CSP VPN Gate 3.11 и рабочим местом администратора для удаленной настройки шлюза» документа [«Настройка шлюза»](#).



## Интерфейс пользователя

**cs\_console** является терминальным приложением. Существует ситуации, в которых важное значение имеет определение правильных размеров терминала. Примеры таких ситуаций:

- редактирование длинных строк (которые не полностью помещаются в окне терминала)
- паузы при выводе длинной конфигурации по команде `show running-config`
- вызов внешних терминальных программ (например `vi`, `less`, `top` и т.п.) с помощью команды `run`.

При старте `cs_console` в некоторых случаях могут возникать проблемы, связанные с некорректным определением размеров терминала. Такие проблемы возникают, если используется системная консоль, подключенная по COM-порту, в том числе если используется системная консоль NME-RVPN (MCM).

**Примечание:** непосредственный доступ к системной консоли NME-RVPN (MCM) всегда происходит через COM-порт, даже если пользователь осуществляет его из терминальной сессии Cisco IOS по протоколу SSH или telnet.

Далее подробно описаны данные проблемы и рекомендации по их решению.

При старте `cs_console` происходит определение размеров терминала (ширина и длина):

1. сначала делается попытка прочитать размеры терминала из переменных окружения:

ширина терминала:

`COLUMNS`

длина терминала:

`LINES`

2. Эти переменные окружения могут быть переопределены пользователем при запуске `cs_console`, например:

```
COLUMNS=80 LINES=24 /opt/VPNagent/bin/cs_console
```

Только в случае реальной необходимости, когда система не может корректно определить реальные размеры терминала, следует переопределять переменные окружения. Если выставить некорректные значения, то это может привести к сбоям в работе `cs_console` и иных терминальных приложений.

3. если размеры терминала в переменных окружения не выставлялись, то делается попытка прочитать параметры терминала с помощью системного вызова (`ioctl`).
4. если системный вызов вернул ошибку или выдал значения ширины и длины, равные 0 (такое происходит, если используется системная консоль, подключенная по COM-порту, в том числе если используется системная консоль NME-RVPN (MCM)), то делается попытка прочитать характеристики терминала "`co`" (ширина) и "`li`" (длина) с помощью системного вызова `tgetnum`.

Следует учитывать, что в подобной ситуации разные операционные системы ведут себя по-разному: одни выставляют некоторые значения по умолчанию (как правило по описанию используемого терминала), а другие – могут вообще не выставлять данные характеристики.

Например:

ОС Red Hat Enterprise Linux 5 при использовании терминала VT100 выставляет значения "`co`"=80 "`li`"=24.

5. если ширину и длину терминала получить не удалось ни одним из указанных выше способов, то выставляются значения по умолчанию: ширина – 511, длина – 0.

**Примечание:** данное поведение отличается от поведения Cisco IOS: там в подобной ситуации выставляются значения: ширина – 80, длина – 24.

Результат определения размеров терминала (если не используются переменные окружения COLUMNS / LINES) может отличаться в зависимости от:

- типа подключения терминала (COM-порт, SSH и т.п.)
- операционной системы, на которой установлен CSP VPN Gate
- клиентского терминального приложения, используемого для подключения к консоли.

Например, при подключении к системной консоли по COM-порту, в том числе к системной консоли NME-RVPN (MCM), будут выданы следующие результаты:

OC Red Hat Enterprise Linux 5: ширина – 80, длина – 24. Причем, данный результат не будет зависеть от реальных размеров окна терминального приложения.

Проверить размеры терминала в запущенной консоли можно с помощью команды `show terminal`.

Если `cs_console` уже стартовала, а в ней заданы некорректные размеры терминала, то их можно исправить с помощью команд `terminal width` / `terminal length`.

Возможна реакция `cs_console` на изменение размеров терминала, если для этого существует техническая возможность:

данную реакцию можно наблюдать, например, следующим образом: начать вводить очень длинную строку, инициирующую горизонтальный скроллинг; и после этого изменить ширину терминального окна.

Реакция на изменение размеров терминала различается в зависимости от операционной системы:

в ОС Linux: перерисовка строки происходит только после ввода следующего символа или нажатия управляющей клавиши.

Наличие или отсутствие реакции на изменение размеров терминала также зависит от разных факторов:

типа подключения терминала (COM-порт, SSH и т.п.)

клиентского терминального приложения, используемого для подключения к консоли.

Как правило, реакция на изменение размеров окна:

присутствует в случае подключения по SSH (при условии, что клиентское приложение корректно обрабатывает изменение размеров терминального окна и оповещает SSH-сервер о нем)

отсутствует при подключении к системной консоли по COM-порту, в том числе к системной консоли NME-RVPN (MCM).

Если размеры терминала переопределены с помощью команд `terminal width`, `terminal length`, то реакция на изменение размеров терминала отсутствует (значения, заданные в этих командах, считаются более приоритетными).

## Специальные команды редактирования

Cisco-like консоль поддерживает специальные команды редактирования командной строки. Символы для вызова этих команд и действия перечислены в Таблица 2.

Таблица 2

Символ	Название	Действие
<b>Команды перемещения курсора</b>		
Ctrl-A, Home	Beginning of line	Перемещает курсор на начало строки. Примечание: кнопка Home работает не во всех сочетаниях типа терминала и используемого клиентского терминального приложения.
Ctrl-B, <-	Back character	Перемещает курсор на одну позицию влево
Ctrl-E, End	End of line	Перемещает курсор в конец строки. Примечание: кнопка End работает не во всех сочетаниях типа терминала и используемого клиентского терминального приложения.
Ctrl-F, ->	Forward character	Перемещает курсор на одну позицию вправо
Esc B	Back word	Перемещает курсор на одно слово назад
Esc F	Forward word	Перемещает курсор на одно слово вперед
<b>Вызов подсказки</b>		
Ctrl-I, Tab	Auto complete	Дополняет команду, если начало строки однозначно определяет возможное продолжение.
?	List possible commands	Если ? введен без пробела - распечатывает команды, начинающиеся так же как и введенная строка  Если ? введен после пробела – распечатывает все возможные для дальнейшего ввода команды
<b>Команды работы с историей</b>		
Ctrl-P, ↑	Previous	Вызывает на экран предыдущие команды, начиная с последней введенной. Повторный ввод символа вызывает более старые команды.
Ctrl-N, ↓	Next	Вызывает на экран более свежие команды после вызова более старых командой Ctrl-P или ↑.
<b>Команды удаления</b>		
Ctrl-H, Delete, Backspace	Delete to the left	Удаляет символ слева от курсора
Ctrl-D	Delete	Удаляет символ над курсором

### Cisco-like команды

Ctrl-K	Delete line forward	Удаляет все символы от курсора до конца строки
Ctrl-U, Ctrl-X	Delete line backward	Удаляет все символы от курсора до начала строки
Ctrl-W	Delete previous word	Удаляет символы от курсора до начала слова
ESC D	Delete next word	Удаляет символы от курсора до конца слова
<b>Преобразование букв</b>		
ESC C	Capitalize word	Преобразовать буквы от курсора до конца слова: начать с прописной буквы, остальные строчные
ESC U	Make word uppercase	Сделать все буквы от курсора до конца слова прописными
ESC L	Make word lowercase	Сделать все буквы от курсора до конца слова строчными
<b>Перестановка символов</b>		
Ctrl-T	Transpose	Меняет местами символ слева от курсора и символ над курсором
<b>Ввод непечатных символов</b>		
Ctrl-V, ESC Q	Ignore editing	Следующий введенный символ будет воспринят не как команда редактирования, а как часть вводимой пользователем команды.
<b>Завершение ввода команды</b>		
Ctrl-J, Ctrl-M, Enter	Execute	Ввод команды
<b>Повторный показ командной строки</b>		
Ctrl-L, Ctrl-R	Redisplay Line	Повторно показать prompt и содержимое командной строки

## Команды, родственные Cisco Systems

Ниже приведено описание команд, базирующихся на аналогичных командах от Cisco IOS.

Работают только те команды, которые описаны в этой главе, остальные команды Cisco IOS игнорируются.

Максимальная длина вводимой команды – 512 символов и не зависит от настроек терминала. При достижении данного значения дальнейший ввод команды блокируется (возобновляется, если удалить какие-либо из введенных ранее символов).

Действие cisco-like команд начинается только после выхода из конфигурационного режима консоли. После этого происходит конвертирование Cisco-like конфигурации в Native-конфигурацию и ее загрузка на CSP VPN Gate. Исключение составляют команды настройки IP-маршрутизации и SNMP-трапов: `ip route` и `snmp-server enable traps`, а при заданной команде `snmp-server enable traps` также `snmp-server host` и `snmp-server trap-source`. При задании этих команд сразу же формируется и загружается **инкрементальная конфигурация** при включенном режиме синхронизации политик. Подробнее см. раздел «Конвертор VPN политики» в отдельном документе [«Приложение»](#).

**Предупреждение:** при запущенной специализированной консоли – `cs_console`, перед остановкой сервиса `vpngate` необходимо выйти из консоли, иначе консоль окажется неработоспособной при выключенном сервисе.

# Команды входа в режимы настроек

## configure terminal

Для входа в глобальный конфигурационный режим системы используйте команду `configure terminal` в привилегированном режиме.

**Синтаксис**                      `configure terminal`

Эта команда не имеет аргументов или ключей.

**Режимы команды**                      privileged EXEC

### **Рекомендации по использованию**

Используйте эту команду для входа в глобальный конфигурационный режим. Следует помнить, что команды в этом режиме будут записаны в файл действующей конфигурации сразу после ввода (использования ключей Enter или Carriage Return).

При входе в конфигурационный режим происходит синхронизация политик, описанная в документе [«Приложение»](#).

После ввода команды `configure` системная строка изменится с `<Router-name>#` на `<Router-name>(config)#`, что показывает переход в глобальный конфигурационный режим. Для выхода из глобального конфигурационного режима и возврата в привилегированный EXEC режим следует ввести команду `end` или `exit`.

Для того, чтобы увидеть сделанные изменения в конфигурации, используйте команду `show running-config` в EXEC режиме.

### **Пример**

Ниже приведен пример перехода в глобальный конфигурационный режим:

```
Router#configure terminal
Enter configuration commands, one per line.
Router(config)#
```

## enable

Для входа в привилегированный режим EXEC или для некоторых других настроек уровня защиты системным администратором используйте команду `enable`.

### Синтаксис

`enable`

### Режимы команды

EXEC

### Рекомендации по использованию

Вход в привилегированный режим EXEC позволяет использовать привилегированные команды. Поскольку многие из привилегированных команд устанавливают операционные параметры, привилегированный доступ должен быть защищен паролем, чтобы предотвратить неправомерное использование. Если системный администратор установил пароль командой глобальной настройки `enable password` или `enable secret`, этот пароль будет у Вас запрошен до того, как Вам будет разрешен допуск к привилегированному режиму EXEC. Пароль чувствителен к регистру.

Если для входа в привилегированный режим EXEC пароль не был установлен, то в консоль можно будет зайти только привилегированным пользователям.

### Пример

В приведенном ниже примере пользователь входит в привилегированный режим, вводя команду `enable` и предъявляя пароль. При вводе пароль не показывается. После этого командой `disable` пользователь выходит из привилегированного режима в пользовательский режим:

```
Router> enable
Password: <letmein>
Router# disable
Router>
```

# Команды выхода из режимов настроек

## end

Для завершения сессии конфигурационного режима и возврата в привилегированный режим EXEC используйте команду `end` в глобальном режиме.

**Синтаксис**                      `end`

Эта команда не имеет аргументов или ключей.

**Значение по умолчанию**                      Значение по умолчанию отсутствует.

**Режимы команды**                      Global configuration

### **Рекомендации по использованию**

Команда `end` позволяет вернуться в привилегированный режим EXEC независимо от того, в каком конфигурационном режиме вы находитесь.

При выходе из глобального конфигурационного режима, при необходимости происходит попытка конвертирования конфигурации и все сделанные изменения вступают в силу. При этом происходит удаление всех установленных ранее соединений (IPsec и ISAKMP SA).

Эта команда может использоваться в различных конфигурационных режимах.

Используйте эту команду когда вы закончили операции по настройке и желаете возвратиться в режим EXEC для выполнения шагов по верификации.

### **Отличие данной команды от подобной команды Cisco IOS:**

только после выхода из конфигурационного режима при необходимости происходит попытка конвертирования конфигурации и вступают в действие изменения, произведенные в конфигурации. Исключение составляют только настройки IP-маршрутизации и SNMP-трапов: команды `ip route` и `snmp-server enable traps`, а при заданной команде `snmp-server enable traps` и команды `snmp-server host`, `snmp-server trap-source`. ( См. документ «[Приложение](#)».)

### **Пример**

В приведенном примере команда `end` используется для выхода из режима настройки Router.

```
Router# configure terminal
Router(config)# interface fastethernet 0/1
Router(config-if)# exit
Router(config)# end
Router#
```



## exit (EXEC)

Для завершения сессии работы с Продуктом используйте команду `exit` в пользовательском режиме EXEC .

**Синтаксис**                      `exit`

Эта команда не имеет аргументов или ключей.

**Значение по умолчанию**                      Значение по умолчанию отсутствует.

**Режимы команды**                      EXEC

**Рекомендации по использованию**

Используйте команду `exit` в EXEC режиме для закрытия сессии работы с Продуктом.

**Пример**

В приведенном примере команда `exit (global)` используется для выхода из глобального конфигурационного режима в привилегированный режим EXEC, затем используется команда `disable` для перехода в пользовательский режим EXEC и в конце используется команда `exit (EXEC)` для выхода из активной сессии.

```
Router(config)# exit
Router# disable
Router> exit
```

## exit (global)

Для выхода из любого конфигурационного режима с переходом в более высокий режим иерархии интерфейса командной строки используйте команду `exit` в любой конфигурационной моде.

**Синтаксис**                      `exit`

Эта команда не имеет аргументов или ключей.

**Значение по умолчанию**                      Значение по умолчанию отсутствует.

**Режимы команды**                      Все конфигурационные режимы

### **Рекомендации по использованию**

Команда `exit` используется в интерфейсе командной строки для перехода из текущего командного режима в режим более высокого уровня иерархии.

Например, при выполнении команды `exit` из глобального конфигурационного режима будет произведен переход в привилегированный режим EXEC. Аналогично производится переход из режимов заданных командами `interface`, `ip access-list extended`, `crypto map` в глобальный конфигурационный режим.

При выходе из глобального конфигурационного режима все сделанные изменения вступают в силу. При этом происходит удаление всех установленных ранее соединений (IPsec и ISAKMP SA).

### **Отличие данной команды от подобной команды Cisco IOS:**

только после выхода из конфигурационного режима вступают в действие изменения, произведенные в конфигурации. Исключение составляют только настройки IP-маршрутизации и SNMP-трапов: команды `ip route` и `snmp-server enable traps`, а при заданной команде `snmp-server enable traps` и команды `snmp-server host`, `snmp-server trap-source`. (См. документ «Приложение».)

### **Пример**

Приведенный ниже пример демонстрирует переход из режима настройки `interface` в глобальный конфигурационный режим:

```
Router(config-if)# exit
Router(config)#
```

## disable

Команда `disable` используется для выхода из привилегированного режима EXEC и перехода в пользовательский режим EXEC.

**Синтаксис**                      `disable`

**Значение по умолчанию**                      Выход в пользовательский EXEC режим.

**Режимы команды**                      privileged EXEC

**Рекомендации по использованию**

С помощью команды `disable` можно осуществить переход в пользовательский режим EXEC.

**Пример**

Приведенный ниже пример демонстрирует выход из привилегированного режима в пользовательский EXEC режим:

```
Router> enable
Password: <letmein>
Router# disable
Router>
```

# Команды вывода информации (информационные команды)

## show version

Команда `show version` реализована для обеспечения совместимости с Cisco VMS. Ее вывод эмулирует сообщения Cisco IOS о модели аппаратной платформы и версии программного обеспечения.

### Синтаксис

<b>show version</b>	<b>[  include {line_to_include}]</b>
include	модификатор фильтрации вывода
line_to_include	выводимая строка должна содержать этот аргумент

### Режимы команды

EXEC, privileged EXEC

### Рекомендации по использованию

Данная команда используется для получения информации о конфигурации аппаратной и программной платформ.

Для вывода строк, которые содержат указанный аргумент `line_to_include`, используйте команду в следующем виде:

```
show version | include {line_to_include}
```

где `|` – обязательный символ, а не знак «или». После символа `|` обязательно должен следовать пробел, иначе команда будет ошибочной.

### Отличие данной команды от подобной команды Cisco IOS:

- первая строка вывода отсутствует у Cisco. Две последующие строки присутствуют в выводе команды `show run` в Cisco IOS, но выводятся и другие строки.
- в команде `show version` дополнительные модификаторы, кроме фильтрации вывода `include`, не допускаются, в отличие от Cisco IOS
- проверяется прямое вхождение `line_to_include` в выводимой строке. В Cisco IOS проверяется regular expression.

Для получения информации о конфигурации аппаратной и программной платформ из *конфигурационного режима* используется команда `do show version`.

### Пример

Приведенный ниже пример содержит информацию, которая выводится при выполнении команды `show version` при наличии зарегистрированной лицензии на продукт:

```
Router#show version
```

```
CSP VPN GATE1000 build 3.11.xxxx. Emulates:
```

```
Cisco IOS Software, 2800 Software (C2800NM-ADVIPSERVICESK9-M), Version  
12.4(13a), RELEASE SOFTWARE (fc1)
```

```
Cisco 2811 (revision 53.50) with 249856K/12288K bytes of memory.
```

**При отсутствии зарегистрированной лицензии вывод команды show version следующий:**

```
CSP VPN GATE build 3.11.xxxx (no valid license). Emulates:
```

```
Cisco IOS Software, 2800 Software (C2800NM-ADVIPSERVICESK9-M), Version  
12.4(13a), RELEASE SOFTWARE (fc1)
```

```
Cisco 2811 (revision 53.50) with 249856K/12288K bytes of memory.
```

## show version csp

Для вывода информации о версии программного обеспечения CSP VPN Gate, типе и номере сборки используйте команду `show version csp`.

**Синтаксис**                      `show version csp`

Эта команда не имеет аргументов или ключей.

**Режимы команды**                      EXEC, privileged EXEC

### **Рекомендации по использованию**

Данная команда используется для получения информации о Продукте CSP VPN Gate. Аналогичной команды в Cisco IOS не существует.

Если в продукте зарегистрирована правильная лицензия, то по команде выдается следующая информация:

```
CSP VPN <product-type> build 3.11.xxxx,
```

где <product-type> – тип продукта из лицензии (GATE100, ,,,).

Если в продукте не зарегистрирована лицензия, то по команде выдается следующий текст:

```
CSP VPN GATE build 3.11.xxxx (no valid license).
```

Для команды `show version csp` отсутствует возможность фильтрации вывода (модификатор `include`).

### **Отличие данной команды от подобной команды Cisco IOS:**

команда `show version csp` отсутствует у Cisco.

Для вывода информации о версии программного обеспечения CSP VPN Gate, типе и номере сборки используйте команду из *конфигурационного режима* используется команда `do show version csp`.

### **Пример**

Приведенный ниже пример содержит информацию, которая выводится при выполнении команды `show version csp`:

```
Router> show version csp  
CSP VPN Gate 1000 build 3.11.7539
```

## show privilege

Команда `show privilege` отображает текущий уровень привилегий пользователя.

**Синтаксис**                      `show privilege`

**Значение по умолчанию**                      Значение по умолчанию отсутствует.

**Режимы команды**                      EXEC, privileged EXEC

### **Рекомендации по использованию**

С помощью команды `show privilege` можно посмотреть текущий уровень привилегий.

В результате выполнения команды `show privilege` отображается строка:

`Current privilege level is <n>`,

где `<n>` текущий уровень привилегий.

Примечание: При входе в `cs_console` пользователя, присутствующего в Cisco-like конфигурации и имеющего уровень привилегий отличный от максимального (15), в качестве текущего уровня привилегий выставляется значение из Cisco-like конфигурации для этого пользователя. Этот уровень будет сохраняться, пока пользователь будет находиться в EXEC-режиме консоли.

В привилегированном режиме текущий уровень привилегий всегда 15. При выходе из привилегированного режима в EXEC режим по команде `disable`, текущий уровень привилегий устанавливается в значение 1.

Команда `do show privilege` позволяет увидеть текущий уровень привилегий из *конфигурационного режима*.

## show load-message

Для вывода информации о работе конвертора используйте команду `show load-message`.

**Синтаксис**                      `show load-message`

Эта команда не имеет аргументов или ключей.

**Режимы команды**                      privileged EXEC

### **Рекомендации по использованию**

Использовать эту команду имеет смысл только после выхода из конфигурационного режима, т.е. после завершения работы конвертора конфигурации.

В случае, если настройка конфигурации была неуспешной (завершилось с ошибкой), команда `show load-message` выдаст детализированное сообщение об ошибке.

Если настройка конфигурации завершилось успешно, но с предупреждениями – команда покажет все предупреждения, которые были выданы конвертором.

Если настройка конфигурации завершилось без ошибок и предупреждений – команда не выдаст ничего.

Все сообщения, которые может выдать команда, также выдаются конвертором в лог во время конвертирования.

### **Отличие данной команды от подобной команды Cisco IOS:**

команда `show load-message` отсутствует у Cisco.

### **Пример**

Приведенный ниже пример содержит информацию, которая выводится при выполнении команды `show load-message`:

```
Router#show load-message
Crypto map(s) "cmap 10" contain transform sets with different
encapsulation modes.
Tunnel mode is used.
```



## show running-config

Команда `show running-config` используется для вывода на экран загруженной конфигурации.

**Синтаксис** `show running-config [| include {line_to_include}]`

`| include {line_to_include}`      модификатор фильтрации вывода.

**Альтернативный синтаксис** `write terminal`

**Режимы команды** privileged EXEC

**Значение по умолчанию** Значение по умолчанию отсутствует.

**Рекомендации по использованию**

Для просмотра полного текста загруженной политики безопасности используйте команду `show running-config`.

Для вывода строк текста политики безопасности, которые содержат указанный аргумент `line_to_include`, используйте команду в следующем виде:

```
show running-config | include {line_to_include}
```

где `|` – обязательный символ, а не знак «или». После символа `|` обязательно должен следовать пробел, иначе команда будет ошибочной.

В команде `write terminal` модификатор фильтрации вывода задавать нельзя.

**Отличие данной команды от подобной команды Cisco IOS:**

- в команде `show running-config` дополнительные модификаторы, кроме фильтрации вывода `include`, не допускаются, в отличие от Cisco IOS
- проверяется прямое вхождение `line_to_include` в выводимой строке. В Cisco IOS проверяется regular expression.

Для просмотра текста загруженной политики безопасности в *конфигурационном режиме* используйте команду `do show running-config`.

**Пример**

```
Router# show running-config
```

```
Building configuration...
```

```
interface FastEthernet0/0
```

```
ip address 10.0.21.100 255.255.0.0
```

```
crypto map fat
```

```
interface FastEthernet0/1
```

```
ip address 192.168.15.10 255.255.255.0
```

```
end
```

## show terminal

Команда `show terminal` используется просмотра настроек терминала.

**Синтаксис**                      `show terminal`

**Режимы команды**                      privileged EXEC

**Значение по умолчанию**                      Значение по умолчанию отсутствует.

**Рекомендации по использованию**

При выполнении команды `show terminal` выводится только одна строка:

Length: <length> lines, Width: <width> columns

**Отличие данной команды от подобной команды Cisco IOS:**

данная команда в Cisco IOS выдает больше информации.

# show ip route

Команда `show ip route` выводит содержимое таблицы маршрутизации.

**Синтаксис**                      `show ip route`

**Режимы команды**                      privileged EXEC

## **Рекомендации по использованию**

Данная команда используется для отображения текущего состояния таблицы маршрутизации.

Данная команда показывает только маршруты connected ("C") и статический ("S"). Маршруты, заданные по протоколам RIP или OSPF, будут показаны как статические.

Раздел "Codes" (вывод легенды) содержит описание и других, реально неиспользуемых типов маршрутов. Этот вывод сделан аналогичным Cisco IOS для поддержания совместимости с продуктами мониторинга и управления Cisco (например, Cisco MARS).

При выполнении команды не показываются маршруты:

- если в системе присутствует маршрут через интерфейс, который не зарегистрирован в продукте, то этот маршрут не показывается
- если существует маршрут через интерфейс, который зарегистрирован в продукте и которому соответствуют несколько физических интерфейсов, то такой маршрут не показывается. Например, "wan".

## **Пример вывода команды**

```
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS
level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static
route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 10.1.1.1 to network 0.0.0.0

    1.0.0.0/32 is subnetted, 4 subnets
S      1.2.3.4 [1/0] via 10.2.2.2
          [1/0] via 10.3.3.3
          is directly connected, FastEthernet0/0
S      1.2.3.5 is directly connected, FastEthernet0/0
S      1.2.3.6 [1/0] via 10.2.2.2
S      1.2.3.7 [1/0] via 10.2.2.2
    174.0.0.0/16 is variably subnetted, 3 subnets, 2 masks
S      174.0.0.0/24 [1/0] via 10.3.3.3
S      174.0.1.0/24 [1/0] via 10.3.3.3
```

```

S      174.0.0.0/19 [1/0] via 10.3.3.3
C      192.168.111.0/24 is directly connected, FastEthernet1/0
S      181.111.0.0/16 [1/0] via 10.3.3.3
              is directly connected, FastEthernet0/0
      10.0.0.0/16 is subnetted, 1 subnets
C      10.0.0.0 is directly connected, FastEthernet0/0
S      172.0.0.0/8 [1/0] via 10.3.3.3
S*     0.0.0.0/0 [1/0] via 10.1.1.1

```

**Правила формирования таблицы маршрутизации (аналогичны Cisco IOS, за исключением случаев, отмеченных специально):**

1. В качестве «шлюза последней надежды» (термин заимствован из документации Cisco IOS – шлюз по умолчанию) берется маршрут до подсети 0.0.0.0/0:
  - если такой маршрут отсутствует, то пишется фраза: Gateway of last resort is not set.
  - маршрут подсети вида 0.0.0.0/x, где  $x > 0$ , за «шлюз последней надежды» не признается
  - логика выбора «шлюза последней надежды» аналогична Cisco IOS с тем отличием, что в Cisco IOS существуют и другие способы задания - с помощью команд `ip default-gateway` и `ip default-network`
  - если маршрут до подсети 0.0.0.0/0 задан через интерфейс, то выдается фраза: Gateway of last resort is 0.0.0.0 to network 0.0.0.0
  - если существуют несколько маршрутов до подсети 0.0.0.0/0, то в качестве «шлюза последней надежды» выбирается первый из них
  - запись в таблице маршрута «шлюз последней надежды» помечается звездочкой.
2. Формирование записи таблицы маршрутизации:
  - тип записи формируется следующим образом:
    - если маршрут прописан через интерфейс, причем подсеть сформирована адресом на интерфейсе (а не специальной командой маршрутизации), то пишется тип “C”
    - во всех остальных случаях, включая маршрут, явно прописанный через интерфейс, пишется тип “S”
  - адрес очередной подсети соотносится с классами сетей “A”, “B” и “C”:
    - маршруты пишутся в виде отдельных записей (не группируются) в случаях:
      - подсети, более широкие, чем предполагаемый их класс (например, 172.0.0.0/8)
      - адреса вида 0.0.0.0/x
      - адреса, не принадлежащие к классам “A”, “B” или “C”
    - подсети, более узкие, чем предполагаемый их класс (например, 10.0.0.0/16), обязательно помечаются как “Subnetted” и, при необходимости, группируются несколько подсетей вместе
    - подсети, совпадающие с классом (например, 192.168.111.0/24), включаются в группу “Subnetted”, если в ней присутствуют более узкие подсети. Если более узких подсетей нет, подсети, совпадающие с классом, пишутся в виде отдельной записи.
3. Группирование записей в случае совпадения масок подсетей:
  - вначале пишется строка вида:

```
class-ip/mask-postfix is subnetted, N subnets
```

где

`class-ip` IP-адрес с наложенной на него маской классовой подсети (не путать с общей для данных подсетей маской!!!)

`mask-postfix` общая для данных подсетей маска

`N` количество подсетей в данной группе.

Например, для записей вида `1.2.x.0/24` будет написано:

```
1.0.0.0/24 is subnetted, <N> subnets
```

- в записях, принадлежащих к этой группе, пишутся только IP-адреса без масок.

#### 4. Группирование записей в случае разных масок подсетей:

- вначале пишется строка вида:

```
class-ip/class-mask-postfix is variably subnetted, N subnets, M masks
```

где

`class-ip` IP-адрес с наложенной на него маской классовой подсети

`class-mask-postfix` классовая маска

`N` количество подсетей в данной группе

`M` количество масок подсетей в данной группе.

Пример:

```
174.0.0.0/16 is variably subnetted, 3 subnets, 2 masks
```

- в записях, принадлежащих к этой группе, пишутся IP-адреса с масками.

#### 5. Группирование записей в случае одинаковых адресов:

- первая строка пишется полностью, включая тип записи, адресную информацию и указание через `gateway` или интерфейс пишется маршрут
- во второй и последующих строках - тип записи и адресная информация опускаются
- если для данного адреса присутствуют маршруты как через интерфейсы, так и `gateways`, то сначала пишутся маршруты через `gateways`, а потом – через интерфейсы.

#### 6. Для записей типа “S” в квадратных скобках пишется информация, связанная с метрикой маршрута, в виде:

```
[metric/0]
```

Параметр `metric` зависит от операционной системы:

- ОС Linux:
  - если системная метрика маршрута равна 0, то выдается 1
  - в противном случае - выдается значение системной метрики

Для маршрутов, заданных в консоли с помощью команды `ip route`, всегда выдается метрика в виде `[1/0]`. Такое поведение аналогично Cisco IOS, при условии использования параметра `administrative distance` по умолчанию.

#### Отличие данной команды от подобной команды Cisco IOS:

- присутствует только указанный вариант команды, в отличие от Cisco IOS, где могут присутствовать дополнительные параметры
- показывает только connected ("C") и статический ("S") маршруты
- параметр, связанный с метрикой маршрута имеет вид `[metric/0]`, а в Cisco IOS - `[administrative-distance/metric]`

## show crypto isakmp policy

Команда `show crypto isakmp policy` используется для вывода на экран ISAKMP политики.

### Синтаксис

`show crypto isakmp policy`

### Значение по умолчанию

Значение по умолчанию отсутствует.

### Режимы команды

privileged EXEC

### Рекомендации по использованию

Для просмотра в конфигурации текста политики ISAKMP.

При отсутствии в конфигурации политики ISAKMP выводится следующее:

Global IKE policy.

### Отличие данной команды от подобной команды Cisco IOS:

при выводе ISAKMP политики не показывается Default protection suite в силу отсутствия.

### Пример

Пример вывода на экран политики ISAKMP:

```
Protection suite of priority 10
    encryption algorithm:  DES - Data Encryption Standard (56 bit
keys).
    hash algorithm:        Message Digest 5
    authentication method: Pre-Shared Key
    Oakley group:          VKO GOST R 34.10-2001
    lifetime:              86400 seconds, no volume limit
Protection suite of priority 20
    encryption algorithm:  Three key triple DES
    hash algorithm:        Secure Hash Standard
    authentication method: Rivest-Shamir-Adleman Signature
    Diffie-Hellman group:  #1 (768 bit)
    lifetime:              10000 seconds, no volume limit
Protection suite of priority 30
    encryption algorithm:  AES - Advanced Encryption Standard (192
bit keys).
    hash algorithm:        Secure Hash Standard
    authentication method: Rivest-Shamir-Adleman Signature
    Diffie-Hellman group:  #5 (1536 bit)
    lifetime:              86400 seconds, no volume limit
```

# Команды настройки терминала

## terminal width

Команда `terminal width` устанавливает число символьных столбцов экрана терминала в текущей сессии. Влияет на скроллинг длинных команд.

Для установки ширины терминала по умолчанию используется команда `terminal no width`.

### Синтаксис

`terminal width {characters}`

`characters`

количество символьных столбцов терминала – от 0 до 512.

### Режимы команды

privileged EXEC

### Значение по умолчанию

Значение по умолчанию зависит от режима работы:

если в терминальной сессии можно получить ширину терминала, то выставляется полученная ширина терминала

если не удастся получить ширину терминала, то устанавливается значение 511.

### Рекомендации по использованию

Данная команда используется, если значение по умолчанию не соответствует потребностям.

В зависимости от ОС различается реакция на изменение размеров терминала (можно наблюдать перерисовку строки при изменении ширины терминала, если начать вводить очень длинную строку, инициирующую скроллинг):

- в ОС Linux: перерисовка строки происходит только после ввода следующего символа или нажатия управляющей клавиши.

Размеры терминала, выставленные с помощью команд `terminal width` / `terminal length`, являются более приоритетными, чем размеры, полученные иным способом:

если заданы данные команды, то они отключают реакцию на изменение размеров терминального окна (см. раздел [“Интерфейс пользователя”](#)).

Команды `terminal width` и `terminal length` также выставляют размер терминала для программ, запускаемых с помощью команды `run`. Если выставлены нестандартные размеры, то это может привести к проблемам в работе терминальных приложений.

### Отличие данной команды от подобной команды Cisco IOS:

значение ширины терминала по умолчанию в Cisco IOS равно 80.

### Пример

Приведенный ниже пример выставляет ширину терминала 130 символьных столбцов.

```
Router#terminal width 130
```



## terminal length

Команда `terminal length` устанавливает число строк экрана терминала в текущей сессии. Влияет на паузы при длинном выводе (например, команды `show running-config`).

Выставить число строк терминала по умолчанию можно командой `terminal no length`.

### Синтаксис

**terminal length** {screen-length}

screen-length

количество символьных строк терминала – от 0 до 512. Значение 0 имеет специальный смысл – отсутствуют паузы при длинном выводе на экран.

### Режимы команды

privileged EXEC

### Значение по умолчанию

Значение по умолчанию зависит от режима работы:

если в терминальной сессии можно получить количество строк терминала, то выставляется полученное количество строк терминала,

если не получается получить количество строк терминала, то устанавливается значение 0.

### Рекомендации по использованию

Команда дает возможность изменить количество отображаемых строк при выводе или запретить выдачу информации позкранно при многоэкранном выводе.

Размеры терминала, выставленные с помощью команд `terminal width` / `terminal length`, являются более приоритетными, чем размеры, полученные иным способом:

если заданы данные команды, то они отключают реакцию на изменение размеров терминального окна (см. раздел [“Интерфейс пользователя”](#)).

Команды `terminal width` и `terminal length` также выставляют размер терминала для программ, запускаемых с помощью команды `run`. Если выставлены нестандартные размеры, то это может привести к проблемам в работе терминальных приложений.

### Отличие данной команды от подобной команды Cisco IOS:

значение длины терминала по умолчанию в Cisco IOS равно 24.

### Пример

Приведенный ниже пример выставляет длину терминала 0, запрещая паузы при многоэкранном выводе.

```
Router#terminal length 0
```

# Команды вызова системных команд и системные команды

## run

Команда `run` позволяет выполнять команды операционной системы из CLI.

### Синтаксис

<code>run</code>	<code>{command}</code>
<code>command</code>	команда, предназначенная для выполнения командным интерпретатором. Для шлюза используется командный интерпретатор <code>sh</code> , который запускается в директории Продукта под тем же пользователем, под которым запущена консоль.

### Значение по умолчанию

Значение по умолчанию отсутствует

### Режимы команды

privileged EXEC

### Рекомендации по использованию

Данная команда предназначена для выполнения команд операционной системы, а также для **запуска утилит** Продукта, описанных в документе «[Специализированные команды](#)». Вывод команды передается на экран без изменения.

Прервать выполнение внешнего приложения можно комбинацией клавиш `Ctrl-Shift-6`. Если по каким-либо причинам внешняя программа не отреагировала на прерывание, можно нажать `CTRL-C`. Эта команда посылает SIGKILL – перехватываемый сигнал, по которому выполнение внешней программы прекращается.

### Отличие данной команды от подобной команды Cisco IOS:

команда `run` отсутствует у Cisco.

Команда `do run` позволяет выполнять команды командного интерпретатора операционной системы из *конфигурационного режима*.

### Пример

Приведенный ниже пример содержит информацию, которая выводится при выполнении команды `run /sbin/ifconfig`

```
Router#run /sbin/ifconfig
```

```
eth0      Link encap:Ethernet  HWaddr 00:0E:0C:6F:0F:E6
          inet          addr:192.168.16.2          Bcast:192.168.16.255
Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:34 errors:0 dropped:0 overruns:0 frame:0
          TX packets:39 errors:0 dropped:0 overruns:0 carrier:0
```

```
collisions:0 txqueuelen:1000
RX bytes:2226 (2.1 KiB) TX bytes:2539 (2.4 KiB)
Base address:0xcc00 Memory:c0100000-c0120000

eth1      Link encap:Ethernet  HWaddr 98:00:54:76:10:33
          inet      addr:192.168.17.133      Bcast:192.168.17.255
Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1239 errors:0 dropped:0 overruns:0 frame:0
          TX packets:134 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:131023 (127.9 KiB) TX bytes:11978 (11.6 KiB)
          Base address:0xc800 Memory:c0120000-c0140000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:27 errors:0 dropped:0 overruns:0 frame:0
          TX packets:27 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:2323 (2.2 KiB) TX bytes:2323 (2.2 KiB)
```

# ping

Для выполнения системной команды `Ping` используйте команду `ping`.

<b><u>Синтаксис</u></b>	<b><code>ping</code></b> {ip-address hostname}
ip-address	IP-адрес хоста, на который посылается ping.
hostname	имя хоста, на который посылается ping.

**Значение по умолчанию**                      Значение по умолчанию отсутствует.

**Режимы команды**                              privileged EXEC

## **Рекомендации по использованию**

Утилита `ping` вызывается из состава операционной системы.

Формат вывода данной команды зависит от операционной системы.

Прервать выполнение внешнего приложения можно комбинацией клавиш `ctrl-shift-6`. Если по каким-либо причинам внешняя программа не отреагировала на прерывание, можно нажать `CTRL-C`. Эта команда посылает SIGKILL – перехватываемый сигнал, по которому выполнение внешней программы прекращается.

## **Отличие данной команды от подобной команды Cisco IOS:**

формат вывода команды отличается от формата вывода команды Cisco.

Команда `do ping` позволяет выполнить команду `ping` из *конфигурационного режима*.

## **Пример**

Приведенный ниже пример содержит информацию, которая выводится при выполнении команды `ping`

```
Router#ping 10.0.10.1
Ping 10.0.10.1: 100 data bytes
108 bytes from 10.0.10.1: bytes=100 time=0 ms
108 bytes from 10.0.10.1: bytes=100 time=0 ms
108 bytes from 10.0.10.1: bytes=100 time=0 ms
108 bytes from 10.0.10.1: bytes=100 time=0 ms
108 bytes from 10.0.10.1: bytes=100 time=0 ms
-----10.0.10.1 PING Statistic-----
5 Packets transmitted, 5 packets received, 0% packets loss
round trip <ms>   min/avg/max = 0/0/0
```

# Команды создания пользователей, назначения паролей, уровня привилегий

## enable password

Команда `enable password` используется для назначения локального пароля доступа в привилегированный режим консоли пользователям всех уровней привилегий. Для снятия защиты паролем привилегированного режима используется та же команда с префиксом `no`.

### Синтаксис

```
enable password {password}
no enable password {password}

password          значение пароля.
```

### Значение по умолчанию

значение по умолчанию отсутствует.

### Режимы команды

Global configuration

### Рекомендации по использованию

По команде `enable password` пароль задается и хранится в открытом виде. Если посмотреть конфигурацию командой `show running-config`, то в команде `enable password` пароль будет выведен в открытом виде.

По сравнению с Cisco формат данной команды сокращен, там есть возможность задать зашифрованный пароль командой `enable password 7 <encrypted-password>`, в которой используется некоторый обратимый алгоритм шифрования, по которому можно восстановить исходный пароль. Поэтому Cisco не рекомендует использовать эту команду, что равносильно заданию открытого пароля.

Чтобы зашифровать вводимый в открытом виде пароль, используйте команду `enable secret 0 password`.

Не поддерживается также дополнительный параметр `level` в командах `enable password` и `enable secret`.

В `cs_console` команды `enable password` и `enable secret` являются взаимозаменяемыми, т.е. ввод команды обозначает замену пароля вне зависимости от того, как он был задан ранее. Иначе говоря, ввод команды `enable secret` отменяет команду `enable password` и наоборот.

В начальной конфигурации (после инсталляции Продукта) присутствует команда:

```
enable password csp
```

Настоятельно рекомендуется сменить этот пароль на другой – лучше с помощью команды `enable secret`.

Если задать одну из двух команд (в данной версии Продукта они эквивалентны друг другу):

```
no enable password
no enable secret
```

это означает, что вход в привилегированный режим отключается:

- в этом случае запрещается вход в консоль непривилегированному пользователю (уровень привилегий, отличный от 15). При попытке войти в консоль, будет выдано сообщение: "Password required, but none set" (сообщение, аналогичное сообщению Cisco). После этого программа завершит работу.
- следует соблюдать осторожность: если удалить всех привилегированных пользователей (с уровнем 15) и отключить пароль на вход в привилегированный режим, то зайти в консоль больше не удастся!
- если при отключенном пароле на вход в привилегированный режим зайти привилегированным пользователем, затем с помощью команды `disable` выйти из привилегированного режима, а потом задать команду `enable` – будет выдано сообщение об ошибке: "% Error in authentication." (сообщение, аналогичное сообщению Cisco). Войти в привилегированный режим в рамках данной сессии уже не удастся.
- по команде `show running-config` в этом случае не будут показываться команды `enable password` и `enable secret`.

**Отличие данной команды от подобной команды Cisco IOS:**

не поддерживается вариант записи команды:

`enable password 0 <pwd>` **!!! не поддерживается!!!**

**Пример**

Приведенный ниже пример демонстрирует текст команды для назначения пароля "qwerty":

```
Router<config>#enable password qwerty
Router<config>#exit
```

## enable secret

Команда `enable secret` используется для назначения локального пароля доступа в привилегированный режим консоли в открытом виде и хранении в зашифрованном виде пользователям всех уровней привилегий. Для снятия защиты паролем привилегированного режима используется та же команда с префиксом `no`.

### Синтаксис

`enable secret {0|5} {password}`

`no enable secret {0|5} {password}`

`password`

значение пароля

0

при этом значении пароль вводится в открытом виде и зашифровывается внутри

5

при этом значении считается, что вводимый пароль является результатом функции хэширования, и сохраняется без изменения.

### Значение по умолчанию

Значение по умолчанию отсутствует.

### Режимы команды

Global configuration

### Рекомендации по использованию

При значении `{0}` пароль вводится в открытом виде, а затем вычисляется функция хэширования пароля. Если посмотреть конфигурацию командой `show running-config`, то команда

```
enable secret 0 {password}
```

будет представлена с паролем, который является результатом функции хэширования, в виде:

```
enable secret 5 {password_encrypted}.
```

При значении `{5}` считается, что введенный пароль является результатом функции хэширования пароля и в конфигурации сохраняется без изменения в том виде, в каком и был введен в команде:

```
enable secret 5 {password_encrypted}
```

Команда может быть задана и в другом виде:

```
enable secret {password}
```

`password` значение пароля, которое не может быть равно 0 или 5, в противном случае - данный синтаксис недопустим.

Если задать одну из двух команд (в данной версии Продукта они эквивалентны друг другу):

```
no enable password
```

```
no enable secret
```

это означает, что вход в привилегированный режим отключается:

- в этом случае запрещается вход в консоль непривилегированному пользователю (уровень привилегий, отличный от 15). При попытке войти в консоль, будет выдано сообщение: "Password required, but none set" (сообщение, аналогичное сообщению Cisco). После этого программа завершит работу.

- следует соблюдать осторожность: если удалить всех привилегированных пользователей (с уровнем 15) и отключить пароль на вход в привилегированный режим, то зайти в консоль больше не удастся!
- если при отключенном пароле на вход в привилегированный режим зайти привилегированным пользователем, затем с помощью команды `disable` выйти из привилегированного режима, а потом задать команду `enable` – будет выдано сообщение об ошибке: "% Error in authentication." (сообщение, аналогичное сообщению Cisco). Войти в привилегированный режим в рамках данной сессии уже не удастся.
- по команде `show running-config` в этом случае не будут показываться команды `enable password` и `enable secret`.

**Отличие данной команды от подобной команды Cisco IOS:**

формат зашифрованного пароля отличается от формата подобной команды в IOS.

**Пример**

Приведенный ниже пример демонстрирует команду для назначения пароля "qwerty" для хранения ее внутри в зашифрованном виде:

```
Router<config>#enable secret 0 qwerty
Router<config>#exit
```

В конфигурации эта команда будет храниться в виде:

```
enable secret 5 2Fe034RYzgb7xibt2pYxcpA==
```



## username password

Для создания нового пользователя, изменения имени пользователя, пароля, уровня привилегий или удаления существующего пользователя, используйте команду `username password`. В конфигурации пароль будет храниться в открытом виде. Для удаления пользователя достаточно указать `no username {name}`.

### Синтаксис

```
username {name} [privilege level] password [0] {pwd}
no username {name}
```

name	имя пользователя. Имя должно начинаться с буквы латинского алфавита (строчной или прописной). Далее могут идти буквы латинского алфавита (строчные или прописные), цифры, _ (подчеркивание) и - (дефис). Имя должно быть уникальным и не превышать 8 символов.
level	уровень привилегий, диапазон значений 0 – 15. Значение по умолчанию – 1.
0	необязательный параметр, указывающий на то, что пароль хранится в незашифрованном виде. Он обязателен только в случае, если пароль тоже «0»:  <pre><b>username</b> {name} [<b>privilege level</b>] <b>password</b> 0 0.</pre> При выводе <code>no show running-config</code> ноль показывается всегда.
pwd	пароль пользователя. Допускаются латинские буквы, цифры и спецсимволы. Нельзя использовать пробелы и нелатинские символы.

### Режимы команды

Global configuration

### Рекомендации по использованию

#### Добавление пользователя, изменение его параметров

Данная команда используется для создания нового пользователя, изменения пароля или уровня привилегий существующего пользователя.



Note

В ОС Linux пользователь создается с `home` в директории `/var/cspvpn/users/<name>` (`<name>` – имя пользователя). Директория создается с атрибутами `750 (drwxr-x---)`.  
  
В качестве `shell` у пользователя выставляется `/opt/VPNagent/bin/cs_console`.

Ограничения на имя пользователя являются более строгими, чем в Cisco IOS. Это связано с особенностями используемых операционных систем.

Команда создания пользователя завершается с ошибкой, если пользователь с указанным в команде именем уже присутствует на машине, но не представлен в Cisco-like конфигурации.

Команда создания пользователя воспринимается как команда редактирования (например, сменить пароль, `privilege` и т.п.), если пользователь уже присутствует в конфигурации и на машине. При добавлении нового пользователя или изменении пароля существующего, добавляются или изменяются данные пользователей операционной системы.

Пользователю может быть назначен уровень привилегий из диапазона 0 – 15. Этот диапазон разделен на два класса: в первом – пятнадцатый уровень, а во втором – с 0 по 14 уровни. Пользователи с уровнем привилегий от 0 до 14 имеют одинаковые права.

Пользователь с пятнадцатым уровнем привилегий в интерфейсе командной строки сразу получает доступ к привилегированному режиму специализированной консоли. Пользователей с пятнадцатым уровнем может быть несколько.

Пользователь с уровнем привилегий от 0 по 14 имеет право доступа к пользовательскому режиму специализированной консоли. А если этот пользователь знает пароль доступа к привилегированному режиму, то он может настраивать CSP VPN Gate.

Если не указан в команде параметр [privilege level], то будет создан пользователь с 1 (первым) уровнем привилегий.

Если надо изменить уровень привилегий существующего пользователя, то в Cisco достаточно набрать команду `username <name> privilege <level>`, а в `cs_console` надо обязательно еще задать пароль.

По команде `show running-config` в конфигурации будет показана команда `username password` в том виде, в каком она была введена. Будьте осторожны, пароль хранится и показывается в открытом виде.

В `cs_console` команды `username password` и `username secret` являются взаимозаменяемыми – ввод любой из этих команд для существующего пользователя обозначает изменение пароля, независимо от того, как он был задан ранее.

### Удаление пользователя

Удаление пользователя с именем `name` производится командой

```
no username {name}
```

Допустимо указывать более длинную команду, например, `no username {name} privilege 10 password {pwd}`. Однако, никакой необходимости в этом нет.

Если имеется только один пользователь с уровнем привилегий 15, то удалять такого пользователя не рекомендуется.

Удалить пользователя, из-под которого запущена `cs_console`, технически возможно, но данное действие категорически не рекомендуется.

Если удаляется пользователь из системы, из-под которого не запущена `cs_console`:

- если пользователь успешно удален из системы: команда завершается успешно и пользователь удаляется из Cisco-like конфигурации.
- если пользователя в системе не существует: команда также завершается успешно и пользователь удаляется из Cisco-like конфигурации.
- если удаление пользователя не прошло (пользователь в системе остался): то команда завершается с ошибкой, пользователь не удаляется из Cisco-like конфигурации. или любого другого пользователя, который в данный момент зарегистрирован в системе.

### Выдаваемые сообщения

При попытке добавления нового пользователя могут возникать следующие ошибки:

Неправильный синтаксис имени пользователя (использование недопустимых символов):  
% User "<username>" was not created. Username is invalid.

Длина имени пользователя превышает 8 символов: % User "<username>" was not created. Username is too long (8-chars limit exceeded).

Пользователь с таким именем уже существует в системе: % User addition failed. User "<username>" already exists in the system.

Произошла системная ошибка (возможно нарушена системная политика в отношении имени пользователя или пароля; например слишком короткий пароль): % User addition failed: System error. Possibly the password or the user name violates some system policy (e.g. the password is too short).

Кроме указанной, возможны и другие причины появления данной ошибки, например исчерпание ресурсов. В Linux такая ошибка может возникнуть при попытке создать пользователя с именем, совпадающим с именем группы пользователей (список групп можно посмотреть в файле /etc/group).

При попытке смены пароля пользователя может возникать ошибка: % User password change failed. Possibly the password violates some system policy (e.g. it's too short).

При удалении пользователя, в ошибочных случаях выдается сообщение: % User account cannot be removed

#### **Отличие данной команды от подобной команды Cisco IOS:**

- не поддерживаются всевозможные варианты задания username и другие параметры:
  - не поддерживается `nopassword`
  - не поддерживается шифрование пароля – не поддерживается команда `username {name} password 7 {encrypted-password}`
- имеется ограничение на длину имени пользователя.
- в `cs_console` команды `username password` и `username secret` являются взаимозаменяемыми – ввод любой из этих команд для существующего пользователя обозначает изменение пароля, независимо от того, как он был задан ранее. В Cisco: если пароль для пользователя задан командой `username password` (пароль хранится в открытом виде), то пароль нельзя потом изменить, используя команду `username secret` (пароль хранится в зашифрованном виде), и наоборот – если пароль для пользователя задан командой `username secret`, то потом изменить его командой `username password` нельзя. В обоих случаях выдается сообщение об ошибке.
- невозможно изменить уровень привилегий пользователя без его пароля.

#### **Пример**

Ниже приведен пример изменения пароля пользователя с именем "cscons":

```
Router(config)#username cscons password security
Router(config)#end
```

## username secret

Для создания нового пользователя, изменения пароля, уровня привилегий или удаления существующего пользователя применяйте команду `username secret`. В конфигурации пароль будет храниться либо в зашифрованном виде либо в том виде, в каком он был введен в команде.

### Синтаксис

```
username {name} [privilege level] secret {0|5} {pwd}
```

```
no username {name}
```

name	имя пользователя. Имя должно начинаться с буквы латинского алфавита (строчной или прописной). Далее могут идти буквы латинского алфавита (строчные или прописные), цифры, _ (подчеркивание) и - (дефис). Имя должно быть уникальным и не превышать 8 символов.
level	уровень привилегий, диапазон значений 0 – 15. Значение по умолчанию – 1.
pwd	пароль пользователя. Допускаются латинские буквы, цифры и спецсимволы. Нельзя использовать пробелы и нелатинские символы.
0	при этом значении пароль вводится в открытом виде и зашифровывается внутри
5	при этом значении пароль вводится и считается, что он является результатом функции хэширования, и сохраняется без изменения.

### Значение по умолчанию

Значение по умолчанию отсутствует.

### Режимы команды

Global configuration

### Рекомендации по использованию

#### Добавление пользователя, изменение его параметров

Ограничения на имя пользователя являются более строгими, чем в Cisco IOS. Это связано с особенностями используемых операционных систем.



**Note**

В ОС Linux пользователь создается с `home` в директории `/var/cspvpn/users/<name>` (`<name>` – имя пользователя). Директория создается с атрибутами `750 (drwxr-x---)`.

В качестве `shell` у пользователя выставляется `/opt/VPNagent/bin/cs_console`.

Команда создания пользователя завершается с ошибкой, если пользователь с указанным в команде именем уже присутствует на машине, но не представлен в Cisco-like конфигурации.

Команда создания пользователя воспринимается как команда редактирования (например, сменить пароль, `privilege` и т.п.), если пользователь уже присутствует в конфигурации и на машине. При добавлении нового пользователя или изменении пароля существующего, добавляются или изменяются данные пользователей операционной системы.

При значении {0} пароль вводится в открытом виде, а затем вычисляется и хранится функция хэширования пароля. Если посмотреть конфигурацию командой `show running-config`, то команда

```
username {name} [privilege level] secret 0 {pwd}
```

будет представлена в виде

```
username {name} [privilege level] secret 5 {pwd_encrypted}.
```

При значении {5} считается, что введенный пароль является результатом функции хэширования пароля и в конфигурации сохраняется без изменения в том виде, в каком и был введен в команде:

```
username {name} [privilege level] secret 5 {pwd_encrypted}
```

Пользователю может быть назначен уровень привилегий из диапазона 0 – 15. Этот диапазон разделен на два класса: в первом – пятнадцатый уровень, а во втором – с 0 по 14 уровни. Пользователи с уровнем привилегий от 0 до 14 имеют одинаковые права.

Пользователь с пятнадцатым уровнем привилегий сразу получает доступ к привилегированному режиму специализированной консоли. Пользователей с пятнадцатым уровнем может быть несколько.

Пользователь с уровнем привилегий от 0 по 14 имеет право доступа к пользовательскому режиму специализированной консоли. А если этот пользователь знает пароль доступа к привилегированному режиму, то он может настраивать CSP VPN Gate. Но пользователь с таким уровнем привилегий не имеет право доступа к графическому интерфейсу.

Если не указан в команде параметр `[privilege level]`, то будет создан пользователь с 1 (первым) уровнем привилегий.

### Удаление пользователя

Удаление пользователя с именем `name` производится командой

```
no username {name}
```

Если имеется только один пользователь с уровнем привилегий 15, то удалить такого пользователя не рекомендуется.

В ОС Linux – удалить пользователя, из-под которого запущена `cs_console`, технически возможно, но данное действие категорически не рекомендуется.

Если удаляется пользователь из системы, из-под которого не запущена `cs_console`:

- если пользователь успешно удален из системы: команда завершается успешно и пользователь удаляется из Cisco-like конфигурации.
- если пользователя в системе не существует: команда также завершается успешно и пользователь удаляется из Cisco-like конфигурации.
- если удаление пользователя не прошло (пользователь в системе остался): то команда завершается с ошибкой, пользователь не удаляется из Cisco-like конфигурации.

В `cs_console` команды `username password` и `username secret` являются взаимозаменяемыми – ввод любой из этих команд для существующего пользователя обозначает изменение пароля, независимо от того, как он был задан ранее.

### Выдаваемые сообщения

При попытке добавления нового пользователя могут возникать следующие ошибки:

Неправильный синтаксис имени пользователя (использование недопустимых символов):  
% User "<username>" was not created. Username is invalid.

Длина имени пользователя превышает 8 символов: % User "<username>" was not created. Username is too long (8-chars limit exceeded).

Пользователь с таким именем уже существует в системе: % User addition failed. User "<username>" already exists in the system.

Произошла системная ошибка (возможно нарушена системная политика в отношении имени пользователя или пароля; например слишком короткий пароль): % User addition failed: System error. Possibly the password or the user name violates some system policy (e.g. the password is too short).

При попытке смены пароля пользователя может возникать ошибка: % User password change failed. Possibly the password violates some system policy (e.g. it's too short).

При удалении пользователя, в ошибочных случаях выдается сообщение: % User account cannot be removed

#### **Отличие данной команды от подобной команды Cisco IOS:**

- не поддерживаются иные всевозможные варианты задания команды username, не указанные здесь
- имеется ограничение на длину имени пользователя.
- в cs\_console команды username password и username secret являются взаимозаменяемыми – ввод любой из этих команд для существующего пользователя обозначает изменение пароля, независимо от того, как он был задан ранее. В Cisco: если пароль для пользователя задан командой username password (пароль хранится в открытом виде), то пароль нельзя потом изменить, используя команду username secret (пароль хранится в зашифрованном виде), и наоборот – если пароль для пользователя задан командой username secret, то потом изменить его командой username password нельзя. В обоих случаях выдается сообщение об ошибке.
- невозможно изменить уровень привилегий пользователя без указания его пароля.

#### **Пример**

Ниже приведен пример создания пользователя с именем "admin" и паролем "security", который будет зашифрован, и уровнем привилегий 15:

```
Router#configure terminal
Enter configuration commands, one per line.
Router(config)#username admin privilege 15 secret 0 security
Router(config)# exit
```

# Команды настройки протоколирования событий

## logging

Команда `logging` используется для задания IP-адреса хоста, на который будут посылаться сообщения о протоколируемых событиях. Сообщения можно посылать только на один адрес. No-форма команды восстанавливает значение по умолчанию.

### Синтаксис

```
logging {ip-address}
```

```
no logging {ip-address}
```

альтернативный вариант команды:

```
logging host {ip-address}
```

ip-address

IP-адрес хоста, на который будет направлен лог.

### Значение по умолчанию

`logging 127.0.0.1`

### Режимы команды

Global configuration.

### Рекомендации по использованию

Команда `logging` задает адрес хоста, на который будут направляться сообщения о происходящих событиях на шлюзе. Для отсылки сообщений используется только протокол Syslog и получатель сообщений может быть только один. При вводе команды `logging`, изменения в настройках протокола событий консоли вступают в силу немедленно.

При старте консоли получатель протокола сообщений записан в файл `syslog.ini`. После зачитывания начальной конфигурации выставляется получатель протокола сообщений, описанный в `cisco-like` конфигурации. Если в `cisco-like` конфигурации команды протоколирования отсутствуют, то выставляются значения по умолчанию.

Также значение по умолчанию выставляется и при задании одной из команд:

```
no logging {ip-address}
```

```
logging 127.0.0.1
```

Заданная команда `no logging {ip-address}` аналогична команде `logging 127.0.0.1`. Если задана команда `logging 127.0.0.1`, то она не показывается по команде `show running-config`.

Команда `no logging` не поддерживается.

В следующих случаях могут возникать побочные эффекты сохранения получателя протокола сообщений в файл `syslog.ini`:

при старте консоли, даже если не была введена ни одна команда, файл `syslog.ini` может поменяться, если перед стартом консоли файл менялся "вручную". В этом случае его содержимое будет заменено на то, что прописано в `cisco-like` конфигурации

настройка в `cs_console` может повлиять на получателя протокола сообщений в том случае, если после этого будет загружена LSP, в которой не указана структура `SyslogSettings` (это означает, что протокол сообщений будет направлен получателю, указанному в файле `syslog.ini`). Примечание: такая LSP может быть написана только вручную и не может быть получена при конвертировании `cisco-like` конфигурации.

настройка в `cs_console` может повлиять на получателя протокола сообщений в случаях, когда не загружена LSP (при старте сервиса или при отгрузке LSP).

**Отличие данной команды от подобной команды Cisco IOS:**

- не допускается использование `hostname` в качестве аргумента
- не допускается задание списка SYSLOG-серверов, разрешен только один адрес. Повторно заданная команда `logging` заменяет предыдущий адрес. Заданный адрес сохраняется в файле `syslog.ini`.

**Пример**

Ниже приведен пример, в котором сообщения о протоколируемых событиях отправляются на адрес 10.10.1.101:

```
Router(config)#logging 10.10.1.101
```



## logging facility

Для задания канала протоколирования событий используйте команду `logging facility`. Данная команда позволяет выбрать необходимый источник сообщений, который будет создавать сообщения об ошибках. No-форма команды восстанавливает значение по умолчанию.

### Синтаксис

`logging facility {name}`

`no logging facility`

name

имя канала протоколирования событий, возможные варианты:

auth, cron, daemon, kern, local0, local1, local2,  
local3, local4, local5, local6, local7, lpr, mail,  
news, sys10, sys11, sys12, sys13, sys14, sys9,  
syslog, user, uucp

### Значение по умолчанию

`logging facility local7`

### Режимы команды

Global configuration.

### Рекомендации по использованию

Команда `logging facility` задает процесс, который будет выдавать сообщения об ошибках. Заданное значение `logging facility` сохраняется в файле `syslog.ini`.

При старте консоли источник сообщений записан в файл `syslog.ini`. После считывания начальной конфигурации выставляется источник сообщений, описанный в cisco-like конфигурации. Если в cisco-like конфигурации такое описание отсутствует, то выставляется значение по умолчанию.

Также значение по умолчанию выставляется и при задании одной из команд:

```
no logging facility
```

```
logging facility local7
```

Команда `no logging facility` аналогична команде `logging facility local7`.

Если задана команда `logging facility local7`, то она не показывается по команде `show running-config`.

### Пример

Ниже приведен пример задания канала лога local1:

```
Router(config)#logging facility local1
```

## logging trap

Для задания уровня детализации протоколирования событий используйте команду `logging trap`. Данная команда позволяет выбрать необходимый уровень важности протоколируемых событий. No-форма команды восстанавливает значение по умолчанию.

### Синтаксис

`logging trap {severity}`

`no logging trap`

severity

уровень важности событий, возможные варианты:

alerts, critical, debugging, emergencies, errors,  
informational, notifications, warnings

### Значение по умолчанию

`logging trap informational`

### Режимы команды

Global configuration.

### Рекомендации по использованию

Команда `logging trap {severity}` задает необходимый уровень важности протоколируемых событий. Если данная команда в конфигурации отсутствует, то выставляется значение по умолчанию.

Также значение по умолчанию выставляется и при задании одной из команд:

`no logging trap`

`logging trap informational`

Команда `no logging trap` аналогична команде `logging trap informational`.

Команда `logging trap` – не поддерживается !!!

Если задана команда `logging trap informational`, то она не показывается по команде `show running-config`.

### Отличие данной команды от подобной команды Cisco IOS:

- не допускается задавать уровень в виде числа, например:  
`logging trap 5` !!! не поддерживается!!!
- не поддерживается сокращенный вариант выставления уровня протоколирования `informational` (по умолчанию):  
`logging trap` !!! не поддерживается!!!
- в Cisco IOS команда `no logging trap` отключает протоколирование событий по протоколу syslog

### Пример

Ниже приведен пример задания уровня лога `critical`:

`Router(config)#logging trap critical`

## logging on

Команда `logging on` используется для включения протоколирования событий. `no`-форма команды отключает протоколирование.

### Синтаксис

```
logging on
no logging on
```

### Значение по умолчанию

`logging on`

### Режимы команды

Global configuration.

### Рекомендации по использованию

Команда `logging on` включает передачу сообщений о событиях в файл протокола.

Если отключить настройки протоколирования командой `no logging on`, то:

- в файл `syslog.ini` прописывается настройка `Enable=0` – протоколирование отключено
- в сконвертированной LSP не будет никаких настроек протоколирования – уровней протоколирования (атрибуты `...LogMessageLevel` в структуре `GlobalParameters`) и получателя протокола (структура `SyslogSettings`)
- команды настройки протоколирования (`logging trap`, `logging facility` и `logging host`) выполняться не будут, но сохраняются в `cisco-like` конфигурации и вступят в действие по команде `logging on`.

Все команды настройки протоколирования событий (`logging trap`, `logging facility` и `logging host`), введенные после команды `no logging on`, вступят в действие только после команды `logging on`.

Команда `logging on` не показывается по команде `show running-config`.

Команда `no logging on` показывается по команде `show running-config`.

# Команды настройки SNMP-сервера

## snmp-server community

Для настройки SNMP-сервера, который поддерживает базу данных MIB и выдает статистику по запросу SNMP-менеджера, используйте команды `snmp-server`. В команде `snmp-server community` задается идентификатор (пароль), который используется для аутентификации запросов от SNMP-менеджера и разрешает ему чтение статистики из базы управления SNMP-сервера.

`No` – форма команды отключает ранее введенное значение идентификатора и отключает получение статистики по SNMP.

### Синтаксис

`snmp-server community {string} [ro]`

`no snmp-server community [string]`

`string`

строка, играющая роль идентификатора сообщений для SNMP сервера. Допускаются латинские буквы, цифры, знаки !"#\$%&'()\*+,-./:;>=<@[ ]^\_`{|}~. Пробелы не допускаются.

`ro`

спецификатор, указывающий на то, что SNMP-сервер разрешает только чтение статистики. Необязательный параметр, по умолчанию разрешается только чтение статистики.

### Значение по умолчанию

отсутствует

### Режимы команды

Global configuration.

### Рекомендации по использованию

Команда `snmp-server community` задает значение `community string`, выполняющее роль идентификатора отправителя, в настройках SNMP сервера.

Допускается только одна такая команда, так как можно задать только одно значение `community`. Повторный запуск этой команды меняет значение строки `community`.

Если в запросе от SNMP-менеджера строка `community` отличается от `community`, прописанной на шлюзе командой `snmp-server community`, то статистика не отсылается.

`No`-форма этой команды отключает получение статистики по SNMP.

Отключить получение статистики по SNMP можно и командой `no snmp-server`.

### Отличие данной команды от подобной команды Cisco IOS:

- в `cs_console` разрешается задавать только одно значение `community`
- не допускается спецификатор `RW`, который поддерживает возможности чтения и записи статистики
- не поддерживаются `views` (фильтрация по отдельным веткам MIB) и `ACLs` (фильтрация по адресам SNMP managers)
- не существует никаких взаимосвязей между командой `snmp-server community` и `snmp-server host` (в Cisco существует неявное прописывание `SNMP-polling community` при вводе команды `snmp-server host`)

**Пример**

Ниже приведен пример задания community string:

```
Router(config)#snmp-server community public
```

## snmp-server location

Для задания информации о размещении SNMP-сервера используйте команду `snmp-server location`. `No` – форма команды отключает ранее введенное значение.

### Синтаксис

`snmp-server location {string}`

`no snmp-server location {string}`

string

строка, в которой допускаются латинские буквы, цифры, знаки `!"#$%&'()*+,-./:;>=<@[\]^_`{|}~` и пробелы.

### Значение по умолчанию

отсутствует

### Режимы команды

Global configuration.

### Рекомендации по использованию

Команда `snmp-server location` задает значение `system location` в настройках SNMP сервера.

### Пример

Ниже приведен пример задания `system location string`:

```
Router(config)#snmp-server location Building 1, room 3
```

## snmp-server contact

Для задания информации о контактном лице, ответственном за работу устройства, используйте команду `snmp-server contact`. `No` – форма команды отключает ранее введенное значение.

### Синтаксис

`snmp-server contact {text}`

`no snmp-server contact {text}`

text

строка с контактной информацией, в которой допускаются латинские буквы, цифры, знаки `!"#$%&'()*+,-./:;>=<@[\]^_`{|}~` и пробелы.

### Значение по умолчанию

отсутствует

### Режимы команды

Global configuration.

### Рекомендации по использованию

Команда `snmp-server contact` задает значение `system contact` в настройках SNMP сервера.

### Пример

Ниже приведен пример задания `contact string`:

```
Router(config)#snmp-server contact Dial system operator
```

## snmp-server host

Для задания параметров получателя SNMP-трапов используйте команду `snmp-server host`.  
**No** – форма команды устраняет из конфигурации получателя SNMP-трапов.

### Синтаксис

```
snmp-server host {host-addr} [traps] [version {1|2c}]
{community-string} [udp-port {port}]

no snmp-server host {host-addr} [traps] [version {1|2c}]
{community-string} [udp-port {port}]
```

host-addr	IP-адрес получателя трапов
1 2c	версия SNMP, в которой формируются трапы (по умолчанию – 1)
community-string	строка, играющая роль идентификатора отправителя, прописываемая в трапе, обязательный параметр. Не имеет никакой связи с <code>snmp-server community</code> , может совпадать или отличаться.
port	UDP-порт получателя, на который отправляются SNMP-трапы (по умолчанию – 162)

### Значение по умолчанию

по умолчанию трапы не отсылаются

### Режимы команды

Global configuration

### Рекомендации по использованию

Таких команд может быть несколько, задающих список получателей трапов.

Для отсылки трапов должна быть указана хотя бы одна команда `snmp-server host` и команда `snmp-server enable traps`.

Выбирать отдельные трапы в текущей версии Продукта нельзя.

В команде `no snmp-server host` обязательно должны присутствовать {host-addr} и {community-string}. Остальные параметры можно не указывать.

Если в команде встречается пара {host-addr} и {community-string}, которые были введены ранее, то эта команда заменяется на новую введенную команду (в ней могут поменяться версия и порт). Такое поведение аналогично Cisco IOS 12.2 (устаревший), но отличается от логики Cisco IOS 12.4,- там еще учитывается и порт.

При заданной команде `snmp-server enable traps` команда `snmp-server host` может порождать инкрементальную политику.

### Пример

Ниже приведен пример задания получателя SNMP-трапов:

```
Router(config)#snmp-server host 10.10.1.101 version 2c netsecur udp-
port 162
```



## snmp-server enable traps

Эта команда используется для включения отсылки SNMP-трапов. `no` –форма этой команды используется для отключения отсылки трапов.

### Синтаксис

```
snmp-server enable traps
no snmp-server enable traps
```

### Значение по умолчанию

по умолчанию трапы не отсылаются

### Режимы команды

Global configuration.

### Рекомендации по использованию

Без указания команды `snmp-server enable traps` трапы отсылаться не будут. Для отсылки трапа требуется команда `snmp-server enable traps` и хотя бы одна команда `snmp-server host`.



Note

При задании этих двух команд сразу же формируется и загружается **инкрементальная конфигурация**, если режим инкрементального настраивания конфигурации включен. Включение осуществляется в настройках конвертора – в файле `cs_conv.ini`. Параметру включения синхронизации политик `policy_sync` присваивается значение `on`. По умолчанию это значение и установлено. Подробнее см. описание “Конвертор VPN политики” в документе [«Приложение»](#).

### Пример

Ниже приведен пример включения отсылки SNMP-трапов:

```
Router(config)#snmp-server enable traps
```

## snmp-server trap-source

Эта команда используется для указания интерфейса, с которого посылаются SNMP-трапы. Для устранения источника трапа используется `no` –форма этой команды.

### Синтаксис

```
snmp-server trap-source {interface}
no snmp-server trap-source

interface          имя интерфейса – fastethernet
```

### Значение по умолчанию

по умолчанию в поле Agent Address трапа прописывается значение 0.0.0.0.

### Режимы команды

Global configuration.

### Рекомендации по использованию

В конфигурации используется только одна команда `snmp-server trap-source`.

Если указана данная команда, то при формировании трапа в SNMP версии 1 в поле Agent Address прописывается первый адрес указанного интерфейса (primary-адрес).

Если команда `snmp-server trap-source` не задана или задана ее `no`-форма, то в трапе в поле Agent Address прописывается значение 0.0.0.0.

При заданной команде `snmp-server enable traps` команда `snmp-server trap-source` может породить инкрементальную политику.

Заметим, что изменения вступят в действие не сразу после ввода команды `ip-address (interface)` назначения IP-адреса интерфейсу, а только после выхода из конфигурационного режима.

### Пример

Ниже приведен пример указания имени интерфейса, с которого отсылаются SNMP-трапы:

```
Router(config)#snmp-server trap-source fastethernet 0/1
```

# Команды для назначения имени хоста и имени домена

## hostname

Команда `hostname` применяется для назначения или изменения имени хоста.

### Синтаксис

**hostname** name

name

новое имя хоста.

### Значение по умолчанию

По умолчанию установлено имя `cspgate`

### Режимы команды

Global configuration

### Рекомендации по использованию

Данная команда прописывает имя хоста как в `cisco-like` конфигурации, так и в системе. Имя хоста изменится немедленно.

При назначении или изменении имени хоста следует придерживаться следующих правил:

- имя хоста – полное доменное имя, включая домен первого уровня
- имя хоста состоит из одного или нескольких слов, разделенных точкой
- каждое слово обязательно должно начинаться с буквы латинского алфавита и может состоять из букв латинского алфавита (как строчных, так и прописных), цифр и знака " – " (дефис).

В ОС Linux при выполнении этой команды в файле `/etc/sysconfig/network` параметру `HOSTNAME` будет присвоено новое имя хоста. При следующем рестарте системы это имя будет использовано как системное имя хоста.

### Пример

Ниже приведен пример изменения имени хоста на "juke-box":

```
Router(config)# hostname juke-box
```

## ip domain name

Команда `ip domain name` используется для определения имени домена, которое будет использоваться для дополнения неполных имен хостов (имен, состоящих только из имени хоста). Для блокирования этой функциональности используйте ту же команду с префиксом `no`.

### Синтаксис

`ip domain name name`

`no ip domain name name`

name

имя домена, которое используется по умолчанию для автоматического завершения неполного имени хоста. Полное имя формируется посредством добавления доменного имени через точку в конец неполного имени хоста..

### Значение по умолчанию

Enabled

### Режимы команды

Global configuration.

### Рекомендации по использованию

Используйте эту команду для назначения доменного имени по умолчанию. В этом случае все имена хостов, которые не содержат отделенного точкой доменного имени, будут дополнены доменным именем по умолчанию.

### Пример

Ниже приведен пример назначения доменного имени по умолчанию `example.com`:

```
Router(config)#ip domain name example.com
```

# Команды для работы с таблицей маршрутизации

## ip route

Для добавления записи в таблицу маршрутизации используйте команду `ip route`. Для удаления маршрута используется `no`-форма команды.

### Синтаксис

```
ip route prefix mask {ip-address |
fastethernet0/interface-number} [distance]
```

```
no ip route prefix mask
```

prefix	старшая общая часть IP-адресов, до которой прописывается маршрут. Для задания маршрута, который будет использоваться по умолчанию, IP-адрес должен быть равен 0.0.0.0
mask	маска хоста или подсети, до которой прописывается маршрут. Для задания маршрута, который будет использоваться по умолчанию, маска подсети должна быть равна 0.0.0.0
ip-address	IP-адрес шлюза, через который прописывается маршрут
fastethernet0	сетевой интерфейс. В данной версии Продукта любой интерфейс, например, PPP или GigabitEthernet, представлен как fastethernet
interface-number	порядковый номер интерфейса
distance	административная дистанция (метрика) имеет разный смысл в разных ОС и в данной команде будет проигнорирована. Поэтому, использовать ее не рекомендуется.

**Недопустимо указывать одновременно параметры интерфейса и IP-адрес шлюза, через который прописывается маршрут.**

Маршрут по умолчанию – маршрут, по которому будет отправлен пакет, если IP-адрес назначения, указанный в заголовке пакета, не совпадает ни с одним адресом назначения в таблице маршрутизации.

### Значение по умолчанию

отсутствует

### Режимы команды

Global configuration.

### Рекомендации по использованию

Используйте эту команду для добавления записи в таблицу маршрутизации.

Используемые ОС налагают требование, чтобы шлюз, через который прописывается маршрут, был доступен с сетевого интерфейса устройства.

Параметр `distance` игнорируется. При добавлении маршрута выставляется системная метрика, аналогичная той, которая выставляется по умолчанию при добавлении маршрута с помощью команды `OS route add`. Но по команде `show ip route` для данного маршрута будет показано значение `distance`, равное 1.

В LSP параметр `distance` будет записан как `metric`, но реально будет проигнорирован.

Эта команда порождает загрузку инкрементальной политики. (если это допустимо в данный момент).

Удаление маршрута производится командой `no ip route prefix mask`. Можно указывать и другие параметры в команде, но они будут проигнорированы. Разрешается удалять только маршрут, заданный командой `ip route` в консоли.

### **Отличие данной команды от подобной команды Cisco IOS:**

- в команде необходимо прописывать маршрут через шлюз, который является доступным с сетевого интерфейса
- в консоли параметром, связанным с метрикой является `distance`, а в Cisco IOS – параметр `administrative distance`
- параметр `distance` игнорируется
- отсутствует команда `clear ip route` для удаления маршрута из системной таблицы маршрутизации.

### **Пример**

```
Router(config)#ip route 10.10.10.1 255.255.255.255 10.2.2.1
```

# Команды для работы с сертификатами

## crypto pki trustpoint

Команда `crypto pki trustpoint` используется для объявления имени CA (Certificate Authority – Сертификационный Центр), а также для входа в режим `ca trustpoint configuration` для настройки параметров получения списка отозванных сертификатов (CRL). Для удаления всех идентификаторов и сертификатов, связанных с CA, используйте ту же команду с префиксом `no`.

Для регистрации CA и локального сертификата в базе продукта, а также списка отозванных сертификатов используется утилита `cert_mgr import`.

### Синтаксис

`crypto pki trustpoint name`

`no crypto pki trustpoint name`

name

имя CA. Если нужно изменить параметры уже объявленного CA введите имя, которое этому CA было назначено ранее.

### Значение по умолчанию

Значение по умолчанию отсутствует.

### Режимы команды

Global configuration. Выполнение этой команды осуществляет вход в режим `ca trustpoint configuration`.

### Рекомендации по использованию

Команда `crypto pki trustpoint` замещает команду в старом формате `crypto ca trustpoint`, которая использовалась в Cisco IOS версии 12.2 и CSP VPN Gate версии 2.x. Можно использовать и старый формат команды, но по команде `show running-config` будет показана команда в новом формате.

Используйте эту команду для объявления имени корневого CA, который имеет самоподписанный сертификат. Выполнение этой команды также осуществляет вход в режим `ca trustpoint configuration`, в котором могут выполняться следующие команды:

`curl query` – служит для настройки параметров получения CRL

`revocation-check` – указывает режим использования CRL

`exit` – осуществляет выход из режима `ca trustpoint configuration`.

Настройки получения и использования CRL берутся из первого по счету `trustpoint`. Из остальных `trustpoint` настройки игнорируются.

### Удаление

Удаление CA `trustpoint` осуществляется командой `no crypto pki trustpoint name`. После этого выдается сообщение:

% Removing an enrolled trustpoint will destroy all certificates

received from the related Certificate Authority.

Are you sure you want to do this? [yes/no]:

Если ввести “yes” (можно сократить до одной буквы “y”), то `trustpoint` удалится из конфигурации. Если при этом существуют CA-сертификаты, которые привязаны к данному

trustpoint, они удаляются как из Cisco-like конфигурации, так и из базы локальных настроек продукта.

Если ввести “no” (можно сократить до одной буквы “n”), то действие команды отменяется.

**Отличие данной команды от подобной команды Cisco IOS:**

- подкоманда enrollment игнорируется, производится только задание сертификатов с помощью cert\_mgr import
- читаются только CA-сертификаты, локальные сертификаты (сертификаты устройств) игнорируются. Локальные сертификаты могут быть зарегистрированы в Продукте только утилитой cert\_mgr import.
- добавление одного trustpoint и перечисление нескольких trustpoints фактически не отличается друг от друга и всегда приводит к перечислению CA-сертификатов:
  - единственное отличие – адрес LDAP-сервера и настройки режима получения CRL всегда берутся из первого по счету trustpoint в конфигурации, остальные – игнорируются.

**Пример**

Ниже приведен пример использования команды `crypto pki trustpoint`. Объявляется СА с именем "ka" и указывается, что при проверке сертификата действующий CRL используется, если он предустановлен в базе продукта или получен в процессе IKE обмена. Если это не так, то попытка получить CRL по протоколу LDAP не предпринимается и сертификат принимается:

```
Router(config)#crypto pki trustpoint ka
Router(ca-trustpoint)#revocation-check none
```



## crl query

Команда `crl query` используется для явного указания адреса LDAP-сервера, с которого можно запросить CRL (Certificate Revocation List), промежуточные CA сертификаты, сертификат партнера. CRL содержит список отозванных сертификатов (действие которых прекращено по той или иной причине). Использование CRL защищает от принятия от партнеров отозванных сертификатов.

Перед обращением к LDAP-серверу шлюз сначала смотрит поле CDP сертификата, если в этом поле прописанный путь к LDAP-серверу является неполным, то добавляются данные (IP-адрес и порт) из команды `crl query`. Если CDP содержит полный путь, `crl query` не используется. Если в сертификате нет поля CDP, то используется эта команда.

Для возврата в режим по умолчанию (когда запрос CRL осуществляется по адресу, указанному в поле сертификата CDP (CRL Distribution Point)) используйте команду `crl query` с префиксом `no`.

### Синтаксис

`crl query ldap://ip-addr[:port]`

`no crl query ldap://ip-addr[:port]`

ip-addr

IP-адрес LDAP-сервера, на котором CA публикует CRLs и куда следует отправлять запросы на CRL.

port

порт, необязательный параметр, по умолчанию 389.

### Значение по умолчанию

Если адрес LDAP сервера явно не задан, то запросы на CRL будут отправляться на адрес, указанный в поле CDP сертификата. Если порт не задан, то подразумевается 389.

### Режимы команды

ca trustpoint configuration.

### Рекомендации по использованию

Используйте команду `crl query`, если сертификаты не содержат точного указания места, откуда может быть получен CRL. При задании LDAP сервера используйте только IP-адрес и возможно порт.

Сначала делается попытка установить соединение по LDAP версии 2. Если эта попытка завершается с ошибкой LDAP\_PROTOCOL\_ERROR (наиболее вероятная причина – не поддерживается версия 2), то повторяется попытка установить соединение по LDAP версии 3.

### Отличие данной команды от подобной команды Cisco IOS:

- на url для LDAP сервера наложено ограничение – допускается задание только IP-адреса и, возможно, порта. Если задано DNS-name, то данный url игнорируется.
- добавление одного trustpoint и перечисление нескольких trustpoints фактически не отличается друг от друга и всегда приводит к перечислению CA-сертификатов:
  - единственное отличие – адрес LDAP-сервера и настройки режима получения CRL всегда берутся из первого по счету trustpoint в конфигурации, остальные – игнорируются.

### Пример

Ниже приведен пример использования команды `crl query`. Объявляется CA с именем "bar" и указывается адрес, по которому следует искать CRL:

```
Router(config)#crypto pki trustpoint bar
```

```
Router(ca-trustpoint)#crl query ldap://10.10.10.10
```

## revocation-check

Команда `revocation-check` задает последовательность допустимых вариантов проверки сертификата партнера. В команде указываются разные режимы использования CRL.

Для возврата в режим по умолчанию используйте ту же команду с префиксом `no`.

### Синтаксис

**`revocation-check method1 [method2]`**

**`no revocation-check`**

`method1`

параметр, принимающий одно из двух значений:

`crl` при проверке сертификата обязателен действующий CRL. Если действующий CRL не найден в базе продукта и его не удалось получить по протоколу LDAP, то сертификат не принимается

`none` при проверке сертификата действующий CRL используется, если он предустановлен в базе продукта или получен в процессе IKE обмена. Если это не так, то попытка получить CRL по протоколу LDAP не предпринимается и сертификат принимается.

`method2`

параметр необязательный, имеет одно значение:

`none` если действующий CRL не найден в базе продукта и его не удалось получить по протоколу LDAP, то сертификат принимается. Используется только тогда, когда `method1=crl`.

Последовательность допустимых вариантов проверки сертификата описана в Рекомендациях по использованию.

### Значение по умолчанию

По умолчанию используется `revocation-check crl`. По команде `show running-config` будет показана данная команда, даже если она не вводилась в явном виде.

### Режимы команды

ca trustpoint configuration.

### Рекомендации по использованию

Для команды `revocation-check crl` обязателен действующий CRL в базе продукта, но если это не так, то CRL может быть получен по протоколу LDAP. Если CRL получить по LDAP не удалось, то сертификат партнера не принимается. Этот режим используется по умолчанию.

По команде `revocation-check none` при проверке сертификата партнера будет производиться попытка воспользоваться CRL из базы продукта или CRL, полученным в процессе IKE обмена, но не будет производиться попытка получить его по LDAP. Если действующий CRL не найден, то сертификат партнера принимается.

Команда `revocation-check none` замещает в старом формате команду `crl optional`, которая использовалась в Cisco IOS версии 12.2 и CSP VPN Gate версии 2.x. Можно использовать и старый формат команды, но по команде `show running-config` будет показана команда в новом формате.

При проверке сертификата по команде `revocation-check crl none` используется действующий CRL из базы продукта, но если это не так, то CRL может быть получен по протоколу LDAP. Если CRL получить по LDAP не удалось, то сертификат партнера принимается.

Команда `revocation-check crl none` замещает в старом формате команду `crl best-effort`, которая использовалась в Cisco IOS версии 12.2 и CSP VPN Gate версии 2.x. Можно использовать и старый формат команды, но по команде `show running-config` будет показана команда в новом формате.

Для получения CRL по протоколу LDAP запросы отправляются на адрес LDAP сервера, указанный в команде `crl query`, в противном случае на адрес, указанный в поле сертификата CDP.

По командам `revocation-check none` и `revocation-check crl none` единственными условиями принятия сертификата партнера будут неистекший срок его действия и что его издал CA, который объявлен как `trusted CA`.

Если задано несколько `trustpoints`, в которых задана команда `revocation-check`, то используется только команда из первого по счету `trustpoint` в конфигурации. Остальные команды `revocation-check` игнорируются.

**Отличие данной команды от подобной команды Cisco IOS:**

не используется режим `ocsp`.

**Пример**

Ниже приведен пример использования команды. Объявляется CA с именем "bar" и указывается адрес LDAP сервера, по которому следует получить CRL для проверки сертификата партнера:

```
Router(config)#crypto pki trustpoint bar
Router(ca-trustpoint)#crl query ldap://10.10.10.10
Router(ca-trustpoint)#revocation-check crl none
Router(ca-trustpoint)#exit
```

## crypto pki certificate chain

Команда `crypto pki certificate chain` используется для входа в режим настройки цепочки сертификатов CA.

### Синтаксис

`crypto pki certificate chain name`

name

Имя CA. Используйте тоже имя, когда вы объявляете CA, используя команду `crypto pki trustpoint`.

### Значение по умолчанию

Значение по умолчанию отсутствует.

### Режимы команды

Global configuration

### Рекомендации по использованию

Команда `crypto pki certificate chain` замещает в старом формате команду `crypto ca certificate chain`, которая использовалась в Cisco IOS версии 12.2 и CSP VPN Gate версии 2.x. Можно использовать и старый формат команды, но по команде `show running-config` будет показана команда в новом формате.

На момент ввода команды `crypto pki certificate chain` имя CA должно быть уже объявлено командой `crypto pki trustpoint`. Если имя не задано, то выдается сообщение об ошибке: “% CA trustpoint for cert chain not known”.

Используйте эту команду для входа в режим настройки цепочки CA сертификатов с помощью команды `certificate`. В пределах одного trustpoint допускаются любые CA сертификаты, не только из одной цепочки. Находясь в этом режиме, можно удалять сертификаты.

### Удаление

Удаление цепочки сертификатов командами

`no crypto pki certificate chain name`

или

`no crypto ca certificate chain name`

не допускается, выдается сообщение об ошибке: % Remove the trustpoint to remove the cert chain.

Удаление CA сертификата из цепочки осуществляется командой `certificate`.

### Отличие данной команды от подобной команды Cisco IOS:

- в Cisco по `show run` в команде `crypto pki certificate chain` показываются CA сертификаты и локальные сертификаты. В Cisco через эту команду можно посмотреть и удалить CA и локальные сертификаты, а ввести можно только CA сертификаты, локальные сертификаты таким образом ввести нельзя (они будут неработоспособны без секретного ключа). В Продукте в `cs_console` данная команда используется только для работы с CA сертификатами.
- в Cisco используются только RSA-сертификаты. В Продукте под обозначением RSA могут использоваться RSA, ГОСТ и DSA-сертификаты. Но должно соблюдаться строгое соответствие: RSA CA сертификат подписывает только RSA-сертификаты, ГОСТ CA сертификат подписывает только ГОСТ сертификаты, DSA CA сертификат подписывает только DSA-сертификаты.

- следует учитывать, что в конфигурации не задается точных критериев выбора локального сертификата (в терминах Native LSP задается USER\_SPECIFIC\_DATA). В связи с этим возможны ситуации, при которых не установится соединение, если присутствуют больше одного локального сертификата, подписанного разными CA.
- пример подобной ситуации: у партнера не прописана посылка Certificate Request, и партнер ожидает от локального шлюза конкретный сертификат (который действительно присутствует), но шлюз по своим критериям выбирает другой сертификат, который не подходит партнеру.
- как правило, таких проблем не возникает, если соблюдаются следующие условия:
  - у обоих партнеров прописана отсылка Certificate Request. По умолчанию конвертер именно так и делает. Cisco в большинстве случаев поступает также.
  - не используется Aggressive Mode при работе с сертификатами (экзотический случай).
  - у партнера должны быть явно указаны CA-сертификаты, которыми может быть подписан локальный сертификат. В Native LSP – атрибут AcceptCredentialFrom (cs\_converter вписывает все CA-сертификаты, лежащие в базе). В Cisco – должен быть прописан подходящий trustpoint.

### **Пример**

Пример использования команды `crypto pki certificate chain` приведен к команде `certificate`.

## certificate

Команда `certificate` используется для регистрации CA сертификатов в базе продукта. Данная команда работает в режиме `certificate chain configuration`. Для удаления сертификатов используйте эту команду с префиксом `no`.

### Синтаксис

`certificate` `certificate-serial-number`

`no certificate` `certificate-serial-number`

`certificate-serial-number` порядковый номер CA сертификата в шестнадцатеричном представлении

### Значение по умолчанию

Значение по умолчанию отсутствует.

### Режимы команды

Certificate chain configuration

### Рекомендации по использованию

Указанный в команде порядковый номер CA сертификата в шестнадцатеричном представлении может быть любым, так как в данном релизе не используется.

Используйте эту команду для добавления CA сертификата в базу продукта или удаления CA сертификата.

Для добавления сертификата после ввода порядкового номера сертификата и нажатия Enter осуществляется переход в режим `config-pubkey`, в котором нужно ввести CA сертификат в виде последовательности шестнадцатеричных чисел. Для конвертирования файла с CA сертификатом из бинарного представления в шестнадцатеричное можно воспользоваться любыми свободно распространяемыми утилитами. Заметим, что длина строки с телом сертификата в шестнадцатеричном представлении должна удовлетворять условиям:

- максимальная длина вводимой строки - 512 символов. Допускается пары шестнадцатеричных чисел разбивать между собой пробелами и переводами строки
- количество символов в строке должно быть четным, чтобы не разбивать шестнадцатеричное число.

Прекращение ввода сертификата заканчивается командой `quit`.

Заметим, что в CSP VPN Gate версии 2.X допускалось введение сертификата в виде одной строки. В версии 3.11 это невозможно, так как появилось ограничение на длину строки ввода – 512 символов, реальные сертификаты в эту длину не помещаются.

### Замечание:

Пользоваться командой `certificate` для регистрации CA сертификата неудобно. Наиболее удобным способом регистрации CA сертификата в базе продукта является использование утилиты `cert_mgr import`. После регистрации при следующем старте `cs_console` CA сертификат будет добавлен в `cisco-like` конфигурацию (логика по автоматической синхронизации CA-сертификата в `cisco-like` конфигурации и базе локальных настроек описана в пункте ["Синхронизация"](#) в разделе "Запуск консоли").

### Пример

Ниже приведен пример добавления сертификата с порядковым номером 012:

```
Router# configure terminal
```

```
Router(config)# crypto pki certificate chain myca
```

```
Router(config-cert-chain)# certificate 012
Router(config-pubkey)# 30820337308202E4A0030201020210337F
AE6C6B85536F834A8D8E5358333F4F3090A06062A850302020405003038310B30279
060355040613025255310D300B060311400055040A130447494E53310B3009060355
3240B13025141310D300B060355040313F9
Router(config-pubkey)#quit
Router(config-cert-chain)# exit
Router(config)#
```

## crypto identity

Команда `crypto identity` используется для создания списка идентификаторов, которому должен удовлетворять сертификат партнера (партнеров). Список идентификаторов может состоять из идентификаторов типа `dn` и `fqdn` и привязываться к криптографической карте. Для удаления списка идентификаторов используется та же команда с префиксом `no`.

### Синтаксис

	<code>crypto identity name</code>
	<code>no crypto identity name</code>
name	имя списка идентификаторов

### Значение по умолчанию

значение по умолчанию не существует.

### Режимы команды

Global configuration.

### Рекомендации по использованию

После ввода команды `crypto identity name` введите идентификатор типа `dn` и `fqdn`. Идентификатор `dn` представляет собой законченное либо незаконченное значение поля Subject сертификата партнера. Идентификатор `fqdn` имеет формат доменного имени. Ниже дано описание команд `dn` и `fqdn`.

### Пример

```
Router(config)#crypto identity myident
Router(config-crypto-identity)#dn c=ru,o=s-terra
Router(config-crypto-identity)#fqdn s-terra.com
Router(config-crypto-identity)#exit
```

```
Router(config)#crypto map mymap 10 ipsec-isakmp
Router(config-crypto-map)# set identity myident
```



## dn

Команда `dn` используется для задания идентификатора типа `dn`, которому должен удовлетворять сертификат партнера. Для задания этого идентификатора используется поле `Subject` сертификата партнера. Для удаления данного идентификатора используется эта же команда с префиксом `no`.

### Синтаксис

	<code>dn name_attr1=string1[,name_attr2=string2]</code>
	<code>no dn name_attr1=string1[,name_attr2=string2]</code>
<code>name_attr1</code>	сокращенное наименование атрибутов поля <code>Subject</code>
<code>string1</code>	значение атрибутов из поля <code>Subject</code>

### Значение по умолчанию

значение по умолчанию не существует.

### Режимы команды

Crypto identity configuration.

### Рекомендации по использованию

При поиске и сравнении с сертификатом партнера поле `Subject` этого сертификата должно содержать указанное множество атрибутов и их значений в команде `dn`.

### Пример

```
Router(config)#crypto identity myident
Router(config-crypto-identity)#dn c=ru,o=s-terra,ou=test
Router(config-crypto-identity)#exit

Router(config)#crypto map mymap 10 ipsec-isakmp
Router(config-crypto-map)# set identity myident
```

## fqdn

Команда `fqdn` используется для задания идентификатора типа `fqdn`, являющийся именем хоста партнера. Для удаления данного идентификатора используется эта же команда с префиксом `no`.

### Синтаксис

**fqdn** name\_domain

**no fqdn** name\_domain

name\_domain

доменное имя хоста партнера, который удовлетворяет условиям:

состоит из одного или нескольких слов, разделенных точкой

каждое слово обязательно должно начинаться с буквы латинского алфавита

может состоять из букв латинского алфавита (как строчных, так и прописных), цифр и знака "-" (дефис).

### Значение по умолчанию

значение по умолчанию не существует.

### Режимы команды

Crypto identity configuration.

### Пример

```
Router(config)#crypto identity myident
Router(config-crypto-identity)#fqdn s-terra.com
Router(config-crypto-identity)#exit
Router(config)#crypto map mymap 10 ipsec-isakmp
Router(config-crypto-map)# set identity myident
```

# Команды для работы с предопределенным ключом

## crypto isakmp key

Команда `crypto isakmp key` применяется для создания предопределенного ключа для взаимодействия с определенным партнером. Удалить созданный ранее предопределенный ключ можно с помощью той же команды с префиксом `no`.

### Синтаксис

```
crypto isakmp key [0] keystring {address peer-address  
[mask] | hostname hostname} [no-xauth]
```

```
no crypto isakmp key keystring address peer-address
```

```
no crypto isakmp key keystring hostname hostname
```

<b>address</b>	используйте этот параметр, если в качестве идентификатора удаленного партнера используется его IP-адрес
<b>hostname</b>	используйте этот параметр, если в качестве идентификатора удаленного партнера используется имя его хоста
<b>0</b>	не шифровать предопределенный ключ. Необязательный параметр, потому что он игнорируется. Ключ всегда не шифруется. Введен для соответствия такой же команде в Cisco IOS.
<b>keystring</b>	предопределенный ключ, представляющий собой строку произвольной комбинации цифро-буквенных символов. Этот ключ должен быть идентичен у обоих партнеров по защищенному взаимодействию.
<b>peer-address</b>	IP-адрес удаленного партнера.
<b>mask</b>	маска подсети, которой принадлежит компьютер удаленного партнера. Используется только при установке параметра <b>address</b> . Необязательный параметр.
<b>hostname</b>	имя компьютера удаленного партнера. Имя должно быть задано в связке с именем домена, которому он принадлежит. Например <code>host.subnet.com</code> .
<b>no-xauth</b>	расширенная аутентификация в рамках протокола IKE не используется. Необязательный параметр, потому что расширенная аутентификация никогда не используется. Соответствует такому же параметру в Cisco IOS.

### Значение по умолчанию

Значение по умолчанию отсутствует.

### Режимы команды

Global configuration

### Рекомендации по использованию

Используйте эту команду для создания предопределенных ключей аутентификации. Эта процедура должна быть выполнена для обоих партнеров. При создании ключа он автоматически добавляется в базу шлюза.

При использовании параметра **address** можно использовать аргумент **mask**, описывающий подсеть, которой принадлежит компьютер партнера. Если используется аргумент **mask**, то предопределенные ключи перестают быть принадлежностью только описанных двух

партнеров. Если указывается аргумент `mask`, то в качестве IP адреса, должен быть указан адрес сети.

При использовании параметра `hostname` удаленный партнер будет иметь возможность устанавливать защищенное соединение с любого из сетевых интерфейсов своего компьютера.

Параметр `[0]` в команде всегда игнорируется. Предопределенный ключ никогда не шифруется. Параметр введен для совместимости с CSM. По `show running-config` выставленный параметр `[0]` в команде не показывается.

Наличие или отсутствие параметра `[no-xauth]` не оказывает влияния на конвертирование конфигурации. Этот параметр введен для соответствия такому же параметру в Cisco IOS. Если этот параметр указан в команде, то по команде `show running-config` он показывается.

**Отличие данной команды от подобной команды Cisco IOS:**

- не поддерживается шифрование ключа ("6")
- наличие или отсутствие параметра `[no-xauth]` не влияет на результат работы команды, в отличие от Cisco IOS – там результат зависит от этого параметра.

**Пример**

Ниже приведен пример создания предопределенного ключа аутентификации для партнера с адресом 192.168.1.22.

```
Router(config)#crypto isakmp identity address
Router(config)#crypto isakmp key sharedkeystring address 192.168.1.22
```

## ip host

Команда `ip host` связывает predetermined ключ, идентифицируемый по имени хоста партнера, с его IP-адресом (IP-адресами). Для удаления такой связи используется `no`-форма команды.

### Синтаксис

	<code>ip host hostname [additional] address</code>
	<code>no ip host hostname [additional] [address]</code>
hostname	имя хоста партнера. Синтаксис параметра соответствует правилам задания доменного имени (описано в команде <a href="#">hostname</a> )
additional	используйте этот параметр для задания дополнительных IP-адресов для уже существующего соответствия
address	IP-адрес, который соответствует имени хоста партнера.

### Значение по умолчанию

отсутствует

### Режимы команды

Global configuration.

### Рекомендации по использованию

Используйте эту команду только для задания соответствия между именем хоста партнера и его IP-адресом. Создание predetermined ключа и привязка его к имени хоста партнера или к его IP-адресу осуществляется командой `crypto isakmp key`.

Задание команды без модификатора `additional` приводит к удалению всех существующих соответствий для данного `hostname` (если они были) и заменяет их на новое.

Задание команды с модификатором `additional` приводит к добавлению нового адреса к списку адресов для данного `hostname`, но:

- если для данного `hostname` уже задано соответствие указанному адресу, то команда игнорируется
- если для данного `hostname` не заданы соответствия адресам, то наличие или отсутствие модификатора `additional` приводит к одному и тому же результату – добавлению адреса.

Рекомендуется задавать один IP-адрес партнера. При задании нескольких IP-адресов существуют особенности:

- в одной команде можно задавать только один IP-адрес
- при выводе по команде `show running-config` всегда выдается по одному IP-адресу на команду `ip host`. Для второго и последующего адресов в списке для данного `hostname` в команде `ip host` добавляется слово `additional`.

### Пример:

Задание нескольких команд с одним именем хоста:

```
ip host test-host1 192.168.1.1
```

```
ip host test-host1 additional 192.168.1.2
```

Вывод по команде `show running-config`:

```
ip host test-host1 192.168.1.1
ip host test-host1 additional 192.168.1.2
```

### **Удаление**

Удаление установленного соответствия между `hostname` и IP-адресом осуществляется командой:

```
no ip host hostname [additional] [address]
```

При указании параметра `address` удаляется соответствие между `hostname` и указанным адресом. Допустимо указывать только один адрес.

Без указания параметра `address` удаляются соответствия между `hostname` и всеми адресами.

При этом параметр `additional` можно не задавать – он игнорируется.

### **Отличие данной команды от подобной команды Cisco IOS:**

- задает только привязку предопределенного ключа, идентифицируемого по `hostname`, к IP-адресу партнера, а в Cisco IOS – привязка `hostname` к IP-адресам для всех сетевых сервисов
- если параметр `hostname` не соответствует правилам задания доменного имени, то выдается только одно сообщение об ошибке: `%IP: Bad hostname format`, а в Cisco IOS – несколько сообщений:

```
% Hostname must be 2-63 characters of length, alphanumeric only
%IP: Bad hostname format
```

- в одной команде как при установлении соответствия так и при удалении можно задавать только один IP-адрес, список адресов, как в Cisco IOS, задавать нельзя
- по команде `show running-config` в каждой команде `ip host` выдается только по одному IP-адресу, а в Cisco IOS – до 8 адресов
- при удалении соответствия допустимо указывать только один адрес, а в Cisco IOS – список адресов.

### **Пример**

Ниже приведен пример задания соответствия имени хоста `test` двум IP-адресам:

```
Router(config)#ip host test 10.10.10.1
Router(config)#ip host test additional 10.10.10.2
```

# Команды создания и редактирования списков доступа

## ip access-list

Команда `ip access-list` используется для создания именованных списков доступа. Списки доступа могут быть стандартными и расширенными.

Выполнение команды `ip access-list` осуществляет вход в режим настройки списка, в котором с помощью команд `deny` и `permit` следует определить условия доступа.

### Синтаксис

`ip access-list {standard|extended} name`

`no ip access-list {standard|extended} name`

**standard**

Указывает стандартный список доступа .

**extended**

Указывает расширенный список доступа .

**name**

Имя списка доступа. Возможные варианты имени списка:

число из диапазонов <1-99> и <1300-1999> для стандартных списков

число из диапазонов <100-199> и <2000-2699> для расширенных списков

слово, которое не должно начинаться с цифры, и не содержит пробелов и кавычек.

### Значение по умолчанию

Значение по умолчанию отсутствует.

### Режимы команды

Global configuration.

При использовании опции `standard` осуществляется вход в режим настройки стандартных списков доступа (`config-std-nacl`).

При использовании опции `extended` осуществляется вход в режим настройки расширенных списков доступа (`config-ext-nacl`).

### Рекомендации по использованию

Команда `ip access-list` с опцией `standard` используется для создания и редактирования стандартных списков доступа (`config-std-nacl`). Стандартные списки доступа используются для фильтрации пакетов только по IP-адресу отправителя (источника) пакетов.

Команда `ip access-list` с опцией `extended` используется для создания и редактирования расширенных списков доступа (`config-ext-nacl`). Расширенные списки доступа используются для более гибкой фильтрации пакетов – по IP-адресу отправителя пакета, IP-адресу получателя пакета, по типу протокола, порту отправителя пакета и порту получателя.

Если ввести команду `ip access-list extended` с именем, с которым уже существует `standard` список доступа, то выдается сообщение об ошибке (аналогично Cisco IOS):

Access-list type conflicts with prior definition

% A named standard IP access list with this name already exists

Если ввести команду `ip access-list standard` с именем, с которым уже существует extended список доступа, то выдается сообщение об ошибке (аналогично Cisco IOS):

Access-list type conflicts with prior definition

% A named extended IP access list with this name already exists

Редактирование записей списков доступа производится с помощью команд `permit` и `deny`. В зависимости от того в каком режиме производится редактирование, возможности команд `permit` и `deny` будут различаться.

Созданные списки доступа могут использоваться в следующих случаях:

- фильтрующие списки доступа привязываются к сетевому интерфейсу (команда `ip access-group` при настройке интерфейса). Привязывается только входящий трафик, но создадутся симметричные правила как для входящего так и исходящего трафиков.
- списки доступа привязываются к статической криптографической карте и динамической криптокарте для указания защищенного трафика (команда `match address` при настройке `crypto map`),

Удаление списка доступа целиком осуществляется командой

```
no ip access-list {standard|extended} name
```

### **Пример**

Ниже приведен пример создания списка доступа с именем E105:

```
Router(config)#ip access-list extended E105
Router(config-ext-nacl)#deny  udp  host  10.1.1.2  range  500  500  host
10.2.2.2 range 500 500
Router(config-ext-nacl)#deny  udp  host  10.1.1.2  range  500  500  host
10.3.3.2 range 500 500
Router(config-ext-nacl)#deny  udp  host  10.1.1.2  range  500  500  host
4.4.4.4 range 500 500
Router(config-ext-nacl)#permit  ip    10.11.11.0   0.0.0.255   10.4.4.0
0.0.0.255
```



## permit (standard)

Команда `permit` используется для редактирования списков доступа. Данная команда используется для разрешения трафика, приходящего от указанного источника (`source`). Для отмены разрешающей записи в стандартном списке доступа используется та же команда с префиксом `no`.

### Синтаксис

**permit** *source* [**source-wildcard**]

**no permit** *source* [**source-wildcard**]

*source*

Этот параметр описывает отправителя (источник) пакета. Возможны три варианта описания источника:

явное указание IP-адреса в формате четырех десятичных значений, разделенных точками

использование ключевого слова `any`, обозначающего пару значений 0.0.0.0 255.255.255.255 для параметров `source` и `source-wildcard`.

использование ключевого слова `host` перед значением `source`, что предполагает значение 0.0.0.0 для параметра `source-wildcard`.

**source-wildcard**

используется в списках доступа и правилах IPsec для того, чтобы определить соответствует ли пакет какой-либо записи списка доступа.

**source-wildcard**

это инвертированная маска подсети, которая указывает какая часть IP-адреса пакета должна совпадать с IP-адресом в записи списка доступа. **source-wildcard** содержит 32 бита, такое же количество битов и в IP-адресе. Если в **source-wildcard** какой-либо бит равен 0, то тот же самый бит в IP-адресе пакета должен точно совпадать по значению с соответствующим битом в IP-адресе записи списка доступа. Если в **source-wildcard** какой-либо бит равен 1, то соответствующий бит в IP-адресе пакета проверять не нужно, он может принимать значение либо 0 либо 1, т.е. он является несущественным битом. Например, если **source-wildcard** равна 0.0.0.0, то все значения битов в IP-адресе пакета должны точно совпадать с соответствующими битами в IP-адресе записи списка доступа. При **source-wildcard** равной 0.0.255.255 значения первых 16 битов в IP-адресе пакета должны точно совпадать со значениями этих же битов в IP-адресе записи списка доступа. Важно, чтобы в **source-wildcard** в двоичном представлении не чередовались 0 и 1. Например, можно использовать инвертированную маску 0.0.31.255, которую можно записать в двоичном представлении как 00000000.00000000.00011111.11111111 и нельзя 0.0.255.0 (00000000.00000000.11111111.00000000). Установка значения инвертированной маски 255.255.255.255 для любого IP-адреса будет интерпретироваться, как установка значения `source` равного `any` IP-адрес..

Поэтому, возможны три варианта описания **source-wildcard**:

явное указание инвертированной маски подсети в формате четырех десятичных значений, разделенных точками

255.255.255.255, что означает для `source` значение 0.0.0.0, т.е. источник имеет значение `any`. Никакие биты в IP-адресе пакета сравнивать с записями списка доступа не нужно.

0.0.0.0, что означает использование ключевого слова `host` перед значением `source`. В IP-адресе поступившего пакета

нужно сравнивать все биты с соответствующими битами в адресе записей списка доступа.

### **Режимы команды**

config-std-nacl (режим редактирования стандартных списков доступа).

### **Рекомендации по использованию**

Команда `permit` в режиме редактирования стандартных списков доступа используется для разрешения трафика, исходящего от указанного источника.

### **Нумерация записей в списке**

Перед командой `permit` или `deny` допускается вводить порядковый номер записи в списке, который можно использовать для упрощения редактирования записей, например,

```
ip access-list standard acl1
  10 permit 10.1.1.1
  20 deny 10.2.1.0 0.0.0.255
  30 permit any
```

В режиме редактирования списка доступа запись с указанным номером будет вставлена на нужную позицию, например,

```
15 permit 10.1.1.1 0.0.255.255
```

Если запись с таким номером существует, то будет выдано сообщение об ошибке: % Duplicate sequence number.

По умолчанию первой записи в списке присваивается номер 10, а следующие номера в списке следуют с приращением 10. Максимальный порядковый номер 2147483647. Если сгенерированный порядковый номер превысил максимальный, то выдается сообщение об ошибке: % Exceeded maximum sequence number.

При выходе из консоли нумерация записей теряется. При следующем старте консоли записи располагаются в порядке возрастания номеров в режиме по умолчанию.

### **Просмотр по команде show running-config**

По команде `show running-config` нумерованные списки доступа показываются в виде последовательности команд `access-list` за одним исключением:

если после редактирования нумерованного списка доступа он становится пустым (в нем нет записей вида `permit` или `deny` (no permit, no deny)), то он будет показан в виде:

```
ip access-list {standard|extended} name
```

По команде `show running-config` выводится конфигурация, в которой слово `host` может отсутствовать.

Так как по команде `show running-config` ранее введенные номера записей в списке не показываются, то при редактировании чтобы внести запись на нужную позицию, можно еще раз упорядочить записи в списке с заданным начальным номером и приращением. Для этого используется команда: `ip access-list resequence`.

### **Удаление**

Удаление записи в списке доступа осуществляется:

- командой `no <полная запись>`, например:  
`no permit host 10.1.1.1`
- или по номеру записи, например: `no 15`.

Привязка списка доступа к криптокарте (шифрованный список) осуществляется командой `match address (crypto map)`, а уже криптокарта к интерфейсу – командой `crypto map (interface)`. Для привязки списка доступа к интерфейсу (фильтрующий список) используйте команду `ip access-group (interface)`

**Отличие данной команды от подобной команды Cisco IOS:**

- в инвертированной маске подсети `source-wildcard` и `destination-wildcard` должна быть непрерывная линейка из установленных битов в конце, не допускается чередование 0 и 1.
- не допускается использование `hostname` в качестве `source` и `destination`
- показывается пустой нумерованный список по команде `show running-config`

**Пример**

Приведенный ниже пример демонстрирует создание стандартного списка доступа с именем "a133", в котором используются команды запрета трафика от подсети 192.168.110.0 и хоста 10.10.1.101, и разрешение трафика от любого другого источника. Если выполнена команда запрета трафика от подсети 192.168.110.0, то проверка следующих правил уже не осуществляется. Если данное правило не выполнено, то происходит проверка следующего, если оно выполнено, то следующее не проверяется и т.д.

```
Router(config)#ip access-list standard a133
Router(config-std-nacl)#deny 192.168.110.0 0.0.0.255
Router(config-std-nacl)#deny host 10.10.1.101
Router(config-std-nacl)#permit any
Router(config-std-nacl)#exit
```

## permit (extended)

Команда `permit (extended)` используется для редактирования расширенных списков доступа. Эта команда разрешает прохождение трафика между указанным источником и получателем. Для отмены разрешающей записи в расширенном списке доступа используется та же команда с префиксом `no`.

### Синтаксис

```
permit protocol source source-wildcard [operator port  
[port]] destination destination-wildcard [operator port  
[port]]
```

```
no permit protocol source source-wildcard [operator  
port [port]] destination destination-wildcard [operator  
port [port]]
```

protocol

Протокол. Задается в виде номера протокола. Протоколы IP, TCP, UDP, AH, ESP, ICMP, EIGRP, GRE, IGMP, IPINIP, NOS, OSPF, PCP, PIM могут быть заданы аббревиатурой ip, tcp, udp, ahp, esp, icmp, eigrp, gre, igmp, ipinip, nos, ospf, pcp, pim. Соответствие названия протокола и его номера приведено в Таблица 3.

source

Этот параметр описывает отправителя пакета.

Возможны три варианта описания:

явное указание IP-адреса в формате четырех десятичных значений, разделенных точками

использование ключевого слова `any`, обозначающего пару значений 0.0.0.0 255.255.255.255 для параметров `source` и `source-wildcard`.

использование ключевого слова `host` перед значением `source`, что предполагает значение 0.0.0.0 для параметра `source-wildcard`.

**source-wildcard**

инвертированная маска подсети отправителя (получателя) пакета. Описан в разделе "[Permit \(standard\)](#)". Используется в списках доступа для того, чтобы определить: соответствует ли IP-адрес в заголовке пакета IP-адресу в записях списка доступа.

operator

Описывает условие сравнения, применяемое к портам источника и получателя. Используются операторы `eq` (equal, равно) и `range` (диапазон). Иные операторы не допускаются. Необязательный параметр.

port

Только для протоколов TCP или UDP можно указывать порт или диапазон портов. Целое число из диапазона от 0 до 65535. Используется только в связке с параметром **operator**. При использовании **operator=range** после него следуют два числа (лежащих в диапазоне от 0 до 65535), определяющие границы диапазона портов. Перечисление портов не допускается. Необязательный параметр. Поддерживаемые имена портов протоколов TCP и UDP приведены в Таблица 4 и Таблица 5.

Замечание 1:

Если задать два одинаковых порта, например,  
`permit udp any range non500-isakmp 4500 any`,  
то это будет эквивалентно оператору `eq`.

Замечание 2:

Если задать сначала порт с большим номером, то порты в диапазоне автоматически поменяются местами.

destination

Этот параметр описывает получателя пакета.

Возможны три варианта описания:

явное указание IP-адреса в формате четырех десятичных значений, разделенных точками

использование ключевого слова `any`, обозначающего пару значений 0.0.0.0 255.255.255.255 для параметров `destination` и `destination-wildcard`.

использование ключевого слова `host` перед значением `destination`, что предполагает значение 0.0.0.0 для параметра `destination-wildcard`.

**`destination-wildcard`** инвертированная маска подсети получателя пакета. Аналогичен `source-wildcard`, который описан в разделе "[Permit \(standard\)](#)".

### **Режимы команды**

`config-ext-nacl` (режим редактирования расширенных списков доступа).

### **Рекомендации по использованию**

Используйте эту команду после входа в режим редактирования расширенного списка доступа для разрешения прохождения трафика между отправителем и получателем.

### **Нумерация записей в списке**

Перед командой `permit` или `deny` допускается вводить порядковый номер записи в списке, который можно использовать для упрощения редактирования записей, например,

```
ip access-list extended acl2
  10 permit udp any any
  20 permit tcp any any
  30 deny udp host 10.1.1.1 eq snmp any
```

В режиме редактирования списка доступа запись с указанным номером будет вставлена на нужную позицию, например,

```
15 permit udp 10.1.1.1 0.0.255.255 host 10.2.2.2
```

Если запись с таким номером существует, то будет выдано сообщение об ошибке: `% Duplicate sequence number`.

По умолчанию первой записи в списке присваивается номер 10, а следующие номера в списке следуют с приращением 10. Максимальный порядковый номер 2147483647. Если сгенерированный порядковый номер превысил максимальный, то выдается сообщение об ошибке: `% Exceeded maximum sequence number`.

При выходе из консоли нумерация записей теряется. При следующем старте консоли записи располагаются в порядке возрастания номеров в режиме по умолчанию.

### **Просмотр по команде show running-config**

По команде `show running-config` нумерованные списки доступа показываются в виде последовательности команд `access-list` за одним исключением:

если после редактирования нумерованного списка доступа он становится пустым (в нем нет записей вида `permit` или `deny` (`no permit`, `no deny`)), то он будет показан в виде:

```
ip access-list {standard|extended} name
```

По команде `show running-config` выводится конфигурация, в которой слово `host` может отсутствовать.

Так как по команде `show running-config` ранее введенные номера записей в списке не показываются, то при редактировании чтобы внести запись на нужную позицию, можно еще раз упорядочить записи в списке с заданным начальным номером и приращением. Для этого используется команда: `ip access-list resequence`.

### Удаление

Удаление записи в списке доступа осуществляется:

- командой `no` <полная запись>, например:  
`no permit tcp host 10.1.1.1 eq telnet any`
- или по номеру записи, например: `no 15`.

Привязка списка доступа к криптокарте (шифрованный список) осуществляется командой `match address (crypto map)`, а уже криптокарта к интерфейсу – командой `crypto map (interface)`. Для привязки списка доступа к интерфейсу (фильтрующий список) используйте команду `ip access-group (interface)`.

### Отличие данной команды от подобной команды Cisco IOS:

- в инвертированной маске подсети `source-wildcard` и `destination-wildcard` должна быть непрерывная линейка из установленных битов в конце, не допускается чередование 0 и 1.
- отсутствует спецификатор `established` для TCP.
- не поддерживаются TCP-флаги
- отсутствует возможность задавать отдельные ICMP-type и ICMP-code, только ICMP протокол целиком.
- не допускается использование `hostname` в качестве `source` и `destination`
- не допускаются операторы кроме `eq` и `range`
- пустой нумерованный список по команде `show running-config` показывается в виде `ip access-list name`. В Cisco IOS данный список вообще не показывается.

### **Имя и номер протокола**

Таблица 3

Имя протокола	Описание протокола	Номер протокола
ip	Any Internet Protocol	
tcp	Transmission Control Protocol	6
udp	User Datagram Protocol	17
ahp	Authentication Header Protocol	51
icmp	Internet Control Message Protocol	1
esp	Encapsulation Security Payload	50
eigrp	Cisco's EIGRP routing protocol	88
gre	Cisco's GRE tunneling	47

### Cisco-like команды

igmp	Internet Gateway Message Protocol	2
ipinip	IP in IP tunneling	4
nos	KA9Q NOS compatible IP over IP tunneling	94
ospf	OSPF routing protocol	89
pcp	Payload Compression Protocol	108
pim	Protocol Independent Multicast	103

### Поддерживаемые имена портов протокола TCP

Таблица 4

Имя протокола	Описание протокола	Номер порта
bgp	Border Gateway Protocol	179
chargen	Character generator	19
cmd	Remote commands (rcmd)	514
daytime	Daytime	13
discard	Discard	9
domain	Domain Name Service	53
drip	Dynamic Routing Information Protocol	3949
echo	Echo	7
exec	Exec (rsh)	512
finger	Finger	79
ftp	File Transfer Protocol	21
ftp-data	FTP data connections	20
gopher	Gopher	70
hostname	NIC hostname server	101
ident	Ident Protocol	113
irc	Internet Relay Chat	194
klogin	Kerberos login	543
kshell	Kerberos shell	544
login	Login (rlogin)	513

### Cisco-like команды

lpd	Printer service	515
nntp	Network News Transport Protocol	119
pim-auto-rp	PIM Auto-RP	496
pop2	Post Office Protocol v2	109
pop3	Post Office Protocol v3	110
smtp	Simple Mail Transport Protocol	25
sunrpc	Sun Remote Procedure Call	111
syslog	Syslog Примечание: по команде show running-config заменяется на cmd (аналогично Cisco).	514
tacacs tacacs-ds	TAC Access Control System Примечание: вторая запись эквивалентна первой, но не показывается в подсказке (аналогично Cisco).	49
talk	Talk	517
telnet	Telnet	23
time	Time	37
uucp	Unix-to-Unix Copy Program	540
whois	Nickname	43
www	World Wide Web (HTTP)	80

### Поддерживаемые имена портов протокола UDP

Таблица 5

Имя протокола	Описание протокола	Номер порта
biff	Biff (mail notification, comsat)	512
bootpc	Bootstrap Protocol (BOOTP) client	68
bootps	Bootstrap Protocol (BOOTP) server	67
discard	Discard	9
dnsix	DNSIX security protocol auditing	195
domain	Domain Name Service (DNS)	53
echo	Echo	7



### Cisco-like команды

isakmp	Internet Security Association and Key Management Protocol	500
mobile-ip	Mobile IP registration	434
nameserver	IEN116 name service (obsolete)	42
netbios-dgm	NetBios datagram service	138
netbios-ns	NetBios name service	137
netbios-ss	NetBios session service	139
non500-isakmp	Internet Security Association and Key Management Protocol	4500
ntp	Network Time Protocol	123
pim-auto-rp	PIM Auto-RP	496
rip	Routing Information Protocol (router, in.routed)	520
snmp	Simple Network Management Protocol	161
snmptrap	SNMP Traps	162
sunrpc	Sun Remote Procedure Call	111
syslog	Syslog	514
tacacs	TAC Access Control System	49
tacacs-ds	Примечание: вторая запись эквивалентна первой, но не показывается в подсказке (аналогично Cisco).	
talk	Talk	517
tftp	Trivial File Transfer Protocol	69
time	Time	37
who	Who service (rwho)	513
xdmcp	X Display Manager Control Protocol	177

### Пример

Приведенный ниже пример демонстрирует добавление в расширенный список доступа с именем "a101" записи, разрешающей трафик между хостами 10.10.1.101 и 10.11.1.101 по протоколу udp:

```
Router(config)#ip access-list extended a101
Router(config-ext-nacl)#permit udp host 10.10.1.101 host 10.11.1.101
Router(config-ext-nacl)#exit
```

## deny (standard)

Команда `deny (standard)` используется при редактировании стандартных списков доступа. Эта команда определяет запрет на прохождение трафика с указанного адреса. Для удаления запрещающей записи из списка доступа используйте ту же команду с префиксом `no`.

### Синтаксис

`deny source [source-wildcard]`

`no deny source [source-wildcard]`

`source`

Описан в разделе ["Permit \(standard\)"](#)

`source-wildcard`

Описан в разделе ["Permit \(standard\)"](#)

### Режимы команды

`config-std-nacl` (режим редактирования стандартных списков доступа).

### Рекомендации по использованию

Команда `deny` в режиме редактирования стандартного списка доступа используется для запрета трафика, исходящего от указанного источника.

См. рекомендации в разделе ["Permit \(standard\)"](#).

### Пример

Приведенный ниже пример демонстрирует создание стандартного списка доступа с именем "a133", в котором используются команды запрета трафика от подсети 192.5.34.0 и разрешение трафика от подсетей 128.88.0.0 и 36.0.0.0

```
Router(config)#ip access-list standard a133
Router(config-std-nacl)#deny 192.5.34.0 0.0.0.255
Router(config-std-nacl)#permit 128.88.0.0 0.0.255.255
Router(config-std-nacl)#permit 36.0.0.0 0.255.255.255
Router(config-std-nacl)#exit
Router(config)#
```

## deny (extended)

Команда `deny (extended)` используется для редактирования расширенных списков доступа. Эта команда запрещает прохождение трафика между указанными источниками и получателями. Для отмены запрещающей записи в расширенном списке доступа используется та же команда с префиксом `no`.

### Синтаксис

```
deny protocol source source-wildcard [operator port  
[port]] destination destination-wildcard  
[operator[port]]
```

```
no deny protocol source source-wildcard [operator port  
[port]] destination destination-wildcard  
[operator[port]]
```

<code>protocol</code>	Протокол. Задается в виде номера протокола. Протоколы IP, TCP и UDP могут быть заданы аббревиатурой <code>ip</code> , <code>tcp</code> и <code>udp</code> .
<code>source</code>	Описан в разделе " <a href="#">Permit (extended)</a> "
<code>source-wildcard</code>	Описан в разделе " <a href="#">Permit (extended)</a> "
<code>operator</code>	Описывает условие сравнения, применяемое к портам источника и получателя. Используются операторы <code>eq</code> (equal, равно) и <code>range</code> (диапазон). Необязательный параметр.
<code>port</code>	Целое число из диапазона от 0 до 65535. Используется только в связке с параметром <code>operator</code> . При использовании <code>operator=range</code> после него следуют два числа (лежащих в диапазоне от 0 до 65535), определяющие границы диапазона портов. Необязательный параметр.
<code>destination</code>	описан в разделе " <a href="#">Permit (extended)</a> "
<code>destination-wildcard</code>	описан в разделе " <a href="#">Permit (extended)</a> "

### Режимы команды

`config-ext-nacl` (режим редактирования расширенных списков доступа).

### Рекомендации по использованию

Используйте эту команду после входа в режим редактирования расширенного списка доступа для запрета прохождения трафика между указанными источником и получателем.

См. рекомендации в разделе "[Permit \(extended\)](#)".

### Пример

Приведенный ниже пример демонстрирует добавление в расширенный список доступа с именем "a101" записи, запрещающей весь трафик к хосту 2.2.2.5:

```
Router(config)#ip access-list extended a101
Router(config-ext-nacl)#deny ip any host 2.2.2.5
```

## ip access-list resequence

Команда `ip access-list resequence` используется для нумерования записей в списке доступа. No-форма этой команды не используется.

### Синтаксис

```
ip access-list resequence name starting-sequence-number  
increment
```

name                    имя списка доступа.

starting-sequence-number номер, с которого начинается нумерация записей в списке (1–2147483647). По умолчанию первой записи в списке присваивается номер 10.

increment              Приращение номера записи в списке. По умолчанию приращение равно 10.

### Значение по умолчанию

Значение по умолчанию отсутствует.

### Режимы команды

Global configuration.

### Рекомендации по использованию

Для упрощения редактирования записей в списке могут использоваться номера записей, которые задают порядок следования записей в списке.

По умолчанию первой записи в списке присваивается номер 10, а следующие номера в списке следуют с приращением 10. Максимальный порядковый номер записи - 2147483647. Если сгенерированный порядковый номер превысил максимальный, то выдается сообщение об ошибке: % Exceeded maximum sequence number.

Нумерацию записей можно задавать явным образом перед командой `permit` или `deny` в режиме редактирования списка доступа (в команде `ip access-list`). Созданная запись с указанным номером будет вставлена на нужную позицию. Например,

```
15 permit udp 10.1.1.1 0.0.255.255 host 10.2.2.2
```

Если запись с таким номером существует, то будет выдано сообщение об ошибке: % Duplicate sequence number.

При выходе из консоли нумерация записей теряется. При следующем старте консоли записи располагаются в порядке возрастания номеров в режиме по умолчанию.

Так как по команде `show running-config` ранее введенные номера записей в списке не показываются, то при редактировании чтобы внести запись на нужную позицию, можно еще раз упорядочить записи в списке с заданным начальным номером и приращением, используя команду `ip access-list resequence`.

### Пример

Пример нумерации записей в списке `acl1`, где первая запись имеет номер 100, а последующие 105, 110 и т.д.

```
ip access-list resequence acl1 100 5
```

## access-list (standard)

Команда `access-list` используется для создания нумерованных стандартных списков доступа IP. No-форма этой команды отменяет ранее созданный список доступа.

### Синтаксис

	<code>access-list</code> number <b>permit deny</b> source [source-wildcard]
	<code>no access-list</code> number
number	номер списка доступа IP. Для задания стандартного списка доступа номер должен находиться в пределах 1–99 или 1300–1999
permit	разрешает прохождение пакета.
deny	запрещает прохождение пакета
source	описан в разделе " <a href="#">Permit (standard)</a> "
source-wildcard	описан в разделе " <a href="#">Permit (standard)</a> ".

### Значение по умолчанию

Значение по умолчанию отсутствует.

### Режимы команды

Global configuration.

### Рекомендации по использованию

Команда `access-list` используется для создания и редактирования нумерованных стандартных списков доступа. Стандартные списки доступа используются для фильтрации пакетов только по IP-адресу отправителя (источника) пакетов.

Удаление указанного списка целиком осуществляется командой `no access-list number`. Все остальные записи в этой команде игнорируются.

### Пример

Ниже приведен пример создания списка доступа с номером 10, запрещающий трафик от хоста с адресом 10.1.1.2:

```
Router(config)#access-list 10 deny host 10.1.1.2
```

## access-list (extended)

Команда `access-list` используется для создания нумерованных расширенных списков доступа IP. No-форма этой команды отменяет ранее созданный список с этим номером.

### Синтаксис

```
access-list number permit|deny protocol source source-wildcard [operator port[port]] destination destination-wildcard [operator port [port]]  
  
no access-list number
```

number

номер списка доступа IP. Для задания расширенного списка доступа номер должен находиться в пределах 100–199 или 2000–2699.

Все остальные параметры команды были описаны в разделе "[Permit \(extended\)](#)".

### Значение по умолчанию

Значение по умолчанию отсутствует.

### Режимы команды

Global configuration.

### Рекомендации по использованию

Команда `access-list` используется для создания и редактирования нумерованных расширенных списков доступа. Расширенные списки доступа используются для более гибкой фильтрации пакетов - по адресу отправителя пакета, адресу получателя пакета, по типу протокола, порту отправителя пакета и порту получателя.

Удаление указанного списка целиком осуществляется командой `no access-list number`. Все остальные записи в этой команде игнорируются. Например, если задать команду `no access-list 101 permit ip host 1.2.3.4 any`, то эта команда удалит весь список под номером 101.

### Пример

Ниже приведен пример создания списка доступа с номером 100:

```
Router(config)#access-list 100 deny tcp host 10.1.1.2 host 2.2.2.2 eq 22
```

# Команды создания IKE политики

## crypto isakmp policy

Команда `crypto isakmp policy` используется для создания IKE политики, в которой указываются желаемые алгоритмы и параметры создаваемого защищенного канала, которые будут предложены партнеру для согласования. Этот канал будет обеспечивать защиту части обменов информацией первой фазы и все обмены второй фазы IKE.

Таких политик может быть указано несколько с присвоением им приоритета.

Выполнение данной команды осуществляет вход в режим настройки параметров ISAKMP SA.

Для удаления IKE политики используется та же команда с префиксом `no`.

### Синтаксис

`crypto isakmp policy {priority}`

`no crypto isakmp policy`

`priority`

уникальный идентификатор IKE политики. В качестве идентификатора следует использовать целое число от 1 до 10000. При этом следует учитывать, что чем больше число, тем ниже приоритет создаваемой политики.

### Значение по умолчанию

По умолчанию в IKE политике используются параметры, приведенные ниже.

`encryption = des (ГОСТ 28147-89)`

`hash = sha (SHA-1)`

`authentication = rsa-sig`

`group = 1`

`lifetime = 86,400`

### Режимы команды

Global configuration

### Рекомендации по использованию

Используйте данную команду для указания параметров, о которых будут вестись переговоры с партнером, для создания ассоциации защиты ISAKMP (ISAKMP SA).

Команда `crypto isakmp policy` осуществляет вход в режим ISAKMP policy configuration. В этом режиме и указываются параметры ISAKMP SA с помощью команд:

`authentication (IKE policy)`

`encryption (IKE policy)`

`hash (IKE policy)`

`group (IKE policy)`

`lifetime (IKE policy)`

Если в процессе создания IKE политики какой-либо из параметров не был задан, то будет использоваться его значение по умолчанию.

**Примечание:** При использовании параметров по умолчанию аутентификация сторон в IKE на ГОСТовых сертификатах работать не будет. Для устранения этого необходимо использовать команду `hash md5`, указывающую, что в качестве хэш-алгоритма должен использоваться алгоритм ГОСТ Р 34.11-94 HMAC. Также нельзя одновременно использовать значения по умолчанию для `encryption` и `hash`, т.е. сочетание алгоритма шифрования `des` (подразумевающего применение алгоритма ГОСТ 28147-89) и хэш-алгоритма SHA-1 недопустимо.

#### **Отличие данной команды от подобной команды Cisco IOS:**

Следует учесть, что если задать несколько команд `crypto isakmp policy` с разными методами аутентификации и различными алгоритмами шифрования и хэширования, то после конвертирования cisco-like конфигурации в native-конфигурацию, последняя будет содержать весь список методов аутентификации и весь список алгоритмов. В результате возможна ситуация, при которой партнер предложит в IKE метод аутентификации из одной `crypto isakmp policy`, а алгоритмы – из другой `crypto isakmp policy`. А шлюз согласится на работу с партнером, с которым у него параметры ни в одной `crypto isakmp policy` не совпадают.

#### **Пример**

Ниже приведен пример создания IKE политики, состоящей из двух наборов параметров и имеющих приоритеты 15 и 20:

```
Router(config)#crypto isakmp policy 15
Router(config-isakmp)#hash md5
Router(config-isakmp)#authentication rsa-sig
Router(config-isakmp)#group 2
Router(config-isakmp)#lifetime 5000
Router(config-isakmp)#exit
Router(config)#crypto isakmp policy 20
Router(config-isakmp)#authentication pre-share
Router(config-isakmp)#lifetime 10000
Router(config-isakmp)#exit
```



## authentication (IKE policy)

Команда `authentication` применяется для указания метода аутентификации сторон.

Восстановить значение по умолчанию можно с помощью той же команды с префиксом `no`.

<b><u>Синтаксис</u></b>	<code>authentication {rsa-sig   pre-share}</code> <code>no authentication {rsa-sig   pre-share}</code>
<b><code>rsa-sig</code></b>	аутентификация осуществляется с использованием цифровых сертификатов стандарта X.509
<b><code>pre-share</code></b>	аутентификация осуществляется с использованием предопределенных ключей

**Значение по умолчанию** `rsa-sig`

**Режимы команды** ISAKMP policy configuration

### **Рекомендации по использованию**

Используйте эту команду для указания метода аутентификации сторон, которая происходит в первой фазе IKE.

Данная команда работает в режиме ISAKMP policy configuration.

Аутентификация может осуществляться с использованием предопределенного ключа (Preshared Key).

При указании параметра `rsa-sig` аутентификация осуществляется с использованием электронной цифровой подписи и цифровых сертификатов открытых ключей. Ключевая пара, к которой принадлежит открытый ключ локального сертификата, может быть создана с использованием алгоритма RSA, DSA или ГОСТ Р 34.10-2001. Локальный сертификат с открытым ключом по RSA алгоритму должен быть подписан CA сертификатом с открытым ключом, созданным по RSA алгоритму. Локальный ГОСТ сертификат должен быть подписан CA ГОСТ сертификатом. Локальный DSA сертификат – CA DSA сертификатом.

В файле настроек конвертора `cs_conv.ini` параметрам `send_cert` и `send_request` присвоено значение ALWAYS, и поэтому по умолчанию партнеру всегда будет отсылаться локальный сертификат по протоколу IKE и запрашиваться сертификат партнера.

По команде `show running-config` команда `authentication rsa-sig` не показывается.

### **Отличие данной команды от подобной команды Cisco IOS:**

не допускается тип аутентификации RSA encryption.

### **Пример**

Ниже приведен пример назначения метода аутентификации сторон на предопределенных ключах, используемого в рамках протокола IKE. Остальные параметры устанавливаются по умолчанию:

```
Router(config)#crypto isakmp policy 10
Router(config-isakmp)#authentication pre-share
Router(config-isakmp)#exit
```

## encryption (IKE policy)

Команда `encryption` применяется для указания алгоритма шифрования сообщений, предлагаемого для согласования партнеру, который будет использован для создания защищенного канала.

Восстановить значения по умолчанию можно с помощью той же команды с префиксом `no`.

<b><u>Синтаксис</u></b>	<code>encryption {des  3des   aes  aes 128  aes 192  aes 256}</code> <code>no encryption</code>
<b><code>des</code></b>	в качестве алгоритма шифрования используется алгоритм ГОСТ 28147-89
<b><code>3des</code></b>	в качестве алгоритма шифрования используется 168-bit DES-CBC (3DES)
<b><code>aes aes 128</code></b>	в качестве алгоритма шифрования используется 128-bit AES. Значения <code>aes</code> и <code>aes 128</code> – эквивалентны.
<b><code>aes 192</code></b>	в качестве алгоритма шифрования используется 192-bit AES
<b><code>aes 256</code></b>	в качестве алгоритма шифрования используется 256-bit AES

<b><u>Значение по умолчанию</u></b>	<code>des</code>
-------------------------------------	------------------

<b><u>Режимы команды</u></b>	ISAKMP policy configuration
------------------------------	-----------------------------

### Рекомендации по использованию

Используйте данную команду для назначения алгоритма шифрования, который будет использоваться для защиты обменов IKE.

Данная команда работает в режиме ISAKMP policy configuration.

Для шифрования с использованием сертифицированного российского криптографического алгоритма ГОСТ 28147-89 укажите параметр `des`. Алгоритм 56bit DES, который используется в ПАК Cisco, для которого зарезервирован параметр `des`, заменен на алгоритм ГОСТ 28147-89.

Используемые алгоритмы шифрования указываются в файле `cs_conv.ini`. По умолчанию `des` отображается в ГОСТ 28147-89, а остальные алгоритмы остаются без изменений.

No-форма команды выставляет значение по умолчанию.

По команде `show running-config` команда сокращается до `enchr` и показывается всегда, а значения `aes` и `aes 128` – показываются как `aes`.

### Отличие данной команды от подобной команды Cisco IOS:

по команде `show running-config` данная команда показывается всегда.

### Пример

Ниже приведен пример назначения в качестве алгоритма шифрования 168-bit DES-CBC (3DES) в рамках ISAKMP SA. Остальные параметры устанавливаются по умолчанию:

```
Router(config)#crypto isakmp policy 10
Router(config-isakmp)#encryption 3des
Router(config-isakmp)#exit
```

## hash (IKE policy)

Команда `hash` применяется для указания хэш-алгоритма, используемого для контроля целостности сообщений в рамках ISAKMP SA.

Восстановить значения по умолчанию можно с помощью той же команды с префиксом `no`.

CSP VPN Gate использует для хэширования сертифицированный российский криптографический алгоритм ГОСТ Р 34.11-94 HMAC. Этим алгоритмом заменен штатно используемый в программно-аппаратных комплексах алгоритм MD5, для которого зарезервирован параметр `md5`. Для назначения к использованию криптографического алгоритма ГОСТ Р 34.11-94 HMAC следует устанавливать параметр `md5`.

### Синтаксис

`hash {sha | md5}`

`no hash {sha | md5}`

`sha`

указывает, что в качестве хэш-алгоритма должен использоваться алгоритм SHA-1 (HMAC вариант)

`md5`

указывает, что в качестве хэш-алгоритма должен использоваться алгоритм ГОСТ Р 34.11-94 HMAC

### Значение по умолчанию

`hash sha` (SHA-1)

### Режимы команды

ISAKMP policy configuration

### Рекомендации по использованию

Используйте эту команду для назначения хэш-алгоритма, используемого в рамках протокола IKE или для восстановления значения по умолчанию. Данная команда работает в режиме ISAKMP policy configuration. Если в качестве метода аутентификации была выбрана цифровая подпись и это подпись на ГОСТ-алгоритмах, то для хэширования необходимо применять алгоритм ГОСТ Р 34.11-94 HMAC (т.е. необходимо установить значение хэш-алгоритма `md5`), использовать в данном случае алгоритм хэширования SHA-1 нельзя.

Используемые хэш-алгоритмы указываются в файле `cs_conv.ini`. По умолчанию `md5` отображается в ГОСТ, а `sha` – остается как есть.

No-форма команды выставляет значение по умолчанию.

Следует учесть, что при стандартной схеме отображения алгоритмов значения по умолчанию (`des + sha`) использовать **категорически не рекомендуется**.

При создании новой ISAKMP policy для использования ГОСТ надо обязательно ввести команду `hash md5` (encryption `des` можно не вводить – это значение по умолчанию).

По команде `show running-config` команда показывается всегда.

### Отличие данной команды от подобной команды Cisco IOS:

по команде `show running-config` данная команда показывается всегда, даже при значении по умолчанию.

### Пример

Ниже приведен пример назначения в качестве хэш-алгоритма алгоритма ГОСТ Р 34.11-94 HMAC. Остальные параметры устанавливаются по умолчанию:

```
Router(config)#crypto isakmp policy 10
Router(config-isakmp)#hash md5
Router(config-isakmp)#exit
```

## group (IKE policy)

Команда `group` применяется для указания алгоритма, используемого в рамках протокола IKE для выработки ключевого материала. Используется алгоритм Диффи-Хеллмана или алгоритм VKO GOST R 34.10-2001 [RFC4357]. Восстановить значения по умолчанию можно с помощью той же команды с префиксом `no`.

### Синтаксис

```
group {vko | 1 | 2 | 5}
```

```
no group
```

vko

используется алгоритм VKO GOST R 34.10-2001

1

используется алгоритм Диффи-Хеллмана, длина ключа 768 бит

2

используется алгоритм Диффи-Хеллмана, длина ключа 1024 бит

5

используется алгоритм Диффи-Хеллмана, длина ключа 1536 бит

### Значение по умолчанию

group 1

### Режимы команды

ISAKMP policy configuration

### Рекомендации по использованию

Используйте эту команду для указания алгоритма, который будет использоваться в рамках протокола IKE для выработки общего секретного ключа и сессионных ключей. Данная команда работает в режиме `ISAKMP policy configuration`.

Используемые алгоритмы генерации ключей указываются в файле `cs_conv.ini`.

### Пример

Ниже приведен пример указания алгоритма Диффи-Хеллмана с длиной ключа в 1024 бита. Остальные параметры устанавливаются по умолчанию:

```
Router(config)#crypto isakmp policy 10
```

```
Router(config-isakmp)#group 2
```

```
Router(config-isakmp)#exit
```

## lifetime (IKE policy)

Команда `lifetime` применяется для настройки времени жизни IKE SA. Восстановить значения по умолчанию можно с помощью той же команды с префиксом `no`.

### Синтаксис

`lifetime seconds`

`no lifetime`

`seconds`

время жизни IKE SA в секундах. Разрешено использовать целое число из диапазона от 1 до 4294967295.

### Значение по умолчанию

86400 (1 сутки)

### Режимы команды

ISAKMP policy configuration

### Рекомендации по использованию

Используйте эту команду для указания времени жизни IKE SA или для восстановления значения по умолчанию. Отсутствует возможность установить неограниченное время жизни IKE SA. Данная команда работает в режиме ISAKMP policy configuration.

### Отличие данной команды от подобной команды Cisco IOS:

ограничения по времени жизни имеют больший диапазон, чем у команды Cisco: 60 – 86400.

### Пример

Ниже приведен пример установки времени жизни IKE SA равным 1200 секунд (20 минут). Остальные параметры устанавливаются по умолчанию:

```
Router(config)#crypto isakmp policy 10
Router(config-isakmp)#lifetime 1200
Router(config-isakmp)#exit
```

## crypto isakmp peer

Команда `crypto isakmp peer` применяется для выбора партнера и входа в режим ISAKMP peer configuration, в котором можно установить aggressive mode для организации информационных обменов в рамках IKE протокола с этим партнером. Для отключения этой функциональности используйте команду с префиксом `no`.

<b><u>Синтаксис</u></b>	<code>crypto isakmp peer {address ip-address}</code> <code>no crypto isakmp peer {address ip-address}</code>
ip-address	IP-адрес партнера

<b><u>Значение по умолчанию</u></b>	Значение по умолчанию отсутствует
-------------------------------------	-----------------------------------

<b><u>Режимы команды</u></b>	Global configuration
------------------------------	----------------------

### **Рекомендации по использованию**

После выполнения этой команды используйте команду `set aggressive-mode client-endpoint` для установления aggressive режима в рамках протокола IKE.

### **Отличие данной команды от подобной команды Cisco IOS:**

не поддерживается вариант команды с `hostname`:  
`crypto isakmp peer {hostname ip-address}`

### **Пример**

Ниже приведен пример назначения адреса партнера, с которым предполагается aggressive mode для инициации IKE обменов:

```
Router(config)#crypto isakmp peer address 4.4.4.1
```

## set aggressive-mode client-endpoint

Команда `set aggressive-mode client-endpoint` применяется для установки `aggressive mode` для организации информационных обменов в рамках IKE протокола с партнером. Для удаления этого режима используйте команду с префиксом `no`.

### Синтаксис

**set aggressive-mode client-endpoint** {ipv4-address ipv4-address | fqdn fqdn | fqdn-user fqdn-user}

**no set aggressive-mode client-endpoint** {ipv4-address ipv4-address | fqdn fqdn | fqdn-user fqdn-user}

ipv4-address	идентификатор инициатора соединения типа IPV4-address (т.е. локальный ID типа IP-address)
fqdn	идентификатор инициатора типа FQDN (локальный ID типа полное доменное имя)
fqdn-user	идентификатор инициатора типа E-mail.

### Значение по умолчанию

Значение по умолчанию отсутствует

### Режимы команды

ISAKMP peer configuration

### Рекомендации по использованию

Команда `set aggressive-mode client-endpoint` может быть использована только в режиме ISAKMP peer configuration. Для входа в этот режим необходимо выполнить команду `crypto isakmp peer address`.

### Отличие данной команды от подобной команды Cisco IOS:

- включение данной команды в конфигурацию означает включение `aggressive mode` (`AggrModePriority=TRUE`) для данного партнера
- аргумент данной команды игнорируется (не делается различий между локальными ID). Данная команда работает как признак включения `AggrModePriority`
- если для команды `crypto isakmp peer` отсутствует команда `set aggressive-mode client-endpoint`, то команда `crypto isakmp peer` игнорируется.

### Пример

Для описания правила создания туннеля по нашей инициативе в `Aggressive mode` с учетом того, что IP-адрес партнера 4.4.4.1, а IP-адрес локального устройства 4.4.4.2 используются команды:

```
Router(config)#crypto isakmp peer address 4.4.4.1
```

```
Router(config-isakmp-peer)#set aggressive-mode client-endpoint ipv4-address 4.4.4.2
```

```
Router(config-isakmp-peer)#set aggressive-mode password 1234567890
```

## set aggressive-mode password

Команда `set aggressive-mode password` применяется для ввода Preshared ключа для данного партнера. Для удаления Preshared ключа из конфигурации используйте команду с префиксом `no`.

### Синтаксис

`set aggressive-mode password {password}`

`no set aggressive-mode password {password}`

password

значение предустановленного ключа

### Значение по умолчанию

Значение по умолчанию отсутствует

### Режимы команды

ISAKMP peer configuration

### Рекомендации по использованию

Данная команда игнорируется в конфигурации и не влияет на логику работы конвертора.



## crypto isakmp identity

Команда `crypto isakmp identity` применяется для назначения типа идентификатора, используемого в рамках протокола IKE. Отменить назначенный тип идентификатора можно с помощью той же команды с префиксом `no`.

### Синтаксис

	<code>crypto isakmp identity {address  dn  hostname}</code>
	<code>no crypto isakmp identity {address  dn  hostname}</code>
<b>address</b>	Устанавливает идентификатор address.
<b>hostname</b>	Устанавливает идентификатор hostname.
<b>dn</b>	устанавливает идентификатор dn

### Значение по умолчанию

По умолчанию установлен тип идентификатора address.

### Режимы команды

Global configuration

### Рекомендации по использованию

Используйте эту команду для указания, какой тип идентификатора должен быть использован в рамках протокола IKE. Возможно три варианта address, hostname и dn.

Идентификатор типа address как правило используется, если компьютер имеет только один интерфейс с постоянным IP-адресом.

Идентификатор типа hostname как правило используется, если компьютер имеет более одного интерфейса или же если имеется один интерфейс, но нет постоянного IP-адреса.

Рекомендуется для всех партнеров использовать единый тип идентификатора: либо address, либо hostname, либо dn.

Идентификатор dn используется только при работе с сертификатами.

### Пример

Ниже приведен пример указания типа идентификатора address:

```
Router(config)#crypto isakmp identity address
```

## crypto isakmp keepalive

Команда `crypto isakmp keepalive` применяется для активизации процесса обмена сообщениями, подтверждающими активность (в рамках протокола IKE) между роутерами. Отключить этот процесс можно с помощью той же команды с префиксом `no`.

### Синтаксис

**`crypto isakmp keepalive secs [retries]`**

**`no crypto isakmp keepalive secs [retries]`**

`secs`

Задаёт допустимый период времени отсутствия входящего трафика от партнера, по истечению которого, при наличии исходящего трафика, активируется DPD-сессия. Диапазон величины – от 10 до 3600 секунд.

`retries`

Задаёт время ожидания ответа от партнера на DPD-запрос. Диапазон величины – от 2 до 60 секунд. По умолчанию значение этой величины равно 2.

### Значение по умолчанию

По умолчанию команда не активирована.

### Режимы команды

Global configuration

### Рекомендации по использованию

Используйте эту команду для отправки сообщений, подтверждающих активность партнера (в рамках протокола IKE).

### Пример

Ниже приведен пример активации процесса отправки сообщений, в случае если от партнера не было получено пакетов в течение 30 секунд. Пакеты процесса будут отсылаться через 3 секунды:

```
Router(config)#crypto isakmp keepalive 30 3
```

## crypto ipsec security-association lifetime

Данная команда используется для установки времени жизни SA (Security Association, ассоциация защиты). Под временем жизни понимается время, разрешенное для действия SA. По истечении этого времени SA прекращает свое существование и начинает работать новая SA.

Время жизни может задаваться как в секундах, так и в килобайтах (объем проходящего, в рамках установленного SA, трафика). Для восстановления значения по умолчанию используйте ту же команду с префиксом `no`.

### Синтаксис

```
crypto ipsec security-association lifetime {seconds  
seconds | kilobytes kilobytes}
```

```
no crypto ipsec security-association lifetime {seconds  
| kilobytes}
```

`seconds` время жизни SA в секундах. Допустимые значения от 1 до 4294967295.

`kilobytes` время жизни SA в килобайтах. Допустимые значения от 1 до 4294967295.

### Режимы команды

Global configuration

### Значение по умолчанию

3600 секунд (1 час) и 4608000 килобайт (1 час при 10 Мбайт/с).

### Рекомендации по использованию

Используйте эту команду для изменения установленных значений времени жизни SA. Следует помнить, что уменьшение времени жизни SA ведет к повышению уровня защиты соединения, но повышает нагрузку на процессор, что, в свою очередь, ведет к снижению пропускной способности.

На стадии обсуждения условий создания новой SA устанавливается минимальное время жизни SA из предложенных сторонами.

Существуют два параметра, ограничивающие время жизни SA – время в секундах и количество переданной и принятой информации в килобайтах. Ограничение всегда будет действовать по достижении лимита любым из этих параметров. Например, закончилось время жизни, установленное в секундах, а ограничение по трафику не выполнено и на половину. В этом случае будет действовать ограничение по времени. Пересоздание SA не будет в случае отсутствия трафика между партнерами.

Если закончилось время жизни и SA уже не существует, то новый SA не установится, если не будет трафика.

Изменения вступят в силу после выхода из режима global configuration командой `exit`.

### Пример

Ниже приведен пример установки времени жизни SA равного 1600 сек:

```
Router(config)#crypto ipsec security-association lifetime seconds 1600
```

# Команды формирования набора преобразований IPsec

## crypto ipsec transform-set

Команда `crypto ipsec transform-set` используется для формирования набора преобразований – комбинации протоколов защиты и криптографических алгоритмов.

Для удаления набора преобразований используется та же команда с префиксом `no`.

### Синтаксис

```
crypto ipsec transform-set transform-set-name transform1  
[transform2 [transform3]]
```

```
no crypto ipsec transform-set transform-set-name
```

`transform-set-name` имя, присваиваемое набору преобразований.

`transform1..3` наборы преобразований. Разрешено использовать до 3 наборов преобразований.

### Режимы команды

Global configuration. Выполнение этой команды осуществляет вход в режим `crypto transform configuration`.

### Значение по умолчанию

Значение по умолчанию отсутствует.

### Рекомендации по использованию

Набор преобразований – это приемлемая комбинация протоколов защиты, криптографических алгоритмов и других параметров, применяемых в защищаемом IPsec трафике. В процессе согласования параметров IPsec SA партнеры соглашаются на использование конкретного набора преобразований для защиты конкретного потока данных.

Вы можете создать несколько наборов преобразований и затем назначить один или более из них каждой конкретной записи криптографической карты. Набор преобразований, указанный в записи криптографической карты, используется при согласовании параметров IPsec SA для защиты потока данных, разрешенного в списке доступа только для этой записи криптографической карты.

Перед тем как назначить набор преобразований трафика для записи криптографической карты, набор преобразований должен быть задан с помощью этой команды.

Набор преобразований задает использование протоколов IPsec: Encapsulation Security Protocol (ESP) и Authentication Header (AH), и указывает какие криптографические алгоритмы следует использовать с этими протоколами. Данные протоколы могут использоваться как по отдельности, так и оба одновременно.

Для создания набора преобразований следует описать от одного до трех преобразований. Каждое из преобразований должно содержать описание используемых протоколов (AH, ESP) и криптографических алгоритмов.

Для установления режима, используемого набором преобразований, предназначена команда `mode`.

**Допустимые комбинации преобразований**

Тип преобразования	Имя	Описание
AH Transform (один из списка)	ah-md5-hmac	Протокол AH с алгоритмом аутентификации ГОСТ Р 34.11-94 HMAC
	ah-sha-hmac	Протокол AH с алгоритмом аутентификации SHA
ESP Encryption Transform (один из списка)	esp-null	Протокол ESP с алгоритмом Null.
	esp-des	Протокол ESP с алгоритмом ГОСТ 28147-89
	esp-3des	Протокол ESP с 168-битным алгоритмом 3DES
	esp-aes-128	Протокол ESP с 128-битным алгоритмом AES
	esp-aes-192	Протокол ESP с 192-битным алгоритмом AES
	esp-aes-256	Протокол ESP с 256-битным алгоритмом AES
ESP Authentication Transform (один из списка)	esp-md5-hmac	Протокол ESP с алгоритмом аутентификации MD5 ГОСТ Р 34.11-94 HMAC
	esp-sha-hmac	Протокол ESP с алгоритмом аутентификации SHA

**Отличие данной команды от подобной команды Cisco IOS:**

- в Продукте CSP VPN Gate отсутствует поддержка преобразования IP Compression Transform.
- в CSP VPN Gate при установлении параметра `des` для шифрования используется сертифицированный российский криптографический алгоритм ГОСТ 28147-89, а у Cisco – 56bit DES
- в CSP VPN Gate при установлении параметра `md5` для хэширования используется сертифицированный российский криптографический алгоритм ГОСТ Р 34.11-94 HMAC, а у Cisco – штатный алгоритм MD5.

**Пример**

В приведенном ниже примере заданы два набора преобразований, использующие криптографические алгоритмы различной сложности:

```
Router(config)#crypto ipsec transform-set ts esp-3des esp-sha-hmac
Router(config)#crypto ipsec transform-set gost ah-md5-hmac esp-des
```

## mode (IPsec)

Команда `mode` применяется для изменения режима, используемого набором преобразований. Для восстановления режима по умолчанию используйте эту команду с префиксом `no`.

### Синтаксис

`mode [tunnel | transport]`

`no mode`

`tunnel`

параметр, устанавливающий туннельный режим

`transport`

параметр, устанавливающий транспортный режим

### Режимы команды

Crypto transform configuration.

### Значение по умолчанию

туннельный режим

### Рекомендации по использованию

Используйте команду `mode` для явного указания режима используемого набором преобразований или для восстановления режима по умолчанию. Если команда `mode` введена без параметров, то будет установлено значение по умолчанию.

**Если созданные наборы преобразований будут использоваться одной и той же записью криптографической карты (см. команду `set transform-set`), то эти наборы преобразований должны иметь один и тот же режим.**

### Пример

```
Router(config)#crypto ipsec transform-set inner-tunnel ah-md5-hmac esp-  
des esp-md5-hmac  
Router(cfg-crypto-trans)#mode tunnel  
Router(cfg-crypto-trans)# exit
```

# Команды для работы с IKECFG пулом

## ip local pool

Команда `ip local pool` применяется для создания IKECFG пула адресов – набора (диапазона) IP-адресов, которые будут выдаваться партнерам, например, мобильному клиенту, после установления соединения и запроса IP-адреса из IKECFG пула.

Для удаления пула адресов используется та же команда с префиксом `no`.

### Синтаксис

```
ip local pool poolname low-ip-address [high-ip-address]
no ip local pool poolname low-ip-address [high-ip-address]
```

Для удаления всего набора локальных адресов используется команда

```
no ip local pool poolname
```

`poolname` имя, присваиваемое пулу адресов.

`low-ip-address` начальный адрес диапазона локальных адресов.

`high-ip-address` конечный адрес диапазона локальных адресов. Необязательный параметр.

### Значение по умолчанию

Значение по умолчанию отсутствует

### Режимы команды

Global configuration

### Рекомендации по использованию

Используйте эту команду для создания IKECFG пула IP-адресов.

Повторный вызов команды с другим диапазоном адресов добавляет этот диапазон в пул.

Если новый диапазон пересекается с ранее введенным, то команда не выполняется и выдается сообщение об ошибке: `%IP address range overlaps with pool: <pool-name>`.

Если первый адрес диапазона больше второго, то команда не выполняется и выдается сообщение об ошибке: `%Bad IP range, <low-ip-address> - <high-ip-address>`.

В пул адресов могут быть выделены адреса как из защищаемой шлюзом (CSP VPN Gate) подсети, так и адреса, непересекающиеся с защищаемой подсетью.

При подключении пользователей они будут получать IP-адреса из этого набора.

Если конечный адрес пула не задан – будет создан пул, состоящий из одного адреса.

Один созданный пул адресов можно сделать общим для тех криптокарт, которые не имеют собственного пула и у которых установлен флаг `crypto map map-name client configuration address {initiate|respond}`. Для этого нужно ввести команду

```
crypto isakmp client configuration address-pool local pool-name.
```

Если общий пул уже задан, то последняя команда не выполняется и выдается сообщение об ошибке: `% Remove current pool first.`

**Удаление**

Удалить пул можно целиком либо только один диапазон адресов из пула.

Для удаления всего пула используется команда:

```
no ip local pool poolname
```

Удаление диапазона из пула производится командой:

```
no ip local pool poolname low-ip-address [high-ip-address]
```

Удаление последнего диапазона из пула эквивалентно удалению всего пула. Такая команда может быть отвергнута с ошибкой, если на пул присутствует ссылка из команды `set pool` (режим настройки `crypto map`). В этом случае выдается сообщение: `% Cannot remove the pool. It is used by: crypto map(s): "cmap 10", "cmap 20"; dynamic map(s): "dmap 10", "dmap 20"`

**Отличие данной команды от подобной команды Cisco IOS:**

- допускается удаление всего пула, в Cisco IOS – нет
- поведение при удалении диапазона пула отличается от Cisco IOS, так как там нет команды `set pool`.

**Пример**

Ниже приведен пример создания пула IP-адресов с именем `'localpool'`, содержащего 1024 IP-адреса:

```
Router(config)#ip local pool localpool 10.1.1.0 10.1.4.255
```



## crypto isakmp client configuration address-pool local

Команда `crypto isakmp client configuration address-pool local` применяется для назначения пула адресов в качестве общего пула.

Отменить назначенный общий пул можно с помощью той же команды с префиксом `no`.

### Синтаксис

```
crypto isakmp client configuration address-pool local
pool-name

no crypto isakmp client configuration address-pool
local
```

pool-name

имя общего пула IP-адресов.

### Значение по умолчанию

Значение по умолчанию отсутствует

### Режимы команды

Global configuration

### Рекомендации по использованию

После создания пула командой `ip local pool`, используйте команду `crypto isakmp client configuration address-pool local` для назначения созданного пула в качестве общего.

Для привязки такого общего пула ко всем криптокартам с именем map-name используйте команду `crypto map map-name client configuration address {initiate|respond}`. Пул будет являться общим для всех криптокарт с именем map-name, за исключением тех карт, для которых пул задан явно командой `set pool name` в режиме настройки команды `crypto map map-name seq-num ipsec-isakmp`.

Допускается задавать несуществующий пул адресов, но при конвертировании конфигурации необходимо, чтобы присутствовала ссылка на существующий пул, в противном случае конвертирование остановится с выдачей ошибки: Address pool "<pool-name>" not found. Conversion aborted.

Допускается удалять пул адресов, на который ссылается данная команда.

Если задан общий пул для всех криптокарт с именем map-name, но для одной из этих криптокарт задана команда `set pool <none>`, то для этой криптокарты пул не используется..

### Пример

Ниже приведен пример назначения общего пула адресов "main" и привязки его к криптокартам с именем "dmap" для использования в рамках протокола IKE:

```
Router(config)#crypto isakmp client configuration address-pool local
main

Router(config)# crypto map dmap client configuration address initiate
```

## crypto map client configuration address

Команда `crypto map client configuration address` используется для привязки общего пула адресов ко всем криптокартам с заданным именем, а также задает способ выдачи IP-адреса партнеру по протоколу IKECFG, работа с которым будет происходить по указанной криптографической карте.

Отменить привязку к общему пулу можно с помощью той же команды с префиксом `no`.

### Синтаксис

```
crypto map map-name client configuration address
{initiate|respond}

no crypto map map-name client configuration address
{initiate|respond}
```

map-name	имя криптографической карты.
initiate	без запроса партнера CSP VPN Gate выдает IP-адрес из IKECFG пула партнеру, при его попытке создать IPsec SA с использованием своего реального IP.
respond	по запросу партнера CSP VPN Gate выдает партнеру IP-адрес из IKECFG пула.

### Значение по умолчанию

По умолчанию роутер не будет работать по данной криптографической карте по протоколу IKECFG

### Режимы команды

Global configuration

### Рекомендации по использованию

Команда `crypto map client configuration address` используется для привязки общего пула адресов, назначенного командой `crypto isakmp client configuration address-pool local`, ко всем криптокартам с именем `map-name`.

В данной версии Продукта опции `initiate` и `respond` работают одинаково в том смысле, что если задана команда

```
crypto map map-name client configuration address initiate,
```

то это означает, что задана и команда

```
crypto map map-name client configuration address respond
```

и наоборот.

### Пример

Ниже приведен пример задания пула "main", назначение его в качестве общего и привязка его ко всем криптокартам с именем "card2":

```
Router(config)#ip local pool main 1.1.1.1 1.1.1.2
```

```
Router(config)#crypto isakmp client configuration address-pool local
main
```

```
Router(config)#crypto map card2 client configuration address initiate
```

## crypto dynamic-map client configuration address

Команда `crypto dynamic-map client configuration address` используется для привязки общего пула адресов ко всем криптокартам с заданным именем, а также задает способ выдачи IP-адреса партнеру по протоколу IKECFG, работа с которым будет происходить по указанной криптографической.

Отменить привязку к общему пулу можно с помощью той же команды с префиксом `no`.

<b><u>Синтаксис</u></b>	<pre>crypto dynamic-map map-name client configuration address {initiate respond}  no crypto dynamic-map map-name client configuration address {initiate respond}</pre>
map-name	имя динамической криптографической карты.
initiate	без запроса партнера CSP VPN Gate выдает IP-адрес из IKECFG пула партнеру, при его попытке создать IPsec SA с использованием своего реального IP.
respond	по запросу партнера CSP VPN Gate выдает партнеру IP-адрес из IKECFG пула.

**Значение по умолчанию** По умолчанию роутер не будет работать по данной криптографической карте по протоколу IKECFG.

**Режимы команды** Global configuration

### **Рекомендации по использованию**

Команда `crypto dynamic-map client configuration address` используется для привязки общего пула адресов, назначенного командой `crypto isakmp client configuration address-pool local`, ко всем криптокартам с именем map-name.

В данной версии Продукта опции `initiate` и `respond` работают одинаково в том смысле, что если задана команда

```
crypto dynamic-map map-name client configuration address initiate,
```

то это означает, что задана и команда

```
crypto dynamic-map map-name client configuration address respond
```

и наоборот.

### **Отличие данной команды от подобной команды Cisco IOS:**

данная команда отсутствует в Cisco IOS.

### **Пример**

Ниже приведен пример создания общего пула "main", назначение его в качестве общего и привязка его ко всем криптокартам с именем "card2":

```
Router(config)#ip local pool main 1.1.1.1 1.1.1.2
```

```
Router(config)#crypto isakmp client configuration address-pool local
main
```

```
Router(config)#crypto dynamic-map card2 client configuration address
initiate
```

# Команды создания и редактирования криптографических карт

## crypto map (global IPsec)

Команда `crypto map` используется для создания или изменения записей криптографических карт. Также с помощью команды `crypto map` осуществляется переход в режим настройки криптографических карт (Crypto map configuration).

Для удаления записи или набора записей криптографических карт используются те же команды, но с префиксом `no`.

### Синтаксис

```
crypto map map-name seq-num ipsec-isakmp [dynamic
dynamic-map-set]
```

```
no crypto map map-name seq-num
```

map-name	имя набора записей криптографической карты. Это имя присваивается в момент создания криптографической карты.
seq-num	номер, присваиваемый отдельной записи в криптографической карте.
<b>ipsec-isakmp</b>	указывает на то, что для данной записи при создании IPsec SA будет использоваться процедура согласования параметров IKE. Это ключевое слово обязательно только при создании новой криптокарты, при редактировании уже существующей – можно не указывать.
<b>dynamic</b>	указывает на то, что данная запись ссылается на уже существующий набор динамических криптографических карт, созданных командой <code>crypto dynamic-map</code> . При использовании этого ключевого слова доступ к командам настройки криптографической карты будет запрещен. Необязательный параметр.
dynamic-map-set	имя набора записей динамической криптографической карты, который используется в качестве шаблона политики безопасности. Используется только в связке с параметром <code>dynamic</code> .

### Режимы команды

Global configuration. Данная команда осуществляет переход в режим `crypto map configuration`.

### Значение по умолчанию

Нет предустановленных криптографических карт.

### Рекомендации по использованию

Данная команда используется для создания новой криптокарты, новых записей в ней или изменения существующих записей.

Записи в криптографических картах устанавливают параметры IPsec SA для подлежащего шифрованию или аутентификации трафика.

Если требуется создать более одной записи в криптографической карте, то следует учитывать, что обработка трафика будет производиться в соответствии с приоритетами записей. Наименьший номер (seq-num) записи соответствует ее наивысшему приоритету и наоборот – чем выше значение номера записи, тем ниже ее приоритет. Пакеты обрабатываемого трафика сначала будут сравниваться с записями высшего приоритета.

Команда `crypto map` осуществляет переход в режим настройки криптографической карты (Crypto map configuration). В этом режиме могут быть настроены (отредактированы) такие параметры, как привязка к записи криптографической карты списка доступа (access list), партнера, установка опции PFS, установка времени жизни SA и др. В режиме настройки могут использоваться следующие команды:

<code>set pfs</code>	указывает, что на стадии согласования параметров IPsec для данной записи криптографической карты должна быть затребована опция PFS.
<code>set security-association lifetime</code>	устанавливает время жизни SA для конкретных записей криптографической карты.
<code>set transform-set</code>	указывает, какие наборы преобразований (transform set) могут использоваться с данной записью криптографической карты.
<code>set peer</code>	указывает IPsec партнера для записи криптографической карты.
<code>set identity</code>	устанавливает списки идентификаторов, которые используются
<code>set pool</code>	устанавливает имя пула криптографической карты
<code>match address</code>	осуществляет привязку списка доступа к записи криптографической карты.
<code>reverse-route</code>	включает механизм Reverse Route Injection (RRI).

### Создание статической криптокарты

При создании новой `crypto map` (также как в Cisco) ключевое слово `ipsec-isakmp` обязательно должно присутствовать в команде, при редактировании уже существующей криптокарты допускается сокращенная запись – это ключевое слово можно не указывать.

### Ограничения

Аналогично Cisco существуют ограничения на модификацию уже существующих криптокарт (указание с тем же именем и порядковым номером). Запрещены следующие ситуации:

- попытка замены существующей статической криптокарты на динамическую. Например:

```
crypto map cmap 1 ipsec-isakmp
```

```
...
```

```
crypto map cmap 1 ipsec-isakmp dynamic dmap !!! Ошибочная команда !!!
```

- попытка замены существующей динамической криптокарты на статическую. Например:

```
crypto map cmap 1 ipsec-isakmp dynamic dmap
```

```
...
```

```
crypto map cmap 1 ipsec-isakmp !!! Ошибочная команда !!!
```

- попытка замены ссылки на другой dynamic-map-set в уже существующей криптокарте. Например:

```
crypto map cmap 1 ipsec-isakmp dynamic dmap
```

```
...
```

```
crypto map cmap 1 ipsec-isakmp dynamic another-dmap !!! Ошибочная команда !!!
```

Во всех указанных случаях введенная команда игнорируется и на консоль выдается сообщение, аналогичное Cisco: "Attempt to change dynamic map tag for existing crypto map is ignored."

### **Редактирование**

Если задать корректную команду для уже существующей криптокарты (т.е. не попадающую в один из указанных ранее ошибочных случаев), поведение различается для разных типов crypto map (поведение аналогично Cisco):

- для динамической криптокарты команда ничего не делает (поскольку совпадает с введенной ранее), однако воспринимается как корректная
- для статической криптокарты происходит вход в конфигурационный режим, в котором можно поменять настройки crypto map (peer, ACL, transform-set и т.д.).

### **Удаление**

1. Основной вариант команды удаления отдельной записи в криптокарте:

```
no crypto map map-name seq-num
```

Добавление дополнительных ключевых слов не допускается.

Если указанного в команде имени набора записей криптокарты или номера записи в криптокарте не существует, то выдается сообщение об ошибке:

"Could not find crypto map entry <map-name> <seq-num>".

Если указанная в команде запись является единственной в наборе записей криптокарты и криптокарта привязана к интерфейсу, то команда не выполняется и выдается сообщение об ошибке:

"Crypto-map <map-name> is in use by interface(s): Fa<NUM>. Please remove the crypto map from the above interface(s) first".

2. Команда удаления всего набора записей в криптокарте (криптокарты):

```
no crypto map map-name
```

Если указанная в команде криптокарта отсутствует, то команда не выполняется и выдается сообщение об ошибке:

"Could not find crypto map <map-name>"

Если указанная в команде криптокарта привязана к интерфейсу, то команда не выполняется и выдается сообщение об ошибке:

"Crypto-map <map-name> is in use by interface(s): Fa<NUM>. Please remove the crypto map from the above interface(s) first".

Допускается (хотя и необязательно) добавление дополнительных ключевых слов, например:

```
no crypto map cmap 1 ipsec-isakmp
```

```
no crypto map cmap 1 ipsec-isakmp dynamic dmap !!! Только для динамической  
crypto map !!!
```

Команда `no` с указанием ключевого слова `dynamic` (как в последнем примере) работает только для динамической crypto map. Если такую команду задать для статической crypto map, команда завершится с ошибкой и проигнорируется.

**Отличие данной команды от подобной команды Cisco IOS:**

- существует специфический подход в случае, если в `crypto map set` присутствует несколько `crypto maps`, а в их `crypto-map-acls` существуют пересечения по адресам, причем в части правил присутствует `permit`, а в других правилах – `deny`. Подробнее логика конвертирования для данной ситуации описана в документе-Приложении в п.5 раздела "Описание обработки интерфейсов".
- существуют особенности при использовании `crypto map` с несколькими `peers` в случае, если используется аутентификация на `preshared keys` и для разных `peers` используются разные ключи и/или используется смешанная аутентификация (на `preshared keys` и сертификатах). Эти особенности описаны в документе Приложении в п.8 раздела "Описание обработки интерфейсов".
- не поддерживается тип `ipsec-manual` и задание `crypto map profile`.

Команды `crypto isakmp profiles` и `crypto ipsec profiles` в данной версии Продукта не реализованы, тем не менее, имеется возможность сформировать инфраструктуру работы с удаленными пользователями. Например, имеется команда `set identity`, которая устанавливает `identity` инициатора и при работе с удаленными клиентами параметры шифрования и выделяемые туннельные адреса могут определяться в зависимости от DN сертификата и FQDN клиента. Одной из команд, формирующих инфраструктуру, является команда `set pool`, задающая пул адресов, из которого будут выделяться адреса по IKECFG для мобильных пользователей.

**Пример**

Ниже приведен пример использования команды `crypto map`:

```
Router(config)#crypto dynamic-map mydynamicmap 10
Router(config-crypto-map)#match address 103
Router(config-crypto-map)#set transform-set my_t_set1 my_t_set2
my_t_set3

Router(config)#crypto map mymap 10 ipsec-isakmp
Router(config-crypto-map)#match address 101
Router(config-crypto-map)#set transform-set my_t_set1
Router(config-crypto-map)#set peer 10.0.0.1
Router(config-crypto-map)#set peer 10.0.0.2
Router(config)#crypto map mymap 20 ipsec-isakmp
Router(config-crypto-map)#match address 102
Router(config-crypto-map)#set transform-set my_t_set1 my_t_set2
Router(config-crypto-map)#set peer 10.0.0.3
Router(config)#crypto map mymap 30 ipsec-isakmp dynamic mydynamicmap
!
```

## match address (crypto map)

Команда `match address` используется для связывания стандартного или расширенного списка доступа с записью криптографической карты. Команда работает в режим настройки криптографических карт (Crypto map configuration).

Для удаления связи списка доступа с записью криптографической карты используется та же команда, но с префиксом `no`.

### Синтаксис

```
match address [access-list-id | name]
no match address [access-list-id | name]
```

`access-list-id`      имя или номер списка доступа.

`name`                имя списка шифрованного доступа.

### Режимы команды

Crypto map configuration

### Значение по умолчанию

Значение по умолчанию отсутствует

### Рекомендации по использованию

Данная команда используется для всех записей статических криптографических карт.

Используйте эту команду для назначения стандартного или расширенного списка доступа записи криптографической карты. Предварительно следует определить этот список доступа с помощью команд `access-list` или `ip access-list`.

Список доступа, назначенный этой командой, будет использоваться IPsec для определения трафика, который следует или не следует защищать шифрованием. (Трафик, который разрешен списком доступа, будет защищаться. Трафик, который запрещен списком доступа, не будет защищаться.)

При определении списка шифрованного доступа, который используется в команде `match address`, в командах `access-list` или `ip access-list` параметры `source` и `destination` определяются следующим образом: в качестве `source` используются адреса того, кого будет защищать данный шлюз, а в качестве `destination` - адреса, которые защищает партнер по соединению.

Таким образом, при привязке к криптокарте список шифрованного доступа указывает исходящий трафик (также и в Cisco IOS).

Помните, что список шифрованного доступа не отвечает за разрешение или запрет прохождения трафика через сетевой интерфейс. Эту функцию выполняет список доступа.

### Пример

Ниже приведен пример с минимальными требованиями настройки параметров криптографической карты с использованием IKE для создания SA.

```
Router(config)#crypto map mymap 10 ipsec-isakmp
Router(config-crypto-map)#match address 101
Router(config-crypto-map)#set transform-set my_t_set1
Router(config-crypto-map)#set peer 10.0.0.1
```



## set peer (crypto map)

Команда `set peer` используется для указания партнера по защищенному соединению в записи криптографической карты. Для удаления партнера из записи криптографической карты используется та же команда, но с префиксом `no`.

### Синтаксис

`set peer ip-address`

`no set peer ip-address`

`ip-address` IP-адрес партнера по защищенному соединению.

### Режимы команды

Crypto map configuration

### Значение по умолчанию

Значение по умолчанию отсутствует

### Рекомендации по использованию

Данная команда используется для указания партнера по защищенному взаимодействию в криптографической карте.

Эта команда требуется для всех статических криптографических карт. Для динамических карт эта команда не обязательна и, в большинстве случаев, не используется (потому что в основном партнер неизвестен).

Можно назначить несколько партнеров путем повторения выполнения команды. Попытка создать SA будет предпринята с партнером, заданным первым. Если попытка не удастся для первого партнера, IKE пробует обратиться к следующему партнеру из списка криптографической карты.

### Пример

Ниже приведен пример с минимальными требованиями настройки параметров криптографической карты с использованием IKE для создания SA.

```
Router(config)#crypto map mymap 10 ipsec-isakmp
Router(config-crypto-map)#match address 101
Router(config-crypto-map)#set transform-set my_t_set1
Router(config-crypto-map)#set peer 10.0.0.1
```

## set pfs (crypto map)

Команда `set pfs` используется для установки опции PFS. Использование данной опции позволяет повысить уровень защищенности трафика – при создании каждого IPsec SA производится выработка новых сессионных ключей. Для снятия опции PFS используется та же команда, но с префиксом `no`.

### Синтаксис

`set pfs [vko | group1 | group2 | group5]`

`no set pfs`

`vko`

используется алгоритм VKO GOST R 34.10-2001 [RFC4357]

`group1`

используется алгоритм Диффи-Хеллмана, длина ключа 768 бит

`group2`

используется алгоритм Диффи-Хеллмана, длина ключа 1024 бита

`group5`

используется алгоритм Диффи-Хеллмана, длина ключа 1536 бит

### Режимы команды

Crypto map configuration

### Значение по умолчанию

По умолчанию опция PFS отключена.

### Рекомендации по использованию

В процессе согласования параметров SA будет затребовано включение опции PFS. Если при формировании записи криптографической карты алгоритм не был указан, то будет предложено использовать `group1` (значение по умолчанию). Если создание SA инициировано партнером, а локальная конфигурация требует использования PFS, то, либо партнер принимает условие использования PFS, либо SA не будет установлена. Если в локальной конфигурации явно прописано использование `group2`, эту же группу должен принять партнер в процессе согласования параметров, иначе SA не будет установлена.

Использование PFS усиливает уровень защиты потому, что даже если один из сессионных ключей будет взломан атакующей стороной, то только та часть данных, которая была зашифрована на этом ключе, может быть скомпрометирована. Без использования PFS скомпрометированными могут оказаться все данные, передаваемые в рамках созданной SA.

При использовании PFS при каждом создании новой SA будет производиться новый обмен ключами. Подобный обмен потребует дополнительных ресурсов процессора.

Используемые алгоритмы генерации ключей указываются в файле `cs_conv.ini`.

### Пример

Ниже приведен пример требования на использования PFS с группой `group2` для записи номер 10 криптографической карты "mymap":

```
Router(config)#crypto map mymap 10 ipsec-isakmp
```

```
Router(config-crypto-map)#set pfs group2
```

## set pool (crypto map)

Команда `set pool` используется для привязки созданного пула адресов для IKECFG к данной криптографической карте. Для устранения связи пула адресов и криптографической карты используется та же команда, но с префиксом `no`.

### Синтаксис

`set pool name`

`no set pool`

name

имя пула, из которого будут выдаваться IP-адреса для партнеров в данной криптографической карте. Имеется зарезервированное слово `<none>` (в угловых скобках) для указания, что к данной криптокарте не привязан пул. Данный пул должен быть задан в режиме Global configuration mode.

### Режимы команды

Crypto map configuration

### Значение по умолчанию

Нет значения по умолчанию

### Рекомендации по использованию

Использование данной команды возможно только для ipsec-isakmp записей в криптографических картах.

Команда указывает пул адресов для IKECFG, заданный командой `ip local pool`.

Если в конфигурации не создан указанный пул адресов, то выдается сообщение об ошибке: % Attempt to set unknown pool is ignored.

Если в криптокарте пул не указан явно командой `set pool`, но в конфигурации присутствует команда `crypto map map-name client configuration address {initiate|respond}`, которая привязывает все криптокарты с именем `map-name` к пулу с именем `pool-name`, а также команда `crypto isakmp client configuration address-pool local pool-name`, задающая глобальную привязку криптокарт к пулу с именем `pool-name` и указывающая общий пул для IKECFG, то этот пул и будет использоваться в криптокартах с именем `map-name`, кроме тех криптокарт, в которых пул задан явно.

Если задан пул по умолчанию, а в криптокарте указана команда `set pool <none>`, то пул адресов игнорируется.

### Удаление

Для удаления связи между пулом адресов и криптокартой используется команда `no set pool`. Возможно указать в команде дополнительные параметры.

### Замечание:

Если адреса для пула выделены из внутренней подсети, защищаемой шлюзом (CSP VPN Gate), то при выделении партнерам адресов из такого пула необходимо прописать в таблице маршрутизации маршрут на IP-адреса из этого пула через интерфейс роутера, а не через внешний интерфейс шлюза (CSP VPN Gate) командой `ip route`.

Если адреса пула не пересекаются с адресами внутренней подсети, защищаемой шлюзом (CSP VPN Gate), то при выделении адресов из такого пула маршрут на адреса из такого пула можно прописать через внешний интерфейс шлюза, установленного по умолчанию.

### Отличие данной команды от подобной команды Cisco IOS:

данная команда отсутствует в IOS у Cisco.

**Пример**

Приведен пример создания и привязки пула адресов "mypool" к записи номер 10 криптографической карты "mymap":

```
Router(config)#ip local pool mypool 10.10.10.10 10.10.10.20
Router(config)#crypto map mymap 10 ipsec-isakmp
Router(config-crypto-map)#set pool mypool
```

Пример использования команды `set pool <none>`, когда ко всем криптокартам с именем `сmap` привязывается пул с именем `pool1`, но к 10 записи криптокарты `сmap` пул не привязан:

```
Router(config)#crypto isakmp client configuration address-pool local
pool1
Router(config)#crypto map cmap client configuration address initiate
Router(config)#crypto map cmap 10 ipsec-isakmp
Router(config-crypto-map)#set pool <none>
```

Для случая динамической криптокарты:

```
Router(config)#crypto isakmp client configuration address-pool local
pool2
Router(config)#crypto dynamic-map dmap client configuration address
initiate
Router(config)#crypto map cmap 20 ipsec-isakmp dynamic dmap
Router(config-crypto-map)#set pool <none>
```

## set identity (crypto map)

Команда `set identity` используется для указания списка идентификаторов, который будет использоваться конкретной записью криптографической карты. Для устранения связи списка идентификаторов и криптографической карты используется та же команда с префиксом `no`.

### Синтаксис

`set identity [name]`

`no set identity`

name

имя списка идентификаторов. Данный список идентификаторов был создан командой `crypto identity` в режиме Global configuration.

### Режимы команды

Crypto map configuration

### Значение по умолчанию

Нет значения по умолчанию

### Рекомендации по использованию

Использование данной команды возможно только для ipsec-isakmp записей в криптографических картах.

### Пример

Ниже приведен пример создания списка идентификаторов "myident" и использование этого списка записью номер 10 криптографической карты "mymap":

```
Router(config)#crypto identity myident
Router(config-crypto-identity)#dn c=ru,o=s-terra,cn=test
Router(config-crypto-identity)#exit
```

```
Router(config)#crypto map mymap 10 ipsec-isakmp
Router(config-crypto-map)# set identity myident
```

## set security-association lifetime (crypto map)

Команда `set security-association lifetime` используется для изменения значения глобального времени жизни SA. Данная команда изменяет глобальное время жизни SA для конкретной записи криптографической карты. Для восстановления действия глобального времени жизни применяется та же команда с префиксом `no`.

### Синтаксис

```
set security-association lifetime {seconds seconds |
kilobytes kilobytes}
```

```
no set security-association lifetime {seconds |
kilobytes}
```

**seconds seconds** Устанавливает время действия SA в секундах. Допустимые значения от 1 до 4294967295.

**kilobytes kilobytes** Устанавливает время действия SA в объемах проходящего трафика (в килобайтах). Допустимые значения от 1 до 4294967295.

### Режимы команды

Crypto map configuration

### Значение по умолчанию

Глобальное время жизни.

### Рекомендации по использованию

Использование данной команды возможно в статических и динамических криптографических картах.

При согласовании параметров SA выбор времени жизни определяется из расчета минимального значения из предложенных партнерами.

Существуют два параметра, ограничивающие время жизни SA – время в секундах и количество переданной и принятой информации в килобайтах. Ограничение всегда будет действовать по достижении лимита любым из этих параметров. Например, закончилось время жизни, установленное в секундах, а ограничение по трафику не выполнено и на половину. В этом случае будет действовать ограничение по времени. Если закончилось время жизни и SA уже не существует, то новый SA не установится, если не будет трафика.

Более короткое время жизни SA уменьшает риск компрометации трафика, но требует большего процессорного времени.

Отсутствует возможность установить неограниченные значения трафика и времени жизни SA, как и у команд IOS в Cisco.

Для того, чтобы изменить время жизни в секундах, используйте команду `set security-association lifetime seconds`.

Для того, чтобы изменить время жизни в килобайтах, используйте команду `set security-association lifetime kilobytes`.

Все сделанные изменения времени жизни SA вступают в силу при выходе из режима `global configuration` командой `exit`. При этом происходит удаление всех установленных ранее соединений (IPsec и ISAKMP SA).

### Отличие данной команды от подобной команды Cisco IOS:

ограничения по трафику и времени жизни имеют больший диапазон, чем у команды Cisco: 120 – 86400 (sec), 2560 – 536870912 (kb).

**Пример**

Приведен пример изменения времени жизни для записи номер 10 криптографической карты "тутар":

```
Router(config)#crypto map mymap 10 ipsec-isakmp
Router(config-crypto-map)#set security-association lifetime seconds
2700
```

## set transform-set (crypto map)

Для указания набора преобразований, который может использоваться с записью в криптографической карте, используйте команду `set transform-set` в режиме `crypto map configuration`. Для удаления связи записи криптографической карты со всеми наборами преобразований используется та же команда с префиксом `no`.

### Синтаксис

```
set transform-set transform-set-name1 [transform-set-name2..transform-set-name7]
```

```
no set transform-set
```

transform-set-nameN           Имя набора преобразований.

Для записи криптографической карты можно использовать до 6 наборов преобразований.

### Режимы команды

Crypto map configuration

### Значение по умолчанию

Значение по умолчанию отсутствует.

### Рекомендации по использованию

Данная команда обязательна для всех записей статических и динамических криптографических карт.

Используйте эту команду для указания какие наборы преобразований следует связать с записью криптографической карты. **Все указанные наборы преобразований должны использовать один и тот же режим.**

Для **ipsec-isakmp** записи криптографической карты можно указывать до 7 наборов преобразований. При перечислении наборов преобразований следует помнить, что наибольший приоритет имеет первый набор преобразований.

Инициатор создания IPsec SA отправляет партнеру в числе прочих параметров и список наборов преобразований, выстроенный в соответствии с приоритетами. Партнер выбирает из предложенного списка первый набор преобразований, который совпадает с одним из его собственного списка набора преобразований. Если не найдено совпадений в списках наборов преобразований инициатора и партнера, то IPsec SA не будет установлена.

Если необходимо изменить список наборов преобразований, ассоциированных с записью криптографической карты, то следует просто заново выполнить команду `set transform-set` с указанием нового списка. Изменения вступят в силу при выходе из конфигурационного режима командой `exit`.

### Пример

В приведенном ниже примере показаны шаги по формированию наборов преобразований и назначению их конкретной (10) записи криптографической карты "туннель":

```
Router(config)#crypto ipsec transform-set my_t_set1 esp-des esp-sha-hmac
```

```
Router(config)#crypto ipsec transform-set my_t_set2 ah-sha-hmac esp-des esp-sha-hmac
```

```
Router(config)#crypto map mymap 10 ipsec-isakmp
```

```
Router(config-crypto-map)#match address 101
```

```
Router(config-crypto-map)#set transform-set my_t_set1 my_t_set2
```

```
Router(config-crypto-map)#set peer 10.0.0.1
```

```
Router(config-crypto-map)#set peer 10.0.0.2
```



## reverse-route (crypto map)

Команда `reverse-route` включает использование механизма Reverse Route Injection (RRI). Для отключения использования механизма RRI на данной криптокарте применяется та же команда с префиксом `no`.

### Синтаксис

```
reverse-route
no reverse-route
```

### Режимы команды

Crypto map configuration

### Значение по умолчанию

Значение по умолчанию отсутствует.

### Рекомендации по использованию

RRI (Reverse Route Injection) – это новый механизм связи управления топологией VPN и системой маршрутизации, позволяющий маршрутам к удаленным защищенным подсетям и клиентам, автоматически принимать участие в процессе маршрутизации.

Смысл механизма RRI состоит в том, что после создания защищенного соединения IPsec SA, в таблицу маршрутизации CSP VPN Gate с включенным RRI автоматически вносится запись о маршруте к удаленной сети партнера или клиенту. При нарушении защищенного соединения добавленный маршрут из таблицы шлюза удаляется.

Механизм RRI может использоваться в сетях большого размера для обеспечения надежности – в схемах резервирования с балансировкой сетевой нагрузки.

Для оповещения соседних сетевых устройств, стоящих за CSP VPN Gate, о доступных ему хостах, сетях, новых маршрутах, соответствующих изменениям в топологии VPN, используются протоколы динамической маршрутизации, например, RIP. Такие протоколы маршрутизации реализованы в пакете программ Quagga.

Более подробное описание применения механизма RRI дано в документе [«Использование RRI»](#) (RRI.pdf)

### Отличие данной команды от подобной команды Cisco IOS:

отсутствуют дополнительные параметры.

**Предупреждение:** недопустимо вручную изменять или удалять правила маршрутизации, которые автоматически формируются при использовании технологии RRI.

## crypto dynamic-map

Команда `crypto dynamic-map` используется для создания набора динамических криптографических карт. Также эта команда используется для входа в режим `crypto map configuration`.

Для удаления набора записей или одной записи динамической криптографической карты используется та же команда с префиксом `no`.

### Синтаксис

```
crypto dynamic-map dynamic-map-name dynamic-seq-num
no crypto dynamic-map dynamic-map-name [dynamic-seq-num]
```

<code>dynamic-map-name</code>	указывает имя набора записей динамической криптографической карты.
<code>dynamic-seq-num</code>	указывает номер конкретной записи динамической криптографической карты.

### Значение по умолчанию

Значение по умолчанию отсутствует.

### Режимы команды

Global configuration. Данная команда осуществляет переход в режим `crypto map configuration`.

### Рекомендации по использованию

Используйте эту команду для создания шаблонов политики, которые могут быть использованы в процессе согласования параметров SA с партнером, даже если вы не знаете всех параметров криптографической карты, требуемых для взаимодействия с удаленным партнером (таких, как его IP address). Например, если вы не имеете полной информации обо всех IPsec партнерах, использование динамических криптографических карт позволит вам создать SA с подобным партнером. Однако, процесс создания SA не будет начат до тех пор, пока успешно не завершится аутентификация IKE.

В режиме настройки параметров криптографической карты могут использоваться следующие команды (синтаксис этих команд совпадает с синтаксисом таких же команд при переходе в режим настройки криптографической карты командой `crypto map`):

`set pfs` – устанавливает опцию PFS

`set security-association lifetime` – устанавливает время жизни IPsec SA.

`set transform-set` – связывает запись криптографической карты с наборами преобразований

`set pool` – устанавливает пул адресов для записи криптографической карты.

`set identity` – связывает запись криптографической карты со списком идентификаторов

`match address` – связывает расширенный список доступа с записью криптографической карты

`exit` – выход из конфигурационного режима.

Обязательной командой в этом списке является команда `set transform-set`.

Записи динамической криптографической карты, подобно записям статических криптографических карт группируются в наборы записей (сеты). После того, как с помощью команды `crypto dynamic-map` определен набор записей динамической криптографической карты (который обычно содержит только одну запись), его необходимо связать с записью в "родительской" криптографической карте. Эта операция производится с помощью команды

`crypto map`. Затем эта "родительская" криптографическая карта должна быть привязана к интерфейсу.

Записи в "родительской" криптографической карте, ссылающиеся на динамические криптографические карты должны иметь более низкий приоритет, по сравнению с остальными записями. Это достигается присваиванием таким записям наивысших номеров (чем выше номер записи, тем ниже ее приоритет).

### **Пример**

Ниже приведен пример использования команды `crypto dynamic-map`. В этом примере запись статической криптографической карты "mymap 30" ссылается на динамическую криптографическую карту

```
Router(config)#crypto dynamic-map mydynamicmap 10
Router(config-crypto-map)#match address 103
Router(config-crypto-map)#set      transform-set      my_t_set1      my_t_set2
my_t_set3

Router(config)#crypto ipsec transform-set my_t_set1 esp-3des esp-sha-
hmac
Router(config)#crypto ipsec transform-set my_t_set2 esp-md5-hmac
Router(config)#crypto map mymap 10 ipsec-isakmp
Router(config-crypto-map)#match address 101
Router(config-crypto-map)#set transform-set my_t_set1
Router(config-crypto-map)#set peer 10.0.0.1
Router(config-crypto-map)#set peer 10.0.0.2
Router(config)#crypto map mymap 20 ipsec-isakmp
Router(config-crypto-map)#match address 102
Router(config-crypto-map)#set transform-set my_t_set1 my_t_set2
Router(config-crypto-map)#set peer 10.0.0.3
Router(config)#crypto map mymap 30 ipsec-isakmp dynamic mydynamicmap
!
```

# Команды настройки сетевых интерфейсов

## interface

Команда `interface` применяется для настройки сетевых интерфейсов, осуществляя вход в режим interface configuration.

### Синтаксис

<b><code>interface</code></b>	<b><code>type port/number</code></b>
<code>type</code>	тип интерфейса. В данной версии Продукта любой интерфейс, например, PPP или GigabitEthernet, представлен как <code>fastethernet</code>
<code>port</code>	номер порта. В данной версии Продукта поддерживается только 0
<code>number</code>	порядковый номер интерфейса

### Значение по умолчанию

Значение по умолчанию отсутствует

Режимы команды

Global configuration

### Рекомендации по использованию

При старте `cs_console` зачитываются существующие настройки сетевых интерфейсов, зарегистрированных в базе Продукта (при помощи команды `if_mgr add`), которые замещают настройки, присутствующие в конфигурации.

Данная команда позволяет управлять настройками только зарегистрированных сетевых интерфейсов. Изменения, сделанные в этом режиме, вступают в действие немедленно и сохраняются в загрузочных скриптах ОС (для восстановления при перезагрузке ОС).

Имя сетевого интерфейса в консоли формируется по шаблону `"FastEthernet0/x"` (где `x` – неотрицательное число), независимо от реального типа интерфейса.

Если не указано иное, то все команды в режиме настройки интерфейса сначала выполняют действия над текущим состоянием интерфейса. Если действие выполнено успешно, то состояние интерфейса сохраняется в загрузочных скриптах ОС, чтобы его восстановить при перезагрузке системы. Состояние интерфейса сохраняется целиком – включен/выключен, адрес интерфейса, MTU. Если состояние интерфейса меняется с помощью сторонних утилит ОС, то могут возникать противоречия между текущим статусом и статусом, записанным в загрузочных скриптах. Поэтому рекомендуется изменять состояние интерфейса только в консоли.

В режиме настройки интерфейса могут выполняться следующие подкоманды:

<code>shutdown</code>	включение/выключение интерфейса
<code>ip address</code>	настройка IP-адреса и маски
<code>ip access-group</code>	указание списка доступа, который должен отслеживаться на данном интерфейсе
<code>crypto map</code>	указание криптокарты, по которой будут защищаться пакеты, проходящие через данный интерфейс
<code>crypto ipsec df-bit</code>	установка значения DF-бита во внешнем заголовке пакета при прохождении через данный интерфейс
<code>mtu</code>	установка значения MTU на интерфейсе
<code>exit</code>	выход из конфигурационного режима

<code>description</code>	команда игнорируется	
<code>crypto ipsec fragmentation after-encryption</code>		команда игнорируется
<code>crypto ipsec fragmentation before-encryption</code>		команда игнорируется

**Пример**

Ниже приведен пример выполнения команды `interface`:

```
Router(config)#interface fastethernet 0/1
```

## shutdown (interface)

Команда `shutdown` применяется для изменения административного статуса интерфейса. Используется в режиме `interface configuration`.

### Синтаксис

```
shutdown
no shutdown
```

### Значение по умолчанию

Значение по умолчанию отсутствует

### Режимы команды

Interface configuration

### Рекомендации по использованию

Команда `shutdown` используется для изменения административного статуса (выключения/включения) интерфейса.

Команда изменяет административный статус интерфейса немедленно после ввода команды, который сохраняется в загрузочных скриптах ОС.

Для отключения интерфейса используется команда `shutdown`. При отключении интерфейса остальные настройки сохраняются (IP-адрес и др.).

Если при отключении произойдет ошибка, то выдается сообщение: `Cannot disable the interface.`

Если интерфейс отключился, но состояние интерфейса не удалось сохранить, выдается сообщение: `Interface was disabled, but the state of the interface was not saved. The changes will be lost after reboot.`

По команде `show running-config` отображается текущее системное состояние интерфейса.

Для включения интерфейса используется команда `no shutdown`, статус интерфейса также сохраняется в загрузочных скриптах.

Если при включении произойдет ошибка, то выдается сообщение: `Cannot enable the interface.`

Если интерфейс включился, но состояние интерфейса не удалось сохранить, выдается сообщение: `Interface was enabled, but the state of the interface was not saved. The changes will be lost after reboot.`

Команды `shutdown` и `no shutdown` исполняются даже в том случае, если результат исполнения команды уже соответствует текущему административному статусу интерфейса. Это сделано для того, чтобы избежать ситуаций, когда текущий административный статус может не совпадать со статусом, записанным в загрузочных скриптах ОС. В этом случае введенная команда принудительно запишет указанный статус в скрипты.

## ip address (interface)

Команда `ip address` применяется для назначения адресов и маски данному интерфейсу.

### Синтаксис

```
ip address ip-address mask [secondary]  
no ip address ip-address mask [secondary]
```

`ip-address`            локальный IP-адрес

`mask`                маска подсети

`secondary`            показывается для второго и последующих адресов.

### Значение по умолчанию

Значение по умолчанию отсутствует

### Режимы команды

Interface configuration

### Рекомендации по использованию

Команда `ip address` выполняется немедленно после ввода, изменения IP-адреса интерфейса и маски сохраняются в загрузочных скриптах ОС.

Команда `ip address` будет выполняться даже в том случае, если данный адрес уже присутствует на интерфейсе. Это сделано для того, чтобы избежать ситуацию, когда текущий адрес на интерфейсе не совпадает с адресом, прописанным в загрузочных скриптах. В этом случае введенная команда принудительно запишет указанный адрес в загрузочные скрипты.

При выполнении команды `ip address` автоматически выставляется broadcast address в значение `ip-address | ~mask`. Например, по команде:

```
ip address 192.168.10.10 255.255.255.0
```

автоматически выставляется broadcast address 192.168.10.255.

Различаются `primary` и `secondary` IP-адреса. В качестве `primary` адреса выбирается первый по списку адрес, остальные – в качестве `secondary`. Primary адрес может быть только один и задается командой:

```
ip address primary-ip primary-mask
```

Повторное задание IP-адреса замещает предыдущее значение:

- если смена `primary` адреса не удалась, то выдается сообщение: `Cannot set the primary address`
- если адрес был изменен, но состояние интерфейса не удалось сохранить, то выдается сообщение: `The primary address was set, but the state of the interface was not saved. The changes will be lost after reboot`
- если в качестве нового `primary` адреса задать существующий `secondary` адрес, то сначала будет удален существующий `secondary` адрес, а затем будет изменен `primary` адрес. При этой двойной операции возможны следующие ошибки:
  - если не удалось удалить существующий `secondary` адрес, то выдается сообщение: `Cannot remove the address`
  - если не удалось изменить `primary` адрес, то выдается сообщение: `Cannot set the primary address`
  - если не удалось сохранить состояние интерфейса, то выдается сообщение: `The primary address was set, but the state of the interface was not saved. The changes will be lost after reboot`

Адресов `secondary` может быть несколько. Secondary адрес задается командой:

```
ip address ip-address mask secondary
```

Адрес `secondary` можно задать, если задан `primary` адрес. В противном случае, выдается сообщение об ошибке: `Cannot add secondary without primary.`

Нельзя задавать в качестве `secondary` тот же адрес, что и `primary`. Иначе выдается сообщение об ошибке: `Secondary can't be same as primary`

Нельзя задать IP-адрес `0.0.0.0`. В этом случае выдается сообщение: `Not a valid host address - 0.0.0.0`. Это ограничение приводит к тому, что если задать IP-адрес `0.0.0.0` (с ненулевой маской) с помощью других средств (не в консоли), то он будет показан по команде `show running-config`, но удалить этот адрес в консоли невозможно, он будет отвергаться. В такой ситуации удалить все адреса на интерфейсе (включая и `0.0.0.0`) можно с помощью команды `no ip address`.

Нельзя задать маску `0.0.0.0`. В этом случае выдается сообщение об ошибке: `Bad mask /0 for address <ip>.`

Если попытаться задать некорректную маску (например, `255.0.255.0`), то выдается сообщение вида: `Bad mask 0xFF00FF00 for address <ip>.`

Если не удалось добавить на интерфейс новый адрес, то выдается сообщение: `Cannot add the address`

Если новый адрес был добавлен, но состояние интерфейса не удалось сохранить, то выдается сообщение: `The address was added, but the state of the interface was not saved. The changes will be lost after reboot.`

Допускается задавать полную копию существующего адреса, чтобы предотвратить ситуацию несовпадения текущего адреса и адреса в загрузочных скриптах ОС. Также можно для существующего адреса изменить маску:

- в случае ошибки выдается сообщение: `Cannot change the address`
- если параметры интерфейса удалось изменить, но состояние интерфейса не удалось сохранить, то выдается сообщение: `The address was changed, but the state of the interface was not saved. The changes will be lost after reboot.`

### Удаление

1. Удаление всех адресов с интерфейса осуществляется командой:

```
no ip address
```

После этой команды интерфейс будет выключен. Команда показывается по `show running-config`.

Если не удалось удалить все адреса с интерфейса, то выдается сообщение: `Cannot remove all addresses`

Если не удалось сохранить состояние интерфейса после удаления всех адресов, то выдается сообщение: `All addresses were removed, but the state of the interface was not saved. The changes will be lost after reboot`

2. Удаление конкретного адреса с интерфейса осуществляется командой:

```
no ip address ip-address mask
```

```
no ip address ip-address mask secondary
```

Удаление `primary` адреса по последствиям аналогично команде:

```
no ip address
```

При удалении `secondary` адреса, в команде слово `secondary` можно и не писать.



### **Сообщения при удалении**

При попытке удалить несуществующий адрес выдается сообщение об ошибке: `Invalid address`.

При указании маски, отличающейся от используемой для данного адреса, выдается сообщение об ошибке: `Invalid address mask`

Не допускается удалять `primary` адрес, если присутствует хотя бы один `secondary`.  
Выдается сообщение об ошибке: `Must delete secondary before deleting primary`

В команде удаления `primary` адреса не допускается писать слово `secondary`, в противном случае, выдается сообщение об ошибке: `Secondary can't be same as primary`.  
`Invalid address`

Если по каким-то причинам не удалось удалить адрес, выдается сообщение: `Cannot remove the address`

Если удаление выполнилось, но состояние интерфейса не удалось сохранить, выдается сообщение: `The address was removed, but the state of the interface was not saved. The changes will be lost after reboot.`

### **Просмотр по команде show running-config**

Команда `show running-config` всегда показывает текущее системное состояние интерфейса.

Если адрес на интерфейсе изменен каким-либо образом помимо консоли, то по команде `show running-config` это изменение будет показано. Отсюда возможна ситуация, когда текущий адрес интерфейса отличается от адреса, прописанного в загрузочных скриптах ОС, и это отличие никак не проявляется в `cisco-like` конфигурации:

- если администратор осведомлен о данной ситуации и ему требуется сохранить текущие адреса в загрузочных скриптах, то он может войти в режим настройки консоли и повторно прописать те же самые адреса на сетевых интерфейсах. Это приведет к тому, что эти адреса будут прописаны в загрузочные скрипты
- для предотвращения такой ситуации рекомендуется не смешивать выставление адресов на сетевых интерфейсах с помощью консоли с другими средствами (например, командой `ifconfig`).

Если на интерфейсе присутствует адрес `0.0.0.0/0` (нулевой адрес с нулевой маской) наряду с другими, то по команде `show running-config` он не показывается.

Если на интерфейсе отсутствуют адреса или присутствует только адрес `0.0.0.0/0`, то по команде `show running-config` для данного интерфейса показывается команда

`no ip address.`

### **Отличие данной команды от подобной команды Cisco IOS:**

- после команды `no ip address` данный интерфейс выключается
- нельзя задать `secondary` адрес, не задав перед этим `primary` адрес.

## ip access-group (interface)

Команда `ip access group` применяется для привязки списка доступа к интерфейсу, который будет контролироваться на этом интерфейсе. Данная команда используется в режиме `interface configuration`. Для удаления списка доступа используется та же команда с префиксом `no`.

<b><u>Синтаксис</u></b>	<b><code>ip access-group</code></b> {access-list-number   access-list-name} <b><code>in</code></b> <b><code>no ip access-group</code></b> {access-list-number   access-list-name} <b><code>in</code></b>
<code>access-list-number</code>	номер списка доступа, который является числом из диапазона 1-199 или 1300-2699.
<code>access-list-name</code>	имя списка доступа.
<b><code>in</code></b>	список доступа для входящего трафика

**Значение по умолчанию**                      Значение по умолчанию отсутствует

**Режимы команды**                              Interface configuration

### **Рекомендации по использованию**

Команда `ip access group` применяется для привязки списка доступа к интерфейсу. Список доступа будет использоваться для фильтрации трафика на данном интерфейсе.

В команде

```
ip access-group {access-list-number | access-list-name} in
```

список доступа указывает входящий трафик. По этому списку доступа производится фильтрация как исходящего так и входящего трафика на интерфейс.

Задание команды в виде

```
ip access-group {access-list-number | access-list-name} out
```

не допускается.

Если указан несуществующий список доступа, то все поступающие пакеты на интерфейс будут пропущены.

### **Отличие данной команды от подобной команды Cisco IOS:**

- в Cisco IOS исходящий с роутера трафик не фильтруется, в CSP VPN Gate исходящий трафик фильтруется
- при использовании фильтрующих списков доступа `access-lists` на `crypto` интерфейсах, выполняются следующие правила:
  - в отличие от IOS, такие `access-lists` дважды не проверяются. В CSP VPN Gate ACL фильтрации и шифрования рассматриваются совместно, при конвертации их в "Native-конфигурацию" в ней создается единый список правил обработки пакетов (`pass`, `encrypt/decrypt`, `drop`), который применяется один раз
  - фильтрация пакетов, не попадающих в `Crypto ACL`, работает естественным образом (как будто `crypto map` не приложена к интерфейсу)
  - формально говоря, фильтровать трафик, идущий внутри туннеля, на `crypto` интерфейсе нельзя. При построении LSP считается, что в `crypto` туннель будут попадать пакеты, разрешенные и в `crypto` и фильтрующем `access-lists`. IPsec SA строятся также с учетом этого пересечения

- во входном фильтрующем ACL не требуется явным образом разрешать ESP, AH и IKE. Имеет смысл сразу разрешить тот же трафик, который перечислен в Crypto ACL.

Не представляет сложностей фильтровать трафик, вышедший из туннеля на другом (не крипто) интерфейсе. Нужно только правильно учитывать направление ACL – “in”.

### **Пример**

Ниже приведен пример назначения списка доступа 33 интерфейсу fastethernet:

```
Router(config)#interface fastethernet 0/1  
Router(config-if)#ip access-group 33 in
```

## crypto map (interface)

Команда `crypto map` применяется для привязки криптографической карты к интерфейсу. Данная команда используется в режиме `interface configuration`. Для удаления связи криптографической карты с интерфейсом используется та же команда с префиксом `no`.

### Синтаксис

`crypto map map-name`

`no crypto map [map-name]`

map-name

имя криптографической карты.

### Значение по умолчанию

Значение по умолчанию отсутствует

### Режимы команды

Interface configuration

### Рекомендации по использованию

Используйте эту команду для назначения интерфейсу криптографической карты, которая будет использоваться для защиты трафика. Интерфейсу может быть назначена только одна криптографическая карта. Если создано несколько криптографических карт с одним именем, но с разными порядковыми номерами записей, то они будут считаться частями одной криптографической карты. Первыми будут применяться записи криптографических карт, имеющие высший приоритет (минимальное значение порядкового номера).

Crypto ACL ведут себя так же, как в IOS:

- можно указывать правила как по IP-адресу, так и по TCP/UDP- протоколу (без заметной потери производительности). Также можно назначать диапазон "range" портов, помня при этом, что CSP VPN Gate будет создавать отдельные SA для каждого порта
- при использовании строк с "deny" – соответствующие пакеты будут пропускаться без шифрования (на правила создания SA эти строки не влияют).

### Пример

Ниже приведен пример назначения криптографической карты "mymap" интерфейсу fastethernet:

```
Router(config)#interface fastethernet 0/1
```

```
Router(config-if)#crypto map mymap
```

## crypto ipsec df-bit (interface)

Команда `crypto ipsec df-bit` используется для установки DF-бита во внешнем заголовке пакета после IPsec инкапсуляции в туннельном режиме. Установка распространяется на один конкретный интерфейс. Команда доступна в режиме настройки интерфейса.

### Синтаксис

`crypto ipsec df-bit {clear | set | copy}`

`no crypto ipsec df-bit`

<b>clear</b>	DF-бит внешнего IP-заголовка будет очищен и пакет может быть фрагментирован после IPsec инкапсуляции
<b>set</b>	DF-бит внешнего IP-заголовка будет установлен, фрагментация пакета запрещена
<b>copy</b>	DF-бит внешнего IP-заголовка устанавливается в то же значение, какое было у оригинального пакета.

### Значение по умолчанию

значение DF-бита, установленное в глобальном конфигурационном режиме .

### Режимы команды

Interface configuration

### Рекомендации по использованию

Используйте команду `crypto ipsec df-bit` в режиме настройки интерфейса для установки бита DF в пакетах, проходящих через данный интерфейс.

Эта команда аннулирует установки DF-бита для данного интерфейса, выполненные в глобальном конфигурационном режиме.

При возникновении проблем с передачей больших пакетов (например, если по какой-то причине не удастся заставить работать механизм Path MTU Discovery) можно установить параметр `clear` на интерфейсе шлюза CSP VPN Gate, если размер пакета после инкапсуляции превышает значение MTU маршрутизаторов на пути следования IPsec пакета.

Команда `no crypto ipsec df-bit` отменяет установленное значение DF-бита для интерфейса и начинает действовать значение DF-бита, установленное по умолчанию (в глобальном конфигурационном режиме значение DF-бита устанавливается командой `crypto ipsec df-bit`).

### Пример

Ниже приведен пример как установить DF-бит в заголовке пакетов, проходящих через конкретный интерфейс:

```
Router(config-if)#crypto ipsec df-bit set
```

## mtu (interface)

Команда `mtu` применяется для задания значения MTU на интерфейсе - максимальный размер пакета, передаваемый без фрагментации через интерфейс. Команда используется в режиме `interface configuration`. Для задания значения по умолчанию используется та же команда с префиксом `no`.

### Синтаксис

`mtu bytes`

`no mtu`

bytes

диапазон значений 68 – 65535 байт.

### Значение по умолчанию

1500

### Режимы команды

Interface configuration

### Рекомендации по использованию

Команда `mtu` выставляет значение MTU для данного интерфейса (может не совпадать с `ip mtu`).

Команда `mtu` выполняется после ввода немедленно и заданное значение MTU сохраняется в загрузочных скриптах ОС.

На конкретном сетевом интерфейсе допустим не весь диапазон значений 68 – 65535 байт, а только его конкретная часть (зависит от интерфейса).

При выходе за границы диапазона допустимых значений выдается сообщение об ошибке и команда игнорируется.

Команда `mtu` выполняется даже в том случае, если данное значение MTU уже присутствует на интерфейсе. Это сделано для того, чтобы избежать ситуацию, когда текущее значение MTU на интерфейсе не совпадает с MTU, записанным в загрузочных скриптах. В этом случае введенная команда принудительно запишет указанное значение MTU в загрузочные скрипты.

Команда `no mtu` аналогична команде: `mtu 1500`, устанавливает значение по умолчанию.

В случае ошибки выдается сообщение: `Cannot set MTU`.

Если MTU было выставлено, но состояние интерфейса не удалось сохранить, выдается сообщение:

```
MTU was set, but the state of the interface was not saved
The changes will be lost after reboot.
```

По команде `show running-config` значение по умолчанию не показывается.

По команде `show running-config` выдается текущее системное значение, которое может отличаться от значения, записанного в загрузочных скриптах ОС.

### Отличие данной команды от подобной команды Cisco IOS:

- диапазон значений MTU не зависит от типа интерфейса
- нижняя граница диапазона MTU отличается от диапазона в Cisco IOS – 64
- значение по умолчанию может не совпадать со значениями по умолчанию, установленными для интерфейсов в Cisco IOS, так как там это значение зависит от типа интерфейса. Совпадает только для интерфейсов типа Ethernet и Serial.

## crypto ipsec df-bit (global)

Команда `crypto ipsec df-bit` используется для установки DF-бита для заголовка инкапсуляции в туннельном режиме. Установка распространяется на все интерфейсы CSP VPN Gate. С префиксом `no` команда устанавливает значение по умолчанию. Команда доступна в режиме глобальной настройки конфигурации.

### Синтаксис

`crypto ipsec df-bit {clear | set | copy}`

`no crypto ipsec df-bit`

### **clear**

DF-бит внешнего IP-заголовка будет очищен и шлюз может фрагментировать пакет после IPsec инкапсуляции

### **set**

DF-бит внешнего IP-заголовка будет установлен, фрагментация пакета будет запрещена

### **copy**

DF-бит внешнего IP-заголовка устанавливается в то же значение, какое было у оригинального пакета.

### Значение по умолчанию

По умолчанию установлено значение `copy`.

### Режимы команды

Global configuration

### Рекомендации по использованию

Используйте команду `crypto ipsec df-bit` в режиме глобальной настройки конфигурации вашего шлюза в части установки параметра DF-бит.

При возникновении проблем с передачей больших пакетов (например, если по какой-то причине не удастся заставить работать механизм Path MTU Discovery) можно установить параметр `clear` на шлюзе CSP VPN Gate, если размер пакета после инкапсуляции превышает значение MTU интерфейса на пути следования IPsec пакета.

### Пример

Ниже приведен пример как очистить поле DF bit в пакетах, проходящих через все интерфейсы:

```
Router(config)#crypto ipsec df-bit clear
```

# Игнорируемые команды

Команды, перечисленные в этом разделе, при правильном синтаксисе вводятся без ошибок, но игнорируются и никак не влияют на работу консоли (в том числе не отображаются по команде show running-config).

## Управление XAuth и AAA:

```
crypto map <map-name> client authentication list <list-name>
crypto map <map-name> isakmp authorization list <list-name>
aaa authorization network <list-name> local
aaa authorization network default local
```

## Текстовые комментарии:

ACLs (standard и extended):

```
remark <remark>
no remark <remark>
```

Interface:

```
description <string>
```

## Управление QoS:

QoS preclassification (режим настройки crypto map). У нас данный режим работает всегда:

```
qos pre-classify
```

## Команды работы с конфигурацией:

```
write memory
```

## Команды работы с терминалом:

```
terminal no editing
```

## Настройка CA-сертификатов:

```
enrollment mode ra
enrollment retry count <1-100>
enrollment retry period <1-60>
enrollment url <url>
serial-number [none]
ip-address none | <ip-address> | <interface>
password
auto-enroll
rsakeypair <key-label> [ <key-size> [<encryption-key-size>] ]
fqdn none | <name>
```

## Управление паролями:

```
no service password-encryption
```

Примечание: данная команда всегда показывается по команде show running-config (в Cisco IOS – поведение по умолчанию).



**Команды управления перестроением, которые посылает CSM:**

Глобальная:

```
crypto ipsec fragmentation { after-encryption | before-encryption }  
no crypto ipsec fragmentation
```

В режимнастройки интерфейса:

```
crypto ipsec fragmentation { after-encryption | before-encryption }  
no crypto ipsec fragmentation
```