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

Программный комплекс С-Терра Шлюз. Версия 4.1

Руководство администратора

Cisco-like команды

РЛКЕ.00009-01 90 03

16.07.2015

Содержание

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 S-Terra 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 «Программный комплекс С-Терра Шлюз. Версия 4.1. 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 vpngate 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).

Одним из первых действий при работе с cs_console устанавливаются параметры логирования, как и для сервиса vpnsvc (те же самые, что демонстрируются и выставляются с помощью утилиты log_mgr см. документ «Специализированные команды»).

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 «Программный комплекс С-Терра Шлюз. Версия 4.1. 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 `truspoint` с именем `s-terra_technological_trustpoint`. Если этот `trustpoint` отсутствует, он создается автоматически.

Также при старте консоли происходит синхронизация описания preshared 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.

При запуске утилиты ***cs_console*** возможны ошибки, которые выдаются на консоль:

Таблица 1

Текст сообщения	Пояснение
ERROR: failed to read cs_conv.ini[:	Не удалось прочитать файл настроек cs_conv.ini

<reason>] где <reason> (если присутствует) один из:	Возможная причина:
product was damaged or not installed	продукт поврежден или некорректно установлен
file has invalid format	файл имеет неправильный формат (вероятно допущена ошибка при редактировании)
integrity check failed	не пройдена проверка целостности (одна из возможных причин – файл был отредактирован, при этом не был сделан вызов integr_mgr calc -f /opt/VPNagent/etc/cs_conv.ini)
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.

При старте cs_console читается файл `/etc/ifaliases.cf`.

cs_console воспринимает алиасы интерфейсов (параметр "`name`") следующих форматов:

- `FastEthernet<n>/<m>`
- `GigabitEthernet<n>/<m>`
- `TenGigabitEthernet<n>/<m>`
- `Async<n>`

где `<n>` и `<m>` – произвольные неотрицательные числа. Пробелы в данных форматах не допускаются.

Интерфейс с алиасом "`default`" игнорируется без выдачи дополнительных сообщений.

Если присутствуют интерфейсы с алиасами, не попадающими в вышеперечисленные форматы, они игнорируются с выдачей предупреждения на консоль:

```
Warning: Interface(s) <interface_list> ignored due to incompatible name
format
```

где `<interface_list>` – список алиасов интерфейсов, которые проигнорированы cs_console.

Для работы cs_console необходимо, чтобы присутствовал хотя бы один интерфейс с подходящим алиасом. В противном случае cs_console завершит работу с выдачей сообщения об ошибке:

```
ERROR: At least one interface with compatible name must be present in
file "/etc/ifaliases.cf".
```

Присутствующие на момент старта консоли физические сетевые интерфейсы распределяются по зачитанным логическим интерфейсам.

Если параллельно с запущенной cs_console были произведены действия, которые привели к появлению или исчезновению сетевых интерфейсов, то возможна рассинхронизация между реальным состоянием системы и его отображением в cs_console. При возникновении таких ситуаций, рекомендуется выйти и снова войти в cs_console.

При старте cs_console производится проверка соответствия пользователей операционной системы и пользователей, указанных в Cisco-like конфигурации. Возможные ситуации и действия, выполняемые cs_console описаны в Таблица 2.

Таблица 2

Присутствие пользователя в Cisco-like конфигурации	Присутствие пользователя в системе	Совпадение пароля в Cisco-like конфигурации и в системе	Указание cs_console в качестве shell у пользователя	Действие cs_console
+	+	+	+	Ничего не делается
+	+		*	Смена пароля в системе (Cisco-like конфигурация имеет приоритет)
+	+	*		Смена shell на cs_console
+		N/A	N/A	Создание пользователя (аналогично ручному вводу команды)
	+	N/A	+	Только при соблюдении следующих условий: а) Формат имени пользователя соответствует допустимому в команде `username`. б) У пользователя установлен непустой пароль. Добавление пользователя в Cisco-like конфигурацию. Использование зашифрованного пароля, зарегистрированного в системе. Выставление для пользователя минимального уровня привилегий (0). Дополнительно в этом случае на консоль выдается предупреждение следующего вида: % Warning: User(s) <user-list> were automatically added to configuration. Zero privilege level was assigned to them. где <user-list> – список пользователей, автоматически добавленных в Cisco-like конфигурацию.
	+	N/A		Ничего не делается

Примечания:

Звездочка (*) обозначает, что для данной строки условие не важно.

N/A обозначает, что для данной строки условие неприменимо.

Если на старте выполняется какое-либо действие с пользователями, информация об этом действии выдается в лог.

Если при попытке сменить shell пользователя произошла какая-то ошибка, пользователь не добавляется в Cisco-like конфигурацию. На консоль выдается сообщение об ошибке:

```
% User "<username>" shell change failed.
```

Если при других действия произошла ошибка, пользователь также не добавляется в Cisco-like конфигурацию. На консоль выдается сообщение об ошибке, аналогичное сообщению, выдаваемому в подобной ситуации при попытке ручного добавления пользователя.

Удаленная настройка по SSH

Создание локальной политики безопасности для шлюза S-Terra Gate можно осуществить удаленно при помощи консоли по протоколу SSH1 или SSH2.

Настройку шлюза проводите под защитой IPsec. Для этой цели после инсталляции S-Terra 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 S-Terra Gate 4.1 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.

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 S-Terra Gate;
- клиентского терминального приложения, используемого для подключения к консоли.

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: 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 таблице.

Таблица 3

Символ	Название	Действие
Команды перемещения курсора		
`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.
Вызов подсказки		
`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.
Команды работы с историей		
`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 ↑.
Команды удаления		
`Ctrl-H,` `Delete, Backspace`	Delete to the left	Удаляет символ слева от курсора.
`Ctrl-D`	Delete	Удаляет символ над курсором.

Ctrl-K	Delete line forward	Удаляет все символы от курсора до конца строки.
Ctrl-U, Ctrl-X	Delete line backword	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.
Преобразование букв		
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.
Перестановка символов		
Ctrl-T	Transpose	Меняет местами символ слева от курсора и символ над курсором.
Ввод непечатных символов		
Ctrl-V, ESC Q	Ignore editing	Следующий введенный символ будет воспринят не как команда редактирования, а как часть вводимой пользователем команды.
Завершение ввода команды		
Ctrl-J, Ctrl-M, Enter	Execute	Ввод команды.
Повторный показ командной строки		
Ctrl-L, Ctrl-R	Redisplay Line	Повторно показать prompt и содержимое командной строки.

Особенности ввода числовых значений

Значение, состоящее только из десятичных цифр и не начинающееся с нуля, трактуется как десятичное число.

Значение, начинающееся с символов 0x или 0X и, далее, состоящее только из шестнадцатеричных цифр (0-9, A-F, a-f), трактуется как шестнадцатеричное число.

Значение, начинающееся с нуля, и, далее, состоящее только из восьмеричных цифр (0-7), трактуется как восьмеричное число.

Допускаются специальные значения:

08 или 0…08 трактуется как число 8,

09 или 0…09 трактуется как число 9,

где 0…0 – произвольное количество идущих подряд нулей. В Cisco IOS используется более широкое правило ввода: число, начинающееся с нуля и содержащее в себе цифры 8 и/или 9, трактуется как десятичное. В cs_console значения такого рода, например 087, 099, кроме специально отмеченных 08, 0…08, 09, 0…09, не допускаются.

Некоторые примеры трактовки введенных числовых значений приведены в таблице.

Вводимое значение	Результат (в десятичном виде)
0	0
1	1
129	129
0XAB	171
0x1f	31
010	8
077	63
08	8
09	9

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. Подробнее см. раздел «Конвертор VPN политики» в отдельном документе «Программный комплекс С-Терра Шлюз. Версия 4.1. Приложение».

Если при записи Cisco-like конфигурации в базу локальных настроек произошла ошибка, на консоль выдается одно из следующих сообщений, приведенных в Таблица 4.

Данные сообщения свидетельствуют о серьезной проблеме в работе cs_console. При их появлении рекомендуется перезапустить консоль (возможна потеря данных). При стабильном появлении данных сообщений рекомендуется обратиться в службу технической поддержки.

Таблица 4

Сообщение	Пояснение
% Configuration save failed: memory allocation error	Не удалось сохранить конфигурацию: ошибка распределения памяти
% Configuration save failed: input/output error	Не удалось сохранить конфигурацию: ошибка ввода/вывода
% Configuration save failed	Не удалось сохранить конфигурацию: неизвестная ошибка

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

Существует три режима настроек, в которых могут выполняться только определенные команды:

- Стандартный режим (EXEC) – выполняются в основном команды, позволяющие получить информацию о модели аппаратной платформы, версии программного обеспечения и версии установленного продукта, а также уровне привилегий пользователя.
- Привилегированный режим (privileged EXEC) – расширен список информационных команд, доступны команды настройки терминала, системные команды, команды управления соединениями и расписанием, команды работы с конфигурацией.
- Глобальный конфигурационный режим – выполняются команды, задающие политику безопасности.

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).

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 неправомочное 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.

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.

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	**show version** [| **include** {line_to_include}]
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


S-Terra GATE1000 build 4.1.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:

```
S-Terra GATE build 4.1.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 S-Terra 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 S-Terra Gate. Аналогичной команды в Cisco IOS не существует.

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

`S-Terra <product—type> build 4.1.xxxx,`

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

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

`S-Terra GATE build 4.1.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 S-Terra Gate, типе и номере сборки используйте команду из *конфигурационного режима* **`do show version csp`**.

Пример

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

```
Router> show version csp
S-Terra Gate 1000 build 4.1.7539
```


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 или отображения сообщений при загрузке конфигурации используйте команду `show load-message`.

Синтаксис **`show load-message`**

Эта команда не имеет аргументов или ключей.

Режимы команды privileged EXEC

Рекомендации по использованию

Информация, выдаваемая по данной команде, меняется в следующих случаях:

- При загрузке конфигурации из базы локальных настроек при старте cs_console.
- При загрузке конфигурации из файла с помощью команды `configure replace`

  В указанных двух случаях команда дублирует сообщения, которые уже выводились на консоль при загрузке конфигурации (может быть полезно при большом объеме выводимой информации).
- При выходе из конфигурационного режима в том случае, если при этом был вызван конвертор VPN политики.

  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.

При выводе информации о сетевых интерфейсах (команда “interface”) возможен вывод дополнительной информационной строки в формате комментария, сигнализирующей об одной из нестандартных ситуаций:

- Данный сетевой интерфейс не соответствует ни одному физическому:

  interface <interface_name>

  ! Warning: no physical interface found (pattern "<pattern>")

  здесь и далее:

  <interface_name> – алиас интерфейса;

  <pattern> – шаблон для имени интерфейса в системе.

- Все физические интерфейсы, соответствующие данному интерфейсу, не контролируются IPsec драйвером:

  interface <interface_name>

  ! Warning: the IPsec driver is not present on the interface (pattern "<pattern>")

  Следует учитывать, что при наличии такого сообщения на указанном интерфейсе не будет производиться обработка трафика (IPsec, Firewall, QoS).

  Если <pattern> соответствует двум и более физическим интерфейсам, и хотя бы один из них контролируется IPsec драйвером, данное предупреждение не выдается.

  В ОС Linux данное сообщение не должно возникать – его появление свидетельствует об ошибочной ситуации.

- Ошибка при обращении к IPsec драйверу:

  interface <interface_name>

  ! ERROR: Can't connect to the IPsec driver

Появление этого сообщений об ошибке в выводе `show running-config`, свидетельствует о нештатной работе продукта.

Примечание: указанные в данном разделе сообщения специфичны для cs_console и не имеют аналогов в Cisco IOS.

По команде show running-config показываются настройки протоколирования событий, актуальные в данный конкретный момент для сервиса vpnsvc. При этом возможна рассинхронизация в следующей ситуации:

- Параллельно, с уже запущенной cs_console, была вызвана утилита log_mgr для изменения настроек протоколирования событий
- данные настройки будут выставлены для сервиса vpnsvc, но не для cs_console
- однако по команде show running-config будут показаны именно новые настройки (выставленные с помощью log_mgr).

Для того, чтобы избежать подобных ситуаций рекомендуется не запускать параллельно cs_console и утилиту log_mgr с командами set и set-syslog.

При выводе команд настройки протоколирования событий по команде show running-config возможны следующие сообщения об ошибках, свидетельствующие о серьезных проблемах с cs_console (например, пропадание связи с сервисом vpnsvc):

- Вместо команды logging trap

  ! Error: Can't get the logging level value – не удалось получить уровень лога.

  ! Error: Unknown logging level value: <n> – получено некорректное значение уровня лога

- Вместо команд logging on / logging facility / logging host

  ! Error: Can't get the syslog parameters – не удалось получить параметры syslog

- Вместо команды logging facility

  ! Error: Unknown logging facility value: <m> – Получено некорректное значение facility

При получении этих сообщений рекомендуется прервать работу с cs_console и запустить ее заново.

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 для 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.

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]
   ```

   - 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
```


show substitution gui

Команда `show substitution gui` используется для вывода на экран списка соответствия алгоритмов в Cisco-like командах с именами в стиле GUI.

Синтаксис **`show substitution gui`**

Значение по умолчанию Значение по умолчанию отсутствует.

Режимы команды privileged EXEC

Рекомендации по использованию

Команда в основном является служебной и используется для работы с Web-based графическим интерфейсом управления (GUI).

Формат строки вывода: `<Algorithm_type> <Cisco_like_algorithm_name> "<GUI_like_algorithm_name>" [CombinedAlg] [default]`

`<Algorithm_type>` – одно из значений:

- ike-auth
- ike-hash
- ike-cipher (примечание: относится как к CipherAlg, так и к CombinedAlg)
- ike-group
- ah-integrity
- esp-integrity
- esp-cipher (примечание: относится как к CipherAlg, так и к CombinedAlg)
- pfs-group

`<GUI_like_algorithm_name>` – имя метода аутентификации, алгоритма или группы в стиле GUI. Заключается в двойные кавычки.

Например: “PRE SHARE”, “SHA1”, “GOST”, “ESP 3DES”, “AH MD5 HMAC” и т.п.

Внутри имени не допускаются двойные кавычки.

Слово `default` обозначает, что данный алгоритм или группа являются значением по умолчанию при создании в GUI новой ISAKMP Policy или IPsec Transform Set.

Слово `CombinedAlg` (допустимо для ike-cipher и esp-cipher) обозначает тип CombinedAlg.

В случае esp-cipher для GUI работа с ним отличается от обычного esp-cipher тем, что данный алгоритм нельзя сочетать с esp-integrity.

В случае ike-cipher для GUI специальные требования отсутствуют.

В GUI должна присутствовать отдельная проверка на имя esp-null (тип esp-cipher): данный алгоритм можно выставлять только вместе с esp-integrity. Других завязок на имена алгоритмов нет.

`<Cisco_like_algorithm_name>` – имя алгоритма или группы в синтаксисе Cisco-like команд.

Внутри имени не допускаются пробелы или табуляции.

Если требуется описать команду, состоящую из двух слов (например “aes 192”), вместо пробела пишется знак подчеркивания. Например: “aes_192”.

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 удается получить ширину терминала, то устанавливается значение 511.

Рекомендации по использованию

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

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.

Для установки числа символьных столбцов экрана терминала в текущей сессии из *конфигурационного режима* используется команда **`do terminal width`**.

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 поэкранно 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.

Для установки числа строк экрана терминала в текущей сессии из *конфигурационного режима* используется команда **`do terminal length`**.

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	**run** {command}
command	команда, предназначенная для выполнения командным интерпретатором. Для шлюза используется командный интерпретатор `sh`, 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-|**. Эта команда посылает SIGKILL – неперехватываемый 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`.

Синтаксис **`ping`** {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-|`**. Эта команда посылает SIGKILL – неперехватываемый 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 Statistisc----------------
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 начение 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 2Fe034RYzgb7xbt2pYxcpA==
```

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»: **username** {name} [**privilege** level] **password 0 0**. При выводе `no show running-config` 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 воспринимается как команда редактирования (например, сменить пароль, privilege и т.п.), если пользователь уже присутствует в конфигурации и в системе. При добавлении нового пользователя или изменении пароля существующего, добавляются или изменяются данные пользователей операционной системы.

Если пользователь с указанным в команде именем уже присутствует в ОС, но не представлен в Cisco-like конфигурации, то далее выполняется проверка, зарегистрирована ли cs_console в качестве shell данного пользователя:

- Если в качестве shell данного пользователя выставлена cs_console, то данный пользователь добавляется в Cisco-like конфигурацию.

  При этом на консоль выдается сообщение:

  Warning: User "<username>" already exists in the system. It was reused.

  Пользователю выдается пароль, заданный в команде username. Если предыдущий пароль пользователя в системе отличался от нового, он будет потерян.

- Если у данного пользователя выставлен другой shell, команда создания пользователя завершается с ошибкой.

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 шлюз безопасности.

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

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`:

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

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 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. 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).

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.

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.

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 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.

Если пользователь с указанным в команде именем уже присутствует в ОС, но не представлен в Cisco-like конфигурации, то далее выполняется проверка, зарегистрирована ли cs_console в качестве shell данного пользователя:

- Если в качестве shell данного пользователя выставлена cs_console, то данный пользователь добавляется в Cisco-like конфигурацию.

  При этом на консоль выдается сообщение:

  Warning: User "<username>" already exists in the system. It was reused.

  Пользователю выдается пароль, заданный в команде username. Если предыдущий пароль пользователя в системе отличался от нового, он будет потерян.

- Если у данного пользователя выставлен другой shell, команда создания пользователя завершается с ошибкой.

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 шлюз безопасности. 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.

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`:

- Пользователь успешно удален из системы: команда завершается успешно и пользователь удаляется из Cisco-like конфигурации.
- Пользователя в системе не существует: команда также завершается успешно, и пользователь удаляется из Cisco-like конфигурации.
- 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 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).

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.

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
```


username privilege

Для изменения уровня привилегий существующего пользователя, используйте команду `username privilege`.

Синтаксис **`username`** {name} [**`privilege`** level]

`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.

Режимы команды Global configuration

Рекомендации по использованию

Данная команда меняет уровень привилегий пользователя, присутствующего в конфигурации.

Если попытаться выполнить команду для пользователя, отсутствующего в Cisco-like конфигурации, будет выдано сообщение об ошибке:

```
% User "<name>" not found
```

Отличие данной команды от подобной команды Cisco IOS:

В Cisco IOS если пользователь отсутствует, то он будет создан с указанным уровнем привилегий.

Команды настройки протоколирования событий

Настройки протоколирования событий читаются при старте cs_console из сервиса vpnsvc.

Если между двумя запусками cs_console настройки менялись с помощью утилиты log_mgr (log_mgr описана в документе «Специализированные команды»), будут отображены новые настройки, выставленные с помощью этой утилиты.

При вводе команд настройки протоколирования событий, изменения в настройках протокола событий консоли вступают в силу немедленно. Также немедленно вступают в действие аналогичные изменения настроек протоколирования и для сервиса vpnsvc.

Настройки протоколирования событий не влияют на Native-конфигурацию.

Команды logging on, logging facility и logging host имеют внутренние зависимости. При вводе любой из трех команд выполняются следующие действия:

- читаются текущие настройки syslog для сервиса vpnsvc (включено/выключено, facility, адрес получателя syslog);
- в настройках меняется один из параметров (в зависимости от команды);
- далее настройки выставляются для cs_console и для vpnsvc.

Если произошла рассинхронизация из-за того, что параллельно с уже запущенной cs_console была вызвана утилита log_mgr для изменения настроек протоколирования событий, то вызов любой из этих команд восстановит эту синхронизацию. При этом остальные два параметра (не относящиеся к данной команде) будут выставлены для cs_console в значение, полученное из сервиса vpnsvc.

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`. Аргумент `ip-address` в команде `no logging` должен совпадать с IP-адресом хоста уже существующего в конфигурации, иначе команда не выполняется с диагностикой `% No such logging host`.

Если задана команда `logging 127.0.0.1`, то она не показывается по команде `show running-config`.

Команда `no logging` не поддерживается.

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`.

Сообщения об ошибках при выполнении данной команды, свидетельствующие о серьезных проблемах с cs_console (например, пропадание связи с сервисом vpnsvc) приведены в нижеследующей таблице. При их получении рекомендуется прервать работу с cs_console и запустить ее заново.

Сообщение	Пояснение
% Can't set logging host for cs_console	Не удалось выставить получателя лога для cs_console.
% Can't set logging host	Не удалось выставить получателя лога в сервисе vpnsvc.
% Can't set logging host: can't get the syslog parameters	Не удалось выставить получателя лога: невозможно получить существующие параметры логирования.

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 facilicy`. 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`.

Возможные сообщения об ошибках при выполнении команды logging facilicy приведены в таблице. Сообщения свидетельствуют о серьезных проблемах с cs_console (например, пропадание связи с сервисом vpnsvc). При их получении рекомендуется прервать работу с cs_console и запустить ее заново.

Сообщение	Пояснение
% Internal error: unknown facility name	Внутренняя ошибка: неизвестное имя facility. Примечание: данное сообщение может свидетельствовать о повреждении ресурсных файлов cs_console.
% Can't set syslog facility for cs_console	Не удалось выставить facility для cs_console.

% Can't set syslog facility logging	Не удалось выставить facility в сервисе vpnsvc.
% Can't set syslog facility: can't get the syslog parameters	Не удалось выставить facility: невозможно получить существующие параметры логирования.

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.

Возможные сообщения об ошибках при выполнении команды logging trap приведены в нижеследующей таблице. Сообщения свидетельствуют о серьезных проблемах с cs_console (например, пропадание связи с сервисом vpnsvc). При их получении рекомендуется прервать работу с cs_console и запустить ее заново.

Таблица 5

Сообщение	Пояснение
% Internal error: unknown logging level name	Внутренняя ошибка: неизвестное имя severity. Примечание: данное сообщение может свидетельствовать о повреждении ресурсных файлов cs_console.
% Can't set logging level for cs_console	Не удалось выставить уровень лога для cs_console.
% Can't set logging level	Не удалось выставить уровень лога в сервисе vpnsv.c

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 немедленно после ввода команды отключается логирование в cs_console и в сервисе vpnsvc.

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.

Возможные сообщения об ошибках приведены в нижеследующей таблице. Эти сообщения свидетельствуют о серьезных проблемах с cs_console (например, пропадание связи с сервисом vpnsvc). При их получении рекомендуется прервать работу с cs_console и запустить ее заново.

Таблица 6

Сообщение	Пояснение
% Can't enable or disable logging for cs_console	Не удалось включить или выключить логирование для cs_console.
% Can't enable or disable logging	Не удалось включить или выключить логирование в сервисе vpnsvc.
% Can't enable or disable logging: can't get the syslog parameters	Не удалось включить или выключить логирование: невозможно получить существующие параметры логирования.

Команды настройки SNMP-сервера

Следует учитывать, что при использовании команд настройки SNMP-сервера, при загрузке конвертированной Native-конфигурации могут возникнуть проблемы (предупреждения), приводящие к неработоспособности введенных настроек SNMP. Рекомендуется при выходе из конфигурационного режима проверить наличие данных проблем с помощью команды `show load-message` или чтения сообщениий протоколирования событий.

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 commutity 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**}] {comminity-string} [**udp-port** {port}]

no snmp-server host {host-addr} [**traps**] [**version** {**1**|**2c**}] {comminity-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 snmp-server community, 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 `{comminity-string}`. Остальные параметры можно не указывать.

Если в команде встречается пара `{host-addr}` и `{comminity-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.

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`.

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 сетевого интерфейса

Значение по умолчанию если значение не задано, то адрес выбирается ОС в зависимости от адреса назначения.

Режимы команды Global configuration

Рекомендации по использованию

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

Если указана данная команда, то в качестве адреса-источника всех SNMP traps прописывается первый адрес указанного интерфейса (primary-адрес).

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 sterragate

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).

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 {gw-ip-addr | interface-name} [distance] [permanent]`

`no ip route prefix mask { gw-ip-addr | interface-name } [distance] [permanent]`

`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
`gw-ip-addr`	IP-адрес шлюза, через который прописывается маршрут
`interface-name`	имя сетевого интерфейса. Сетевой интерфейс должен точно соответствовать конкретному системному интерфейсу. Использование интерфейсов, заданных в файле ifaliases.cf с помощью перечислений или шаблонов не допускается
`distance`	административная дистанция (метрика) имеет разный смысл в разных ОС и в данной команде будет проигнорирована. Поэтому, использовать ее не рекомендуется
`permanent`	обозначение постоянного маршрута. Параметр запоминается и показывается по show running-config, однако реально не используется. Присутствует для совместимости с продуктами управления Cisco.

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. Реальное добавление маршрута осуществляется при прогрузке сконвертированной Native-конфигурации.

Повторное добавление существующего маршрута не считается ошибкой (поведение, аналогичное Cisco IOS).

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 ОС `route add`. Но по команде `show ip route` для данного маршрута будет показано значение `distance`, равное 1.

Удаление

Команда может быть введена только с консоли

Удаление единичного маршрута:

```
no ip route prefix mask { gw-ip-addr | interface-name } [distance]
[permanent]
```

Параметры `distance` и `permanent` игнорируются. Остальные параметры должны точно соответствовать параметрам, которые выдаются по show running-config.

Удаление маршрутов по адресной информации:

```
no ip route prefix mask
```

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
```

Возможные сообщения об ошибках приведены в таблице.

Таблица 7

Сообщение	Пояснение
%No matching route to delete	В команде no ip route задан маршрут, отсутствующий в конфигурации. Сообщение, аналогичное Cisco IOS.
%Inconsistent address and mask	Один из двух случаев: Задан некорректный параметр <mask> (например, 255.0.255.0). Значения <prefix> и <mask> не соответствуют друг другу (например, 192.168.10.10 255.255.255.0). Сообщение, аналогичное Cisco IOS. Ниже в данной таблице приведены сообщения, специфичные для cs_console.

% The network interface must exactly correspond to a system network interface	Попытка прописать маршрут через сетевой интерфейс, заданный в файле ifaliases.cf с помощью шаблона или списка значений.

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.

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:

`crl 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 CA 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.

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.

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, которое было объявлено командой `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.

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 truspoint 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. Теперь 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
06035504061302525310D300B060311400055040A130447494E53310B3009060355
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

`crypto identity` name

`no crypto identity` `name`

`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

dn name_attr1=string1[,name_attr2=string2]

no dn name_attr1=string1[,name_attr2=string2]

`name_attr1` сокращенное наименование атрибутов поля Subject

`string1` значение атрибутов из поля Subject

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

address	используйте этот параметр, если в качестве идентификатора удаленного партнера используется его IP-адрес
hostname	используйте этот параметр, если в качестве идентификатора удаленного партнера используется имя его хоста
0	не шифровать предопределенный ключ. Необязательный параметр, потому что он игнорируется. Ключ всегда не шифруется. Введен для соответствия такой же команде в Cisco IOS.
keystring	предопределенный ключ, представляющий собой строку произвольной комбинации цифро-буквенных символов. Этот ключ должен быть идентичен у обоих партнеров по защищенному взаимодействию.
peer-address	IP-адрес удаленного партнера.
mask	маска подсети, которой принадлежит компьютер удаленного партнера. Используется только при установке параметра `address`. Необязательный параметр. Отсутствие параметра всегда эквивалентно 255.255.255.255.
hostname	имя компьютера удаленного партнера. Имя должно быть задано в связке с именем домена, которому он принадлежит. Например – host.subnet.com.
no-xauth	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. Предопределнный 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.

Не разрешается вводить некорректную маску, например 255.0.255.0. В этом случае выводится сообщение об ошибке:

```
Invalid address-mask pair
```

Если задана маска, не разрешается вводить адрес, не соответствующий маске. Например – 192.168.1.0 255.255.0.0. В этом случае выводится сообщение об ошибке:

```
Invalid address-mask pair
```

Нельзя повторно вводить команду с адресной информацией, уже присутствующей в конфигурации. В этом случае выводится одно из следующих сообщений об ошибке:

```
A pre-shared key for address mask <peer-address> <mask> already exists!
```

```
A pre-shared key for for host <hostname> already exists.
```

Для смены ключа следует сначала удалить старую информацию, а потом ввести новую.

Удаление

Удаление существующего ключа выполняется командой:

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

Адресная информация является единственной значащей в данной команде: `keystring`, а также наличие или отсутствие `no-xauth` игнорируется.

Если ввести команду с адресной информацией, отсутствующей в конфигурации, будет выдано одно из следующих сообщений об ошибке:

ISAKMP: no key for address <peer-address>

ISAKMP: no key for hostname <hostname>.

При выводе текущей конфигурации по `show running-config` производится сортировка команд по следующим правилам:

- первыми пишутся команды “`address`” для отдельных хостов (параметр `mask` отсутствует или равен 255.255.255.255)
- далее пишутся команды “`address`” для подсетей, при этом они сортируются от узких подсетей к широким
- в конце пишутся команды “`hostname`”.

Сортировка адресов для подсетей с одинаковыми масками, а также сортировка по `hostname` не производится (сохраняется порядок ввода команд).

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.
- В Cisco IOS можно ввести адрес, не соответствующий маске.

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

Синтаксис	**ip host** hostname [**additional**] address **no ip host** hostname [**additional**] [address]
hostname	имя хоста партнера. Синтаксис параметра соответствует правилам задания доменного имени (описано в команде `hostname`)
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 предопределенного ключа и привязка его к имени хоста партнера или к его IP-адресу осуществляется командой `crypto isakmp key`.

Если ввести параметр `hostname`, который отсутствует в конфигурации (независимо от IP-адреса), будет выдано сообщение об ошибке:

```
No such hostname
```

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);
- списки доступа привязываются к статической криптографической карте и динамической криптокарте для указания защищенного трафика (команда `match address` при настройке crypto map);
- стандартные нумерованные списки доступа используются для ограничения сервисов (протоколов) (команда `ip port-map`);
- задавать критерий соответствия трафика данному классу (команда `match access-group` при настройке class-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] [log]

no permit source [source-wildcard] [log]

`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

`log` — Флаг `log` задает ведение журнала. В Syslog выдаются сообщения о пакетах, удовлетворяющих условиям данного списка доступа. В сообщении указан номер списка доступа, разрешено или запрещено прохождение пакета, адрес отправителя и количество пакетов. Сообщение формируется для первого совпавшего пакета, а затем с периодичностью в 5 минут выдается сообщение о количестве пропущенных или запрещенных пакетов за этот интервал времени.

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`.

В стандартных списках доступа при последующем вводе наличие или отсутствие модификатора `log` в записи не учитывается при сравнении записей:

Пример:

```
ip access-list standard st-acl-1
 permit  10.20.30.40
 permit  10.20.30.40 log
ip access-list standard st-acl-2
 permit  10.20.30.40 log
 permit  10.20.30.40
```

По `show running-config` будет выдано:

```
ip access-list standard st-acl-1
 permit  10.20.30.40
ip access-list standard st-acl-2
 permit  10.20.30.40 log
```

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`.

Пример удаления записи с модификатором `log`:

```
ip access-list standard st-acl-1
 permit  10.20.30.40
 permit  10.20.30.41 log
!
 no permit  10.20.30.40 log
 no permit  10.20.30.41
```

В результате обе записи в списке доступа будут удалены.

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]] [established] flag-name | {match-any | match-all} {+ | -}flag-name] [log | log-input] [time-range time-range-name]`

`no permit` `protocol source source-wildcard [operator port [port]] destination destination-wildcard [operator port [port]] [established] flag-name |{match-any | match-all} {+ | -}flag-name] [log | log-input] [time-range time-range-name]`

`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 8.

`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 9 и Таблица 10.

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)".
Замечание 3:	Для указания TCP-флагов используется старый или новый формат. Старый формат используется в нумерованных и именованных расширенных списках доступа, и представляет собой комбинацию ключевого слова `established` и перечисления TCP-флагов – flag-name. Новый формат используется только в именованных расширенных списках доступа, и представляет собой комбинацию ключевого слова `match-any|match-all` и и перечисления TCP-флагов – {+|-}flag-name.
`established`	Только для протокола TCP. Состояние соединения. Выделяются только установленные TCP-соединения и по ним могут передаваться данные.
`flag-name`	Имена TCP-флагов – `fin`, `syn`, `rst`, `psh`, `ack`, `urg`. Порядок флагов при вводе не важен. Перечисление флагов работает как «ИЛИ» (аналог `match-any` в новом формате). Ключевое слово `established` эквивалентно флагам `rst ack` и не может с ними сочетаться (синтаксическая ошибка).
Замечание 4:	В пределах одной команды `permit/deny` старый формат указания TCP-флагов не может сочетаться с новым.
`match-any|match-all`	Только для протокола TCP и именованных списков доступа. Указывает условие сравнения TCP-флагов в пакете и правиле. Ключевое слово `match-any` означает, что должно выполняться одно из указанных далее условий по TCP-флагам. Ключевое слово `match-all` означает, что должны выполняться все заданные условия по TCP-флагам. Если попытаться использовать эти ключевые слова для нумерованного списка доступа, то будет выдано сообщение об ошибке: %match-all/match-any are allowed on named ACLs only
`{+|-}flag-name`	Имена TCP-флагов – `fin`, `syn`, `rst`, `psh`, `ack`, `urg`. Префикс “+” перед флагом означает, что этот флаг должен быть выставлен в заголовке пакета, а префикс “–“ означает, что этот флаг не должен быть выставлен в заголовке пакета. Порядок флагов при вводе не важен.
`log|log-input`	Флаг `log` или `log-input` задает ведение журнала. Оба флага задают одну и ту же функциональность (отличие от Cisco IOS). В Syslog выдаются сообщения о пакетах, удовлетворяющих условиям данного списка доступа. В сообщении указан номер списка доступа, разрешено или запрещено прохождение пакета, адрес отправителя и

количество пакетов. Сообщение формируется для первого совпавшего пакета, а затем с периодичностью в 5 минут выдается сообщение о количестве пропущенных или запрещенных пакетов за этот интервал времени.

Флаги логирования могут смешиваться с другими флагами, например с TCP-флагами. Два флага логирования `log` и `log-input` не могут применяться вместе в одной команде `permit/deny`.

`time-range time-range-name` Ссылка на расписание. В расписании указывается диапазон времени, в который будет работать данный список доступа. В другой период времени данный фильтр действовать не будет.

Ссылка на расписание может смешиваться с другими дополнительными параметрами, например с TCP-флагами.

Допускается ссылка на расписание, отсутствующее в конфигурации на момент ввода команды. Однако на момент конвертирования расписание должно существовать, в противном случае конвертирование будет прервано с сообщением об ошибке.

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`.

По команде `show running-config` флаги `fin`, `syn`, `rst`, `psh`, `ack`, `urg` будут указаны в этом порядке. А сочетание флагов «`rst ack`» в команде будет заменено на `established` при выводе.

Флаги логирования `log`, `log-input` показываются после TCP-флагов, а расписание (`time-range`) – после флагов логирования.

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`.

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 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 8

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
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 9

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
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	Nicname	43
www	World Wide Web (HTTP)	80

Поддерживаемые имена портов протокола UDP

Таблица 10

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

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 tacacs-ds	TAC Access Control System Примечание: вторая запись эквивалентна первой, но не показывается в подсказке (аналогично Cisco).	49
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
```

Примеры указания TCP-флагов в старом формате:

```
permit tcp any any established
```



```
permit tcp host 10.10.1.101 host 10.11.1.101 established syn urg
deny tcp any any psh
```

Примеры указания TCP-флагов в новом формате:

```
permit tcp any any match-any +rst +ack
permit tcp host 10.10.1.101 host 10.11.1.101 match-all +syn –fin
permit tcp any any match-any -psh +urg
```

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] [log]
no deny source [source-wildcard] [log]
```

Параметры команды аналогичны параметрам команды "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]] [established] flag-name |{match-any | match-all} {+ | -}flag-name] [log | log-input] [time-range time-range-name]
```

```
no deny protocol source source-wildcard [operator port [port]] destination destination-wildcard [operator[port]] [established] flag-name |{match-any | match-all} {+ | -}flag-name] [log | log-input] [time-range time-range-name]
```

Параметры команды аналогичны параметрам команды "Permit (extended)".

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 `10.11.1.101`:

```
Router(config)#ip access-list extended a101
Router(config-ext-nacl)#deny ip any host 10.11.1.101
```

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

`access-list` `number` **`permit`** | **`deny`** `source [source-wildcard] [log]`

`no access-list` `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.

Все остальные параметры команды были описаны в разделе "Permit (standard)".

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]] [established] flag-name [log | log-input] [time-range time-range-name]`

`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 10.11.1.101 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 10.11.1.101
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 = gost (ГОСТ 28147-89)
hash = gost (ГОСТ Р 34.11-94)
authentication = gost-sig
group = vko (VKO ГОСТ Р 34.10-2001)
lifetime = 86400
```

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.

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`.

Аутентификация может осуществляться с использованием предопределенного ключа (Preshared Key) или с использованием цифровых сертификатов стандарта X.509.

Синтаксис

authentication {**gost-sig** | **rsa-sig** | **dss-sig** | **sign** | **pre-share**}

no authentication {**gost-sig** | **rsa-sig** | **dss-sig** | **sign** | **pre-share**}

gost-sig	аутентификация осуществляется с использованием цифровых сертификатов, созданных по алгоритму ГОСТ Р 34.10-2001
rsa-sig	аутентификация осуществляется с использованием цифровых сертификатов, созданных по алгоритму RSA
dss-sig	аутентификация осуществляется с использованием цифровых сертификатов, созданных по алгоритму DSA
sign	выбор конкретного типа аутентификации (RSA, DSA или ГОСТ) осуществляется по типу CA-сертификата, лежащего в базе
pre-share	аутентификация осуществляется с использованием предопределенных ключей.

Значение по умолчанию **gost-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.

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.

Примечание: при построении соединения между S-Terra Gate и Cisco Router с использованием аутентификации на сертификатах рекомендуется применять метод аутентификации `sign`. В этом случае при конвертировании, для совместимости с Cisco IOS, в Native-конфигурации дополнительно прописывается ссылка на CA-сертификат, лежащий в базе.

Отличие данной команды от подобной команды Cisco IOS:

Не допускается тип аутентификации RSA encryption.

В Cisco IOS поддерживается аутенификация с использованием цифровых сертификатов, созданных только по алгоритму RSA.

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`.

Синтаксис	**encryption** {**gost** | **des** | **3des** | **aes** | **aes 128** | **aes 192** | **aes 256**} **no encryption**
gost	в качестве алгоритма шифрования используется алгоритм ГОСТ 28147-89
des	в качестве алгоритма шифрования используется алгоритм 56bit DES
3des	в качестве алгоритма шифрования используется 168-bit DES-CBC (3DES)
aes|aes 128	в качестве алгоритма шифрования используется 128-bit AES. Значения `aes` и `aes 128` – эквивалентны.
aes 192	в качестве алгоритма шифрования используется 192-bit AES
aes 256	в качестве алгоритма шифрования используется 256-bit AES

Значение по умолчанию **gost**

Режимы команды 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.

Используемые алгоритмы шифрования указываются в файле `cs_conv.ini`.

`No`-форма команды выставляет значение по умолчанию.

По команде `show running-config` команда сокращается до `encr` 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`.

Синтаксис

hash {**gost** | **gost341112-256-tc26** | **gost341112-512-tc26** | **sha** | **md5**}

no hash {**gost** | **gost341112-256-tc26** | **gost341112-512-tc26** | **sha** | **md5**}

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

gost341112-256-tc26 указывает, что в качестве хэш-алгоритма должен использоваться алгоритм ГОСТ Р 34.11-12 с длиной ключа 256 (применяется только при использовании криптобиблиотеки компании «С-Терра СиЭсПи»)

gost341112-512-tc26 указывает, что в качестве хэш-алгоритма должен использоваться алгоритм ГОСТ Р 34.11-12 с длиной ключа 512 (применяется только при использовании криптобиблиотеки компании «С-Терра СиЭсПи»)

sha указывает, что в качестве хэш-алгоритма дожен использоваться алгоритм SHA (HMAC вариант)

md5 указывает, что в качестве хэш-алгоритма должен использоваться алгоритм MD5 (HMAC вариант).

Значение по умолчанию **gost**

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.

Используемые хэш-алгоритмы указываются в файле `cs_conv.ini`.

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

В приведенной ниже таблице (Таблица 11) приведены возможные значения хэш-алгоритма в зависимости от используемого алгоритма публичного ключа сертификата.

Таблица 11

Алгоритм публичного ключа сертификата	Возможные значения хэш-алгоритма
ГОСТ Р 34.10-2001 с длинами открытого/закрытого ключей 512/256 (1.2.643.2.2.19)	gost, gost341112-256-tc26
ГОСТ Р 34.10-2012 с длинами открытого/закрытого ключей 512/256 (1.2.643.7.1.1.1.1)	gost, gost341112-256-tc26
ГОСТ Р 34.10-2012 с длинами открытого/закрытого ключей 1024/512 (1.2.643.7.1.1.1.2)	gost341112-512-tc26

RSA (1.2.840.113549.1.1.1)	md5, sha
DSA (1.2.840.10040.4.1)	sha

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 gost
 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], или VKO GOST R 34.10-2012. Восстановить значения по умолчанию можно с помощью той же команды с префиксом `no`.

Синтаксис	**group** {**vko** | **vko2** | **1** | **2** | **5**} **no group**
vko	используется алгоритм VKO GOST R 34.10-2001, длина ключа 256 бит
vko2	используется алгоритм VKO GOST R 34.10-2012, длина ключа 256 бит. Алгоритм VKO GOST R 34.10-2012 может применяться, только если используется криптобиблиотека, разработанная компанией «С-Терра СиЭсПи»
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 **vko**

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`.

Синтаксис

`crypto isakmp peer` {**`address`** `ip-address`}

`no crypto isakmp peer` {**`address`** `ip-address`}

`ip-address` IP-адрес партнера

Значение по умолчанию значение по умолчанию отсутствует.

Режимы команды 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 10.0.10.1
```


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 10.0.0.1, а IP-адрес локального устройства 10.0.0.2 используются команды:

```
Router(config)#crypto isakmp peer address 10.0.0.1
Router(config-isakmp-peer)#set aggressive-mode client-endpoint ipv4-address 10.0.0.2
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 `crypto isakmp identity {address|dn|hostname}`

`no crypto isakmp identity {address|dn|hostname}`

address устанавливает идентификатор address

hostname устанавливает идентификатор hostname

dn 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` — Задает 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` — Задает 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 isakmp fragmentation

Команда `crypto isakmp fragmentation` включает режим фрагментирования IKE-пакетов. Максимальный размер IP-пакета выставляется в 576 байт[1] (аналогично Cisco IOS). Отключить фрагментирование можно с помощью той же команды с префиксом `no`.

Синтаксис

```
crypto isakmp fragmentation
no crypto isakmp fragmentation
```

Значение по умолчанию по умолчанию фрагментирование IKE-пакетов отключено.

Режимы команды Global configuration

Рекомендации по использованию

Фрагментирование IKE-пакетов необходимо в тех случаях, когда в процессе доставки длинные UDP-пакеты либо не пропускаются промежуточным узлом, либо некорректно фрагментируется на ip-уровне.

[1] Следует учитывать, что операционная система сама устанавливает длину ip-заголовка, что может приводить к фактическому уменьшению длины ip-пакета с IKE-фрагментом на величину до 44 байт (максимально допустимый размер ip-заголовка – 64 байта, наиболее часто используемый – 20 байт)

Команды, устанавливающие время жизни SA

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 наполовину. В этом случае будет действовать ограничение по времени. Пересоздание SA не будет в случае отсутствия трафика между партнерами. Рекомендуется указывать такое время жизни SA в секундах, что бы в основном удаление IPsec SA происходило по времени, а ограничение на объем трафика выбирать как дополнительную меру.

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`.

Примечание

Если при формировании набора преобразований (`crypto ipsec transform-set`) используются алгоритмы ah-gost-28147-mac, esp-gost28147-mac, esp-gost28147, то в этом случае максимальное допустимое значение время жизни SA в килобайтах – 4032 Кб.

При превышении указанного значения для созданного SA, в журнал протоколирования и на консоль будет выдано сообщение, что в созданном IPsec SA ограничение по трафику не соответствует допустимому ограничению для используемого криптографического алгоритма:

```
"SA traffic limit exceeds limitations imposed by the cryptograghic
algorithm"
```

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.

Повторный ввод команды с уже заданным именем `transform-set-name` заменяет набор преобразований.

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

Таблица 12

Тип преобразования	Имя	Описание
AH Transform (один из списка)	ah-md5-hmac	Протокол AH с алгоритмом аутентификации MD5
	ah-sha-hmac	Протокол AH с алгоритмом аутентификации SHA
	ah-gost-28147-mac	Протокол AH с алгоритмом ГОСТ 28147-89 (в режиме выработки имитовставки)
	ah-gost3411-hmac	Протокол AH с алгоритмом ГОСТ Р 34.11-94
ESP Encryption Transform (один из списка)	esp-null	Протокол ESP с алгоритмом Null.
	esp-des	Протокол ESP с 56-битным алгоритмом DES
	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-gost28147	Протокол ESP с алгоритмом ГОСТ 28147-89 (в режиме простой замены с зацеплением)
	esp-gost28147-4m-imit	Протокол ESP с алгоритмом ГОСТ 28147-89 (в комбинированном режиме: гаммирование и вычисление имитовставки. в соответствии со спецификацией ESP_GOST-4M-IMIT)
ESP Authentication Transform (один из списка)	esp-md5-hmac	Протокол ESP с алгоритмом аутентификации MD5
	esp-sha-hmac	Протокол ESP с алгоритмом аутентификации SHA
	esp-gost28147-mac	Протокол ESP с алгоритмом ГОСТ 28147-89 (в режиме выработки имитовставки)

	esp-gost3411-hmac	Протокол ESP с алгоритмом ГОСТ Р 34.11-94

Не допускается, чтобы был единственный ESP transform esp-null (без ESP authenticator). В этом случае выдается сообщение об ошибке:

```
ESP: NULL cipher requires ESP authenticator
```

Удаление

Если при удалении ввести имя несуществующего набора преобразований, будет выдано сообщение об ошибке:

```
Could not find crypto transform set <transform-set-name>
```

Не допускается удаление набора преобразований, на который присутствуют ссылки в статической и/или динамической криптокартах. В подобной ситуации выдается сообщение вида:

```
Transform-set <transform-set-name> is in use by the crypto-map(s):
<crypto-map-name1> <crypto-map-seq-num1>[, <crypto-map-name2> <crypto-
map-seq-num2>...]

Transform-set <transform-set-name> is in use by the dynamic crypto-map
template(s):  <crypto-dynamic-map-name1> <crypto-dynamic-map-seq-
num1>[, <crypto-dynamic-map-name2> <crypto-dynamic-map-seq-num2>...]

First remove the transform-set from the above crypto map(s)/dynamic
crypto map template(s).
```

Отличие данной команды от подобной команды Cisco IOS:

- В Продукте S-Terra Gate отсутствует поддержка преобразования IP Compression Transform.

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-gost-28147-
mac esp-gost28147 esp-gost3411-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 (S-Terra 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
```

Примечание

Если предполагается использовать для авторизации и аутентификации RADIUS-сервер, то одновременно настраивать IKECFG параметры на отдельном С-Терра Шлюзе и на RADIUS-сервере крайне нежелательно:

1. Если будет указан локальный IKECFG пул, то в случае получения данных авторизации от RADIUS-сервера, будут задействованы данные из локального IKECFG пула, а данные от RADIUS-сервера будут игнорироваться.
2. Если RADIUS-сервер выдал Framed-IP-Address (Framed-IP-Address – атрибут RADIUS-сервера, соответствующий IKECFG-адресу, высылаемому С-Терра Шлюзом партнеру), который попадает в один из пулов адресов, задействованных в создаваемой политике безопасности, то С-Терра Шлюз игнорирует авторизационные данные от RADIUS-сервера и пытается установить соединение с партнёром без IKECFG.

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.

Если в разных криптокартах используется привязка к одному и тому же пулу, в этих криптокартах настройки DNS и доменного суффикса должна полностью совпадать. Подробное описание дано для команды `set pool`.

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 шлюз безопасности выдает IP-адрес из IKECFG пула партнеру, при его попытке создать IPsec SA с использованием своего реального IP.

`respond` — по запросу партнера шлюз безопасности 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`. Допускается ввод данной команды, если записи для указываемой криптографической карты отсутствуют.

В данной версии Продукта ввод команды с опцией `initiate` или `respond` либо ввод двух команд с опцияи `initiate` и `respond` приводит к одинаковому поведению шлюза безопасности.

Если в разных криптокартах используется привязка к одному и тому же пулу, в этих криптокартах настройки DNS и доменного суффикса должна полностью совпадать. Подробное описание дано для команды `set pool`.

Команда удаления всего набора записей в криптокарте `no crypto map map-name` удаляет также и все команды `crypto map client configuration address`, относящиеся к данномой криптокарте.

Однако удаление последней нумерованной записи в криптокарте `no crypto map map-name seq-num` не удаляет команды `crypto map client configuration address`.

Отмена привязки:

```
no crypto map map-name client configuration address {initiate | respond}
```

По данной команде удаляется только один из вариантов – `initiate` или `respond`. Если в конфигурации присутствуют оба варианта команды, то для их удаления надо ввести две команды.

Если команда отмены привязки указывается для варианта, отсутствующего в конфигурации, но, при этом, присутствует хотя бы одна запись, относящаяся к данной криптографической карте, то команда игнорируется без вывода сообщения об ошибке.

Если отмены привязки указывается для криптографической карты, который полностью отсутствует в конфигурации, выдается сообщение об ошибке: `Could not find crypto map <map-name>`.

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 1.192.168.11 192.168.11.254
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`.

Синтаксис

`crypto dynamic-map` `map-name` **`client configuration address`** {**`initiate`** | **`respond`**}

`no crypto dynamic-map` `map-name` **`client configuration address`** {**`initiate`** | **`respond`**}

`map-name` — имя динамической криптографической карты.

`initiate` — без запроса партнера шлюз безопасности выдает IP-адрес из IKECFG пула партнеру, при его попытке создать IPsec SA с использованием своего реального IP.

`respond` — по запросу партнера шлюз безопасности 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`.

Допускается ввод данной команды, если записи для указываемой криптографической карты отсутствуют.

В данной версии Продукта ввод команды с опцией `initiate` или `respond`, или ввод двух команд с опцияи `initiate` и `respond` приводит к одинаковому поведению шлюза безопасности.

Если в разных криптокартах используется привязка к одному и тому же пулу, в этих криптокартах настройки DNS и доменного суффикса должна полностью совпадать. Подробное описание дано для команды `set pool`.

Команда удаления всего набора записей в криптокарте `no crypto map map-name` удаляет также и все команды `crypto dynamic-map client configuration address`, относящиеся к данномой криптокарте.

Отмена привязки:

`no crypto dynamic-map map-name client configuration address {initiate|respond}`. По данной команде удаляется только один из вариантов – `initiate` или `respond`. Если в конфигурации присутствуют оба варианта команды, то для их удаления надо ввести две команды.

Если команда отмены привязки указывается для варианта, отсутствующего в конфигурации, но, при этом, присутствует хотя бы одна запись, относящаяся к данной криптографической карте, то команда игнорируется без вывода сообщения об ошибке.

Если отмены привязки указывается для криптографической карты, который полностью отсутствует в конфигурации, выдается сообщение об ошибке: `Could not find crypto map template <dynamic-map-name>`.

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 192.168.11.1 192.168.11.254
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.
ipsec-isakmp	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, пре редактировании уже существующей – можно не указывать.
dynamic	указывает на то, что данная запись ссылается на уже существующий набор динамических криптографических карт, созданных командой `crypto dynamic-map`. 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 `dynamic`.

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 соответствием 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:

`match address`	осуществляет привязку списка доступа к записи криптографической карты
`set pfs`	указывает, что на стадии согласования параметров IPsec для данной записи криптографической карты должна быть затребована опция PFS
`set security-association lifetime`	устанавливает время жизни SA для конкретных записей криптографической карты
`set transform-set`	указывает, какие наборы преобразований (transform set) могут использоваться с данной записью криптографической карты
`set peer`	указывает IPsec партнера для записи криптографической карты
`set identity`	устанавливает списки идентификаторов, которые используются
`set pool`	устанавливает имя пула криптографической карты
`set ip access-group`	устанавливает правила фильтрации, применяемые к входящим IPsec пакетам после декапсуляции, или к исходящим IPsec пакетам до инкапсуляции
`set dns`	задает DNS для IKECFG
`set domain`	задает доменный суффикс для IKECFG
`set client authentication list`	задает ссылку на список аутентификации (при использовании аутентификации пользователя на RADIUS-сервере)
`set client username`	задает способ получения идентификатора пользователя (при использовании аутентификации пользователя на RADIUS-сервере)
`reverse-route`	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

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”.

Команда удаления всего набора записей в криптокарте (криптокарты):

```
no crypto map map-name
```

Дополнительно данная команда удаляет записи `crypto {map | dynamic-map} client configuration address {initiate | respond}`, относящиеся к данной криптокарте.

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 «Приложение», раздел «Конвертор. 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 «Приложение», в разделе «Конвертор. 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 режиме 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.

Замечание:

Запрещено использование ссылок на расписания (time-range) в списках шифрованного доступа, на которые ссылается криптокарта. В случае присутствия подобных ссылок на расписание, конвертирование будет прервано с сообщением об ошибке.

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 ip access-group

Команда `set ip access-group` задает дополнительные правила фильтрации, присоединяемые к IPsec SA. Проверка на соответствие списку доступа выполняется внутри IPsec после декапсуляции и до инакпсуляции пакета.

Для отмены фильтрации используется та же команда, но с префиксом `no`.

Синтаксис

set ip access-group {access-list-number | access-list-name} {**in** | **out**}

no set ip access-group {access-list-number | access-list-name} {**in** | **out**}

access-list-number	номер списка доступа, который является числом из диапазона 1-199 или 1300-2699
access-list-name	имя списка доступа
in	фильтрация применяется для входящего IPsec трафика после декапсуляции
out	фильтрация применяется для исходящего IPsec трафика перед инкапсуляцией.

Режимы команды

Crypto map configuration.

Значение по умолчанию

значение по умолчанию отсутствует.

Рекомендации по использованию

Используйте эту команду для назначения дополнительной проверки IPsec пакетов проходящих через внешний интерфейс по IPsec туннелю, на соответствие заданному списку доступа. Предварительно следует определить этот список доступа с помощью команд `access-list` или `ip access-list`.

Список доступа, назначенный этой командой, будет использоваться для фильтрации трафика, идущего через IPsec туннель, после декапсуляции – для входящего трафика и до инкапсуляции – для исходящего трафика, в зависимости от заданного параметра (`in`/`out`).

Если список доступа содержит модификаторы `log` или `log-input`, то они игнорируются при подсоединении к криптокарте (фильтр работает также, как если бы не содержал данные модификаторы).

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 удается 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** | **vko2** | **group1** | **group2** | **group5**]
	no set pfs [**vko** | **vko2** | **group1** | **group2** | **group5**]
`vko`	используется алгоритм VKO GOST R 34.10-2001 [RFC4357], длина ключа 256 бит
`vko2`	используется алгоритм VKO GOST R 34.10-2012, длина ключа 256 бит. Алгоритм VKO GOST R 34.10-2012 может применяться, только если используется криптобиблиотека, разработанная компанией «С-Терра СиЭсПи»
`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.

Существует ограничение на привязку одного и того же пула к разным криптокартам:

- Если к двум и более криптокартам привязан один и тот же пул, то, независимо от способа привязки пула, необходимо, чтобы в данных криптокартах полностью совпадали настройки DNS серверов и доменных суффиксов по умолчанию:
  - если в одной криптокарте присутствуют команды `set dns` и/или `set domain`, то в другой криптокарте должны быть идентичные команды
  - либо во всех криптокартах соответствующая команда отсутствует. Не допускается, чтобы в одной криптокарте присутствовала команда, а в другой – нет.

Данное требование обязательно как для статических, так и для динамических криптокарт.

Если данное требование не выполняется, конвертирование конфигурации будет прервано с ошибкой вида:

```
Could not convert { crypto map | dynamic crypto map template } "<name1>
<idx1>" . Reason: { crypto map | dynamic crypto map template } "<name2>
<idx2>" references to the same pool ("<pool-name>") but the additional
parameters to send to client are different.
```

где `<namei> <idxi>` – имена и индексы конфликтующих crypto maps или dynamic crypto map templates (примечание: сообщение об ошибке выдается для первой встреченной

конфликтующей пары; в конфигурации могут присутствовать и другие конфликтующие криптокарты); <pool-name> – имя привязанного пула.

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 (S-Terra 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 (S-Terra Gate) командой ip route.

Если адреса пула не пересекаются с адресами внутренней подсети, защищаемой шлюзом (S-Terra 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 cmap привязывается пул с именем pool1, но к 10 записи криптокарты cmap 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 наполовину. 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 **s**`et 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 "mymap":

```
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 "mymap":

```
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
```


set dns (crypto map)

Команда `set dns` используется для задания DNS сервера для IKECFG. Для удаления DNS сервера используется та же команда, но с префиксом `no`.

Синтаксис **`set dns`** `primary-server-ip [secondary-server-ip]`

`no set dns` `[primary-server-ip [secondary-server-ip]]`

`primary-server-ip` IP-адрес основного DNS-сервера;

`secondary-server-ip` IP-адрес резервного DNS-сервера (может отсутствовать).

Режимы команды Crypto map configuration.

Значение по умолчанию нет значения по умолчанию.

Рекомендации по использованию

Команда актуальна только если к данной crypto map привязан пул адресов для IKECFG либо с помощью команды `set pool`, либо с помощью команд `crypto isakmp client configuration address-pool local` и `crypto map | dynamic-map client configuration address`.

Если к crypto map не привязан пул, данная команда игнорируется.

Если в разных криптокартах используется привязка к одному и тому же пулу, в этих криптокартах настройка DNS должна полностью совпадать. Данное требование обязательно как для статических, так и для динамических криптокарт.

Отличие данной команды от подобной команды Cisco IOS:

Данная команда отсутствует в Cisco IOS.

Пример

Допустимая конфигурация:

```
crypto map cmap 10 ipsec-isakmp
 set pool pool1
 set dns 192.168.10.10
 set domain example.com
! ...
crypto dynamic-map dmap 10
 set pool pool1
 set dns 192.168.10.10
 set domain example.com
```

Ошибочная конфигурация:

```
crypto map cmap 10 ipsec-isakmp
 set pool pool1
 set dns 192.168.10.10
 set domain example.com
! ...
```



```
crypto dynamic-map dmap 10
 set pool pool1
 set dns 192.168.10.11 ! Ошибка! Должно совпадать с cmap 10
 set domain example.com
```

set domain (crypto map)

Команда `set domain` используется для задания доменного суффикса по умолчанию для IKECFG. Для удаления доменного суффикса используется та же команда, но с префиксом `no`.

Синтаксис

`set domain` domain-name

`no set domain` [domain-name]

`domain-name` доменный суффикс по умолчанию.

Режимы команды Crypto map configuration.

Значение по умолчанию нет значения по умолчанию.

Рекомендации по использованию

Команда актуальна только если к данной криптокарте привязан пул адресов для IKECFG либо с помощью команды `set pool`, либо с помощью команд `crypto isakmp client configuration address-pool local` и `crypto map | dynamic-map client configuration address`.

Если попытаться ввести имя с некорректным форматом, будет выдано сообщение об ошибке:

```
% Bad hostname format
```

Если в разных криптокартах используется привязка к одному и тому же пулу, то в этих криптокартах настройка доменного суффикса должна полностью совпадать.

Отличие данной команды от подобной команды Cisco IOS:

Данная команда отсутствует в Cisco IOS.

set client authentication list (crypto map)

Команда `set client authentication list` используется для ссылки на список аутентификации. Для удаления ссылки на список аутентификации используется та же команда, но с префиксом `no`.

Синтаксис

`set client authentication list` `auth-list`

`no set client authentication list`

`auth-list` имя списка аутентификации, который должен совпадать с заданным в команде `aaa authentication login`.

Режимы команды Crypto map configuration.

Значение по умолчанию нет значения по умолчанию.

Рекомендации по использованию

Для того, чтобы задать аутентификацию пользователя на RADIUS-сервере необходимо кроме данной команды указать способ получения идентификатора пользователя – команду `set client username`. Если задать только одну из этих команд, конвертирование Cisco-like конфигураци будет неуспешным.

Отличие данной команды от подобной команды Cisco IOS:

Данная команда отсутствует в Cisco IOS.

set client username (crypto map)

Команда `set client username` задает способ получения идентификатора пользователя. Для удаления заданного способа используется та же команда, но с префиксом `no`.

Синтаксис

`set client username` `ike-id | cert-subj-cn | cert-subj-ou | cert-altsubj-email | cert-altsubj-dns`

`no set client username`

`ike-id`	полное печатное значение IKE-идентификатора партнёра ISAKMP соединения;
`cert-subj-cn`	полное печатное значение поля CommonName (“CN=…”) из описания (Subject) сертификата партнёра ISAKMP соединения, использованного при проверке подписи;
`cert-subj-ou`	полное печатное значение поля OrganizationUnit (“OU=…”) из описания (Subject) сертификата партнёра ISAKMP соединения, использованного при проверке подписи;
`cert-altsubj-email`	полное печатное значение поля EMail (“EMAIL=…”) из альтернативного описания (Alternative subject) сертификата партнёра ISAKMP соединения, использованного при проверке подписи;
`cert-altsubj-dns`	полное печатное значение поля DNS (“DNS=…”) из альтернативного описания (Alternative subject) сертификата партнёра ISAKMP соединения, использованного при проверке подписи.

Режимы команды Crypto map configuration.

Значение по умолчанию нет значения по умолчанию.

Рекомендации по использованию

Для того, чтобы задать аутентификацию пользователя на RADIUS-сервере необходимо кроме данной команды указать список аутентификации – команду `set client authentication list`. Если задать только одну из этих команд, конвертирование Cisco-like конфигураци будет неуспешным.

Отличие данной команды от подобной команды Cisco IOS:

Данная команда отсутствует в Cisco IOS.

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 шлюза безопасности 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 шлюзом безопасности, 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 «Настройка шлюза» (Settings_gate.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]`

`dynamic-map-name` указывает имя набора записей динамической криптографической карты

`dynamic-seq-num` 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.

Удаление

Удаление набора записей динамической криптокарты выполняется командой

`no crypto dynamic-map <dynamic-map-name>`.

В случае, если удаляемый набор записей криптографической карты отсутствуют в конфигурации, то выдается соответствующее сообщение об ошибке: `Could not find crypto map template <dynamic-map-name>`

Если существует хотя бы одна криптокарта, ссылающаяся на набор записей с указанным именем, выдается сообщение об ошибке: `crypto map template in use by crypto map; cannot delete`

Удаление записи динамической криптокарты выполняется командой

`no crypto dynamic-map <dynamic-map-name> <seq-num>`.

В случае, если удаляемая запись динамической криптографической карты отсутствуют в конфигурации, то выдается соответствующее сообщение об ошибке: `Could not find crypto map template entry <dynamic-map-name> <seq-num>`.

Если данная запись единственная с указанным именем и существует хотя бы одна криптокарта, ссылающаяся на данный набор записей, выдается сообщение об ошибке: `crypto map template in use by crypto map; cannot delete`.

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

`set ip access-group` устанавливает правила фильтрации, применяемые к входящим IPsec пакетам после декапсуляции, или к исходящим IPsec пакетам до инкапсуляции

`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 контекстной фильтрации

ip port-map

Команда `ip port-map` используется для ассоциации протоколов (сервисов) прикладного уровня с номерами TCP-портов (PAM – Port to Application Mapping) и позволяет перенаправлять трафик стандартных (системных) протоколов, а также сервисов, заданных пользователем, на любой TCP-порт.

Команда с префиксом `no` устанавливает значение по умолчанию.

Синтаксис

ip port-map appl-name **port** [**tcp**] port-num*| **from** begin-port-num **to** end-port-num [**list** acl-num] [**description** description-string]

no ip port-map appl-name **port** [**tcp**] port-num*| **from** begin-port-num **to** end-port-num [**list** acl-num]

appl-name	название протокола прикладного уровня (сервиса). Могут задаваться стандартные (системные) сервисы и пользовательские, определенные пользователем. Системные сервисы ассоциируются с общеизвестным номером порта и представлены в Таблица 13. Пользовательский сервис задается именем, который должен начинаться с префикса “user-“ и по длине не должен превышать 19 символов
tcp	наличие или отсутствие этого ключевого слова не играет существенной роли
port-num	номер TCP-порта. При наличии в команде слова `tcp` можно задать перечисление до пяти портов или диапазон портов. При отсутствии слова `tcp` – разрешается задать только один порт
begin-port-num	начальный порт диапазона портов, должен быть меньше конечного порта
end-port-num	конечный порт диапазона портов
acl-num	ссылка на имя стандартного нумерованного списка доступа, который ограничивает данный сервис для определенных хостов и подсетей. Если список доступа отсутствует в конфигурации, то данная команда игнорируется при конвертировании конфигурации
description-string	строка с произвольным описанием.

Системно-заданные соответствия

Таблица 13

Имя протокола, сервиса	Номер порта	Описание
ftp	21	File Transfer Protocol
telnet	23	Telnet
smtp	25	Simple Mail Transfer Protocol
gopher	70	Gopher

pop3	110	Post Office Protocol – Version 3
nntp	119	Network News Transport Protocol
imap	143	Internet Message Access Protocol
imap3	220	Interactive Mail Access Protocol 3
ldap	389	Lightweight Directory Access Protocol
login	513	Remote login

Значение по умолчанию Значение по умолчанию отсутствует

Режимы команды Global configuration

Рекомендации по использованию

Используйте эту команду, чтобы перенаправить трафик стандартных сервисов на другие, отличные от общеизвестных, порты. Можно также добавить новый порт к общеизвестному порту. Для приложений, которые используют необщеизвестные порты, создайте пользовательский сервис.

Добавление записи к системному port-map

Системно-заданные соответствия существуют неявно и их можно использовать в команде `ip port-name`, не вводя никаких дополнительных команд.

Для добавления нового порта к системному сервису напишите команду с системным `port map` и она добавит новую запись в уже существующий `port map` (но не заменит его!). Пример:

```
ip port-map ftp port 2100
```

Данная команда приведет к тому, что для ftp будет две записи (одна явная и одна неявная).

```
!!! Неявная запись!!! ip port-map ftp port tcp 21 description File
Transfer Protocol
!!! Явная запись!!! ip port-map ftp port 2100
```

Ограничения на порты

Запрещено задавать порты, уже входящие в другой `port-map` (при условии, что для него не задана `no`-форма команды). Это относится к единичному порту, перечислению или диапазону портов, в которые входит данный порт. Например,

```
ip port-map ftp port tcp 23
```

Будет выдано сообщение об ошибке:

```
%Unable to add port-map entry.
 It conflicts with the system entry for telnet.
 Please delete it before adding this entry
```

А если в конфигурации уже существует пользовательский сервис с именем `user-port-map-1` и он содержит в себе порт 2100, то на команду

```
ip port-map ftp port tcp 2100
```

будет выдано сообщение об ошибке:

```
%Unable to add port-map entry.
 It conflicts with the user-defined entry for user-port-map-1.
 Please delete it before adding this entry
```

Отмена системного port-map

Неявно заданную запись системного `port map` можно отменить с помощью `no`-формы команды. Причем данная no-команда будет отображаться по `show running-config` (возможно в расширенном виде). Пример: хотим перенаправить трафик ftp на нестандартный порт 2100, для этого выполним:

```
no ip port-map ftp
ip port-map ftp port 2100
```

По команде `show running-config` будет показано:

```
no ip port-map ftp port tcp 21 description File Transfer Protocol
ip port-map ftp port tcp 2100
```

Отменить `no`-команду можно следующим образом:

```
ip port-map ftp port tcp 21
```

А по команде `show running-config` будет показано:

```
ip port-map ftp port tcp 21
```

Диапазон портов

При задании диапазона начальный порт обязательно должен быть меньше конечного порта. В противном случае выдается сообщение:

```
%Unable to add port-map entry.
 In a range, beginning value should be smaller than the end
```

Ссылка на лист доступа

Если в нескольких командах `ip port-map` существуют привязки к одному и тому же листу доступа, то при обнаружении коллизий в командах выдаются сообщения об ошибках.

Если в нескольких командах существуют привязки к разным листам доступа (с разными номерами, между ними допускаются пересечения или даже полное совпадение) или если в одной команде задан лист доступа, а в другой – нет, то эти команды не сравниваются. В них допускаются любые пересечения и совпадения номеров портов.

Пример корректной последовательности команд:

```
ip port-map user-port-map-1 port tcp 2100 list 1
ip port-map user-port-map-1 port tcp 21 list 1
ip port-map user-port-map-1 port tcp 23 list 2
ip port-map ftp port tcp 23 list 1
ip port-map ftp port tcp 2100
```

Пример ошибочной последовательности команд:

```
ip port-map user-port-map-1 port tcp 2100 list 1
ip port-map ftp port tcp 2100 list 1 !!! Неправильно !!!
```


Если второй раз прописывается команда, которая уже существует в конфигурации (совпадение с точностью до `description`), она игнорируется без выдачи сообщений об ошибке. Поведение, аналогичное Cisco IOS.

Если в листе доступа используются модификаторы `log` и `log-input`, то будет происходит логирование пакетов, проходящих через inspection фильтры. Сообщения лога показываются в следующем виде:

```
Inspect_<inspect-name>_<acl-name>
```

где `<inspect-name>` – имя inspection; `<acl-name>` – имя листа доступа, присоединенного к port-map, на которую ссылается данный inspect.

Пример:

Фрагмент конфигурации:

```
access-list 95 permit 10.20.30.40 log
!
no ip port-map telnet port 23
ip port-map telnet port tcp 23 list 95
!
ip inspect name inspect1 telnet
```

Фрагмент вывода в сообщении лога:

```
Inspect_inspect1_95
```

В Cisco IOS записи с модификатором log не работают при инспектировании трафика.

Пользовательский port map

На имя пользовательского сервиса существуют жесткие ограничения (аналогично Cisco IOS). Если имя не начинается с префикса “`user-`“, то выдается сообщение:

```
%Unable to add port-map entry.
 Names for user-defined applications must start with 'user-'
```

Имя по длине не должно превышать 19 символов. При несоблюдении этого правила выдается сообщение:

```
%Unable to add port-map entry.
 Application name is too long. Maximum allowed characters for application name are 19
```

Слово `tcp` обязательно должно присутствовать. При несоблюдении этого правила выдается сообщение:

```
%Unable to add port-map entry.
 TCP protocol must be specified for user-defined applications
```

Добавление записей в уже существующий пользовательский `port-map`, ссылка на листы доступа, возможные ошибки аналогичны указанным для системных `port map`.

Команда show running-config

Слово `tcp` показывается всегда, независимо от присутствия в команде.

Системно-заданные соответствия не показываются, хотя и существуют неявно.

Удаление

Существует возможность удалить весь `port map` одной командой. Формат команды:

```
no ip port-map appl-name
```

Примечание: в случае пользовательских `port map` данная команда удаляет весь `port map` целиком; в случае системного `port map` – удаляет все `user-defined` порты и добавляет в конфигурацию `no`-форму команды для `pre-defined` портов (если ее на этот момент еще не было).

Если данного `port map` не существует, выдается сообщение:

```
%Unable to remove port-map entry.
 Port-map entry for application <appl-name> is not found
```

При удалении пользоватльского `port-map` целиком (см. предыдущий пункт) или при удалении последней записи такого `port map` и если имеется привязка к `inspection` правилу, то выдается сообщение вида:

```
Removed <port-map-name> from inspect rule <inspection-name>
```

Если в данном `inspection` правиле не было привязок к другим протоколам (т.е. данный `inspection rule` удаляется), то выдаются два сообщения:

```
Removed <port-map-name> from inspect rule <inspection-name>
Removed inspect rule <inspection-name>
```

Если данный `port map` присутствует в разных `inspection` правилах, указанные выше строки показываются для каждого `inspection` правила.

Пример. На следующую последовательность команд:

```
ip port-map user-port-map-1 port tcp 2100
ip inspect name inspect-1 user-port-map-1
ip inspect name inspect-1 tcp
ip inspect name inspect-2 user-port-map-1
no no ip port-map user-port-map-1
```

будет выдано:

```
Removed user-port-map-1 from inspect rule inspect-1
Removed user-port-map-1 from inspect rule inspect-2
Removed inspect rule inspect-2
```

Отличие данной команды от подобной команды Cisco IOS:

Не используется протокол транспортного уровня UDP.

Системные протоколы и пользовательские обрабатываются одинаково.

Для протокола ftp формируется inspection процедура ftp<>, для всех остальных протоколов – процедура tcp<>, а у Cisco – специфические процедуры для SMTP, HTTP и т.п.

ip inspect name

Команда `ip inspect name` применяется для создания правила проверки трафика для протоколов прикладного уровня и TCP. В этом случае шлюз безопасности выполняет функции межсетевого экрана, используя средства CBAC (Context-Based Access Control – управление доступом на основе контекста).

Удаление правила проверки осуществляется той же командой с префиксом `no`.

Синтаксис

ip inspect name inspection-name protocol [**alert {on | off}**] [**audit-trail {on | off}**] [**timeout** seconds]

no ip inspect name inspection-name protocol [**alert {on | off}**] [**audit-trail {on | off}**] [**timeout** seconds]

inspection-name	имя набора правил проверки. Длина имени не должна превышать 16 символов, при большей длине оно будет сокращено до 16 символов
protocol	протокол, может быть tcp или протокол прикладного уровня (сервис) (системный или пользовательский, заданный в команде `ip port-map`)
alert	для каждого протокола можно включить/выключить выдачу тревожных сообщений на консоль (уровня alert). Если эта опция не установлена, то по умолчанию берется настройка из команды `ip inspect alert-off` (глобальная настройка)
audit-trail	для каждого протокола можно включить/выключить ведение журнала аудита, записи которого выдаются на консоль после закрытия каждой сессии. Если эта опция не установлена, то по умолчанию берется настройка из команды `ip inspect audit-trail` (глобальная настройка)
seconds	время, в течение которого допускается существование неактивного сеанса TCP. Если эта опция не установлена, то по умолчанию берется настройка из команды `ip inspect tcp idle-time` (глобальная настройка).

Значение по умолчанию значение по умолчанию отсутствует.

Режимы команды Global configuration.

Рекомендации по использованию

Правило проверки трафика используется для stateful фильтрации – контексной фильтрации трафика.

Для каждого прикладного протокола создайте свое правило.

Чтобы добавить правило с новым протоколом в уже существующий набор правил проверки используйте то же имя inspection-name набора правил проверки.

Если ввести команду для уже существующей записи, то для нее будут добавлены/изменены настройки (alert, audit-trail и/или timeout). При этом убрать существующую настройку нельзя. Например:

В конфигурации существует запись:

```
ip inspect name inspect-1 user-port-map-1 alert on audit-trail off
```

Если ввести команду:


```
ip inspect name inspect-1 user-port-map-1 alert off timeout 1000
```

То в конфигурации будет сформирована команда:

```
ip inspect name inspect-1 user-port-map-1 alert off audit-trail off
timeout 1000
```

Примечание: соблюдайте осторожность при использовании совместно с фильтрацией по расписанию. Динамическое правило, созданное в диапазоне времени, указанном в расписании, продолжает работать и после завершения данного диапазона времени. Если необходимо, чтобы контекстная фильтрация работала по расписанию, то в данной ситуации политику безопасности можно создать при помощи конфигурационного файла (см. документ «Создание конфигурационного файла»).

Удаление

Удаление записи, связанной с определенным протоколом `protocol`, в наборе правил с именем `inspection-name` осуществляется командой:

```
no ip inspect name inspection-name protocol
```

Для удаления набора правил проверки с именем `inspection-name` используется команда:

```
no ip inspect inspection-name
```

При удалении набора правил проверки, привязанного к одному или нескольким интерфейсам, происходит автоматическое удаление привязки без выдачи специального сообщения.

Для удаления всех наборов правил проверки используется команда:

```
no ip inspect
```

При этом все значения глобальных настроек, связанных с CBAC, принимают значения по умолчанию.

Отличие данной команды от подобной команды Cisco IOS:

В протоколы, которые нужно проверить, не входят стандартные UDP и icmp.

Трафик (входящий или исходящий), одним из конечных пунктов которого является сам роутер, обрабатывается, также как и любой другой. У Cisco такой трафик не попадает под действие inspect правил.

Лист доступа, через который идет трафик, противоположный инспектируемому, может быть стандартным, Cisco требует, чтобы лист доступа обязательно был extended.

ip inspect alert-off

Команда `ip inspect alert-off` применяется для отмены выдачи тревожных сообщений (уровня alert) на консоль при проверке трафика для всех протоколов прикладного уровня.

Команда с префиксом `no` разрешает выдачу alert-сообщений для протоколов прикладного уровня.

Синтаксис

```
ip inspect alert-off
no ip inspect alert-off
```

Значение по умолчанию на консоль не выдаются сообщения уровня alert.

Режимы команды Global configuration.

Рекомендации по использованию

Эта команда является глобальной настройкой для всех протоколов прикладного уровня и используется при отсутствии опции `alert {on|off}` в команде `ip inspect name` для указанного протокола.

Тревожные сообщения будут выдаваться при обнаружении атак блокирования сервиса и других предусмотренных в конфигурации.

ip inspect audit-trail

Команда `ip inspect audit-trail` применяется для ведения журнала аудита, записи которого будут выдаваться на консоль о каждой сессии, после ее закрытия.

Команда с префиксом `no` запрещает ведение журнала аудита.

Синтаксис

```
ip inspect audit-trail
no ip inspect audit-trail
```

Значение по умолчанию на консоль не выдаются сообщения.

Режимы команды Global configuration.

Рекомендации по использованию

Эта команда является глобальной настройкой для всех протоколов прикладного уровня и используется при отсутствии опции `audit-trail {on|off}` в команде `ip inspect name` для указанного протокола.

Команда `ip inspect audit-trail` предоставляет средство мониторинга, которое можно использовать для отладки CBAC.

Используйте данную команду, чтобы регистрировать факты нарушения информационной безопасности и принять меры к устранению возможных угроз.

В журнале ведутся записи о времени сессии, адресах хостов источника и получателя, номерах портов, продолжительности существования соединения и количестве переданных байтов.

ip inspect tcp synwait-time

Команда `ip inspect tcp synwait-time` является командой управления состоянием сеанса в системе CBAC. Данная команда указывает интервал времени, по истечении которого программное обеспечение закроет сеанс TCP, если он не успеет завершить процесс установки и перейти в установленное состояние.

Команда с префиксом `no` устанавливает значение по умолчанию.

Синтаксис

`ip inspect tcp synwait-time` `seconds`

`no ip inspect tcp synwait-time`

`seconds` интервал времени в секундах. Диапазон значений 1 – 65535.

Значение по умолчанию 30 секунд.

Режимы команды Global configuration.

Рекомендации по использованию

Используйте эту команду, чтобы задать, как долго S-Terra Gate будет следить за состоянием TCP сеанса и когда его закрыть, если процесс установки сеанса остается незавершенным.

Считается, что сеанс TCP перешел в установленное состояние, если обнаружен первый пакет сеанса TCP, содержащий флаг SYN, который является запросом клиента на окрытие сеанса.

Данная команда является глобальной настройкой, применяемой для всех сеансов TCP, проверяемых с помощью CBAC.

ip inspect tcp finwait-time

Команда `ip inspect tcp finwait-time` является командой управления состоянием сеанса в системе CBAC. Данная команда указывает интервал времени, в течение которого допускается существование сеанса TCP после того, как S-Terra Gate зарегистрирует получение пакета с флагом FIN.

Команда с префиксом `no` устанавливает значение по умолчанию.

Синтаксис

ip inspect tcp finwait-time seconds

no ip inspect tcp finwait-time

`seconds` интервал времени в секундах. Диапазон значений 1 – 65535.

Значение по умолчанию 5 секунд.

Режимы команды Global configuration.

Рекомендации по использованию

Используйте эту команду, чтобы задать интервал времени, в течение которого еще будет поддерживаться TCP сеанс, после того как шлюз зарегистрирует получение пакета с флагом FIN, который является уведомлением о закрытии сеанса TCP. В течение этого времени будет послано подтверждение о получении уведомления с флагом ACK и выслан пакет с флагом FIN от партнера.

Данная команда является глобальной настройкой, применяемой для всех сеансов TCP, проверяемых с помощью CBAC.

ip inspect tcp idle-time

Команда `ip inspect tcp idle-time` является командой управления состоянием сеанса в системе CBAC. Данная команда указывает максимальный интервал времени, в течение которого допускается существование неактивного сеанса TCP.

Команда с префиксом `no` устанавливает значение по умолчанию.

Синтаксис

`ip inspect tcp idle-time` `seconds`

`no ip inspect tcp idle-time`

`seconds` интервал времени в секундах. Диапазон значений 1 – 65535.

Значение по умолчанию 3600 секунд.

Режимы команды Global configuration.

Рекомендации по использованию

Используйте эту команду, чтобы задать интервал времени, в течение которого будет поддерживаться неактивный сеанс TCP.

Данная команда является глобальной настройкой, применяемой для всех сеансов TCP, проверяемых с помощью CBAC, но может быть переопределена для конкретного интерфейса в правиле проверки `ip inspect name` с помощью параметра `timeout`.

ip inspect max-incomplete high

Команда `ip inspect max incomplete-high` является командой управления состоянием сеансов в системе CBAC. Данная команда указывает максимальное количество одновременно существующих полуоткрытых сеансов, при достижении которого S-Terra Gate начинает их удалять.

Команда с префиксом `no` устанавливает значение по умолчанию.

Синтаксис

ip inspect max-incomplete high number

no ip inspect max-incomplete high

number — количество одновременно существующих полуоткрытых сеансов. Диапазон значений 1 – 1000000.

Значение по умолчанию — 500 одновременно существующих полуоткрытых сеансов.

Режимы команды — Global configuration.

Рекомендации по использованию

Большое количество полуоткрытых сеансов (запросов соединения, оставшихся без ответов) может означать атаку блокирования сервиса или опрос портов внешним наблюдателем. Для TCP полуоткрытый сеанс означает, что он не успел перейти в установленное состояние.

Система CBAC подсчитывает общее количество полуоткрытых сеансов TCP и FTP. Когда количество полуоткрытых сеансов превысит число `number`, установленное командой `ip inspect max-incomplete high`, система CBAC удаляет один полуоткрытый сеанс, как только появляется новый запрос на соединение. Удаление происходит до тех пор, пока число полуоткрытых сеансов не станет меньше значения, заданного командой `ip inspect max-incomplete low`.

Если в команде `ip inspect max-incomplete high` указать значение `number` меньше, чем значение `number`, установленное в команде `ip inspect max-incomplete low`, то команда не выполняется и выводится сообщение об ошибке: `%New high threshold <high> cannot be smaller than low threshold <low>`.

Если ввести команду `no ip inspect max-incomplete high`, устанавливающую значение по умолчанию 500, но в тоже время в команде i`p inspect max-incomplete low` значение `number` больше 500, то в этом случае последняя команда задает новое значение `ip inspect max-incomplete low 500`.

Пример

Заданы команды:

```
ip inspect max-incomplete low 600
ip inspect max-incomplete high 900
```

После ввода команды `no ip inspect max-incomplete high` будет установлено:

```
ip inspect max-incomplete low 500.
```


ip inspect max-incomplete low

Команда `ip inspect max-incomplete low` является командой управления состоянием сеансов в системе CBAC. Данная команда указывает минимальное количество одновременно существующих полуоткрытых сеансов, при достижении которого S-Terra Gate прекращает их удалять.

Команда с префиксом `no` устанавливает значение по умолчанию.

Синтаксис

`ip inspect max-incomplete low` `number`

`no ip inspect max-incomplete low`

`number` количество одновременно существующих полуоткрытых сеансов. Диапазон значений 1 – 1000000.

Значение по умолчанию 400 одновременно существующих полуоткрытых сеансов.

Режимы команды Global configuration.

Рекомендации по использованию

Используйте эту команду, чтобы задать число одновременно существующих полуоткрытых сеансов, по достижении которого прекращается их удаление.

Если в команде `ip inspect max-incomplete low` указать значение number больше, чем значение `number`, установленное в команде `ip inspect max-incomplete high`, то команда не выполняется и выводится сообщение об ошибке: `%New low threshold <low> cannot be greater than high threshold <high>`.

Если ввести команду `no ip inspect max-incomplete low`, устанавливающую значение по умолчанию 400, но в тоже время в команде `ip inspect max-incomplete hight` значение `number` меньше 400, то в этом случае последняя команда задает новое значение `ip inspect max-incomplete hight 400`.

Пример

Заданы команды:

```
ip inspect max-incomplete low 200
ip inspect max-incomplete high 300
```

После ввода команды `no ip inspect max-incomplete low` будет установлено:

```
ip inspect max-incomplete high 400.
```


ip inspect one-minute high

Команда `ip inspect one-minute high` является командой управления состоянием сеансов в системе CBAC. Данная команда указывает частоту появления полуоткрытых сеансов в минуту, по достижении которой S-Terra Gate начинает их удаление.

Команда с префиксом `no` устанавливает значение по умолчанию.

Синтаксис

ip inspect one-minute high number

no ip inspect one-minute high

`number` — частота появления полуоткрытых сеансов. Диапазон значений 1 – 1000000.

Значение по умолчанию — 500 полуоткрытых сеансов в минуту.

Режимы команды — Global configuration.

Рекомендации по использованию

Система CBAC подсчитывает не только количество полуоткрытых сеансов, но и частоту появления полуоткрытых сеансов в минуту.

Если частота попыток создания новых соединений превысит значение `number`, заданное командой `ip inspect one-minute high`, то S-Terra Gate начинает удаление полуоткрытых сеансов, чтобы принимать новые запросы на соединение. Удаление полуоткрытых сеансов будет продолжаться до тех пор, пока частота появления полуоткрытых сеансов не будет совпадать с частотой, установленной командой `ip inspect one-minute low`.

Если в команде `ip inspect one-minute high` указать значение `number` меньше, чем значение `number`, установленное в команде `ip inspect one-minute low`, то команда не выполняется и выводится сообщение об ошибке: `%New high threshold <high> cannot be smaller than low threshold <low>`.

Если ввести команду `no ip inspect one-minute high`, устанавливающую значение по умолчанию 500, но в тоже время в команде `ip inspect one-minute low` значение `number` больше 500, то в этом случае последняя команда задает новое значение `ip inspect one-minute low 500`.

ip inspect one-minute low

Команда `ip inspect one-minute low` является командой управления состоянием сеансов в системе CBAC. Данная команда указывает частоту появления полуоткрытых сеансов в минуту, по достижении которой S-Terra Gate прекращает их удаление.

Команда с префиксом `no` устанавливает значение по умолчанию.

Синтаксис

`ip inspect one-minute low` `number`

`no ip inspect one-minute low`

`number` — частота появления полуоткрытых сеансов. Диапазон значений 1 – 1000000.

Значение по умолчанию — 400 полуоткрытых сеансов в минуту.

Режимы команды — Global configuration.

Рекомендации по использованию

Используйте эту команду, чтобы задать частоту появления полуоткрытых сеансов в минуту, по достижении которой прекращается их удаление.

Если в команде `ip inspect one-minute low` указать значение `number` больше, чем значение `number`, установленное в команде `ip inspect one-minute hight`, то команда не выполняется и выводится сообщение об ошибке: `%New low threshold <low> cannot be greater than high threshold <high>`. Команда не выполняется.

Если ввести команду `no ip inspect one-minute low`, устанавливающую значение по умолчанию 400, но в тоже время в команде `ip inspect one-minute hight` значение `number` меньше 400, то в этом случае последняя команда задает новое значение `ip inspect one-minute hight 400`.

Команды QoS

class-map

Команда `class-map` используется для задания класса трафика и критериев этого класса, на основе которых сетевой трафик будет группироваться в классы (классифицироваться).

Синтаксис	**`class-map [match-all|match-any]`** `class-map-name`
	`no class-map [match-all|match-any]` `class-map-name`
`class-map-name`	имя класса трафика
`match-all`	указывает, что классу будут принадлежать пакеты, удовлетворяющие всем критериям, заданным в режиме настройки класса (config-cmap).
`match-any`	указывает, что классу будут принадлежать пакеты, удовлетворяющие хотя бы одному критерию, заданному в режиме настройки класса (config-cmap).

Значение по умолчанию `match-all`

Режимы команды Global configuration.

Рекомендации по использованию

Описанные ниже команды позволяют задать определенный сервис обслуживания сетевого трафика. Они классифицируют пакеты (относят пакеты к определенному классу трафика) и маркируют их (назначают соответствующий приоритет). Формирование трафика выполняется в три шага:

- пакеты распределяются по классам (команды `class-map`);
- задаются правила для каждого класса (команды `policy-map)`;
- заданная политика привязывается к интерфейсу (команды `service-policy`).

Используемая здесь технология QoS – Дифференцированное обслуживание (DiffServ) – основана на классификации трафика и его маркировке.

С помощью команды `class-map` можно задать несколько классов обслуживания и критерии этих классов.

Например, когда трафик из подсети поступает на внутренний интерфейс шлюза, то сначала он разбивается на множество классов обслуживания на основе полей (IP-адрес, порт, поле ToS) заголовка пакета сетевого и транспортного уровней, заданных командой `class-map`. Затем на этом же интерфейсе производится маркировка пакетов – изменяется поле ToS - переносится значение Precedence (приоритет) или значение DSCP, установленные командами `set precedence` или `set dscp` в режиме настройки команды `policy-map`, в поле ToS. Маркировка производится в соответствии с тем классом обслуживания, к которому принадлежит пакет. В названии команды `policy-map` слово «политика» имеет тот смысл, что установленные значения Precedence и DSCP определяют набор процедур, которые будут обеспечивать заданный класс обслуживания.

Для данного примера заданный класс обслуживания трафика нужно обеспечивать на внешнем интерфейсе шлюза безопасности с помощью утилиты `drv_mgr`, которая позволяет управлять загрузкой процессора обработкой трафика – включать/выключать механизм

уничтожения неприоритетных пакетов (по полю ToS), управлять стратегией очередей, включать/выключать механизм защиты от перегрузки и др.

Существует возможность задания независимых команд классификации и маркирования для входящего и исходящего трафика на каждом интерфейсе.

При IPsec обработке исходящего пакета классификация и маркирование пакета будет производиться до его инкапсуляции, для входящего пакета – после его декапсуляции.

При IPsec обработке пакетов будет происходить копирование поля ToS из внутреннего во внешний заголовок.

Критерии, по которым трафик будет ассоциироваться с определенным классом, задаются в режиме настройки класса следующими командами:

- `match access-group` – означает, что классу принадлежат пакеты, которые попадают под действие указанного списка доступа (access-list);
- `match any` – означает, что все пакеты принадлежат этому классу;
- `match dscp` – означает, что классу принадлежат пакеты, у которых значение DSCP равно одному из указанных;
- `match precedence` – означает, что классу принадлежат пакеты, у которых значение Precedence равно одному из указанных.

Для одного класса можно задать любое количество критериев выбора трафика.

При повторном задании критериев для данного класса ключевое слово `match-all` или `match-any` можно не указывать, сохранится прежний тип класса. Если же указать другой тип (например, `match-all` вместо `match-any`), то тип класса изменится.

Удаление класса производится командой:

```
no class-map [match-all|match any] class-map-name
```

Если данный класс используется в команде `policy-map`, то класс не удаляется, а выводится сообщение об ошибке:

```
"% Class-map <class-map-name> is being used"
```

Пример

```
Router(config)# class-map match-any class1
Router(config-cmap)# match access-group 101
Router(config-cmap)# match dscp af41 af31 af21
Router(config-cmap)#exit
```


match access-group

Команда `match access-group` задает критерий соответствия трафика данному классу на основе списка доступа (ACL).

Синтаксис

match access-group {acl-num | **name** acl-name}

no match access-group {acl-num | **name** acl-name}

acl-num — нумерованный список доступа. Номер листа доступа может быть от 1 до 2699

acl-name — именованный список доступа.

Значение по умолчанию — значение по умолчанию отсутствует.

Режимы команды — Class-map configuration.

Рекомендации по использованию

Списки доступа задаются командами `ip access-list` или `access-list`. Все пакеты, попадающие под действие указанного листа доступа, будут принадлежать данному классу. Поэтому, весь трафик будет проверяться – удовлетворяет ли пакет записям списка доступа или нет.

Если в листе доступа используются модификаторы `log` и `log-input`, то будет происходит логирование пакетов, проходящих через `classification` фильтры. Сообщения лога показываются в следующем виде:

```
Classification_<class-map-name>_<acl-name>
```

где `<class-map-name>` – имя class-map; `<acl-name>` – имя листа доступа.

Пример:

Фрагмент конфигурации:

```
ip access-list extended class-acl-1
 permit udp any any log
!
class-map class-map-1
 match access-group name class-acl-1
```

Фрагмент вывода в сообщении лога:

```
Classification _class-map-1_class-acl-1
```

В Cisco IOS запрещено использование записей с модификаторами `log` и `log-input` для class-map.

Примечание: если на момент конвертирования в классе трафика, который входит в политику (policy map), привязанную к сетевому интерфейсу, присутствует ссылка на несуществующий или пустой список доступа, то конвертирование завершается с ошибкой.

match any

Команда `match any` указывает, что все пакеты принадлежат этому классу.

Синтаксис

```
match
no match any
```

Значение по умолчанию значение по умолчанию отсутствует.

Режимы команды Class-map configuration.

match dscp

Команда `match dscp` задает критерий соответствия трафика данному классу на основе значений DSCP (Differentiated Service Code Point – код дифференцированного обслуживания). Значение DSCP задает приоритет и тип обслуживания пакета. В одной команде можно указать до 8 значений DSCP.

Синтаксис

match [ip] dscp dscp-value [dscp-value dscp-value dscp-value dscp-value dscp-value dscp-value dscp-value]

no match dscp dscp-value [dscp-value dscp-value dscp-value dscp-value dscp-value dscp-value dscp-value]

`ip` — ключевое слово, не влияет на функциональность команды

`dscp-value` — значение DSCP, число от 0 до 63 или одно из следующих ключевых слов:

`ef, af11,af12, af13, af21, af22,af23,af31,af32,af33, af41,af42,af43,cs1,cs2,cs3,cs4,cs5, cs6, cs7, default`

Значение по умолчанию `default`

Режимы команды Class-map configuration.

Рекомендации по использованию

Данная команда используется для задания значений DSCP, при которых пакеты будут принадлежать данному классу. Все пакеты, у которых значение DSCP в поле ToS IP-заголовка пакета принадлежит множеству заданных значений DSCP в команде `match dscp`, будут принадлежать данному классу.

Здесь используется стандарт качества обслуживания – дифференцированное обслуживание (DiffServ). Дифференцированное обслуживание не гарантирует определенный уровень сервиса, а стремится упорядочить весь трафик по классам таким образом, чтобы каждый класс получил лучший или худший уровень обслуживания по отношению к остальным. Для дифференцированного обслуживания используется значение DSCP.

Значение DSCP может быть выражено в цифровой форме или с использованием специальных ключевых слов, называемых поведением сетевых участков (PHB – Per-Hop Behavior). Определено три класса DSCP маркировки: доставка по возможности (BE – Best Effort или DSCP 0), гарантированная доставка (AF – Assured Forwarding) (RFC 2597) и срочная доставка (EF – Expedited Forwarding) (RFC 2598).

В дополнение к этим трем определенным классам существуют коды селектора классов (CS1-CS7), которые идентичны значениям IP precedence (1-7) в команде `match precedence`.

Определено четыре класса гарантированной доставки, они начинаются с AF и далее следуют две цифры. Первая цифра определяет AF класс и принимает значения от 1 (низкий приоритет обработки) до 4 (высокий приоритет обработки пакета). Вторая цифра определяет уровень вероятности сброса пакета в пределах каждого класса и принимает значения от 1 (низкая вероятность сброса) до 3 (высокая вероятность сброса). Значения DSCP могут быть выражены в десятичном формате (например, DSCP 12) или с использованием ключевых слов (например, af12).

Негарантированная доставка пакетов имеет значение DSCP 0 или default.

Для немедленной передачи пакетов указывается ключевое слово ef.

Таблица 14

Код селектора классов (CS)	Описание		PHB-политика
CS7	Stays the same (link layer and routing protocol keep alive)		
CS6	Stays the same (used for IP routing protocols)		
CS5	Express Forwarding (EF)		PHB-политика немедленной передачи пакетов, срочная доставка. Рекомендуется для голосового трафика
CS4	Class 4	Assured Forwarding (AF)	PHB-политика гарантированной доставки пакетов. Используется для видеотрафика. Для видеоконференций рекомендуется значение DSCP AF41.
CS3	Class 3		
CS2	Class 2		
CS1	Class 1		
DSCP 0	Best Effort (BE) – default		PHB-политика негарантированной доставки пакетов, доставка по возможности. Рекомендуется для трафика данных – передача файлов, приложения электронной почты, HTTP и др.

Классы гарантированной доставки пакетов

Таблица 15

Приоритет отбрасывания пакета	Class 1	Class 2	Class 3	Class 4
Низкий	001010 AF11 DSCP 10	010010 AF21 DSCP 18	011010 AF31 DSCP 26	100010 AF41 DSCP 34
Средний	001100 AF12 DSCP 12	010100 AF 22 DSCP 20	011100 AF32 DSCP 28	100100 AF42 DSCP 36
Высокий	001110 AF13 DSCP 14	010110 AF23 DSCP 22	011110 AF33 DSCP 30	100110 AF43 DSCP 38

Класс 4 обрабатывается более приоритетно, чем класс 3, класс 3 – более приоритетно, чем класс 2 и т.д.

match precedence

Команда `match precedence` задает критерий соответствия трафика данному классу на основе значений Precedence. В команде можно указать до 4 таких значений.

Значение Precedence используется для указания желаемого качества доставки пакета. Для этого IP-пакету назначается общий приоритет, который показывает уровень важности передаваемых данных в пакете.

Синтаксис

match [ip] precedence `precedence-value [precedence-value precedence-value precedence-value]`

no match precedence `precedence-value [precedence-value precedence-value precedence-value]`

`ip` ключевое слово, не влияет на функциональность команды

`precedence-value` значение Precedence, число от 0 до 7 или одно из следующих ключевых слов:

`routine, priority, immediate, flash, flash-override, critical, internet, network`.

Значение по умолчанию `routine`

Режимы команды Class-map configuration.

Рекомендации по использованию

Данная команда используется для отбора пакетов, у которых в IP-заголовке в поле типа сервиса ToS указаны заданные значения Precedence. Все пакеты, у которых значение Precedence равно одному из указанных в команде, будут принадлежать данному классу.

Таблица соответствия значения приоритета и ключевых слов

Таблица 16

Приоритет	Ключевое слово	Рекомендация к использованию
0	Routine – обычный пакет	По умолчанию
1	Priority – приоритетный (предпочтительный) пакет	Для приложений данных
2	Immediate – немедленный пакет	Для приложений данных
3	Flash – мгновенный (срочный) пакет	Для сигнализации вызовов
4	Flash-override – быстрее, чем мгновенный (экстренный) пакет	Для видеоконференций и потокового видео
5	Critical – критический пакет	Для речевого трафика
6	Internet – пакет межсетевого управления	Зарезервирован
7	Network – пакет управляющей информации	Зарезервирован

Чем выше номер, тем выше приоритет пакета.

policy-map

Команда `policy-map` используется для маркирования пакетов в соответствии с тем классом обслуживания, к которому принадлежит пакет. В одной `policy map` могут задаваться несколько классов.

Синтаксис **`policy-map`** `policy-map-name`

`no policy-map` `policy-map-name`

`policy-map-name` имя `policy-map`

Значение по умолчанию значение по умолчанию отсутствует.

Режимы команды Global configuration.

Рекомендации по использованию

После того, как командой `class-map` заданы классы трафика и их критерии, командой `policy-map` задается политика работа с классами. Для этого производится маркировка пакетов – выставляется в поле ToS пакета значение Precedence (приоритет), установленное командой `set precedence`, или значение DSCP, установленное командой `set dscp`.

В названии команды `policy-map` слово «политика» имеет тот смысл, что установленные значения Precedence и DSCP определяют набор процедур, которые будут обеспечивать заданный класс обслуживания трафика. Заданный класс обслуживания осуществляется с помощью утилиты drv_mgr, которая позволяет управлять загрузкой процессора обработкой трафика – включать/выключать механизм уничтожения неприоритетных пакетов (по полю ToS), управлять стратегией очередей, включать/выключать механизм защиты от перегрузки и др.

Существует возможность задания независимых команд маркирования для входящего и исходящего трафика на каждом интерфейсе.

При IPsec обработке исходящего пакета классификация и маркирование пакета будет производиться до его инкапсуляции, для входящего пакета – после его декапсуляции.

При IPsec обработке пакетов будет происходить копирование поля ToS из внутреннего во внешний IP-заголовок пакета.

Команда `policy-map` осуществляет переход в режим настройки политики, в котором задается класс трафика командой `class`, все пакеты которого будут маркироваться.

Удаляется `policy-map` командой:

```
no policy-map policy-map-name
```

Если ссылка на эту политику есть в каком-нибудь интерфейсе, то ссылка удаляется без предупреждения.

Пример

Пример маркировки всех пакетов класса class1 значением af41 в поле ToS:

```
Router(config)# policy-map policy-map1
Router(config-pmap)# class class1
Router(config-pmap-c)#set dscp af41
Router(config-pmap-c)#exit
```


class

Команда `class` задает имя класса трафика, все пакеты которого будут маркироваться в соответствии со значениями, указанными в командах `set dscp` или `set precedence`.

Класс трафика и его критерии был заранее создан командой `class-map`.

Синтаксис	**`class`** {class-name | class-default} **`no class`** {class-name | class-default}
class-name	имя класса
class-default	имя класса по умолчанию

Значение по умолчанию значение по умолчанию отсутствует.

Режимы команды Policy-map configuration.

Рекомендации по использованию

Данная команда задает имя класса трафика, для которого будет производиться маркирование. Пакеты для данного класса будут маркироваться значениями Precedence или DSCP, которые будут задаваться в режиме настройки класса командами: `set dscp` и `set precedence`.

Для данного класса может использоваться только одна из этих команд.

Если класс с указанным именем не создан, то выдается сообщение об ошибке: "`% class map <class-name> not configured`".

set dscp

В команде `set dscp` устанавливается значение DSCP для данного класса, которым будут маркироваться пакеты – изменяться значение в поле ToS заголовка IP-пакета на значение DSCP, установленное в данной команде. Команда `set dscp` не может одновременно использоваться с командой `set precedence` для одного класса.

Синтаксис

`set dscp` `dscp-value`

`no set dscp` `dscp-value`

`dscp-value` число от 0 до 63 или одно из следующих ключевых слов:

`ef, af11,af12, af13, af21, af22,af23,af31,af32,af33, af41,af42,af43,cs1,cs2,cs3,cs4,cs5, cs6, cs7, default`

Значение по умолчанию значение по умолчанию отсутствует.

Режимы команды Policy-map class configuration.

Рекомендации по использованию

Более подробное описание значений dscp дано в описании команды `match dscp`.

set precedence

В команде `set precedence` устанавливается значение Precedence для данного класса, которым будут маркироваться пакеты – изменяться значение в поле ToS заголовка IP-пакета на значение Precedence, установленное в данной команде. Команда `set dscp` не может одновременно использоваться с командой `set precedence` для одного класса.

Синтаксис

`set precedence` `precedence-value`

`no set precedence` `precedence-value`

`precedence-value` число от 0 до 7 или одно из следующих ключевых слов:

`routine, priority, immediate, flaish, flaish-override, critical, internet, network`

Значение по умолчанию значение по умолчанию отсутствует.

Режимы команды Policy-map class configuration.

Рекомендации по использованию

Значение Precedence используется для указания желаемого качества доставки пакета путем назначения общего приоритета IP-пакету, который показывает уровень важности передаваемых данных и на сетевом уровне позволяет принять обоснованное решение по приоритету передачи пакета.

Более подробное описание значений Precedence дано в описании команды `match precedence`.

Команды настройки сетевых интерфейсов

interface

Команда `interface` применяется для настройки сетевых интерфейсов, зарегистрированных в файле ifaliases.cf, осуществляя вход в режим interface configuration.

Синтаксис **`interface`** `type port/number`

`type` тип интерфейса. В данной версии Продукта возможны следующие типы:

- FastEthernet,
- GigabitEthernet,
- TenGigabitEthernet (для cs_console никаких различий между интерфейсами с названием FastEthernet, GigabitEthernet и TenGigabitEthernet нет),
- Async – данный тип интерфейсов предлагается использовать для PPP-соединений и т.п.

`port` номер порта

`number` порядковый номер интерфейса.

Значение по умолчанию значение по умолчанию отсутствует.

Режимы команды Global configuration.

Рекомендации по использованию

Данная команда позволяет управлять настройками только зарегистрированных сетевых интерфейсов. Изменения вступают в действие немедленно и сохраняются в загрузочных скриптах ОС (для восстановления при перезагрузке ОС).

Не допускается ввод команд настройки интерфейсов в следующих случаях:

- Для интерфейсов с именем Async<n>. Для интерфейсов с таким именем запрещено выполнение команд настройки – `shutdown`, `ip address`, `mtu`. Нет никаких ограничений на ввод команд, которые транслируются в Native-конфигурацию – привязка списков доступа, inspect, crypto map, QoS и т.п.
  Информация с этих интерфейсов может быть отображена по команде `show run`.
- Для интерфейсов с именами вида *Ethernet<n>/<m>, в параметре pattern которых указан не конкретный физический интерфейс, а маска или перечисление.

При попытке ввести команду настройки на интерфейсе, для которого это запрещено, выдается сообщение об ошибке:

```
% Interface '<interface_name>' is not configurable
```

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:

`shutdown`	включение/выключение интерфейса
`ip address`	настройка IP-адреса и маски
`ip access-group`	указание списка доступа для входящего и исходящего трафика, который должен отслеживаться на данном интерфейсе
`crypto map`	указание криптокарты, по которой будут защищаться пакеты, проходящие через данный интерфейс
`ip inspect`	указание правила проверки входящего и исходящего трафика для протоколов прикладного уровня
`service-policy`	указание политики (policy-map), задающей необходимый сервис обслуживания сетевого трафика, основанный на классификации трафика и его маркировке
`crypto ipsec df-bit`	установка значения DF-бита во внешнем заголовке пакета при прохождении через данный интерфейс
`mtu`	установка значения MTU на интерфейсе
`exit`	выход из конфигурационного режима
`description`	команда игнорируется
`crypto ipsec fragmentation after-encryption`	команда игнорируется
`crypto ipsec fragmentation before-encryption`	команда игнорируется

Пример

Ниже приведен пример выполнения команды `interface`:

```
Router(config)#interface fastethernet 0/1
```

В сообщениях об ошибках команд настройки интерфейса присутствует параметр `<Reason>`, который может иметь одно из следующих значений, приведенных в таблице:

Таблица 17

Reason	Пояснение
No IP addresses on the interface	Нет IP адресов на интерфейсе (только для команды shutdown)
Memory allocation failed	Ошибка выделения памяти
Not implemented	Данная функциональность не реализована
System error	Системная ошибка
System error – possibly MTU value exceeds acceptable range	Системная ошибка – возможно значение MTU превышает допустимый диапазон
Unknown	Неизвестная ошибка
Error <n>	Ошика с числовым кодом, для которого отсутствует текстовое описание

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 (Reason: <Reason>).`

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`.

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 (Reason: <Reason>).`

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`.

По команде `show running-config` отображается текущее системное состояние интерфейса.

Если на интерфейсе на момент выполнения команды `no shutdown` отсутствуют IP адреса (по `show running-config` показывается команда “`no ip address`”), то команда обрабатывается нормально (без дополнительной нотификации), однако реального включения интерфейса по данной команде не произойдет – он будет отложен до ввода IP адреса на интерфейсе.

Например имеем следующую ситуацию:

```
interface FastEthernet0/1
 no ip address
 shutdown
```

Последовательность команд (отложенное включение интерфейса):

```
interface FastEthernet0/1
 no shutdown
```

! Реально интерфейс еще не включен


```
! Следующая команда выставляет IP-адрес на интерфейсе и включает интерфейс:
 ip address 192.168.10.10 255.255.255.0
```

и команд (прямое включение интерфейса):

```
interface FastEthernet0/1
 ip address 192.168.10.10 255.255.255.0
 no shutdown
```

в конечном счете приводят к одинаковому результату.

Если после команды `no shutdown`, но до ввода IP-адреса посмотреть конфигурацию с помощью `show running-config`, вместо команды `shutdown` будет выдано предупреждение следующего вида:

```
interface FastEthernet0/1
 no ip address
! Warning: command "no shutdown" was delayed until IP address set
```

Отложенная команда “`no shutdown`” действует только в пределах текущей сессии cs_console. Если после ввода данной команды не выставить IP-адрес на интерфейсе и выйти из cs_console, то данная команда будет проигнорирована.

В этом случае при следующем входе в cs_console по `show running-config` будет показана исходная конфигурация:

```
interface FastEthernet0/1
 no ip address
 shutdown
```

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-addess	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 ситуации, 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 (Reason: <Reason>)`
- 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 следуюшие ошибки:
  - если не удалось удалить существующий secondary адрес, то выдается сообщение: `Cannot remove the address (Reason: <Reason>)`
  - если не удалось изменить primary адрес, то выдается сообщение: `Cannot set the primary address (Reason: <Reason>)`
  - 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`

Если до ввода primary адреса на интерфейсе отсутствовали IP адреса и была введена команда "no shutdown", то после выставления IP-адреса на интерфейсе выполняется отложенное включение интерфейса (подробнее см. команду shutdown).

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 (Reason: <Reason>).

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 (Reason: <Reason>).

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 (Reason: <Reason>);
- 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

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 (Reason: <Reason>).

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.

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 (Reason: <Reason>).

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`.

Синтаксис

ip access-group {access-list-number | access-list-name} {**in** | **out**}

no ip access-group {access-list-number | access-list-name} {**in** | **out**}

access-list-number	номер списка доступа, который является числом из диапазона 1-199 или 1300-2699
access-list-name	имя списка доступа
in	список доступа применяется для входящего трафика
out	список доступа применяется для исходящего 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.

Если указан несуществующий список доступа, то все поступающие пакеты на интерфейс будут пропущены.

При использовании фильтрующих списков доступа на crypto интерфейсах необходимо следить, чтобы были прописаны соответствующие правила пакетной фильтрации для беспрепятственного прохождения IKE пакетов через firewall.

Если в списке доступа используются модификаторы `log` и `log-input`, то будет происходит логирование пакетов, проходящих через интерфейс. В сообщении kernel лога о прохождении пакета будет показыватся название данного списка доступа.

Отличие данной команды от подобной команды Cisco IOS:

В Cisco IOS исходящий с роутера трафик не фильтруется, в S-Terra Gate исходящий трафик фильтруется.

.

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 S-Terra 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
```


ip inspect

Чтобы применить правило проверки к интерфейсу, его нужно привязать командой `ip inspect` к этому интерфейсу. Удаление привязки осуществляется командой с префиксом `no`.

Синтаксис

ip inspect inspection-name {**in** | **out**}

no ip inspect inspection-name {**in** | **out**}

inspection-name	имя набора правил проверки. Длина имени не должна превышать 16 символов, при большей длине оно будет сокращено до 16 символов
in	набор правил проверки применяется на внутреннем интерфейсе к входящему трафику
out	набор правил проверки применяется на внешнем интерфейсе к исходящему трафику.

Значение по умолчанию значение по умолчанию отсутствует.

Режимы команды Interface configuration.

Рекомендации по использованию

Средства CBAC можно разместить как внутреннем или внешнем интерфейсе шлюза безопасности. С внутреннего интерфейса обычно устанавливаются сеансы, и этот трафик CBAC может пропускать или задерживать. С внешнего интерфейса шлюза сеансы устанавливаться не могут.

Для корректной работы средств CBAC на интерфейсе необходимо правильно настроить списки доступа. Чтобы список доступа допускал создание временных проходов, он должен быть расширенным, для применения к возвращенному трафику также требуются расширенные списки доступа. Списки доступа для исходящего трафика, предназначенного для отправки в интернет, должны допускать трафик, проверенный с помощью CBAC.

Для настройки CBAC на внешнем интерфейсе требуется:

- Исходящий список доступа на внешнем интерфейсе должен быть стандартным или расширенным. Этот список должен разрешать трафик, который вы собираетесь проверять средствами CBAC. Если этот трафик запретить, то он не будет проверяться CBAC и будет просто отвергнут.
- Входящий список доступа на внешнем интерфейсе должен быть расширенным. Этот список доступа должен запрещать трафик, который собираетесь проверять средствами CBAC (CBAC создают временные проходы во входящем списке доступа, разрешающие возвратный поток данных в рамках установленного сеанса).

Для настройки CBAC на внутреннем интерфейсе требуется:

- Входящий список доступа на внутреннем интерфейсе и исходящий список доступа на внешнем интерфейсе могут быть стандартными или расширенными. Эти списки должны разрешать трафик, который вы собираетесь проверяться средствами CBAC. Если этот трафик запретить, то он не будет проверяться CBAC и будет просто отвергнут.
- Исходящий список доступа на внутреннем интерфейсе и входящий список доступа на внешнем интерфейсе должны быть расширенными. Эти списки доступа должны запрещать трафик, который собираетесь проверять средствами CBAC (CBAC создают временные проходы во входящем списке доступа, разрешающие возвратный поток данных в рамках установленного сеанса). Необязательно сразу иметь расширенные списки доступа как на исходящем внутреннем интерфейсе так и входящем внешнем интерфейсе, но по крайней мере, один такой список доступа надо иметь для ограничения трафика, идущего через шлюз, во внутреннюю защищаемую подсеть.

Редактирование

Если в команде указать несуществующее правило проверки inspection-name, то будет выдано сообщение: `%Inspect name <inspection-name> is not defined`.

Удаление привязки

Удаление привязки правила проверки к интерфейсу осуществляется командой

`no ip inspect inspection-name {in | out}`.

Если на данном интерфейсе отсутствует привязка к правилу проверки (как `in` так и `out`), то будет выдано сообщение: `%Inspection is currently not configured for interface <interface-name>`.

Если к интерфейсу привязано хотя бы одно правило проверки (даже к противоположному направлению трафика), то в команде удаления привязки правила к интерфейсу:

- При указании неправильного имени правила `inspection-name`, которое при этом существует в конфигурации, будет выдано сообщение: `%Inspect name <inspection-name> is not defined for interface <interface-name> for the specified direction`
- При указании несуществующего правила проверки `inspection-name`, будет выдано сообщение: `%Inspect name <inspection-name> is not defined`.

При удалении правила проверки автоматически будет удалена и привязка правила к интерфейсу.

service-policy

Команда `service-policy` привязывает политику работы с классами к интерфейсу.

Синтаксис

`service-policy` {**`input`** | **`output`**} `policy-map-name`

`no service-policy` {**`input`** | **`output`**} `policy-map-name`

`input`	входящий трафик
`output`	исходящий трафик
`policy-map-name`	имя policy-map

Значение по умолчанию значение по умолчанию отсутствует.

Режимы команды Interface configuration.

Рекомендации по использованию

Команда `service-policy` используется для привязки политики `policy-map` к интерфейсу.

Существует возможность задания независимых команд классификации и маркирования для входящего и исходящего трафика на каждом интерфейсе.

Если задать несуществующую `policy map`, будет выдано сообщение об ошибке:

```
% policy map <policy-map-name> not configured.
```

Пример

Пример привязки к внутреннему интерфейсу шлюза политики `policy-map` для исходящего трафика:

```
Router(config)# interface fastethernet 0/1
Router(config-if)# service-policy output policy-map1
Router(config-if)# exit
```


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**
clear	DF-бит внешнего IP-заголовка будет очищен и пакет может быть фрагментирован после IPsec инкапсуляции
set	DF-бит внешнего IP-заголовка будет установлен, фрагментация пакета запрещена
copy	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 удается заставить работать механизм Path MTU Discovery) можно установить параметр `clear` на интерфейсе шлюза S-Terra 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 (Reason: <Reason>).`

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 шлюза безопасности. 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 удается заставить работать механизм Path MTU Discovery) можно установить параметр clear на шлюзе S-Terra 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
```


Команды управления параметрами логирования сообщений Firewall

ip access-list logging interval

Команда `ip access-list logging interval` задает интервал времени в миллисекундах для сбора статистики, на основании которой формируются лог-сообщения.

Синтаксис **`ip access-list logging interval`** `logging-interval`

`logging-interval` значение в миллисекундах в интервале от 0 до 2147483647.

Значение по умолчанию значение по умолчанию 0 – устанавливает интервал по умолчанию – 300 секунд. Ввод значения 300000 аналогичен вводу 0, но не эквивалентен: по `show running-config` данная команда будет показана, в отличие, если бы было введено значение 0.

Режимы команды Global configuration.

Рекомендации по использованию

Команда `ip access-list logging interval` используется, когда необходимо указать интервал времени, в течение которого будет накапливаться статистика для вывода лог-сообщений, отличающийся от 300 секунд. Следует учитывать, что при конвертировании точность интервала снижается до секунды: значения от 1 до 1999 преобразуются в секунду, последующие округляются до целой части (например, 3876 мсек округляются до 3 сек).

ip access-list log-update threshold

Команда `ip access-list log-update threshold` задает предельное количество пакетов, при достижении которого будет формироваться лог-сообщение.

Синтаксис **`ip access-list log-update threshold`** `log-update-treshold`

`log-update-treshold` – количество пакетов в интервале от 0 до 2147483647.

Значение по умолчанию значение по умолчанию 0 – отменяет действие этой команды.

Режимы команды Global configuration.

Рекомендации по использованию

Команда `ip access-list log-update threshold` используется, когда необходимо определить количество пакетов, при достижении которого будет форсироваться вывод сообщения в лог, не дожидаясь окончания периода накопления статистики, заданного командой `ip access-list logging interval`.

Команды управления соединениями

clear crypto sa

Команда `clear crypto sa` удаляет все IPsec соединения.

Синтаксис **`clear crypto sa`**

Значение по умолчанию значение по умолчанию отсутствует.

Режимы команды privileged EXEC.

Рекомендации по использованию

Команда `clear crypto sa` используется, когда необходимо удалить все IPsec соединения. При этом происходит уведомление партнера о разрыве соединения (отсылка Delete payload).

В случае неудачного выполнения команды выдается сообщение об ошибке:

```
% Connection removal failed.
```

Отличие данной команды от подобной команды Cisco IOS:

Отсутствует возможность задать дополнительные параметры.

Для удаления всех IPsec соединений из *конфигурационного режима* используется команда **`do clear crypto sa`**.

clear crypto isakmp

Команда `clear crypto isakmp` удаляет все ISAKMP соединения.

Синтаксис **`clear crypto isakmp`**

Значение по умолчанию значение по умолчанию отсутствует.

Режимы команды privileged EXEC.

Рекомендации по использованию

Команда `clear crypto isakmp` используется, когда необходимо удалить все ISAKMP соединения. При этом происходит уведомление партнера о разрыве соединения (отсылка Delete payload).

В случае неудачного выполнения команды выдается сообщение об ошибке:

```
% Connection removal failed.
```

Отличие данной команды от подобной команды Cisco IOS:

Отсутствует возможность задать дополнительные параметры.

Для удаления всех ISAKMP соединений из *конфигурационного режима* используется команда **`do clear crypto isakmp`**.

clear crypto session

Команда `clear crypto session` удаляет все IPsec и ISAKMP соединения.

Синтаксис **`clear crypto session`**

Значение по умолчанию значение по умолчанию отсутствует.

Режимы команды privileged EXEC.

Рекомендации по использованию

Команда `clear crypto session` используется, когда необходимо удалить все соединения и ISAKMP и IPsec. Сначала удаляются все IPsec соединения, затем удаляются все ISAKMP соединения. При этом происходит уведомление партнера о разрыве соединения (отсылка Delete payload).

В случае неудачного выполнения команды выдается сообщение об ошибке:

```
% Connection removal failed.
```

Отличие данной команды от подобной команды Cisco IOS:

Отсутствует возможность задать дополнительные параметры.

Для удаления всех IPsec и ISAKMP соединений из *конфигурационного режима* используется команда **`do clear crypto session`**.

Команды работы с конфигурацией

clear running-config

Команда `clear running-config` очищает текущую Cisco-like конфигурацию. Команда доступна в привилегированном режиме. В конфигурационном режиме используется команда `do clear running-config`.

В зависимости от режима различается функциональность команды:

- в случае привилегированного режима, сразу после очистки конфигурации выполняется ее конвертирование
- в случае конфигурационного режима, конвертирование политики безопасности будет произведено при выходе из этого режима.

Синтаксис **`clear running-config`**

Режимы команды privileged EXEC.

Рекомендации по использованию

Данная команда используется для очистки текущей Cisco-like конфигурации.

После ввода этой команды выдается запрос подтверждения:

Also LSP will be converted immediately. It could lead to undesirable network settings.

To prevent this you could use 'do clear running-config' command from the configuration mode.

Are you sure you want to clear current configuration and to convert LSP immediately? [yes/no]:

После очистки конфигурации производится ее конвертирование

При выполнении команды осуществляются следующие действия:

- В текущей конфигурации удаляются или заменяются на значения по умолчанию все существующие команды конфигурации, исключение:
  - команды описания пользователей (username);
  - команды назначения пароля доступа (enable password или enable secret);
  - команды назначения имени хоста (hostname);
  - команды настройки логирования.
- Если в базе локальных настроек присутствуют CA сертификаты, они автоматически добавляются в новую Cisco-like конфигурацию (аналогично, как это происходит на старте cs_console).
- Из текущей конфигурации копируются привязки логических сетевых интерфейсов к физическим:
  - если до этого момента возникла рассинхронизация между зачитанным на старте составом сетевых интерфейсов и их текущим составом в системе (интерфейсы были добавлены или удалены вне cs_console), то эта рассинхронизация останется и после выполнения команды.
- Выполняется сохранение конфигурации в базе локальных настроек
- Конвертирование политики безопасности (только в привилегированном режиме).

После ввода команды `clear running-config` выдается запрос подтверждения:

```
% Warning: This command will irreversibly destroy current configuration
Are you sure you want to do this? [yes/no]:
```

Введите “yes” для подтверждения команды, “no” – для прерывания команды (следует ввести слово целиком, без сокращений). Для отмены команды можно нажать на CTRL+C.

В случае использования команды в привилегированном режиме конвертирование политики безопасности выполняется сразу после очистки конфигурации, что может привести к установке нежелательных сетевых настроек (включая потерю связи при удаленной настройке, а также компрометацию сетевой безопасности устройства). Поэтому при удаленной настройке устройства, а также при настройке устройства, имеющего доступ в незащищенную сеть, настоятельно рекомендуется использовать команду `do clear running-config` в конфигурационном режиме. В этом случае после данной команды и перед конвертированием (при выходе из конфигурационного режима) следует ввести рабочую конфигурацию.

Отличие данной команды от подобной команды Cisco IOS:

Команда `clear running-config` отсутствует у Cisco.

Возможные предупреждения и сообщения об ошибках приведены в Таблица 18. Данные сообщения свидетельствуют о серьезной проблеме в работе cs_console (кроме последнего предупреждения). При их появлении рекомендуется перезапустить консоль (с возможной потерей данных). При стабильном появлении данных сообщений рекомендуется обратиться в службу технической поддержки.

Таблица 18

Сообщение	Пояснение
% Current operating configuration clear failed: can't transfer essential data from previous configuration	Не удалось очистить конфигурацию: не удалось перенести критически важные объекты из старой конфигурации
% Current operating configuration clear failed	Не удалось очистить конфигурацию
% Configuration save failed	Не удалось сохранить новую конфигурацию в базе локальных настроек
% Configuration save failed: memory allocation error	…ошибка выделения памяти
% Configuration save failed: input/output error	…ошибка ввода/вывода
% Warning: Some old preshared keys were not deleted from local settings	Не удалось удалить один или более preshared ключей из базы локальных настроек
LSP conversion failed: <cs_converter_err_msg>	Ошибка конвертирования LSP <cs_converter_err_msg> – сообщение об ошибке конвертора
LSP conversion complete with additional message(s): <cs_converter_msgs>	Конвертирование LSP завершено успешно, но с дополнительными сообщениями: <cs_converter_msgs> – сообщения конвертора

copy running-config file

Команда `copy running-config file` сохраняет текущую Cisco-like конфигурацию в файл. Команда доступна в привилегированном режиме. В конфигурационном режиме используется команда `do copy running-config file`.

Синтаксис **`copy running-config file:`**`file-path`

`file-path` путь к файлу.

Режимы команды privileged EXEC.

Рекомендации по использованию

Данная команда используется для сохранения текущей Cisco-like конфигурации в указанном файле.

После ввода команды выдается запрос на подтверждение пути к файлу:

```
Destination file path [<corrected-file-path>] ?
```

`<corrected-file-path>` – полный путь к файлу:

- если `<file-path>` – абсолютный путь (начинается с прямого слэша), то `<corrected-file-path>` совпадает с `<file-path>`.
- если `<file-path>` – относительный путь (включая просто имя файла), то `<corrected-file-path>=/var/cspvpn/<file-path>`. Например:

```
copy running-config file:test
Destination file path [/var/cspvpn/test] ?
```

В ответ на запрос можно:

- нажать на Enter – подтвердить введенный ранее путь к файлу;
- ввести новый полный путь к файлу;
- ввести новый относительный путь (например, просто имя файла). В этом случае снова будет выдан запрос на подтверждение полного пути к файлу:

```
copy running-config file:test1
Destination file path [/var/cspvpn/test1] ?test2
Destination file path [/var/cspvpn/test2] ?
```

- нажать CTRL+C – прервать выполнение команды.

Если файл по данному пути уже существует, выдается запрос на подтверждение операции:

```
% Warning: There is a file already existing with this path
Do you want to over write? [confirm]
```

- Нажатие на Enter или ввод строки, начинающейся с символов y или Y (латинские), обозначает подтверждение замены старого файла на новый.
- Ввод строки, начинающейся с других символов (например, n), или нажатие CTRL+C прерывает операцию.

Требуется ввод строки с завершающим нажатием на Enter.

При успешном завершении сохранения конфигурации выдается сообщение:

```
File copied successfully
```

Конфигурация в результате выполнения этой команде не изменяется.

Возможные сообщения об ошибках при выполнении команды приведены в таблице.

Таблица 19

Сообщение	Пояснение
% Unknown destination prefix (should be 'file:')	Перед путем к файлу не введен префикс file:
% File path is empty	Введен пустой путь к файлу: copy running-config file:
% File open failed	Не удалось открыть файл
% Input/output error	Ошибка ввода/вывода

configure replace file

Команда `configure replace file` заменяет текущую Cisco-like конфигурацию на конфигурацию, сохраненную в файле. Команда доступна в привилегированном режиме. В конфигурационном режиме используется команда `do configure replace file`. В зависимости от режима существует отличие в функциональности: в привилегированном режиме выполняется конвертирование, в конфигурационном режиме – конвертирование не делается.

Синтаксис **`configure replace file:`**`file-path`

`file-path` путь к файлу.

Если `file-path` – относительный путь (начинается не с прямого слэша; частный случай – просто имя файла), то полный путь к файлу формируется как `/var/cspvpn/file-path`.

Режимы команды privileged EXEC.

Рекомендации по использованию

Команда `configure replace file` используется для восстановления сохраненной в файле конфигурации.

В качестве параметра для данной команды рекомендуется задавать только файлы, полученные с помощью команды `copy running-config`. Не рекомендуется вручную писать и редактировать данные файлы.

После ввода этой команды выдается запрос подтверждения:

```
% Warning: This will replace the current running configuration with the
contents of the specified configuration file, which is assumed to be a
complete configuration, not a partial configuration.

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

На который надо ответить “yes” для подтверждения команды, “no” – для прерывания команды (следует ввести слово целиком, без сокращений). Для отмены команды можно нажать на CTRL+C.

Текущая конфигурация полностью меняется на конфигурацию из файла с учетом следующих особенностей (далее для простоты используются следующие термины: «старая конфигурация» – конфигурация до ввода команды, «новая конфигурация» – конфигурация, загруженная из файла):

Если в старой конфигурации присутствует описание пользователя, из-под которого запущен данный процесс cs_console (команда username), а в новой конфигурации команда с описанием этого пользователя отсутствует, то данная команда будет автоматически перенесена из старой конфигурации в новую с выдачей сообщения:

```
User '<user-name>' added to the current configuration automatically
```

Существуют особенности, связанные с обработкой команд username – их обработка существенно отличается для случаев, когда пользователь присутствовал или отсутствовал в старой конфигурации:

- Если пользователь уже присутствовал в старой конфигурации, логика обработки команды аналогична логике при загрузке начальной конфигурации (см. Таблица 2).
- Если пользователь отсутствовал в старой конфигурации, логика обработки аналогична логике при ручном вводе команды с новым пользователем (см. `username password`).

- Основное отличие этих двух ситуаций состоит в обработке ситуации, когда пользователь с данным именем уже существует в системе.
- Если пользователь уже присутствовал в старой конфигурации и в качестве shell у него прописана cs_console, то он будет перенесен в новую конфигурацию без дополнительных сообщений пользователю, если в качестве shell прописана другая программа, то с выдачей сообщения: `User "<user-name>" shell changed to /opt/VPNagent/bin/cs_console`.
- Если пользователь отсутствовал в старой конфигурации и в качестве shell у него прописана cs_console, то он будет перенесен в новую конфигурацию с выдачей сообщения: `Warning: User "<user-name>" already exists in the system. It was reused`, в противном случае команда будет отвергнута с выдачей сообщения об ошибке: `% User addition failed. User "<user-name>" already exists in the system`.

Примечание 1: если в новой конфигурации отсутствуют пользователи, присутствовавшие в старой конфигурации, они будут удалены из системы с выдачей сообщения: `User '<user-name>' removed from the system automatically`, за исключением пользователя, из-под которого запущен процесс cs_console.

Если в новой конфигурации присутствуют команды настройки сетевых интерфейсов, отсутствующих в данной системе, эти команды будут проигнорированы с выдачей сообщения: `% Warning: network interface(s) <interface-list> currently not present in the system. They are ignored`.

Если в системе присутствуют интерфейсы, отсутствующие в загружаемой конфигурации:

- их системные настройки (IP адреса, MTU, административный статус) останутся без изменений;
- будет выдано сообщение: `% Warning: network interface(s) <interface-list> have not present in the loaded config. They left intact`;
- настройки, специфичные для cs_console (привязки различных фильтров и crypto maps, настройки DF bit и т.п.) удаляются.

Если в новой конфигурации присутствуют системные настройки для ненастраиваемых сетевых интерфейсов, отличные от текущих настроек, они игнорируются с выдачей сообщения: `% Warning: network interface(s) <interface-list> have different settings in the loaded config. They are not configurable, so they left intact`.

Для настраиваемых интерфейсов, присутствующих и в системе, и в новой конфигурации, будет выполнено сравнение системных настроек:

- В случае если на одном интерфейсе будет зафиксировано расхождение в IP-адресах, на данном интерфейсе будут удалены все текущие адреса, а затем будет сделана попытка добавить адреса из новой конфигурации.
- Если расхождения в IP адресах будут зафиксированы на двух и более интерфейсах, то сначала текущие адреса будут удалены на всех настраиваемых интерфейсах, присутствующих в новой конфигурации, а затем будет сделана попытка добавить IP-адреса из новой конфигурации на этих интерфейсах.
- При детектировании любого расхождения в системных настройках на настраиваемом интерфейсе (IP-адреса, MTU, административный статус), в конце на интерфейсе будет принудительно выставлен административный статус из новой конфигурации, даже если он не менялся по конфигурации.

Примечание 2: если в базе локальных настроек агента присутствуют CA сертификаты, отсутствующие в загружаемой конфигурации, они будут удалены из базы локальных настроек агента с выдачей сообщения: `CA '<subject-name>' removed from local settings automatically`.

Примечание 3: если в новой конфигурации отсутствуют описания Preshared Keys (команда crypto isakmp key), присутствующие в старой конфигурации, то из базы локальных настроек будут удалены соответствующие им записи.

Примечание 4: если в новой конфигурации отсутствуют статические маршруты, присутствующие в данный момент в системе, будет сделана попытка удалить эти маршруты из системы. Если в новой конфигурации присутствуют маршруты, отсутствующие в текущей системе, делается попытка их добавить.

В случае неудачи будут выданы сообщения вида:

```
% Can't delete route '<prefix> <mask> { <gw-ip-addr> | <interface-name>
}': <reason>
```

или

```
% Can't add route '<prefix> <mask> { <gw-ip-addr> | <interface-name>
}': <reason>
```

где <prefix> <mask> – адресная информация маршрута (подробнее см. команду ip route), <gw-ip-addr> – адрес шлюза, через который проходит маршрут, <interface-name> – имя сетевого интерфейса, через который проходит маршрут, <reason> – причина ошибки.

Отличие данной команды от подобной команды Cisco IOS:

Используется префикс “file:”, специфичный для cs_console.

Отсутствуют дополнительные параметры команды.

Существенно отличается логика исполнения команды – в Cisco IOS происходит автоматическое формирование дельта-конфигурации, преобразующей текущую конфигурацию в конфигурацию из файла, в cs_console данная команда просто загружает конфигурацию из файла. Указанные различные действия должны приводить к аналогичному результату.

Существенно отличается формат вывода информационных сообщений и сообщений об ошибках.

Возможные сообщения об ошибках при выполнении команды приведены в таблице.

Таблица 20

Сообщение	Пояснение
% Unknown destination prefix (should be 'file:')	Перед путем к файлу не введен префикс file:
% File path is empty	Введен пустой путь к файлу: configure replace file:
% File not found	Не удалось прочитать файл Примечание: неопасная ситуация: никаких изменений в конфигурацию не было сделано
CA '<subject-name>' removed from local settings automatically	CA был автоматически удален из базы локальных настроек, поскольку он отсутствует в новой конфигурации.
% Error: CA '<subject-name>' removal falied	Была сделана неуспешная попытка удалить CA, отсутствующий в новой конфигурации
% Warning: network interface <interface>	Ошибка настройки сетевого интерфейса.

configuration failed: <msg>	<msg> – сообщение, аналогичное сообщению при ручной настройке интерфейса (команды ip address, mtu, shutdown). Примечание: ниже приведены еще несколько сообщений с указанным шаблоном; однако сообщения в них специфичны для загрузки конфигурации из файла и не имеют аналогов при ручном вводе команд.
% Warning: network interface <interface> configuration failed: 'no ip address' command is not allowed in the loaded config	Ошибка настройки сетевого интерфейса: команда no ip address недопустима в загружаемой конфигурации.
% Warning: network interface <interface> configuration failed: more than one primary address are not allowed in the loaded config	Ошибка настройки сетевого интерфейса: больше одного primary адреса на интерфейсе не допускается в загружаемой конфигурации.
% Warning: network interface(s) <interface-list> currently not present in the system. They are ignored.	Сетевые интерфейс(ы) <interface-list> отсутствуют в системе. Их настройки проигнорированы.
% Warning: network interface(s) <interface-list> have not present in the loaded config. They left intact.	Сетевые интерфейс(ы) <interface-list> отсутствуют в загружаемой конфигурации. Их системные настройки оставлены без изменений.
% Warning: network interface(s) <interface-list> have different settings in the loaded config. They are not configurable, so they left intact.	Сетевые интерфейс(ы) <interface-list> имеют отличные от текущих настройки в загружаемой конфигурации. Эти интерфейсы не настраиваемые, поэтому их настройки оставлены без изменений.
User '<user-name>' removed from the system automatically	Пользователь <user-name> автоматически удален из системы.
% Error: User '<user-name>' removal failed	Не удалось автоматически удалить пользователя <user-name> из системы.
User '<user-name>' added to the current configuration automatically	Пользователь <user-name> автоматически добавлен в текущую конфигурацию. Примечание: пользователь <user-name> – пользователь, из-под которого в данный момент запущен процесс cs_console.
User "<user-name>" shell changed to /opt/VPNagent/bin/cs_console	Shell пользователя <user-name> сменен на /opt/VPNagent/bin/cs_console Примечание: только для пользователя, который уже присутствовал в старой конфигурации.
Warning: User "<user-name>" already exists in the system. It was reused.	Пользователь <user-name> уже существует в системе. Консоль теперь будет его использовать. Примечание: только для пользователя, отсутствовавшего в старой конфигурации; shell пользователя – /opt/VPNagent/bin/cs_console.
% User addition failed. User "<user-name>" already exists in the system.	Не удалось добавить пользователя. Пользователь <user-name> уже присутствует

	в системе. Примечание: только для пользователя, отсутствовавшего в старой конфигурации; shell пользователя отличен от /opt/VPNagent/bin/cs_console.
% ERROR: Replace of the current running configuration failed	Не удалось заменить текущую конфигурацию на новую. Возвращается старая конфигурация. Примечание: в данной ситуации возможно некорректное восстановление конфигурации (особенно ссылок на внешние объекты: пользователи, CA, preshared keys). Рекомендуется перезапустить cs_console.
LSP conversion failed: <cs_converter_err_msg>	Ошибка конвертирования LSP <cs_converter_err_msg> – сообщение об ошибке конвертора
LSP conversion complete with additional message(s): <cs_converter_msgs>	Конвертирование LSP завершено успешно, но с дополнительными сообщениями: <cs_converter_msgs> – сообщения конвертора

Команды управления расписанием

time-range

Команда `time-range` позволяет создать новое или отредактировать существующее расписание. Данная команда осуществляет переход в режим редактирования time range (config-time-range). Удаление расписания осуществляется командой с префиксом `no`.

Ссылки на расписание возможны в расширенных списках доступа.

Синтаксис **`time-ramge`** `name`

`no time-ramge` `name`

`name` имя расписания.

Значение по умолчанию значение по умолчанию отсутствует.

Режимы команды Global configuration.

Рекомендации по использованию

Команда `time-range` позволяет задать диапазон времени, в который будет работать список доступа. Диапазон времени может быть абсолютным и периодическим. В расписании должен быть задан хотя бы один временной диапазон. Для того чтобы команда time-range показывалась по show running-config, необходимо, чтобы в данном расписании был сконфигурирован абсолютный временной диапазон (absolute) или хотя бы один периодический (periodic). В противном случае данное расписание в конфигурации отсутствует.

В режиме редактирования расписания могут использоваться следующие команды:

`absolute` задает абсолютный временной диапазон

`periodic` задает периодический временной диапазон.

Ссылки на расписания допустимы в списках доступа:

- используемых для пакетной фильтрации (команда `ip access-group` в режиме настройки сетевого интерфейса; команда `set ip access-group` в режиме создания crypto map или crypto dynamic-map)
- для формирования класса трафика (команда `match access-group` в режиме настройки class map).

Запрещено использование ссылок на расписания в списках шифрованного доступа, на которые ссылается криптокарта (команда `match address` в режиме настройки crypto map или crypto dynamic-map). В случае присутствия подобных ссылок на расписание, конвертирование будет прервано с сообщением об ошибке.

Примечание

Соблюдайте осторожность при использовании расписания совместно с командами настройки контекстной фильтрации (ip inspect). Динамическое правило, созданное в диапазоне времени, указанном в расписании, продолжает работать и после завершения данного диапазона времени.

Например, в ниже приведенном фрагменте конфигурации FTP-соединение может создаться только между 17:00 и 18:00. Однако созданное FTP-соединение будет работать круглые сутки.

```
ip access-list extended deny-any
 deny   ip any any
!
ip access-list extended out-acl
 permit tcp 192.168.100.0 0.0.0.255 192.168.200.0 0.0.0.255 time-range
time-range-ftp
 deny   tcp any any
 permit ip any any
!
ip inspect name ftp-inspect ftp alert on audit-trail on
!
interface FastEthernet0/2
 ip access-group deny-any in
 ip access-group out-acl out
 ip inspect ftp-inspect out
!
time-range time-range-ftp
 periodic daily 17:00 to 18:00
```


absolute

Команда `absolute` задает абсолютный временной диапазон.

Удаление абсолютного временного диапазона осуществляется командой `no absolute`.

Синтаксис **absolute** [**start** time date] [**end** time date]

no absolute

start	время начала периода
end	время завершения периода (период активен до завершения указанной минуты)
time	время в формате hh:mm, где hh – часы (от 00 до 23), mm – минуты (от 00 до 59), незначащие нули допускается опускать
date	дата в формате <day> <month> <year>, где <day> – число месяца (от 1 до 31), <month> – название месяца на английском языке (можно сокращать до первых трех букв; регистр неважен: **Jan**uary, **Feb**ruary, **Mar**ch, **Apr**il, **May**, **Jun**e, **Jul**y, **Aug**ust, **Sep**tember, **Oct**ober, **Nov**ember, **Dec**ember), <year> – год в четырехзначном формате (допустимый диапазон – от 1993 до 2035).

Значение по умолчанию значение по умолчанию отсутствует.

Режимы команды config-time-range.

Рекомендации по использованию

Используйте эту команду, чтобы задать абсолютный интервал времени. В расписании можно указать только один абсолютный временной диапазон, ввод нового абсолютного временного диапазона замещает предыдущий.

При вводе некорректного значения времени выдается стандартное сообщение об ошибке синтаксиса с пометкой ошибочного символа.

Если ввести некорректное название месяца (длина введенного значения меньше трех букв или введенные буквы не совпадают ни с одним из названий), выдается сообщение об ошибке: % Invalid month.

Если ввести некорректную дату (например, 31 апреля и т.п.), выдается сообщение (аналогично Cisco IOS): Invalid date (doesn't exist).

Время завершения периода должно быть больше, чем время начала периода. В противном случае выдается сообщение об ошибке: Ending time must be greater than starting time.

Допускается не задавать время начала или время завершения периода, но хотя бы один из параметров обязательно должен присутствовать.

Если в текущем расписании отсутствуют периодические временные диапазоны, то после удаления абсолютного временного диапазона, данное расписание не показывается по show running-config.

Примеры допустимых абсолютных временных диапазонов:

```
absolute start 12:00 12 April 2011
absolute end 23:59 29 February 2012
absolute start 23:00 1 December 2012 1:00 end 2 December 2012
```

Удаление абсолютного временного диапазона:

```
no absolute
```


periodic

Команда `periodic` задает периодический временной диапазон.

Удаление периодического временного диапазона осуществляется командой с префиксом `no`.

Синтаксис

`periodic` { `days-of-the-week` | **`daily`** | **`weekdays`** | **`weekend`** } `hh:mm` **`to`** [`day-of-the-week`] `hh:mm`

`no periodic` { days-of-the-week | **`daily`** | **`weekdays`** | **`weekend`** } hh:mm **`to`** [day-of-the-week] hh:mm

`days-of-the-week`	одно или несколько названий дней недели на английском языке
`daily`	ежедневно
`weekdays`	с понедельника по пятницу
`weekend`	суббота и воскресенье
`hh:mm`	время
`day-of-the-week`	название дня недели на английском языке (Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday) До слова "`to`" пишется начало диапазона, после слова "`to`" пишется окончание диапазона.

Значение по умолчанию значение по умолчанию отсутствует.

Режимы команды config-time-range.

Рекомендации по использованию

Используйте эту команду, чтобы задать периодический временной диапазон. В расписании можно указывать несколько временных интервалов.

Если в текущем расписании отсутствует абсолютный временной диапазон, то после удаления последнего периодического временного диапазона, данное расписание не показывается по show running-config.

- Дополнительные спецификаторы дней недели (daily, weekdays, weekend) нельзя смешивать с обозначениями конкретных дней недели.
- Если в начале диапазона задан один единственный день недели, то в окончании диапазона можно (опционально) задать день недели.
  Отсутствие дня недели в окончании диапазона совпадает с заданием того же самого дня недели, что и в начале диапазона. Обозначает действие диапазона в данный конкретный день недели.
  Другой день недели задает промежуток между двумя днями недели.
- Если в начале диапазона задано перечисление дней недели или спецификатор daily, weekdays или weekend, то в окончании диапазона день недели писать нельзя. Обозначает отрезки времени в пределах перечисленных дней недели.
- Если задан диапазон между двумя днями недели, допустимо задавать произвольное время в начале и в окончании диапазона.
- Если задан диапазон для одного дня недели, перечисление дней недели или спецификатор daily, weekdays или weekend, то время окончания диапазона должно быть больше времени начала диапазона. В противном случае выдается сообщение об ошибке: Ending time must be greater than starting time.

- При вводе некорректного значения времени (символьное значение, не соответствующее формату hh:mm; значение hh больше 23 или значение mm больше 59), выдается стандартное сообщение об ошибке синтаксиса с пометкой ошибочного символа.

Примеры допустимых периодических временных диапазонов:

Эти две записи задают разные диапазоны:

```
periodic Monday Wednesday 9:20 to 23:10
periodic Monday 9:20 to Wednesday 23:10
```

Первая запись – понедельник и среда: с 9:20 до 23:20; вторая запись – с понедельника 9:20 до среды 23:10).

Если задается промежуток между двумя днями недели, допускается задавать произвольное время начала и конца периода:

```
periodic Sunday 23:59 to Saturday 00:00
```

Следующие две записи эквивалентны друг другу:

```
periodic Monday 10:00 to 12:00
periodic Monday 10:00 to Monday 12:00
```

Следующие две записи эквивалентны друг другу:

```
periodic Saturday Sunday 11:01 to 11:02
periodic weekend 11:01 to 11:02
```


Команды настройки RADIUS-клиента

Описанные ниже команды позволяют задать аутентификацию на RADIUS-сервере. Также используются команды `set client authentication list` и `set client username`, описанные в разделе «Команды создания и редактирования криптографических карт».

aaa new-model

Команда `aaa new-model` применяется для переключения на AAA access control model.

Команда присутствует для совместимости с системами управления Cisco, при вводе игнорируется.

Синтаксис **`aaa new-model`**

Значение по умолчанию значение по умолчанию отсутствует.

Режимы команды Global configuration.

Рекомендации по использованию

Команда всегда присутствует в конфигурации и показывается при выводе show running-config.

Отличие данной команды от подобной команды Cisco IOS:

В Cisco IOS данная команда переключает модель AAA из режима по умолчанию в AAA access control model.

radius-server host

Команда `radius-server host` задает адрес RADIUS-сервера. Для удаления заданного адрес RADIUS-сервера используется та же команда, но с префиксом `no`.

Синтаксис **`radius-server host`** `ip`

`no radius-server host`

`ip` IP-адрес RADIUS-сервера.

Значение по умолчанию Значение по умолчанию отсутствует.

Режимы команды Global configuration

Рекомендации по использованию

Команда `radius-server host` позволяет задать адрес RADIUS-сервера, к которому производится запрос. Поскольку RADIUS протокол не отвечает достаточному уровню безопасности, пользователь сам должен обеспечить нахождение данного адреса в пределах доверяемого защищённого пространства. Для доступа используется UDP порт 1645.

Отличие данной команды от подобной команды Cisco IOS:

Команда аналогичная Cisco IOS, но в ней отсутствуют любые опциональные параметры (порты и т.п.).

В отличие от Cisco IOS допускается только одна такая команда в конфигурации.

radius-server key

Команда `radius-server key` задает пароль доступа к RADIUS-серверу. Для удаления заданного пароль доступа используется та же команда, но с префиксом `no`.

Синтаксис	**`radius-server key`** `[0] secret`
	`no radius-server key`
`secret`	предопределенный ключ, представляющий собой строку произвольной комбинации буквенно-цифровых символов
`0`	не шифровать предопределенный ключ. Необязательный параметр, потому что он игнорируется. Ключ всегда не шифруется. Введен для соответствия такой же команде в Cisco IOS.

Значение по умолчанию значение по умолчанию отсутствует.

Режимы команды Global configuration.

Рекомендации по использованию

Используйте команду `radius-server key`, укажите предопределенный ключ, который будет являться паролем доступа к RADIUS-серверу. Пароль, введенный данной командой, помещается в базу локальных настроек продукта. Его можно посмотреть с помощью специализированной команды `key_mgr show`.

Отличие данной команды от подобной команды Cisco IOS:

Команда аналогичная Cisco IOS, но в ней в отличие от Cisco IOS не допускаются шифрованные пароли.

radius-server retransmit

Команда `radius-server retransmit` задает количество попыток перепосылок запроса к RADIUS-серверу. Для удаления указанного количество попыток перепосылок запроса к RADIUS-серверу используется та же команда, но с префиксом `no`.

Синтаксис **`radius-server retransmit`** `retries`

`no radius-server retransmit`

`retries` диапазон значений 0 – 9.

Значение по умолчанию 3.

Режимы команды Global configuration.

Рекомендации по использованию

Команда `radius-server retransmit` позволяет задать количество попыток перепосылок RADIUS-запроса. Первая попытка запроса не учитывается, т.е. указывается количество дополнительных попыток связаться с Raduis-сервером.

Отличие данной команды от подобной команды Cisco IOS:

Команда аналогичная Cisco IOS, за исключением более узкого диапазона допустимых значений.

radius-server timeout

Команда `radius-server timeout` задает время ожидания ответа от RADIUS-сервера. Для удаления заданного времени ожидания ответа от RADIUS-сервер используется та же команда, но с префиксом `no`.

Синтаксис **`radius-server timeout`** `seconds`

`no radius-server timeout`

`seconds` время ожидания в секундах. Допустимый диапазон 1 – 1000.

Значение по умолчанию 5.

Режимы команды Global configuration.

Рекомендации по использованию

Используйте команда `radius-server timeout`, чтобы устанавливить интервал в секундах между повторными попытками посылки запросов на RADIUS-сервер.

aaa authentication login

Команда `aaa authentication login` задает аутентификацию на RADIUS-сервере. Для удаления заданного списка аутентификации и пароля используется та же команда, но с префиксом `no`.

Синтаксис	**aaa authentication login** auth-list **group radius password** [0] user-password
	no aaa authentication login auth-list **group radius password**
auth-list	имя списка аутентификации;
user-password	неинтерактивный пароль пользователя (единый);
0	необязательный параметр, указывающий на то, что пароль хранится в незашифрованном виде.

Значение по умолчанию значение по умолчанию отсутствует.

.

Режимы команды Global configuration.

Рекомендации по использованию

Используйте команда `aaa authentication login`, чтобы указать параметры аутентификации на RADIUS-сервере.

Можно задать только один список аутентификации. Новая команда замещает значения, заданные в предыдущей.

Пароль, введенный данной командой, помещается в базу локальных настроек продукта. Его можно посмотреть с помощью `key_mgr show`.

Отличие данной команды от подобной команды Cisco IOS:

Команда отсутствует в Cisco IOS. Однако сделана по аналогии с командой `aaa authentication login`. Принципиальное отличие – параметр `password user-password` (в Cisco IOS пароль получается интерактивно через XAuth).

В Cisco IOS допускается задавать несколько команд `aaa authetntication login`.

Пример настройки RADIUS-клиента

```
! Можно не вводить. В конфигурации всегда присутствует.
aaa new-model
!
! Имя списка аутентификации произвольное. Неинтерактивный пароль
пользователя (обязательный параметр).
aaa authentication login RADIUS group radius password 87654321
!
! Адрес RADIUS сервера. Обязательный параметр.
```



```
radius-server host 10.2.0.42
! Пароль доступа к RADIUS серверу. Обязательный параметр.
radius-server key 12345678
!
..
!
crypto map CMAP 1 ipsec-isakmp
..
 ! Имя списка аутентификации должно совпадать с введенным в команде aaa
authentication login
 set client authentication list RADIUS
 ! Необходимо выбрать способ получения идентификатора пользователя
(обязательный параметр):
 set client username { ike-id | cert-subj-cn | cert-subj-ou | cert-
altsubj-email | cert-altsubj-dns }
!
```

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
write
```

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 перефрагментацией, которые посылает CSM:

Глобальная:

```
crypto ipsec fragmentation { after-encryption | before-encryption }
no crypto ipsec fragmentation
```

В режиме настройки интерфейса:

```
crypto ipsec fragmentation { after-encryption | before-encryption }
no crypto ipsec fragmentation
```

