Доступ к устройству через CLI

Удаленное управление устройством по средствам командной строки доступно с использованием протоколов Telnet и SSH.

Для подключения к устройству используйте IP-адрес, назначенный на Ethernet интерфейс устройства, по умолчанию - 10.10.10.1.

После захода на устройство вы увидите приглашение операционной системы **WANFleX**.

telnet

Команда используется для установки соединения с удалённым устройством в режиме эмуляции терминала. В данной реализации используется простая прозрачная трансляция потока символов без какой-либо промежуточной интерпретации, поэтому тип терминала будет определяться тем терминалом, с которого была выполнена данная команда. Аварийное прерывание сеанса выполняется при нажатии клавиш "Ctrl/D".

Синтаксис:

```
telnet address [port] [-S source]
```

Параметр	Описание
port	Порт Telnet.
-S source	IP-адрес устройства.

Протокол SSH

Протокол SSH (Secure Shell) обеспечивает безопасное удаленное управление сетевыми устройствами. Его функциональность аналогична протоколу Telnet, но, в отличие от Telnet, SSH кодирует все протокольные сообщения, включая передаваемые пароли.

Настройка встроенного сервера SSH выполняется с помощью команды "*sshd*". По умолчанию сервер SSH отключен.

Синтаксис:

```
sshd -help, -h
sshd -port=PORT
sshd -window=SIZE
sshd -keepalive=TIME
sshd -banner=on | off
sshd -log-level={emerg|alert|crit|error|warning|notice|info|debug|LEVEL} [notice]
sshd -algo-list
sshd -kex-algos[=ALGO-LIST]
sshd -hostkey-algos[=ALGO-LIST]
sshd -cipher-algos[=ALGO-LIST]
sshd -hash-algos[=ALGO-LIST]
sshd -comp-algos[=ALGO-LIST]
sshd -auth-methods[=AUTH-METHODS-LIST]
sshd start
sshd stop
sshd newkeys
sshd pub[key] {sh[ow] | cl[ear] | de[lete] N}
sshd pub[key] {in[stall] | im[port] [LOGIN[:PASSWORD]@]HOST/FILE} [COMMENT]
```

Параметр	Описание

-help, -h	Вывод синтаксиса команды "*sshd*".
-port=PORT	Номер порта TCP, на котором сервер SSH должен принимать подключения, по умолчанию 22.
-window=SIZE	Размер внутреннего окна приема сервера SSH, указывается в байтах. Размер окна сервера SSH определяет максимально допустимую пропускную способность для канала данных "*SSH Client - SSH Server*". По умолчанию размер окна составляет 24576 байт.
-keepalive=TIME	Установка периода продолжительности проверки активности сеанса в секундах. По умолчанию сервер не выполняет проверку активности, значение 0.
-banner=on | off	Показывать/скрывать информационный баннер ОС WANFleX пользователю после прохождения авторизации.
-log-level={emerg|alert|crit|error|warning|notice|info|debug|LEVEL} [notice]	Уровень журналирования, определяющий детализацию регистрируемых в системном журнале сообщений сервера SSH. Для управления системным журналом используйте команду "*sys log*". Различные уровни журналирования определяются аргументами "*emerg*", "*alert*", "*error*", "*warning*", "*notice*", "*info*", "*debug*", либо могут устанавливаться номером необходимого уровня (от 0 до 7) с использованием числового аргумента "*LEVEL*". По умолчанию включен уровень "*info*" (уровень 6).
-algo-list	Отображение списка всех доступных алгоритмов SSH для обмена ключами (kex), аутентификации (host key), кодирования данных (cipher), проверки данных (hash) и сжатия данных (comp).
-kex-algos[=ALGO-LIST]	Выбор алгоритмов kex из списка алгоритмов (ALGO-LIST), которые будут использоваться в процессе обмена ключами SSH.
-hostkey-algos[=ALGO-LIST]	Выбор алгоритма формирования ключа/отпечатка сервера из списка алгоритмов (ALGO-LIST), которые будут использоваться в процессе аутентификации "Сервер-Клиент" SSH.
-cipher-algos[=ALGO-LIST]	Выбор алгоритмов кодирования из списка алгоритмов (ALGO-LIST), которые будут использоваться при кодировании данных SSH.
-hash-algos[=ALGO-LIST]	Выбор алгоритма хеширования из списка алгоритмов (ALGO-LIST), которые будут использоваться при проверке данных SSH.
-comp-algos[=ALGO-LIST]	Выбор алгоритма сжатия из списка алгоритмов (ALGO-LIST), которые будут использоваться при сжатии данных SSH.
-auth-methods[=AUTH-METHODS-LIST]	Выбор доступного метода аутентификации из списка (AUTH-METHODS-LIST). Значение "*all*" включает все методы аутентификации.
start	Запуск сервера SSH.
stop	Останов сервера SSH.
newkeys	Повторное создание ключей сервера. **ВНИМАНИЕ** При первом запуске сервер SSH генерирует ключи DSS и RSA, которые будут использоваться для аутентификации с использованием публичного ключа.
pub[key] {sh[ow] | cl[ear] | de[lete] N}	• "*show*" – вывод информации о публичных ключах клиентов SSH, зарегистрированных в реестре сервера SSH. • "*clear*" – удаление всех публичных ключей клиентов SSH из реестра. • "*delete*" – удаление публичных ключей клиента SSH из реестра сервера SSH. Параметр "*N*" – индекс ключа в списке.

pub[key] {in[stall] | im[port] [LOGIN[:PASSWORD]@]HOST /FILE} [COMMENT]	Активация аутентификации клиентов SSH с помощью публичного ключа. В этом режиме сервер SSH разрешает клиенту SSH использовать ключ вместо ручного ввода пароля. Этот режим включается автоматически, как только открытый ключ клиента SSH будет добавлен в реестр сервера SSH:
	• "*install*" – установка публичного ключа клиента SSH в реестр сервера SSH.
	• "*import*" – импорт публичного ключа клиента SSH в реестр сервера SSH с удаленного сервера FTP:
	  • "*HOST*" – IP-адрес удаленного сервера FTP.
	  • "*FILE*" – файл, содержащий публичный ключ клиента RSA/DSS в формате OpenSSH или SSH2. Если удаленный сервер FTP требует аутентификацию, то имя пользователя и пароль должны быть указаны в "*LOGIN*" и "*PASSWORD*" соответственно.
	  • "*COMMENT*" – данный аргумент позволяет добавить комментарий к записи публичного ключа в реестре. По умолчанию добавляется комментарий с IP-адресом клиента или IP-адресом сервера FTP, из которого получен ключ.

ВНИМАНИЕ

По умолчанию сервер SSH применяет только парольную аутентификацию. Однако этого может оказаться недостаточно для обеспечения необходимого уровня безопасности. У устройств "Инфинет" есть несколько встроенных методов аутентификации SSH, которые управляются командами "*sshd pubkey*" "и "*sshd -auth-methods*". При этом сервер SSH сохранит открытый ключ подключенного клиента SSH.

Командная строка

Для управления и конфигурации используется простой и понятный командный язык, по структуре напоминающий систему взаимодействия **ОС Unix**. Каждая команда начинает действовать сразу после ввода.

Однако действие каждой команды ограничивается только одним сеансом, до первой перезагрузки.

Чтобы сохранить действие команд нужно записать текущую конфигурацию в постоянную память командой "*config save*".

Несколько команд можно группировать в одну строку, разделяя их символом "**;**" (точка с запятой). Если в строке встретится команда с неверным синтаксисом, то она игнорируется, остаток строки проверяется до конца. Имя команды может быть сокращено до любого недвусмысленного значения.

Если ваш терминал поддерживает стандарт VT100 или ANSI, то вы можете использовать клавиши редактирования и перемещаться по списку ранее выполненных команд стандартными клавишами клавиатуры. Пронумерованный список ранее введённых команд можно просмотреть командой "*!h*". Любую строку из этого списка можно сделать текущей, с помощью команды "*!НОМЕР*". Клавиша "**TAB**" подставляет в командную строку последнюю похожую команду (поиск подстроки).

Команда "*Ctrl/R*" обновляет содержимое строки ввода, если оно было нарушено выводом на экран системных сообщений. Команда, выполненная без аргументов, печатает краткую подсказку о своих ключах и синтаксисе.

Контекстную подсказку можно получить, нажав клавишу "**?**" в любом месте строки.