**SSH. Назначение, схема работы, преимущества, недостатки.**

SSH — защищенный протокол для удаленного доступа к компьютерам. Через SSH можно выполнять операции в командной строке компьютера, который физически находится в другом месте.

Иными словами, SSH — это дистанционная командная строка. Визуально вы работаете на своем компьютере, но в реальности — на другом.

Вся информация передается в зашифрованном виде. Подобно тому, как некоторые сайты работают по HTTPS, шифруя информацию.

Зачем это нужно?

Не всегда есть возможность физически находиться у компьютера, с которым нужно работать. Например, если вы хотите создать свой сайт, то он будет размещен на компьютере хостинг-провайдера. Этот компьютер может находиться на другом конце света. Вам нужен способ запускать команды на этом компьютере не выходя из своего дома.

Схема работы

Есть несколько шагов, которые нужно пройти, чтобы начать SSH-сеанс между компьютерами.

1. Сначала нужно обеспечить безопасный способ обмена сообщениями между компьютерами, то есть настроить зашифрованный канал.
2. Далее нужно проверить целостность данных, отправляемых клиентом.
3. После этого проверяется подлинность клиента.

После этих трёх шагов мы можем безопасно общаться с удалённым компьютером, делиться секретными данными, а также проверить, есть ли у клиента разрешение на доступ к хосту. Каждый из разделов ниже будет более подробно описывать эти действия.

## Настройка зашифрованного канала

Вся информация, отправляемая с использованием SSH, зашифрована. Обе стороны должны знать и понимать способ шифрования.

Для шифрования передаваемых данных используется симметричное шифрование. Суть данного подхода заключается в том, что оба компьютера имеют одинаковый ключ шифрования, который называется «симметричный ключ». Симметричное шифрование работает очень хорошо, но только до тех пор, пока сторонние не имеют доступа к ключу.

Один компьютер может создать ключ и отправить в виде сообщения через интернет. Но сообщение ещё не будет зашифровано, поэтому любой, кто перехватит его, сразу же сможет расшифровать все следующие сообщения.

Решение этой проблемы состоит в использовании протокола обмена ключами Диффи-Хеллмана. Оба компьютера создают свой закрытый и открытый ключ. Вместе они образуют пару ключей. Компьютеры делятся своими открытыми ключами друг с другом через интернет. Используя свой закрытый и чужой открытый ключ, стороны могут независимо сгенерировать одинаковый симметричный ключ.

Верификация

Следующий этап процесса установки сеанса SSH заключается в проверке того, что данные не были подделаны во время их передачи и что другой компьютер действительно является тем, за кого себя выдаёт.

Для верификации используют хеш-функцию. Это математическая функция, которая принимает входные данные и создаёт строку фиксированного размера.

Важной особенностью этой функции является то, что практически невозможно определить входные данные, зная лишь результат её работы.

После того как клиент и хост сгенерировали свои симметричные ключи, клиент использует хеш-функцию для генерации HMAC, что означает «код аутентификации сообщений, использующий хеширование». Клиент отправит этот HMAC на сервер для верификации.

Функция хеширования использует:

* симметричный ключ клиента,
* порядковый номер пакета,
* содержимое сообщения (зашифрованное).

Когда хост получает HMAC, он может использовать ту же самую хеш-функцию с этими тремя компонентами:

* собственный (идентичный клиентскому) симметричный ключ;
* порядковый номер пакета;
* зашифрованное сообщение.

Если сформированный хеш совпадает с HMAC, полученным от клиента, то мы можем быть уверены, что подключаемый компьютер — это компьютер с симметричным ключом, потому что только хост и клиент знают симметричный ключ, а другие компьютеры — нет.

Прелесть этого подхода в том, что мы не просто проверили личность клиента и убедились, что данные не были подделаны, но мы сделали это без передачи какой-либо секретной информации.

## Аутентификация

Даже если мы используем симметричные ключи для безопасного общения, мы не знаем, имеет ли подключающийся компьютер разрешение на доступ к содержимому хоста. Для того чтобы проверить это, необходимо произвести аутентификацию.

Многие используют аутентификацию по паролю. Клиент отправляет хосту зашифрованное сообщение, содержащее пароль. Хост его расшифровывает и ищет пароль в базе данных, чтобы удостовериться, есть ли у клиента разрешение на доступ. Использование пароля для аутентификации допустимо, но имеет свои недостатки, так как необходимо хранить все пароли на сервере.

Более безопасной является аутентификация по сертификату. Сформировав сертификат, клиент единожды вводит пароль для доступа к серверу и отправляет ему открытую часть сертификата. В дальнейшем ввод пароля не требуется. Этот подход считается более безопасным, чем просто использование пароля, поскольку не подразумевает хранение секрета пользователя на хосте.

Преимущества

 Отвечает всем современным требованиям к шифрованию и обеспечивает невозможность подмены трафика путем пересылки контрольных сумм.

Недостатки

Протокол SSH не имеет средств защиты от действий злоумышленника, получившего root-доступ. Одной из мер предосторожности является ограничение использования режима root без острой необходимости.