SSH ( Secure Shell - Защищенная оболочка ) -- это сетевой протокол, обеспечивающий защищенную аутентификацию, соединение и безопасную передачу данных между хостами сети, путем шифрования, проходящего через него трафика, с возможной компрессией данных. Еще одной важной функциональной особенностью, является возможность создания защищенных, шифрованных туннелей, для безопасной передачи через небезопасную среду ( например интернет ), других сетевых протоколов, так-же с возможность сжатия трафика. Кроме того протокол SSH отлично работает с форвардингом ( переадресация, перенаправление ) портов одной машины на порты другой в том числе и форвардинг удаленных клиентов XWindow.

Он позволяет создавать шифрованные туннели для безопасной передачи других сетевых протоколов через незащищенную сеть, например, Интернет. Часто его используют для перенаправления портов одного компьютера на порты другого. Начало SSH было положено Тату Илёненом из Финляндии в 1995 году, который задействовал его как более конфиденциальный протокол. Эта версия была названа SSH-1. На данный момент практически нигде не используется. В 1996 году была разработана усовершенствованная версия SSH-2. Она несовместима с SSH-1, более защищенная и имеет расширенный список алгоритмов шифрования. Сейчас под SSH понимается именно версия SSH-2. С 2006 года протокол признан интернет-стандартом ассоциацией IETF.

Существует две основных реализации SSH. Одна из них проприетарная, которая разрабатывается SSH Communications Security. Вторая - OpenSSH, созданная под руководством Тео де Раадта как свободная открытая альтернатива первой. Является самой распространенной и включена в поставку большинства Unix-подобных систем.

Безопасный доступ организуется с помощью процедуры аутентификации с использованием асимметричного шифрования с публичным ключом при первом подключении. При последующем применяется симметричное шифрование. Стандарт SSH включает в себя три протокола:

1. Протокол транспортного уровня - гарантирует аутентификацию сервера, секретность и целостность. Обеспечивает сжатие данных. Работает поверх TCP/IP.
2. Протокол аутентификации — исполняет аутентификацию клиента для сервера. Действует поверх уровня транспортного протокола.
3. Протокол соединения — представляет зашифрованный канал в виде мультиплексированного канала из нескольких логических, используемых для разных служб. Работает поверх канала аутентификации.

Повышение безопасности гарантируется аутентификацией клиента для сервера, к которому обращается клиент ssh и аутентификацией сервера клиентом. Происходит аутентификация обеих сторон.