Занятие 6. Протокол telnet. Протоколы SSH, SCP, SFTP. Технология VPN

ПРОТОКОЛ TELNET

Протокол Telnet (Teletype Network) - протокол, реализующий текстовое терминальное соединение по сети, работает поверх протокола TCP. Протокол разрабатывался для реализации сетевого взаимодействия между устройствами или процессами. Он часто использовался и сейчас используется для удаленного администрирования.

Протокол полностью симметричен несмотря на то, что в нем выделяют клиентскую и серверную части, после установления транспортного соединения обе стороны могут обмениваться двумя типами данных: командами самого протокола Telnet и прикладными текстовыми данными. Прикладные данные при этом проходят через протокол без изменений, поскольку с точки зрения протокола они представляют последовательность байт.

Исторически протокол служил для удаленного доступа к командной оболочке операционных систем (не только компьютеров и серверов, но и сетевого оборудования), впоследствии его стали использовать и для других текстовых интерфейсов, вплоть до текстовых многопользовательских игр и доступа к другим протоколам прикладного уровня, работающих поверх TCP (например, FTP, HTTP, SMTP и т.п.), для отладки и экспериментов.

В Telnet не предусмотрены какие-либо механизмы защиты такие как шифрование или проверка подлинности данных, поэтому протокол уязвим к любым атакам транспорта. Поэтому использование протокола Telnet для администрирования возможно только в полностью контролируемых сетях или в сетях защищенных на сетевом уровне. Для удаленного доступа к командной оболочке операционных систем в настоящее время используется протокол SSH, при создании которого делался упор на безопасность. По причине ненадёжности от Telnet как средства управления операционными системами давно отказались.

ПРОТОКОЛ SSH

Протокол SSH (Secure Shell) - протокол прикладного уровня, позволяющий производить удаленное управление операционными системами и туннелирование TCP-соединений. В отличие от Telnet шифрует весь трафик и передаваемые учетные данные. SSH позволяет выбор различных алгоритмов шифрования и аутентификации пользователя.

Первая версия протокола SSH была разработана в 1995 году - SSH-1, он был написан для обеспечения большей безопасности и конфиденциальности, чем используемые в то время протоколы telnet, rlogin, rsh. В 1996 году была разработана более безопасная версия протокола - SSH-2, несовместимая с SSH-1. К 2000 году протокол SSH-2 приобрел большую популярность и в 2006 году был утвержден в качестве Интернет-стандарта. В настоящее время под протоколом SSH подразумевается именно SSH-2.

SSH поддерживает несколько видов аутентификации: аутентификация по паролю (самый распространенный способ), аутентификация при помощи ключевой пары (предварительно генерируется пара открытого и закрытого ключей, на клиенте хранится закрытый ключ, на сервере - открытый, сами ключи не передаются при аутентификации,

лишь идет проверка владения закрытым ключом), аутентификация по IP-адресу (самый небезопасный способ, чаще всего он отключен).

Для работы по SSH нужен SSH-сервер и SSH-клиент. Сервер прослушивает соединения на порту 22/TCP, при установлении связи производит аутентификацию. Клиент используется для входа на удалённую машину и выполнения команд. Основной реализацией SSH-сервера является OpenSSH, он по умолчанию доступен во всех *nix-подобные операционные системы, в пакете с сервером OpenSSH идет и клиент.

Посредством протокола SSH можно организовывать шифрованные SSH-туннели, они используются для того, чтобы обезопасить передачу данных в сети Интернет.

ПРОТОКОЛ SCP

SCP (Secure Copy) - это утилита и протокол прикладного уровня, предназначенные для копирования файлов между удаленными хостами, использующие в качестве транспорта SSH. Утилита и протокол работают по уже установленному между клиентом и сервером шифрованному соединению, удаленный процесс scp может работать в одном из двух режимов: исходный режим - передача файлов от сервера клиенту, режим приемника - передача файлов от клиента серверу.

ПРОТОКОЛ SFTP

SFTP (SSH File Transfer Protocol) - протокол прикладного уровня, предназначенный для копирования и выполнения других операций с файлами поверх защищенного соединения SSH. Протокол был разработан как расширение SSH-2, однако допускает реализацию с использованием других протоколов.

По сравнению с протоколом SCP, который разрешает только передачу файлов, протокол SFTP позволяет выполнять ряд операций с удаленными файлами, что делает его более похожим на протокол удаленной файловой системы. Сам протокол не обеспечивает аутентификацию и безопасность; он ожидает, что базовый протокол обеспечит это.

Термин SFTP может так же относиться к консольной утилите, которая реализует клиентскую часть этого протокола. Многие графические клиенты реализуют работу по протоколу SFTP.

ТЕХНОЛОГИЯ VPN

VPN (Virtual Private Network) - обобщённое название технологий, позволяющих обеспечить одно или несколько сетевых соединений поверх другой сети. Благодаря использованию средств шифрования, аутентификации и т.п. в логических сетях VPN уровень доверия к ним не зависит от уровня доверия к сетям, на которых они построены. Обычно VPN развёртывают на уровнях не выше сетевого, так как применение криптографии на этих уровнях позволяет использовать в неизменном виде транспортные протоколы. Технология VPN в последнее время используется не только для создания собственно частных сетей, но и некоторыми провайдерами «последней мили» для предоставления выхода в сеть Интернет. При должном уровне реализации и использовании специального программного обеспечения сеть VPN может обеспечить высокий уровень шифрования передаваемой информации.

VPN состоит из двух частей: «внутренняя» (подконтрольная) сеть, которых может быть несколько, и «внешняя» сеть, по которой проходит соединение. Подключение удалённого пользователя к VPN производится посредством сервера доступа, который подключён как к внутренней, так и к внешней сетям. При подключении удалённого пользователя или сети сервер доступа требует прохождения процесса идентификации, а затем процесса аутентификации. После успешного прохождения обоих процессов происходит процесс авторизации внешнего пользователя или сети для работы во внутренней сети.

Классифицировать решения VPN можно по нескольким основным параметрам:

По степени защищенности используемой среды:

- Защищенные. Наиболее распространённый вариант виртуальных частных сетей. С его помощью возможно создать надежную и защищённую сеть на основе ненадёжной сети. Например, IPSec, OpenVPN, PPTP.
- Доверительные. Используются в случаях, когда передающую среду можно считать надёжной и необходимо решить лишь задачу создания виртуальной подсети в рамках большей сети. Например, MPLS, L2TP.

По способу реализации:

- В виде специально программно-аппаратного обеспечения. Реализация сети VPN осуществляется при помощи специального комплекса программно-аппаратных средств как на стороне защищенной сети, так и на стороне клиента.
- В виде программного решения. Реализация сети VPN при помощи специального программного обеспечения на компьютере пользователей для подключения к VPN-серверу.
- Интегрированное решение. Сеть VPN обеспечивает комплекс, решающий также задачи фильтрации сетевого трафика, организации сетевого экрана и обеспечения качества обслуживания.

По назначению:

- Intranet VPN. Используется для объединения в единую защищенную сеть нескольких филиалов или офисов (сетей) компании. Альтернативой может быть прокладка физических каналов связи между офисами или аренда физических каналов у провайдеров.

- Remote Access VPN. Используется для организации возможности подключения удаленного пользователя в защищенную корпоративную локальную сеть для работы с ее ресурсами.
- Extranet VPN. Используется для подключения внешних пользователей (клиентов, партнеров) к части ресурсов корпоративной сети с добавлением дополнительных ограничений на доступ.
- Internet VPN. Используется провайдерами для организации доступа пользователей к сети Интернет.
- Client/Server VPN. Используется для обеспечения защиты данных между несколькими узлами одной сети, когда необходимо в одной физической сети сделать разделение на несколько логических, но вместо деления сети VLAN-ами (Virtual Local Area Network) или различными сегментами используется шифрование части трафика.

По уровню сетевого протокола (используемого транспорта в соответствии с моделью OSI):

- Канальный. Например, PPPoE (Point-to-Point over Ethernet), L2TP (Layer 2 Tunneling Protocol), L2VPN (Layer 2 Virtual Private Network), EoMPLS (Ethernet over MPLS)
- Сетевой. Например, IPSec (Internet Protocol Security), PPTP (Point-to-Point Tunneling Protocol), L3VPN (Layer 3 Virtual Private Network)
- Транспортный. Например, OpenVPN

VPN-соединения на маршрутизаторах. Многие маршрутизаторы поставляются сразу с поддержкой VPN-клиента, чтобы организовать шифрование исходящего трафика для устройств сети, не поддерживающих технологию VPN. При этом даже в случае организации шифрования всего исходящего трафика, соединение между компьютерами сети и маршрутизатором остается незашифрованным.

Очень часто подключение к VPN-серверу используется не только для получения доступа к каким-либо внутренним ресурсам, но и для анонимизирования пользователя в сети Интернет, шифрования исходящего и входящего трафика как во внутренних, так и во внешних сегментах сети для защиты от прослушивания трафика, организации доступа к необходимым протоколам при ограничениях со стороны провайдера (часто в публичных сетях ограничивается доступ к внешним ресурсам по портам, отличным от 80 и 443), организации возможности использования определенного шлюза для обращения к некоторым ресурсам, находящимся в сети Интернет.