АНАЛИЗ ВЫБОРА И НАСТРОЙКИ ПОДКЛЮЧЕНИЯ К СЕТИ VPN

Алевтина Александровна Мурадова
ТУИТ имени Мухаммада аль-Хорезми, PhD, доцент кафедры
«Телекоммуникационный инжиниринг»
Email: a.muradova1982@inbox.ru

Искандар Лочинович Кудратов
ТУИТ имени Мухаммада аль-Хорезми, магистрант кафедры
«Телекоммуникационный инжиниринг»
Email: mysubuntu@gmail.com

Аннотация: *В статье представлен анализ выбора и настройки подключения к сети VPN. Представлены поддерживаемые протоколы туннелирования, а также методы, поддерживаемые сервером удаленного доступа. Показано значение RADIUS-сервера при подключении к сети VPN.*

Ключевые слова: *VPN, протоколы туннелирования, протокол L2TP, протокол CHAP, методы подключения, RADIUS-сервер.*

Abstract: *The article presents an analysis of the choice and configuration of a connection to a VPN network. Supported tunneling protocols are presented, as well as methods supported by the remote access server. RADIUS server value shown when connecting to VPN.*

Keywords: *VPN, tunneling protocols, L2TP protocol, CHAP protocol, connection methods, RADIUS server.*

Annotatsiya: *Maqolada VPN tarmog‘iga ulanishni tanlash va sozlash tahlili keltirilgan. Qo‘llab-quvvatlanadigan tunnel protokollari, shuningdek masofaviy kirish serveri tomonidan qo‘llab-quvvatlanadigan usullar taqdim etiladi. VPN ga ulanishda RADIUS server qiymati ko‘rsatiladi.*

Kalit so‘zlar: *VPN, tunnel protokollari, L2TP protokoli, CHAP protokoli, ulanish usullari, RADIUS server.*

Введение. При планировании виртуальных частных сетей компания должна учитывать ряд факторов, в том числе соответствующий протокол туннелирования и метод проверки подлинности. Она также должна учитывать, как лучше настроить VPN-серверы для поддержки требований удаленного доступа пользователей. Обычно VPN развёртывают на уровнях не выше сетевого, так как применение криптографии на этих уровнях позволяет использовать в неизменном виде транспортные протоколы (такие как TCP, UDP). В среде Microsoft Windows термином VPN обозначается одна из реализаций виртуальной сети - PPTP, причём, используемую зачастую не для создания частных сетей. Чаще всего для создания виртуальной сети используется инкапсуляция протокола PPP в какой-нибудь другой протокол - IP (такой способ использует реализация PPTP - Point-to-Point Tunneling Protocol) или Ethernet (PPPoE). Технология VPN в последнее время используется не только для создания собственно частных сетей, но и некоторыми провайдерами «последней мили» для предоставления выхода в Интернет. При должном уровне реализации и использовании специального программного обеспечения сеть VPN может обеспечить высокий уровень шифрования передаваемой информации.

Выбор протокола туннелирования

Можно выбрать реализацию VPN с помощью одного из нескольких протоколов туннелирования и методов проверки подлинности. VPN-подключения могут использовать один из следующих протоколов туннелирования: PPTP; Протокол туннелирования уровня 2 с IPsec (L2TP/IPsec); По протоколу SSTP (Secure Sockets Tunneling Protocol); IKEv2.

Все протоколы туннелирования VPN используют три функции: Инкапсуляция. Технология VPN инкапсулирует частные данные с заголовком, содержащим сведения о маршрутизации, что позволяет данным перемещаться по транзитной сети. Аутентификация. Существует три типа проверки подлинности для VPN-подключений, в том числе: Проверка подлинности на

уровне пользователя с помощью аутентификации по протоколу PPP. Проверка подлинности на уровне компьютера с помощью протокола IKE. Проверка подлинности источника данных и целостность данных [1,2].

Шифрование данных. Чтобы обеспечить конфиденциальность данных во время передачи по общей или общедоступной транзитной сети, отправитель шифрует данные, а получатель расшифровывает их.

В следующей таблице описываются поддерживаемые протоколы туннелирования.

Таблица 1

Поддерживаемые протоколы туннелирования

Протокол	**Описание**
PPTP	Вы можете использовать протокол PPTP для удаленного доступа и подключений VPN типа "сеть - сеть". При использовании Интернета в качестве общедоступной сети VPN сервер PPTP - это VPN-сервер с поддержкой протокола PPTP, имеющий один интерфейс в Интернете и один в интрасети.
L2TP/IPsec	Протокол L2TP позволяет шифровать трафик с несколькими протоколами, а затем отправлять его с помощью любого носителя, который поддерживает доставку датаграмм типа "точка - точка", например, протокол IP или асинхронный режим передачи (ATM). L2TP - это сочетание протокола PPTP и переадресации на уровне 2 (L2F). Протокол L2TP представляет лучшие возможности протоколов PPTP и L2F.
SSTP	SSTP - это протокол туннелирования, использующий протокол HTTPS через TCP-порт 443 для передачи трафика через брандмауэры и веб-прокси, которые в противном случае могут блокировать трафик PPTP и L2TP/IPsec. Протокол SSTP обеспечивает механизм инкапсуляции трафика PPP по каналу SSL протокола HTTPS. Использование PPP позволяет поддерживать способы строгой проверки подлинности, такие как EAP-TLS. Протокол SSL обеспечивает безопасность на транспортном уровне благодаря улучшенному согласованию ключа, шифрованию и проверке целостности.
IKEv2	IKEv2 использует протокол туннельного режима IPsec через UDP-порт 500. IKEv2 поддерживает мобильность, поэтому подходит для мобильных сотрудников. VPN на основе IKEv2 позволяет пользователям легко перемещаться между беспроводными точками доступа или между беспроводными и проводными подключениями.

Не следует использовать PPTP из-за уязвимостей системы безопасности. Вместо этого используйте IKEv2 везде, где это возможно, так как он является более безопасным и имеет преимущества по сравнению с L2TP [3-6].

Выбор способа проверки подлинности

Проверка подлинности клиентов, запрашивающих доступ, это важный вопрос безопасности. Методы проверки подлинности обычно используют протокол проверки подлинности, согласованный в процессе установки соединения. Роль сервера удаленного доступа поддерживает методы, описанные в следующей таблице.

Таблица 2

Методы, поддерживаемые сервером удаленного доступа

Метод	Описание
PAP	Протокол PAP использует пароли в виде обычного текста и является наименее защищенным протоколом проверки подлинности. Как правило, он используется, если клиент удаленного доступа и сервер удаленного доступа не могут согласовать более безопасную форму проверки. Windows Server включает протокол PAP для поддержки старых клиентских операционных систем, которые не поддерживают другие методы проверки подлинности.
CHAP	Протокол CHAP - это протокол проверки подлинности типа "запрос - ответ", использующий схему хэширования MD5 по стандартам отрасли для шифрования ответа. Различные поставщики серверов сетевого доступа и клиентов используют протокол CHAP. Однако, поскольку для CHAP требуется использовать обратимо зашифрованный пароль, следует рассмотреть возможность использования другого протокола проверки подлинности, например, MS-CHAPv2.
MS-CHAPv2	Протокол проверки подлинности Microsoft CHAP версии 2 (MS-CHAPv2) является односторонним протоколом взаимной проверки подлинности с зашифрованным паролем и имеет преимущества по сравнению с обычным протоколом CHAP.
EAP	Если используется протокол EAP, произвольный механизм проверки подлинности выполняет проверку подлинности удаленного доступа. Клиент удаленного доступа и средство проверки подлинности, которое является либо сервером удаленного доступа, либо сервером протокола RADIUS, согласовывают точную схему проверки подлинности, которую они будут использовать. Служба маршрутизации и удаленного доступа включает поддержку протокола EAP-TLS по умолчанию. Вы можете подключить другие модули EAP к серверу, на котором выполняется маршрутизация и удаленный доступ, чтобы предоставить другие методы EAP.

Дополнительные сведения

В дополнение к протоколу туннелирования и методу проверки подлинности перед развертыванием решения VPN в организации необходимо учитывать следующее.

Убедитесь, что VPN-сервер имеет два сетевых интерфейса. Необходимо определить, какой сетевой интерфейс будет подключаться к Интернету, а какой - к частной сети. Во время настройки необходимо выбрать сетевой интерфейс, который подключается к Интернету. Если указан неверный сетевой интерфейс, VPN-сервер удаленного доступа будет работать неправильно [7-9].

Определите, будут ли удаленные клиенты получать IP-адреса с DHCP-сервера в частной сети или с настраиваемого VPN-сервера с удаленным доступом. Если у вас есть DHCP-сервер в частной сети, VPN-сервер удаленного доступа может получить от DHCP-сервера 10 адресов за раз, а затем назначить их удаленным клиентам. Если у вас нет DHCP-сервера в частной сети, VPN-сервер с удаленным доступом может автоматически создавать и назначать IP-адреса удаленным клиентам. Если требуется, чтобы VPN-сервер с удаленным доступом назначал IP-адреса из указанного диапазона, необходимо определить этот диапазон [10,11].

Определите, нужен ли вам RADIUS-сервер или VPN-сервер с удаленным доступом, настроенный для проверки подлинности запросов на подключение от VPN-клиентов. Добавление RADIUS-сервера полезно, если планируется установить несколько VPN-серверов удаленного доступа, точек беспроводного доступа или других RADIUS-клиентов в частной сети.

Заключение

При подключении к сети VPN необходимо учитывать все нюансы организации, принципов подключения, способов организации локальной сети самого предприятия, а также безопасность самой сети. Можно выбрать реализацию VPN с помощью одного из нескольких протоколов туннелирования и методов проверки подлинности. VPN-подключения могут использовать один

из следующих протоколов туннелирования: PPTP; Протокол туннелирования уровня 2 с IPsec (L2TP/IPsec); по протоколу SSTP (Secure Sockets Tunneling Protocol); IKEv2. Все протоколы туннелирования VPN используют три функции: инкапсуляция, аутентификация и шифрование данных. Чтобы обеспечить конфиденциальность данных во время передачи по общей или общедоступной транзитной сети, отправитель шифрует данные, а получатель расшифровывает их. А также добавление RADIUS-сервера полезно, если планируется установить несколько VPN-серверов удаленного доступа, точек беспроводного доступа или других RADIUS-клиентов в частной сети.

СПИСОК ЛИТЕРАТУРЫ

1. Файльнер, Маркус. (2005) Виртуальные частные сети нового поколения//*LAN*. № 11.
2. Лукацкий, Алексей. (2001). Неизвестная VPN. *Компьютер Пресс*. № 10.
3. Барсков, Александр. (2010). Говорим WAN, подразумеваем VPN. *Журнал сетевых решений/LAN*, № 06.
4. Снайдер, Джоул. (1999). VPN: поделённый рынок. *Сети.* № 11.
5. Норманн, Райан. (2001). Выбираем протокол VPN. *Windows IT Pro*. № 7.
6. Петренко, Сергей. (2001). Защищённая виртуальная частная сеть: современный взгляд на защиту конфиденциальных данных. *Мир Internet.* № 2.
7. Иванов, М.А. (2001). *Криптографические методы защиты информации в компьютерных системах и сетях*. М.: Кудиц-образ. 368 с.
8. Кульгин, М. (2000). *Технологии корпоративных сетей. Энциклопедия*. СПб.: Питер. 704 с.
9. Олифер, В. Г., Олифер, Н. А. (2001). *Компьютерные сети. Принципы, технологии, протоколы*. Учебник для вузов. СПб.: Питер. 672 с.
10. Романец, Ю. В., Тимофеев, П. А., Шаньгин, В. Ф.(2002). *Защита информации в компьютерных системах и сетях*. 2-е изд. М: Радио и связь. 328 с.
11. Столлингс, В. (2002). *Основы защиты сетей. Приложения и стандарты - Network Security Essentials. Applications and Standards.* М.: Вильямс. С. 432. ISBN 0-13-016093-8.