VPN

Логическая сеть создаваемая поверх другой сети

Классификация

1. По типу использованной среды
    - Защищённый
    - Доверительный Создание надёжной защищённой подсети на основе не защищённой сети (интернет). Используют в случаях когда передающую среду можно считать надёжной и необходимо решить задачу создание вертуальной подсети в рамках большой сети.
2. По способу реализации
    - в виде специализированного программно-аппаратного обеспечения (высокая степень надёжности)
    - в виде программного решения
    - с интегрированным решением
3. По назначению
    - Intranet - используют для объединения в единую защищённую сеть нескольких распределённх филиаллов организации обменяющихся по открытым каналам связи.
    - Extranet - используют для сетей к которым подключается внешний пользователь
    - Remote Access - используют для создания защищённого канала между сегментом корпоративной сети и одиночным пользователем, которые подключаются к корпоративным ресурсам.

Варианты построения VPN

1. Построенние на базе брандмауэр поддерживает туннелирование и шифрование данных. Программное обеспечение добавляет модуль шифрования. Недостаток - зависимость производительности от программного обеспечения. Применяется для небольших сетей с небольшим трафиком
2. На базе маршрутезатора принцип схож с брандмаузером. Для повышения производительности маршрутизатора используется дополнительыйнй модуль шифрования ESA.
3. на базе программного обеспечения - используется по в большинстве случаях выполняет прокси сервера.
4. на базе операционной системы
5. на базе аппаратных средств. Используется в сетях требующих высокую производительность

-

1. туннелирование - обеспечивает передачу данных между 2 точками (окончаниеми тунеля) так что для источника и приёмника данных оказывается скрытой вся сетевая инфоструктура лежащая между ними, так что оказывается между ними 2 сетевых узла.
2. шифрование
3. аутентификация

Протоколы

На сегодняшний день, для построение впн сетей используется 3 уровня:

1. Канальный
2. Сетевой
3. Транспортный

Канальный уровень

Канальный уровень - могут использовать протоколы туннелирования данных l2tp and pptp, которые используют авторизацию и интентификацию **PPTP** - протокол двуточечной туннельной связи. Разработан компаниями 3.Com и Microsoft. Использует существующие открытые стандарты протокола TCP/IP Сервер и рабочая станция используют виртуальную сеть vpn необращая внимания на то насколько безопасной и доступной является глобальная сеть между ними. **L2TP** - появился из объединения PPTP и L2F. На сетевом уровне используется протокол IPSec реализующий шифрование а также аутентификацию абонента. Применение протокола IPsec позволяет реализовать полнофункциональный доступ эквивалентный физическому подключению к сети. **IPSec** - это согласованный набор открытых стандартов, имеющий ядро в которое может быть дополнено новыми функциями и протоколами. Ядро IPSec составляет 3 протокола = AH, ESP, IKE.

AH

Заголовок аутентификации гарантирует ценность и аутентичность данных. Позволяет приёмной стороне убедится

1. Пакет отправлен стороной с которой установлена ассоциация
2. Содержимое пакета не было искажено в процессе передачи по сети
3. Пакет не является дубликатом уже полученного пакета. Выбирается в ассоциации по желанию.

ESP

Инкапсуляция зашифрованных данных - шифрует передаваемые данные обеспечивая конфидентиальноыфа. Протокол решает две группы задач.

1. Обеспечение аутентификацию и целостность данных
2. Защита выдаваемых данных путём шифрования от несанкционированного доступа

Протоколы AH и ESP могут защищать данные в двух режимах

1. в транспортном режиме: передача данных ведётся с оригинальными IP заголовками. Заголовок остаётся неизменным.
2. тунельный режим исходные пакет помещается в новый IP пакет. Передача ведётся с новыми заголовками.

Имеется 3 схемы протокола IPSec

1. Хост - хост
2. Шлюз - шлюз

3. Хост - шлюз

Хост - конечный узел. Шлюз - промежуточный узел.

IKE

Решает вспомогательную задачу автоматического предоставления конечным точкам защищённого канала секретных ключей необходимых для работы протоколов аутентификации и шифрования данных.

SSL/TLS - реализует шифрование и аутентификацию между транспортными уровнями. Может применятся для защиты трафика TCP. каждый браузер и почтовый клиент оснащён протоколами *SSL/TLS*.

Рекомендации по применению IPSec и SSL/TLS

Протокол IPSec рекомендуется применять

1. Если требуется полнофункциональное постоянное подключение к корпоративной сети
2. Если пользователь является сотрудником компании устройством которой он пользуется для доступа к корпоративной сети.
3. Если требуется высокий уровень безопасности корпоротивной сети.
4. Если требуется высокий уровень безопасности передаваемых даннхы.
5. Если требуется масштабируемость решений в будующем

Рекомендации по применению SSL/TLS

1. Если требуется временное подключение к корпоротивной сети.
2. Если пользователь не является сотрудником компании
3. Если требуется среднее
4. Если требуется высокий уровень безопасности корпоративной сети.
5. Если требуется быстрое развертывание сети VPN.

Если требуется быстрое развёртывание и масштабируемость в дальнейшем то рекомендуется комбинацияя IPSec и SSL\TLS: использование SSL/TLS на первом этапе для осуществления доступа к необходимым услугам с последующим внедрением IPSec.