УДК 004.02

ПРОБЛЕМЫ БЕЗОПАСНОСТИ ТЕРРИТОРИАЛЬНО РАСПРЕДЕЛЕННЫХ СЕТЕЙ

Фасхутдинов П.В.
ФГБОУ ВО «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича»
Научный руководитель – преподаватель Кривоносова Н.В.
ФГБОУ ВО «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича»

Большинство современных информационных систем носят распределенный характер и могут функционировать только при наличии не только высокопроизводительной, но и безопасной корпоративной сети передачи данных. Данная работа посвящена обзору проблем безопасности территориально распределенных сетей и оценке их влияния на производительность.

Проектирование безопасной территориально распределенной сети – одна из актуальных и важных задач инженеров и системных администраторов. Поэтому при проектировании сети необходимо учитывать ряд проблем и рисков.

Основными проблемами территориально-распределенной сети являются:

- проблемы ограниченности масштабируемости;
- проблемы восстановления данных в случае возникновение ошибок;
- проблемы балансирования нагрузки.

При проектировании территориально распределенной сети особо выделяется проблема ее масштабируемости. Сеть считается масштабируемой, если она обеспечивает простоту подключения к ней новых узлов. При решении этой задачи необходимо решить проблему увеличения количество узлов системы в связи с ограниченностью служб и алгоритмов.

Автоматическое восстановление данных является очень сложной задачей. В ходе восстановления следует выяснить характер возникшей ошибки, а также классифицировать ее и выполнить автоматическое восстановление данных.

Балансирование нагрузки оказывает решающее влияние на всю эффективность работы территориально распределенной сети. Существует много подходов по решению заданной проблемы. Например, по характеру распределения нагрузки на вычислительные узлы различают: динамическую и статическую балансировки. Статическая балансировка возникает при помощи априорного анализа. При распределении ресурсов по вычислительным узлам анализируется модель территориально распределенной сети, с целью выявления наилучшей стратегии балансировки. Один из основных недостатков данного метода заключается в необходимости ассоциации узлов с различной конфигурацией оборудования с вычислительной скорости задачи, что не всегда представляется возможным.

С помощью развития криптографических технологий появился еще один способ повышения уровня информационной безопасности - с помощью технологии защищенных виртуальных частных сетей (Virtual Private Network – VPN).

Главное заблуждение в том, что VPN – единственное средство, которое может позволить организовать работу мультимедийных систем, доступ к интрасетям и т.д. Все это может существовать и без VPN. Их просто очень опасно использовать без высокой степени защиты. VPN – обеспечивает надежную защиту трафика любой из систем. VPN делает это для всех приложений, не вмешиваясь в их работу.

Основная задача VPN – защищать трафик от злоумышленников. Эта задача сложна и для ее решения VPN должна выполнять некоторые требования такие как: обладать надежной криптографией, защищаемой от прослушивания, изменения, отказа от авторства и т.д. Эти требования определены протоколами IPsec, IKE. Применение таких стандартных протоколов в VPN обязательно, иначе:

- нельзя быть точно уверенным, что поставщик VPN создал криптографически целостную и надежную систему;
- будет в дальнейшем не совместима с VPN, применяемыми контрагентами фирмы, что в конце концов приведет к смене оборудования.

Российское правительство приняло закон о запрете VPN-сервисов на территории России, кроме специализированных программных комплексов, например: ПАК ViPNet.

Таким образом, при организации территориально распределенной сети необходимо учитывать проблемы и риски. Избежав проблем, можно говорить об оптимальном качестве и безопасности ИТ-инфраструктуры.