ПОДХОДЫ К СОЗДАНИЮ ЗАЩИЩЕННОЙ СЕТИ ДОСТАВКИ КОНТЕНТА

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Хасеневич Б.Б.

Скудняков Ю.А.- канд.техн.наук, доцент

Каждый быстроразвивающийся интернет-проект сталкивается с вопросами эксплуатации и масштабирования сетевой инфраструктуры. Возникают задачи по обеспечению доступности высоконагруженных систем, и их отказоустойчивости. Выход на новый региональный рынок для интернет-проекта означает как новые перспективы развития, так и обязательство сохранить качество предоставляемых услуг. Это побуждает к использованию такого решения, как сеть доставки контента [1,2].

Важным стратегическим шагом является применение собственной сети доставки контента, что обеспечивает наиболее эффективное физическое размещение сетевого и серверного оборудования. Доступна любая тонкая настройка оборудования, которую не предоставит ни одна коммерческая сеть. Вложение ресурсов для развития собственной инфраструктуры наиболее экономически выгодно и перспективно.

На рисунке 1 приведена структурная схема сети доставки контента:

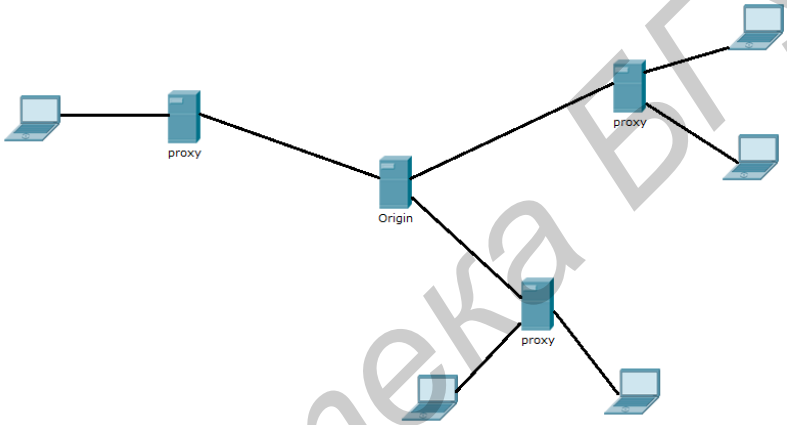

Рисунок 1 – Структурная схема сети доставки контента

Увеличение скорости загрузки контента достигается путем размещения данных как можно ближе к пользователю. За счет сокращения сетевого маршрута снижается задержка на пути между пользователем и ресурсом. Распределение нагрузки между серверами происходит за счет учета доступности и загруженности серверов перед перенаправлением на него очередного запроса. Также получаем преодоление лимитов TCP-сессий. Взаимодействие с сетью доставки контента происходит за счет использования домена 3-го уровня. Контент гибко может быть загружен на сервера путем зеркалирования, кеширования или в потоковом режиме. Зеркалирование отлично подходит для файлов большего размера, возможна преавторизация загрузки. Кэширование отлично подходит для небольших файлов.

Важно не количество точек присутствия и их связность, а прежде всего это сопоставление с потенциальной аудиторией ресурса. Сами точки присутствия не равнозначны, здесь важны связность и пиринговые подключения с локальными провайдерами.

Безопасность между серверами и сетевым оборудованием обеспечивается за счет шифрования с использованием протокола IPSec. Транспортный режим обеспечивает безопасное соединение двух терминалов путем инкапсуляции содержимого IP-данных, в то время как туннельный режим инкапсулирует весь IP-пакет на участке между шлюзами. Последний вариант используется для формирования традиционной VPN, где туннель создает безопасный путь через Интернет.

Таким образом, были определены основные причины использования сети доставки контента. Выявлены конкретные подходы к созданию защищенной сети доставки контента, принципы размещения оборудования, режимы передачи и кеширования контента разного объема. При этом решен вопрос обеспечения сетевой безопасности.

Список использованных источников:

1. habrahabr [Электронный ресурс]. – Электронные данные. – Режим доступа:: http://habrahabr.ru/.
2. wikipedia [Электронный ресурс]. – Электронные данные. – Режим доступа: http://en.wikipedia.org/.