ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ИНФОРМАЦИОННОГО ОБМЕНА В ВИРТУАЛЬНЫХ ЧАСТНЫХ СЕТЯХ НА ОСНОВЕ РЕШЕНИЯ STRONGSWAN

С.С. КАПАЦЕВИЧ

Протокол IP не имеет стандартного механизма безопасности, и IP-пакеты легко перехватывать, просматривать, изменять, пересылать повторно и фальсифицировать. Без защиты и открытые, и частные сети подвержены

несанкционированному доступу. Основанное на паролях управление доступом пользователей не обеспечивает безопасности данных, пересылаемых по сети. Этот факт и послужил причиной создания IPSec — набора протоколов для обеспечения защиты данных, передаваемых по межсетевому протоколу IP, позволяющего осуществлять подтверждение подлинности и/или шифрование IP-пакетов. Предлагается подход по обеспечению информационного обмена в виртуальных частных сетях на основе OpenSource решения StrongSwan 4.5. Суть подхода состоит в организации на межсетевом шлюзе VPN сервера, позволяющего осуществлять тунеллирование на основе стека IPSec протоколов. StrongSwan — OpenSource реализация IPsec и IKEv1/v2 для Linux 2.4/2.6. Настройка IPSec должна производиться на аппаратном маршрутизаторе с поддержкой NAT Traversal (NAT-T) так как маршрутизаторы не извлекают заголовки пакетов и работа через NAT невозможна. Для реализации подключения пользовательских терминалов (VPN клиентов) рекомендуется использовать Shrew Soft VPN Client (Windows\Linux) или KVpnc (Linux). Подход эффективен при выполнении задач быстрого развёртывания и масштабирования VPN сетей, добавление доступа к различным услугам. Уровень безопасности IPSec гораздо выше уровня безопасности, предлагаемого протоколом SSL/TLS.