

следующей тенденции: образовательные учреждения начинают использовать Интернет в большей степени для создания виртуального целостного образа учебного заведения.

Создание школьного веб-сайта – событие, которое повышает имидж образовательного учреждения. Сайт, аккумулируя в себе всю полезную информацию, является отличной визитной карточкой образовательного учреждения. Это – возможность продемонстрировать свои достижения, опубликовать информацию для заинтересованных лиц. Также это способ рассказать о своих успехах, поблагодарить спонсоров, родителей и т. д.

Активное взаимодействие учреждения образования с социальными партнерами может быть с помощью сайта более эффективным, что позволит школе не только учесть социальный заказ на образование, но и оказать на него влияние, снизить уровень конфликтности, повысить конкурентоспособность на рынке услуг образования.

**И.В. Брель (УО «ГГУ им. Ф. Скорины», Гомель)**

Науч. рук. **А.В. Воружев**, канд. техн. наук, доцент

## **ПРИМЕНЕНИЕ ТЕХНОЛОГИИ CISCO GROUP ENCRYPTED TRANSPORT VIRTUAL PRIVATE NETWORK**

Cisco GET VPN – технология от Cisco, призванная обеспечить безопасность туннелей через провайдерские соединения, обладающая рядом полезных особенностей.

Cisco GET VPN разработана для MPLS VPN сетей, позволяя обеспечить шифрование передаваемых данных без ущерба для масштабируемости и достижимости spoke-to-spoke.

GET VPN не осуществляет туннелирования, т.е. замены заголовка, что сводит на нет ее применимость при передаче данных через интернет, поскольку подавляющее большинство хостов во внутренних сетях используют частные IP адреса. В случае же MPLS VPN таких проблем не возникает за счет использования провайдером VPNv4 расширения.

Новшеством GET VPN является введение понятия «доверенной группы», все члены которой разделяют одну и ту же IPSec SA (security association). Это позволяет любому члену группы (GM, group member) расшифровать трафик, зашифрованный любым другим GM. Кроме того, поскольку расшифровать наше сообщение может каждый GM, можно рассылать мультикасты.

Для всех GM определяются одни и те же ключи шифрования. Реализуется это с помощью протокола GDOI (Group Domain of Interpretation). Используется два ключа: один для шифрования данных, другой для шифрования контрольных сообщений. Пакет, который требуется передать, инкапсулируется ESP с помощью полученного общего ключа.

За синхронизацию и обновление ключей отвечают сервера ключей (KS, key servers). Все политики шифрования, используемые протоколы, «интересный» трафик, таймеры и т. п. настраиваются на KS и распространяются по всем GM. GM сначала аутентифицируются в IKE Phase 1, а затем получают необходимые данные от KS во время регистрации. GM настраиваются только параметры IKE Phase 1 и KS. Остальное он получает автоматически.

KS становится точкой отказа для всей сети, предусмотрена возможность создания нескольких KS, называемые COOP KS (cooperative KS), с возможностью подхватывать функции в режиме холодного резерва.

Конфигурацию GET VPN можно разбить на несколько этапов:

- конфигурация PKI;
- конфигурация IKE Phase 1;
- конфигурация GDOI группы;
- конфигурация IPSec profile на KS и crypto map на GM;
- конфигурация COOP KS.

**И.В. Брель (УО «ГГУ им. Ф. Скорины», Гомель)**

Науч. рук. **А.В. Воруев**, канд. техн. наук, доцент

## **АППАРАТНАЯ ПОДДЕРЖКА VPN-ТУННЕЛЕЙ**

Виртуальная частная сеть базируется на трех методах реализации:

- туннелирование;
- шифрование;
- аутентификация.

Туннелирование обеспечивает передачу данных между двумя точками «окончаниями туннеля» таким образом, что для источника и приемника данных оказывается скрытой вся сетевая инфраструктура, лежащая между ними.

Транспортная среда туннеля подхватывает пакеты используемого сетевого протокола у входа в туннель и без изменений доставляет их к выходу. Построения туннеля достаточно для того, чтобы соединить два сетевых узла так, что с точки зрения работающего на них программного обеспечения они выглядят подключенными к одной