УДК 004.7

В.В. Чубукин, С.Н. Юров

Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ»

ВИРТУАЛЬНЫЕ ЧАСТНЫЕ СЕТИ: ВЫБОР РЕШЕНИЙ

В статье рассмотрены основные понятия и способы построения виртуальных частных сетей, предложен вариант систематизации факторов по критериям, влияющим на выбор решений.

виртуальные частные сети, Интернет, Экстранет VPN, Интранет VPN, Frame Relay

Введение

В настоящее время существенно увеличивается число предприятий, которые пользуются виртуальными частными сетями (Virtual Private network, VPN). Интерес к виртуальным частным сетям также усиливается желанием снизить расходы на подключение удаленных офисов и пользователей. Действительно,, стоимость соединения сетей через Интернет по сравнению, например, со стоимостью соединения по каналам Frame Relay существенно ниже. При объединении сетей через Интернет сразу встает вопрос о безопасности передачи данных. Сети, построенные на базе механизмов, позволяющих обеспечить конфиденциальность и целостность передаваемой информации, и получили название VPN [1]. Используя VPN, осуществляется:

– безопасное подключение сотрудников, находящихся вне предела, к корпоративной локальной сети из любой точки Интернета;

– существенное снижение затрат на организацию аутентифицированного защищенного туннеля VPN через Интернет по сравнению с двухточечными существующими сетевыми каналами [2, 3]. Существуют различные варианты построения VPN. При выборе решений необходимо учитывать множество факторов. В данной статье ставится задача систематизировать эти факторы.

Способы реализации

Все продукты для создания VPN можно условно разделить на две категории - программные и аппаратные (рис. 1). Программное решение для VPN, как правило, является готовым приложением, которое устанавливается на подключенном к сети компьютере со стандартной операционной системой. Из соображений защиты и производительности для установки VPN-приложений выделяют отдельные машины, которые устанавливают на всех концах соединений. Ряд производителей, таких как компании Axent Technologies, Check Point Software Technologies и NetGuard, поставляют VPN-пакеты, легко интегрирующиеся с программными межсетевыми экранами и работающие на различных операционных системах, включая Windows NT/XP/2000/2003, Sun Solaris, FreeBSD, Linux и MacOSX.

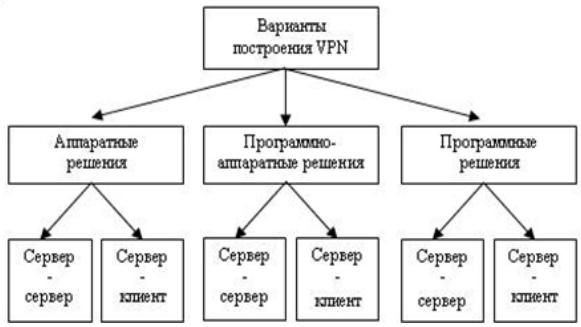

Рис. 1. Варианты построения VPN

Для развертывания программные решения обычно сложнее, чем аппаратные. Создание подобной системы предусматривает конфигурирование сервера для распознавания данного компьютера и его операционной системы, VPN-пакета, сетевых плат для каждого соединения и специальных плат для ускорения операций шифрования. Такая работа сложна и для опытных специалистов. С другой стороны, стоимость программных решений относительно ниже: в зависимости от размера сети можно приобрести VPN-пакет за 1 – 25 тыс. долл. (без стоимости оборудования, установки и обслуживания). Аппаратные VPN-решения включают в себя все, что необходимо для соединения: компьютер; специализированную, как правило, операционную систему и специальное программное обеспечение. Ряд компаний, в том числе Cisco Systems, NetScreen и Sonic, предлагают целый спектр решений, которые могут масштабироваться в зависимости от количества одновременных VPN-соединений, с которыми планируется работать, и ожидаемого объема трафика. Развертывать аппаратные решения значительно проще, и на их запуск требуется всего несколько часов. Еще одним серьезным преимуществом аппаратных VPN-решений является более высокая производительность.

В них используются специальные печатные платы и операционные системы, оптимизированные под данную задачу и освобожденные от необходимости поддерживать другие функции. К минусам аппаратных решений относится их высокая стоимость. Диапазон цен – от 2 тыс. долл. за устройство для удаленного офиса до сотен тысяч долларов за VPN-концентратор уровня предприятия. Выбор решения зависит от:

– размера сети;

– объема трафика;

– производительности оборудования.

Например, если маршрутизатор работает на пределе мощности своего процессора, то добавление туннелей VPN и шифрования информации могут остановить работу всей сети из-за перегрузки основного устройства, не говоря уже о VPN [3, 4].

Возможность построения VPN на оборудовании и ПО различных производителей достигается внедрением некоторого стандартного механизма. В качестве такого механизма выступает протокол Internet Protocol Security (IPSec). Данный стандарт, выбранный международным сообществом, группой Internet Engineering Task Force (IETF), создает основы безопасности для интернет-протокола (IP), незащищенность которого долгое время являлась проблемой. Протокол IPSec обеспечивает защиту на сетевом уровне и требует поддержки стандарта IPSec только от общающихся между собой устройств по обе стороны соединения. Все остальные устройства, расположенные между ними, просто обеспечивают трафик IP-пакетов. Протокол IPSec определяет все стандартные методы VPN, в частности методы идентификации при инициализации туннеля, методы шифрования в конечных точках туннеля и механизмы обмена и управления ключами шифрования между этими точками. К его ограничениям следует отнести работу исключительно с IP-пакетами. В числе других механизмов построения VPN можно назвать протоколы PPTP (Point-to-Point Tunneling Protocol), разработанный компаниями Ascend Communications и 3Com, L2F (Layer-2 Forwarding) компании Cisco Systems и L2TP (Layer-2 Tunneling Protocol), объединивший протоколы L2F и PPTP. Однако, в отличие от IPSec, эти протоколы нельзя назвать полнофункциональными (например, PPTP не определяет метод шифрования), поэтому мы в основном будем ориентироваться на IPSec. Говоря об IPSec, необходимо упомянуть протокол IKE (Internet Key Exchange), позволяющий защитить передаваемую информацию от постороннего вмешательства. Он решает задачи безопасного управления и обмена криптографическими ключами между удаленными устройствами. Протокол IKE, основанный на алгоритме шифрования открытым ключом, автоматизирует обмен ключами и устанавливает защищенное соединение, тогда как IPSec кодирует и «подписывает» пакеты. Кроме того, IKE позволяет изменять ключ для уже установленного соединения, что повышает конфиденциальность передаваемой информации [5].

Таким образом, для систематизации выбора вариантов построения VPN предлагается использовать следующие критерии:

– назначение (сервер, клиент);

– платформа построения (аппаратный, программный проприетарный, программный бесплатный);

– степень защищенности (аутентификация, шифрование);

– удобство эксплуатации;

– сжатие при передаче данных;

– стоимость владения;

– цена.

Ниже приведена табл. 1, представляющая собой выборку из базы данных, построенную на основе вышеприведенных критериев.

Выводы

1. Предлагаемый способ систематизации по критериям позволяет выбрать необходимый вариант построения VPN для каждого конкретного случая, в зависимости от требований потребителя по цене, производительности, защищённости, надёжности.

Таблица 1

Выборка из базы данных

Произв-одитель	Продукт	Назначение		Платформа построения		Степень защищенности		Удобство эксплуатации	Стоимость владения / Сжатие
		сервер	клиент	аппа-ратная	про-граммная	аутентифи-кация	шифрование		
Check Point Software	VPN-1 Gateway Solution	1+	1+		1+	MD5, SHA-1, CBC-DES MAC	DES, Triple-DES, DES-40, Null, CAST	GUI ОС NT, Solaris, HP-UX и AIX, LDAP, bash	1+ / 1-
Symantec	Symantec Gateway Security 400 Series	1+	1+	1+		MD5	MD5	Symantec console	1+ / 1-
	Symantec Gateway Security 1600 Series	1+	1+	1+		MD5	MD5	Symantec console	1+ / 1-
	Symantec Gateway Security 5600 Series	1+	1+	1+		MD5	MD5	Symantec console	1+ / 1-
IBM	IBM 2212 Access Utility	1+	1+	1+		MD5, SHA-1	DES, Triple-DES, DES-40	Web, NT, AIX, HP-UX	3+ / 1+
hp	ProCurve 7203dl+IPsec VPN card	1+	1+	1+		Radius	DES, 3DES, AES	ProCurveAutoSynch, ProCurveSafeMode, LinkLayerDiscovery	1+ / 1-
D-Link	DFL-100	1+	1+	1+		MD5, SHA-1	DES(56-bit) & 3DES (168-bit), Perfect forward	SSH	2+ / 1+
	DFL-200	1+	1+	1+		MD5, SHA-1, RADUS	DES(56-bit) & 3DES (168-bit), Perfect forward, AES	SSH	2+ / 1+
	DI-3660	1+	1+	1+		Radius, PAP, CHAP, TACAS+	1+	SNMP v1, v2, v3, RMON, HP Open View, Cisco View, Cisco Works, Telnet	4+ / 1+
	DI-514		1+	1+		PAP, CHAP	1-	Web интерфейс	3+ / 1+

2. Данный подход позволяет в дальнейшем (при накоплении информации о реализациях VPN в базе данных) автоматизировать процесс выбора.

Список литературы

1. Чубукин В.В. Современные тенденции и технологии организации защищенных каналов в существующих открытых сетях // МНТК ІКТМ'2005. – Х.: Нац. аэрокосм. ун-т «ХАИ», 2005. – С. 42-43.

2. Шахов В. Безопасность VPN: технологии передачи данных // BYTE РОССИЯ. – 2006. – № 6 (93). – С. 33-38.

3. Michael J. Wenstrom Managing Cisco Network Security. – Cisco Press, 2005. – 466 p.

4. Ричард Э.Смит. Аутентификация: от паролей до открытых ключей. – М.: Вильямс», 2004. – 382 с.

5. Lavigne D. VPN и IPSec на пальцах. – Сетевые решения от А до Z. [Электрон. ресурс]. – Режим доступа: http://www.nestor.minsk.by.

6. Аналитика // CNews.ru. – РИА РосБизнес Консалтинг, 2005 – [Электрон. ресурс]. – Режим доступа: http://www.cnews.ru/ newcom /index.shtml?2005 /09/16/187245.

Поступила в редколлегию 9.01.2007

Рецензент: д-р техн. наук проф. В.С. Харченко, Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», Харьков.