Защита высокоскоростного Ethernet WAN

Сравнение двух подходов шифрования данных, передаваемых по WAN-каналам связи: на Уровне 2 (например, Ethernet) и на Уровне 3 (например, IPsec).

Михаил Рожнов – технический директор TESSIS.

Введение

Высокоскоростные WAN-сети – это ответ на вызовы современных приложений и ИТ, которые требуют увеличения пропускной способности. Но знаете ли вы, что обеспечение безопасности вашего нового Ethernet WAN трафика будет вам стоить тысячи долларов каждый месяц, если вы сделаете неправильный выбор? Или что управление политикой безопасности может стать вашей самой большой головной болью и фактически вызвать перебои в работе сети? Или что утилизация ресурсов на поддержку шифрования может "съедать" половину вашей новой полосы пропускания и астрономически увеличивать задержку сети? Если нет, потратьте десять минут на чтение этой статьи.

В каких случаях еще может быть полезна технология, о которой мы хотим рассказать:

- *если есть потребность в бОльшей полосе пропускания;*
- *если необходимо выполнять нормативные требования или/и требования регуляторов;*
- *если необходимо снизить затраты на канал связи;*
- *если необходимо упростить и уменьшить время, затрачиваемое на администрирование безопасности;*
- *если ваша сеть не может справиться с новыми потребностями производительности приложений.*

Взрыв Ethernet WAN

Спрос на увеличение пропускной способности в настоящее время опережает предложения на рынке, что обусловлено, в первую очередь, конвергенцией данных, голоса и видео; новыми вычислительными технологиями и растущей зависимостью от интернета. Чтобы удовлетворить эти вызовы и одновременно снизить затраты, организации ищут не только более крупные сетевые каналы, но и возможность более "тонкого" управления полосы пропускания, а также более эффективные способы ее использования.

Ethernet поддерживает масштабируемость полосы пропускания – от 1 Мбит/с до 100 Гбит/с, обеспечивая при этом более низкие капитальные затраты в пересчете на порт, чем традиционные WAN-технологии. Благодаря этому организации могут оплачивать пропускную способность в зависимости от того, насколько они фактически ее используют, постепенно увеличивая ее по мере роста потребностей. В результате все больше компаний теперь используют собственный Ethernet для передачи данных по WAN.

Ethernet может подключаться к службам Уровня 2 или Уровня 3 для создания сетевого решения, обеспечивая высокоскоростную связь между локациями в пределах мегаполиса, между двумя городами или в рамках глобальной WAN. Ethernet-сервисы помогают расширить привычную LAN-инфраструктуру до глобальной WAN-сети, обеспечивая более высокие возможности управления прикладным уровнем по сравнению с традиционными развертываниями. Трафик центра обработки данных также быстро расширяется благодаря росту требований к доступу и к хранению данных, а также увеличению использования виртуализации. В настоящее время скорость между региональными хабами (концентраторами) при обеспечении взаимодействия между центрами обработки данных превышает 1 Гбит/с многих ведущих компаний.

Сайты для восстановления данных, требующие быстрой синхронизации SAN и адаптации к виртуализации, еще больше повышают требования к скорости сети и репликации. Ethernet WAN для удовлетворения этих требований предлагает высокоскоростные соединения с низкой задержкой через E-LAN или E-Line.

Новые приложения, например, совместная работа в группе и видеоприложения также влияют на трафик удаленных офисов и филиалов вызывают необходимость увеличения пропускной способности. Такие технологии, как IP MPLS, могут создавать длительные задержки и не всегда идеально подходят для эффективной передачи голоса и видео. Поэтому организации, имеющие несколько сайтов, перемещаются в Ethernet WAN для большей масштабируемости, гранулярности и эффективности затрат.

Обработка транзакций в режиме реального времени в брокерских фирмах и передача медицинских снимков (например, при визуализации) также среди приложений, требующих высокоскоростных сетей. Ethernet предлагает эти скорости значительно дешевле по сравнению с конкурирующими технологиями.

Благодаря быстрому распространению услуг Ethernet операторского класса технология "набирает обороты" среди предприятий, которые ценят ее способность обеспечивать более высокую пропускную способность с гранулированными настройками и управлением. Поскольку Ethernet-технология в настоящее время является зрелой, основанной на стандартах и мультивендорной, она помогает предприятиям получать масштабируемость в различных корпоративных средах со значительным снижением выделяемых затрат на ресурсы.

Физические интерфейсы Ethernet доступны в 10-мегабитных, 100-мегабитных, 1-гигабитных, 10-гигабитных скоростях и до 100-гигабитных интерфейсов.

Преимущества Ethernet:

- масштабируемая полоса пропускания для двухточечного и многоточечного соединения;
- уменьшенная сложность из-за известности интерфейсов;
- снижение эксплуатационных расходов (цена за Мбит/с) и капитальных затрат;
- подходящий уровень контроля над безопасностью;
- гибкий дизайн сетевой архитектуры;
- мультивендорная совместимость на основе промышленных стандартов.

Показатели роста

По прогнозам, к 2020 году мировой рынок оборудования для передачи Ethernet (Carrier Ethernet Equipment) достигнет $38 млрд, что обусловлено увеличением трафика данных и ростом использования услуг Carrier Ethernet *(Carrier Ethernet Equipment Market Trends, http://www.strategyr.com/MarketResearch/Carrier_Ethernet_Equipment_Market_Trends.asp)*.

Необходимость шифрования

Поскольку организации впервые начали передавать конфиденциальную информацию по внешним сетям, возникла необходимость в механизмах сетевой безопасности. Но поставщики услуг не принимают

должных мер для обеспечения целостности данных. Как правило, решение, которое они предлагают, это – изоляция трафика или данных.

Такой подход не защищает от прослушивания и несанкционированных подключений на линиях передачи, в точках коммутации и маршрутизации, является источником неправильной конфигурации и ведет к множеству других проблем.

Кроме того, нужно учитывать и то, что в то время как угрозы стали все более изощренными, одновременно все больше "чувствительных" данных стало передаваться по сетям, а это означает, что даже небольшое нарушение может привести к ошеломляющей утечке данных с соответствующими репутационными и финансовыми потерями.

Компании, чьи конфиденциальные данные передаются по разделяемым Ethernet транспортам, имеют значительные риски потерь данных. В медицинских, финансовых и правительственных организациях эти потери могут быть еще более разрушительными.

Тенденции в области информационных технологий направлены на повышение безопасности во всех аспектах управления данными: в системах, центрах обработки данных и сетях. В то время как в новых версиях приложений и операционных систем повышение безопасности значительно, улучшение сетевой безопасности остается на низком уровне. Развитие и распространение протокола IPv6, в котором выделено место для криптографической информации в заголовке, проходит медленно, и его широкое использование все еще находится на горизонте. В то же время использование IPsec с IPv4 стало стандартом для обеспечения передачи данных по сети.

Знаете ли вы, где ваше оптоволокно?

За менее чем 500 долларов человек может купить устройство «microbend tap», которое может "прослушивать" оптоволокно - без повреждения кабеля и "снимать" данные без возможности обнаружения подключения. При скоростях 10 Гбайт/с, десятки тысяч записей могут быть скомпрометированы в течение нескольких секунд после незаконного подключения. Коммерчески доступные оптоволоконные интрузионные детекторы, использующие методы измерения мощности, недостаточно чувствительны к подключениям (интрузиям) этого типа. Хотя для осуществления кражи данных с использованием этого метода, а также для интерпретации результатов требуется некоторое умение, любой – у кого есть достаточные знания и доступ к вашему волокну, может серьезно скомпрометировать вашу организацию.

Основные требования к решениям шифрования

Регулятивные требования

Помимо очевидных потребностей в шифровании в целях защиты от угроз безопасности, многие организации должны гарантировать и демонстрировать соблюдение целого ряда мандатов, включая правительственную, отраслевую и региональную политику. Необходимые механизмы шифрования должны поддерживать эти усилия и предоставлять расширенную аудиторскую отчетность.

Производительность

Производительность является критическим фактором. Поскольку изначально шифрование является ресурсоемкой технологией в части использования CPU, оно может привести к существенному ухудшению производительности. При этом в зависимости от WAN-решений шифрования и развернутой архитектуры расхождения в производительности могут быть большие. Например, некоторые подходы к шифрованию требуют туннелирования, которое использует дополнительную пропускную способность и может "съедать" дополнительную производительность, превышающую значение самого шифрования.

Поддержка конвергентной сети

Сегодня IP-сети используются для передачи голоса, видео и данных, поэтому организациям требуются решения шифрования для передачи этих активов без дополнительных задержек.

Надежная масштабируемость

Для большинства организаций сети постоянно используются практически для всех аспектов бизнеса – от телефонных сервисов до электронной почты и электронной коммерции. Следовательно, очень важно, чтобы шифрование и безопасность не мешали подключению. Например, как GRE/IPsec VPNs, так и IPsec VPNs, обеспечивают безопасную связь между сайтами, но являются сложными для управления и устранения неполадок и не являются масштабируемыми. В результате, когда масштабы и сложность глобальной WAN-сети возрастают, у многих организаций, использующих эти технологии, возникает много проблем.

Гибкость топологии сети

Любое решение для шифрования не должно препятствовать сетевому подключению и должно быть совместимо с существующими и запланированными сетевыми топологиями организации. По этим причинам организации всегда будут избегать решений по шифрованию, которые не являются гибкими и ограничивают типы топологий и дизайн, которые могут быть использованы. Это ключевой фактор, поскольку организации выбирают между интегрированными решениями для шифрования и специальными решениями для шифрования.

Управление

Решение для шифрования должно обеспечивать простое и эффективное управление политиками и удобное, основанное на ролях, администрирование для устранения потребности в высокотехническом персонале. С этой целью интеграция с системами управления сетью является обязательной. Для защиты от внутренних рисков необходимы встроенные, простые в администрировании средства управления внутренней сетью шифрования. Кроме того, решение шифрования должно также поддерживать системы управления отказами, а также такие стандарты, как SNMPv3.

Сетевое шифрование: интегрированное или выделенное?

При внедрении Ethernet WAN-шифрования между сайтами существуют два типа решений, которые наиболее часто используются. *Первый тип* состоит из решений, которые объединяют возможности шифрования в маршрутизаторах, иногда называемые «бортовым шифрованием». *Второй тип* реализует шифрование с помощью специализированных одноцелевых аппаратных устройств, которые отделены от всех других сетевых элементов.

При использовании шифрования в глобальной сети, если интегрированные и специализированные решения шифрования обеспечивают одинаковый уровень безопасности, производительности и стоимости/преимуществ, тогда логично предпочесть интегрированные решения. Но это не так.

Табл.1. Сравнение двух подходов шифрования.

	Уровень 2 (например, Ethernet)	Уровень 3 (например, IPsec)
Производительность	> отсутствие ухудшения производительности для трафика с небольшими пакетами (VoIP, видео в реальном времени); > отсутствие "отъедания" полосы пропускания для обеспечения безопасности; > практически нет латентности;	> плохая производительность, особенно для трафика с небольшими пакетами; > до 50% пропускной способности тратится впустую из-за накладных расходов Ipsec; > высокая латентность, особенно для трафика с небольшими пакетом;
Простота интеграции и обслуживания	> простота интеграция - plug-and play; > отделяет физическую или SDN-сеть от безопасности; > практически не требуется техническое обслуживание;	> трудно интегрировать в IP-сети из-за проблем с управлением IP-адресами; > изменения в сети требуют частых изменений политик и непреднамеренных отключений; > изменения в сетевых настройках влияют на безопасность;
Глубина безопасности	> режим по умолчанию - полная защита; > отделяет шифрование от функции межсетевого экрана; > не подвержены уязвимостям общим ОС маршрутизаторов; > оборудование, сертифицированное FIPS 140-2 и CC; > поддерживает последние стандарты шифрования, такие как AES-256;	> предоставляют более гранулированные опции в настройках безопасности, которые оставляют место для ошибок в реализации безопасности (например, незашифрованные соединения); > оборудование, сертифицированное FIPS 140-2 и CC; > поддерживает последние стандарты шифрования, такие как AES-256;
Надежность	> высокая устойчивость; > изменения в уровне IP не влияют на безопасность уровня 2;	> изменения в IP-сети (например, изменения IP-адреса) могут помешать настройке безопасности;
Цена	> экономически эффективное решение, требующее минимального количества шифраторов для защиты всего контура	> быстрые шифраторы IPsec стоят дорого

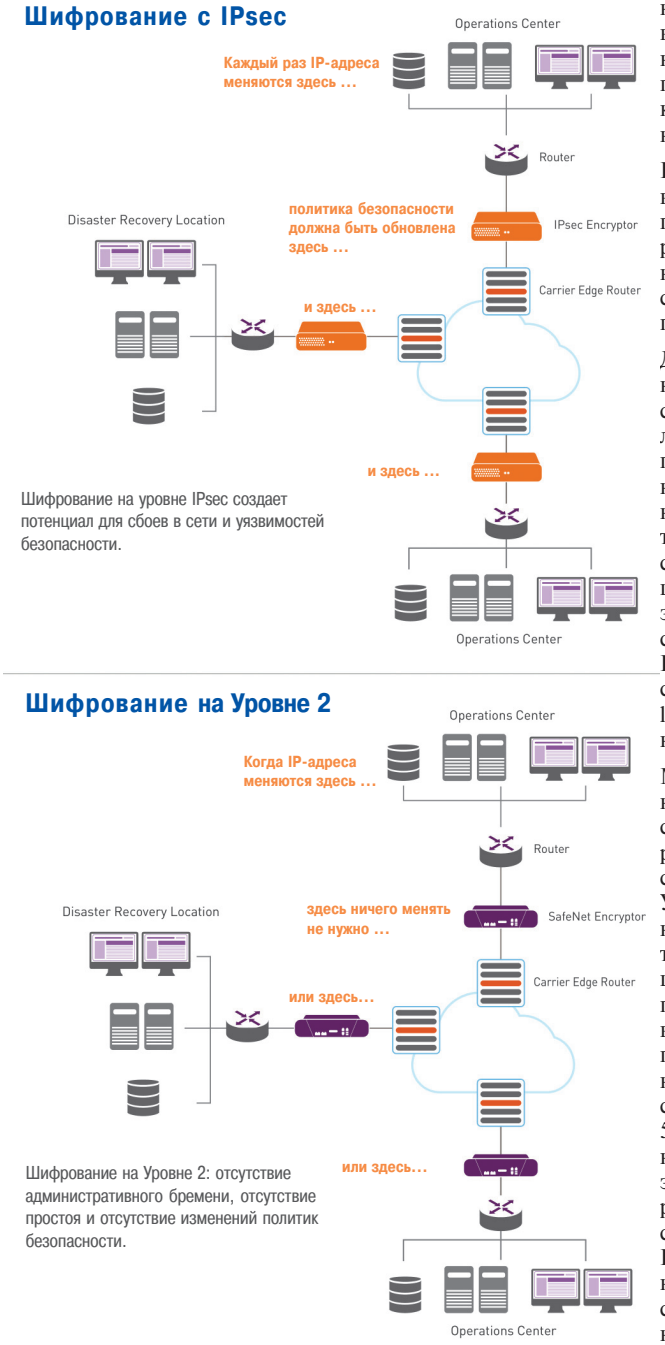

Рис. 1. Сравнение сетевых топологий для двух подходов шифрования

Интегрированные решения обычно предпочтительнее из-за более низких начальных затрат в связи с одним поставщиком и др. Кроме того, перед выбором специального устройства шифрования администраторы должны учитывать другие факторы, такие как ограничения пропускной способности и совместимость с существующей топологией WAN. В результате, многие организации использовали механизмы шифрования Уровня 3, интегрированные в маршрутизаторы сети. Но есть принципиальные преимущества для выделенных устройств шифрования, которые не всегда хорошо известны и которые приносят значительные выгоды тем организациям, которые их развертывают (табл. 1, рис. 1).

Табл.2. Уровни сетевого стека.

Уровень приложения	Уровень 5	HTTP, FTP, SMTP, POP
Транспортный уровень	Уровень 4	TCP, SSL, TLS
Сетевой уровень	Уровень 3	IP
Уровень канала передачи данных	Уровень 2	Ethernet, Frame Relay, ATM
Физический уровень	Уровень 1	SONET, SDH, OTN, DWDM

При реализации сетевого шифрования организации могут выбирать шифрование данных в одном или нескольких слоях сетевого стека (табл. 2).

Далее мы рассмотрим некоторые проблемы, с которыми столкнулись организации, использующие встроенное шифрование Уровня 3 на основе маршрутизатора, и затем рассмотрим другую форму шифрования с использованием выделенных сетевых шифраторов Layer 2 в автономной сети шифрования «overlay» и проведем сравнение этих подходов.

Многие компании обнаружили истинную стоимость накладных расходов, связанных с шифрованием на Уровне 3 с использованием IPsec в маршрутизаторе. При небольших средних размерах пакетов, типичных в сегодняшних конвергентных сетях, накладные расходы IPsec составляют от 40% до 50% общей пропускной способности, при этом связанные с этим расходы растут до тысяч долларов в месяц. Шифрование Ethernet на Уровне 2 практически исключает накладные расходы, восстанавливает пропускную способность сети и снижает совокупную стоимость владения путем оптимизации мер безопасности, упрощения управления политиками безопасности и устранения неэффективности, связанной с обычной безопасностью Уровня 3.

Высокоскоростное шифрование на Уровне 2 с Gemalto

Благодаря высокоскоростному решению SafeNet все в сетевом канале либо зашифровано, либо не зашифровано на основе источника и назначения MAC-адресов, устраняя сложность, предоставляя четкие доказательства шифрования в соответствующих местах и обеспечивая прозрачность для данных Уровня 3. Это делает возможным для протоколов IPv4 или IPv6 или любого другого типа трафика Уровня 3 прозрачно осуществлять передачу данных на высокой скорости.

Решения для шифрования Ethernet могут использоваться в различных корпоративных конфигурациях. Например, компания может использовать его для высокоскоростного внутриофисного соединения, связывая корпоративные LAN, основные офисы, центры обработки данных и центры сетевых операций. Высокоскоростное шифрование также эффективно для высокоскоростных городских сетей (MAN, metropolitan area networks), защищая данные и сети в районе метро. Кроме того, оно подходит для высокоскоростных периферийных приложений, таких как агрегация услуг, тройной режим воспроизведения (голос, видео, данные), агрегация VoIP, потоковое видео и беспроводные локальные сети. Оно также может использоваться в случае, когда происходит централизация серверов, включая серверные фермы и SAN. Наконец, высокоскоростные решения шифрования Уровня 2 могут использоваться в WAN для защиты сетевых магистралей (network backbones), LAN-расширений в многонациональных организациях и wireless backhaul.

Gemalto предлагает усовершенствованные решения для шифрования Уровня 2, которые устраняют проблемы и препятствия, присутствующие в подходах шифрования Уровня 3, обеспечивая при этом надежное шифрование.

Преимущества шифрования на Уровне 2:

– минимальная стоимость владения:
  • лучшая эффективность использования полосы пропускания (до 50%);
  • минимальные затраты на текущее обслуживание – обновления маршрутизаторов прозрачны для шифрования;
  • самое дешевое решение для агрегирования нескольких сайтов;
– максимальная производительность:
  • низкое потребление ресурсов на поддержание протокола;
  • низкая латентность;
  • устраняет GRE и сложные QoS-схемы;
– корпоративная масштабируемость:
  • быстрая, надежная сетевая интеграция;
  • простое масштабирование архитектуры до тысяч устройств;
  • Уровень 3 прозрачен – поддерживаются все протоколы уровня 3 (IPv4, IPv6 и устаревшие).

Высокоскоростные шифраторы SafeNet обеспечивают максимальную пропускную способность, сильную доступную защиту, наименьшие административные издержки и низкую совокупную стоимость владения. Решения Safepoint High Speed Encryptors (SHSE), разработанные для преодоления фундаментальных технологических ограничений шифрования IPsec, быстрее и эффективнее осуществляют передачу конфиденциальных данных на сетевом Уровне 2, тем самым снижая затраты на сетевую безопасность и поддержание регулирующих требований.

Решения SHSE, реализованные в качестве сетевого дополнения, администрируемого через объединенный центр управления, в наибольшей степени подходят для широкомасштабных реализаций сетевого шифрования. Они работают на высокоскоростном уровне 2 MAC прозрачных сетей, что делает их хорошо соответствующими для высокоскоростных город-

ских или WAN-сервисов, а также для удаленного резервного копирования, SAN, центров обработки данных, а также для обеспечения непрерывности бизнеса и восстановления после сбоев.

Снижение общей стоимости владения

Базовая и немедленная экономия затрат заключается в том, что устройства шифрования Уровня 2 устраняют накладные расходы на пропускную способность для дорогих транспортных каналов и обеспечивают полную пропускную способность, доступную с помощью технологии Layer 2 High Speed.

Они также сокращают административные расходы. Благодаря их функционированию на уровне канала передачи данных, SHSE гораздо проще развертывать и администрировать. По сравнению с подходами при шифровании Уровня 3, в решениях SHSE администраторы должны управлять лишь частью настроек, переменных и взаимосвязей при установке шифраторов SHSE. При шифровании на Уровне 3 администраторы должны постоянно поддерживать правила, политики VPN, а также туннелирование данных или соединений из точки в точку.

Основные функции высокоскоростных шифраторов SafeNet:

- полнодуплексное шифрование линии Ethernet сетей до 100 Гбит/с;
- соответствие строгим требованиям FIPS 140 2 Уровень 3, общим критериям, HATO, UC APL и требованиям безопасности CAPS;
- дизайн Bump-in-the-wire для простой установки в существующие сетевые среды;
- минимальная латентность, нулевые накладные затраты обеспечивают прозрачность операций;
- стандартная аутентификация, цифровые сертификаты и управление ключами;
- централизованное конфигурирование, мониторинг и управление;
- минимальные затраты на администрирование и низкая общая стоимость владения.

Каждый раз, когда новое устройство добавляется в меш-архитектуру, например, все соединения должны быть сконфигурированы в сложных таблицах маршрутизации. Напротив, одно и то же изменение в решениях при поддержании безопасности на Уровне 2 потребует только добавления сертификата проверки подлинности безопасности, позволяющего другим устройствам безопасно разговаривать с новым устройством без дополнительного времени и затрат на управление. Общие преимущества включают простое развертывание, простоту управления и снижение общей стоимости владения.

Решения SHSE управляются надежным веб-приложением, основанным на политиках, которое является простым в использовании и безопасном, а также предоставляет расширенные возможности аудита и мониторинга, необходимые для обеспечения безопасности.

Интегрированное управление позволяет администраторам удаленно настраивать, контролировать и обновлять все высокоскоростные шифраторы SafeNet в сети. Это также дает возможность определять интегрированные политики безопасности, которые могут быть распределены между несколькими устройствами, что снижает сложность и стоимость управления. Gemalto также имеет ряд высокоуровневых операторского класса опций высокой доступности, чтобы ваша система управления была устойчивой к сбоям в сети и системе.

Упрощение выполнения требований соответствия

Проверка соответствия в решениях SHSE гораздо проще, чем в средах при шифровании на Уровне 3. Gemalto предоставляет подробный, централизованный архив журналов, который значительно упрощает отчетность по соблюдению регулятивных требований и ремедиацию. Все высокоскоростные шифраторы SafeNet сертифицированы FIPS на соответствие 140-2 Уровня 3, обеспечивая соблюдение множества правительственных и коммерческих требований. Gemalto также предлагает ряд шифров, которые сертифицированы Common Criteria, NATO, UC APL и CAPs (UK), а также FIPS 140-2 L3. Кроме того, Gemalto благодаря приобретению SafeNet, является одним из немногих поставщиков безопасности, которые в течение многих лет поставляют продукты для высоконадежных правительственных сетей, а также коммерческих сетей. 85% межбанковских переводов осуществляется на высокоскоростных шифраторах SafeNet.

Повышение производительности

В отличие от шифрования IPsec, высокоскоростные шифраторы SafeNet шифруют весь IP-пакет без накладных расходов, отдельно зашифровывая дополнительный IP-заголовок. Это означает, что по мере того, как высокоскоростной кадр Уровня 2 перемещается по промежуточным сетям между двумя первичными сайтами, MAC-адрес исходного кадра не изменяется. Поскольку маршрутизаторы, работающие на Уровне 3, изменяют MAC-адрес высокоскоростного фрейма, зашифрованный кадр не может проходить через маршрутизатор до дешифрования.

По сравнению с использованием IPsec высокоскоростные шифраторы SafeNet лучше подходят для WAN-соединений, потому что они менее сложны и более эффективны. Зашифровав конфиденциальные данные на Уровне 2, весь высокоскоростной кадр и, следовательно, все данные, проходящие через сеть, зашифрованы. Кроме того, заменяя устаревшее решение шифрования IPsec с помощью высокоскоростного шифрования SafeNet, пропускная способность практически удваивается, а задержка через сетевое соединение IPsec сокращается в 13 раз. Это более привлекательная альтернатива, чем покупка или лизинг дорогостоящего канала с высокими ежемесячными расходами.

Архитектура

Благодаря простой имплементации, решения SHSE обеспечивают большую гибкость в подходах к развертыванию. Благодаря этим решениям полное меш- развертывание на большом количестве сайтов является выполнимым и экономичным. Кроме того, благодаря поддержке VLAN, SHSE также упрощают hub-and-spoke развертывание

Совместимость

Развертывание SHSE-шифраторов в качестве дополняющего решения на Ethernet никак не влияет на существующую инфраструктуру. В результате все системы, расположенные в данной сети, работают без каких-либо изменений. Это дает организациям гибкость, необходимую им для максимизации существующих инвестиций, а также полную гибкость в будущем. SafeNet High Speed Encryptors совместимы со следующими типами сетей:

- Carrier High Speed (E-Line / E-LAN);
- DWDM/Dark Fibre;
- High Speed over MPLS;
- High Speed over OTN (G.709);
- High Speed II, IEEE 802.3;
- Jumbo Frames;
- VLAN, QinQ.

Пропускная способность при шифровании на уровне IPsec

Независимое исследование Рочестерского технологического института (RIT, Rochester Institute of Technology) продемонстрировало, что потенциальные преимущества дорогостоящих высокоскоростных сетей могут быть серьезно омрачены потерей пропускной способности, что часто увеличивает, а не уменьшает общую стоимость владения из-за чрезмерного управления и проблем с пропускной способностью. Полученные данные показали, что технологии шифрования SafeNet High Speed Encryptor Layer 2 обеспечивают превосходную пропускную способность и значительно меньшую задержку, чем IPsec VPNs операции на Уровне 3. Фактически, из-за большого снижения пропускной способности при использовании решений шифрования IPsec их можно характеризовать как “решения с пропускной способностью, направленной внутрь». Рассмотрим некоторые из этих различий в деталях.

Проблема с IP-заголовком

В транспортном режиме IPsec имеет меньше служебных данных, но не обеспечивает конфиденциальность для IP-заголовка Уровня 3. Это означает, что конфиденциальная информация об адресе внутренней сети может быть злонамеренно получена путем мониторинга сети общего пользования, по которой проходит трафик.

Туннельный режим IPsec решает эту проблему безопасности, шифруя весь IP-пакет и инкапсулируя его в другой IP-пакет, который содержит только адрес устройств шифрования в любой конечной точке, а не фактические хосты, взаимодействующие во внутренней сети.

Однако, хотя туннельный режим устраняет проблемы безопасности и конфиденциальности транспортного режима IPsec, но одновременно он добавляет значительный объем служебных данных. Обработка этого дополнительного IP-заголовка приводит к некоторым проблемам с производительностью с точки зрения задержек.

SHSE-шифраторы снимают проблемы, возникающие в туннельном режиме IPsec, за счет того, что размещаются на краю сети и шифруют весь IP-пакет без добавления служебных данных дополнительного IP-заголовка.

Тестирование

В тестах RIT, моделируемых на RFC 2544, использовались две карты Cisco Gigabit Ethernet, установленные в двух высокопроизводительных шасси Cisco Catalyst 6509, два модуля Cisco Services IPsec VPN Services, два выделенных высокопроизводительных SafeNet Ethernet шифратора Уровня 2 и Ixia 250 тестовая платформа, соединенных простой сетью (рис. 2). В тестах была установлена базовая инфраструктура для учета сокращения полосы пропускания, вызванного служебными данными протокола Ethernet. Затем измерения включали потерю кадров, пропускную способность и задержку зашифрованных и незашифрованных данных для диапазона размеров кадров.

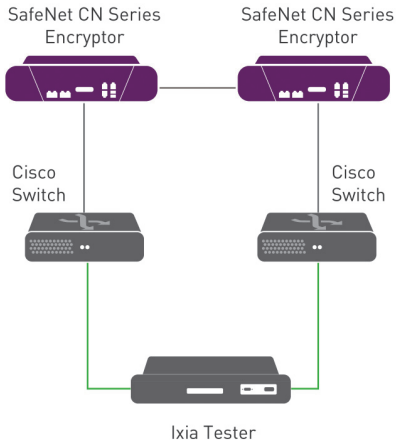

Рис. 2. Конфигурация при тестировании.

Потеря кадров

Потеря кадров – это разница между количеством кадров, передаваемых одним интерфейсом, и количеством кадров, полученных другим. Тесты RIT определяли максимальную скорость, с которой устройства могли работать без потери кадров.

Решение SHSE испытало потерю менее 1/1000-го из 1% потерь кадров для каждого заданного размера кадра. Эта величина потери кадров статистически незначительна и приводит к средней потере кадра 0 для 100% скорости линии.

Для сравнения, тест шифрования IPsec показал, что потеря значительна для всех размеров кадра. По мере увеличения нагрузки также наблюдалась потеря кадров. По мере уменьшения размеров кадров, потеря кадров увеличивалась логарифмически. При 64 байтах фрейма (малые размеры фреймов типичны для чувствительных к задержкам видео- и VoIP-приложений) более 40% потерь кадров наблюдалось при 30% максимальной теоретической пропускной способности (рис. 3).

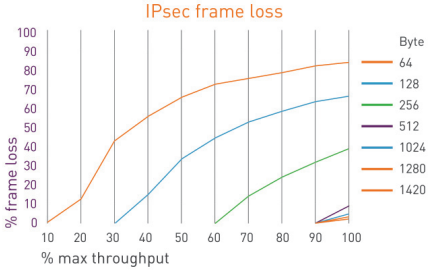

Рис. 3. Процент потерь фреймов в зависимости от их размера при шифровании на уровне IPsec.

Это значительно ограничивает доступную полосу пропускания, которая может использоваться при шифровании IPsec.

Пропускная способность

Стандартный Ethernet-фрейм способен передавать 1500-байтовую полезную нагрузку, не включая CRC, MAC, поле управления, UDP, ссылку или Ethertype-данные. Ethernet включает в себя преамбулу 8 байтов в начале кадра и межкадровый разрыв 12 байтов, которые вместе уменьшают максимальную теоретическую пропускную способность данного канала.

Было обнаружено, что высокоскоростные шифраторы SafeNet не влияют на пропускную способность в любом направлении, независимо от размера кадра, а пропускная способность остается на уровне 100% от максимальной теоретической пропускной способности.

Использование шифрования IPsec добавляет 57 байтов служебных данных, инкапсулированных в IP-заголовк исходного. Как видно на рис. 4, при меньших размерах кадра добавление 57 байт оказывает

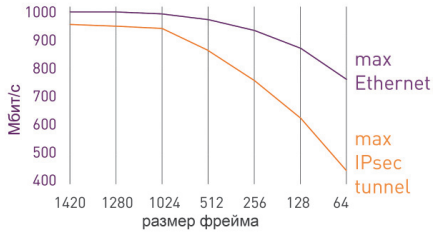

Рис. 4. Сравнение теоретической и реальной пропускной способности при шифровании на уровне IPsec.

значительное влияние на максимальную теоретическую пропускную способность.

Решение шифрования IPsec не смогло достичь максимальной теоретической пропускной способности при меньших размерах кадров. При размерах в 512 байт, 1024 байта и 1280 байт достигалось приблизительно 100% максимальной теоретической пропускной способности. Но при 256-байтных кадрах производительность составила всего 73%, при 128-байтных кадрах она упала еще до 47%, а в 64-байтных кадрах она составляла всего 27% от максимальной теоретической пропускной способности.

SafeNet High Speed Encryption:
100% пропускная способность (все размеры кадра)
Шифрование IPsec:
27% пропускной способности (64-байтовые кадры)

Задержка

Тесты RIT измеряли время, необходимое первому биту кадра для прохождения тестовой сети от источника до места назначения, используя в среднем 10 проб. Сравнение результатов было выполнено как процентное увеличение по сравнению с соответствующей незашифрованной базовой задержкой для каждого теста (рис. 5).

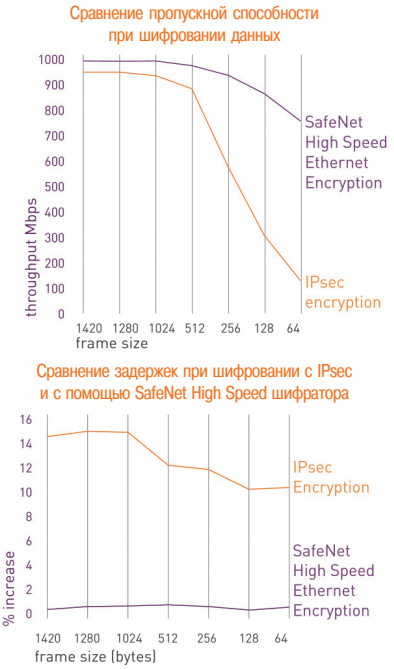

Рис. 5. Сравнение пропускной способности и задержек при разных подходах шифрования.

Ожидается, что каждое сетевое устройство, добавленное в систему, вводит дополнительную задержку. Средняя задержка для трафика, проходящего через тестовую сеть, варьировалась от 1210 мкс (1,2 мс) для 64-байтовых кадров до 1308 мкс (1,3 мс) для 1420-байтовых кадров. Добавление SafeNet Ethernet шифрования добавило менее 1% от этой базовой линии.

IPsec шифрование, в среднем, показало задержку в 13 раз бОльшую в сравнении с задержкой достигнутой при использовании SafeNet High Speed шифраторов.

Заключение

С теоретической точки зрения производительность шифрования Ethernet Уровня 2 должна превосходить производительность шифрования IPsec Уровня 3. Тестирование подтверждает реальность ограничений по пропускной способности и задержкам, вызванных добавлением служебных данных к фрейму при шифровании IPsec.

В отличие от IPsec шифрования, SafeNet Ethernet Encryptor работает на линейной скорости, практически не внося задержки и не сужая полосу пропускания.

Тестирование также не выявило значительных потерь кадров с помощью решения SafeNet Ethernet для шифрования, тогда как при использовании шифрования IPsec была установлена значительная потеря кадров и сравнительно низкие скорости передачи данных.

Наконец, измеренная латентность решения Cisco IPsec для шифрования оказалась более чем в 13 раз выше, чем решение SafeNet Ethernet для шифрования. В средах, где технология шифрования Ethernet отвечает потребностям организации, ее производительность явно превосходит производительность шифрования IPsec.

Михаил Рожнов,
компания TESSIS.