УДК 681.3.07

ВЛИЯНИЕ АЛГОРИТМОВ ШИФРОВАНИЯ И ХЕШИРОВАНИЯ НА СКОРОСТЬ ПЕРЕДАЧИ ДАННЫХ ПО VPN-СОЕДИНЕНИЯМ ПОД НАГРУЗКОЙ

Васин Н.Н., Аленников Е.М., Субботская А.Ю.
Поволжский государственный университет телекоммуникаций и информатики, Самара, РФ
E-mail: vasin-nn@psuti.ru

Технология виртуальных частных сетей в настоящее время является основной для обмена конфиденциальной информацией по сети Интернет. Технологии, используемые для защиты трафика, передаваемого по таким сетям, задействуют ресурсы маршрутизатора и влияют на скорость обработки данных. Использование маршрутизаторов для шифрования и дешифрования данных может сказаться на скорости передачи этих данных по такой сети, особенно если по такой сети передается не только трафик VPN, но и трафик обычных пользователей сети Интернет. В данной работе сравнивается влияние алгоритмов шифрования и хеширования на процесс передачи пакетов по двум типам VPN-соединений: Client-to-Site и Site-to-Site. Проведено исследование влияния алгоритмов шифрования и хеширования на скорость и работоспособность двух технологий VPN-соединения при загрузке канала связи. Данный эксперимент проводился на компьютерной и физической моделях. Компьютерная модель сети была создана в эмуляторе сетей GNS3, физическая модель была собрана с помощью маршрутизаторов нового поколения с интегрированными услугами Cisco RV 340. Результаты исследования представлены в виде графиков и диаграмм.

Ключевые слова: *VPN-туннель, шифрование, хеширование, компьютерная модель, физическая модель*

Введение

При передаче сообщений по общедоступной сети Интернет основным требованием является безопасность сетей телекоммуникаций [1; 2]. Стоимость виртуальных частных сетей (VPN) значительно ниже выделенных линий, притом что создаваемые VPN-соединения обеспечивают требуемый уровень защиты от угроз. Для обеспечения безопасности таких сетей широко используется набор протоколов IPsec, реализуемых на сетевом уровне [3].

IPsec включает три основных протокола:

– заголовка аутентификации (Authentication Header – AH);

– обеспечения конфиденциальности (Encapsulating Security Payload – ESP);

– обмена секретными ключами (Internet Security Association and Key Management Protocol – ISAKMP).

Функции AH и ESP в значительной степени перекрываются, поэтому для создания VPN выбирают один из протоколов, в предлагаемой работе – ESP.

Таблица. Протоколы и алгоритмы IPsec

Функция	Название протокола			
IPsec	AH		ESP	
Шифрован.	DES	3DES	AES	SEAL
Целостность	MD5	SHA-1	SHA-2	SHA-3
Аутентифик.	PSK		RSA	
Ключи	DH1	DH2	DH5	DH14

Для создания туннеля IPsec применяется ряд алгоритмов: шифрования, проверки целостности (хеширования), аутентификации, обмена ключами (таблица), которые требуют дополнительных ресурсов маршрутизатора, что влияет на скорость передаваемых файлов по VPN-соединению.

Проведение эксперимента

Для изучения влияния степени загрузки канала связи на скорость передачи данных по VPN-соединению было реализовано две модели сети с различными типами VPN [4]: Client-to-Site (рисунок 1), Site-to-Site (рисунок 2).

Компьютерное моделирование соединений VPN проведено на эмуляторе GNS3 [5], где на маршрутизаторах был задан ряд параметров, предусмотренных стандартом IPSec [3].

Для настройки IPSec необходимо:

• настроить систему авторизации и учета событий для добавления пользователей, которым будет разрешен доступ по VPN (только для Client-to-Site);

• настроить политику ISAKMP: выбрать алгоритм шифрования, алгоритм хеширования, выбрать группу Диффи – Хелмана, выбрать метод аутентификации, где данные настройки соответствуют настройке первой фазы IPSec;

• настройка второй фазы включает в себя настройку набора преобразований (настройку используемых алгоритмов шифрования и хеширования), а также настройку алгоритмов передачи AH или ESP;

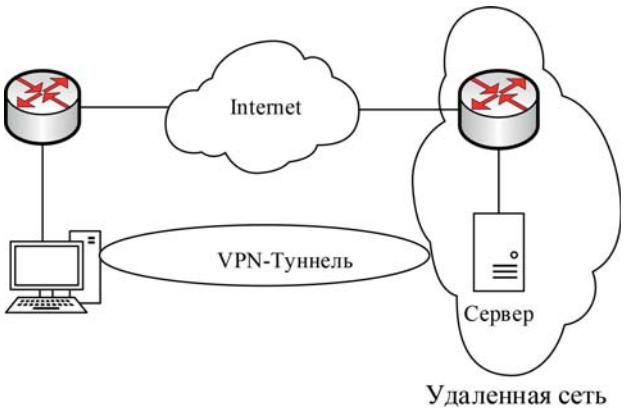


Рисунок 1. Модель с VPN-туннелем Client-to-Site

• настроить динамическую криптографическую карту и привязать настройки IPSec к ней;

• так как динамическую криптографическую карту нельзя привязать к интерфейсу, то необходимо создать обычную криптографическую карту и связать ее с динамической, затем привязать созданную криптографическую карту к выходящему интерфейсу маршрутизатора.

В первой фазе настройки IPsec указан ряд алгоритмов и протоколов:

– crypto isakmp policy 101;
– encr aes;
– hash md5;
– authentication pre-share;
– group 2.

Приведенная последовательность команд задает политику (101). При моделировании используется алгоритм шифрования (encr aes), который рекомендован в настоящее время. Алгоритм проверки целостности (hash md5) считается устаревшим, но MD5 широко используется при обучении студентов, поскольку принцип его работы тот же, что и новых алгоритмов [6]. Для аутентификации использован алгоритм общего секретного ключа (pre-shared secret key – PSK). Параметр (group 2) позволяет устройствам на двух сторонах туннеля создать общий секретный ключ для шифрования данных при обмене по сети открытыми ключами (метод Diffie-Hellman – DH). Алгоритмы DH1, DH2, DH5 вполне пригодны для моделирования, т. к. реальных угроз при моделировании нет. Затем производится обмен ключами аутентификации:

```
RA(config)#crypto isakmp key cisco2021-1 address 200.10.10.2
RB(config)#crypto isakmp key cisco2021-1 address 200.10.10.1
```

Вторая фаза создания VPN-туннеля начинается с создания набора преобразования (Transform Set), который назван **VPN-SET-1**:

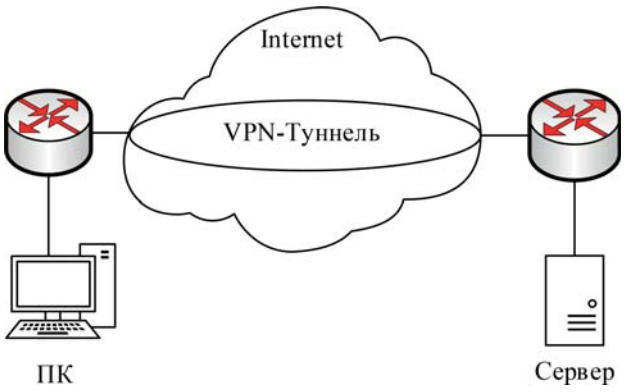


Рисунок 2. Модели с VPN-туннелем Site-to-Site

```
RA(config)#crypto ipsec transform-set VPN-SET-1 esp-aes esp-md5-hmac
```

Алгоритмы шифрования (**esp-aes**) и «хеширования» набора **VPN-SET-1** (**esp-md5-hmac**) должны совпадать с соответствующими параметрами политики ISAKMP.

Создаваемая далее криптографическая карта (crypto map) содержит наборы правил для разных VPN-туннелей. Набор правил идентифицирует порядковый номер (10 в нижеприведенном примере):

```
RA(config)#crypto map MAP-1 10 ipsec-isakmp
RA(config-map)#set peer 200.10.10.2
RA(config-map)#set transform-set VPN-SET-1
RA(config-map)#match address SPISOK
```

Последняя строка конфигурации разрешает передачу данных по туннелю при совпадении адресов со списком доступа SPISOK.

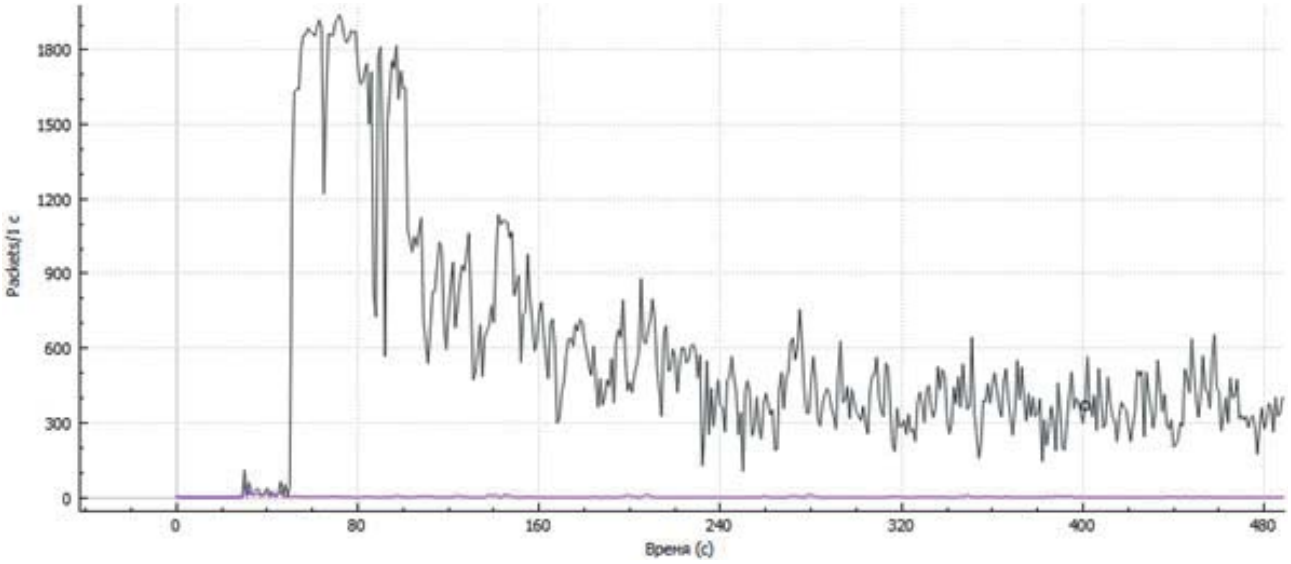
Привязка криптокарты к исходящему интерфейсу производится по команде:

```
RA(config)#interface FastEthernet0/1
RA(config-if)#crypto map MAP-1
```

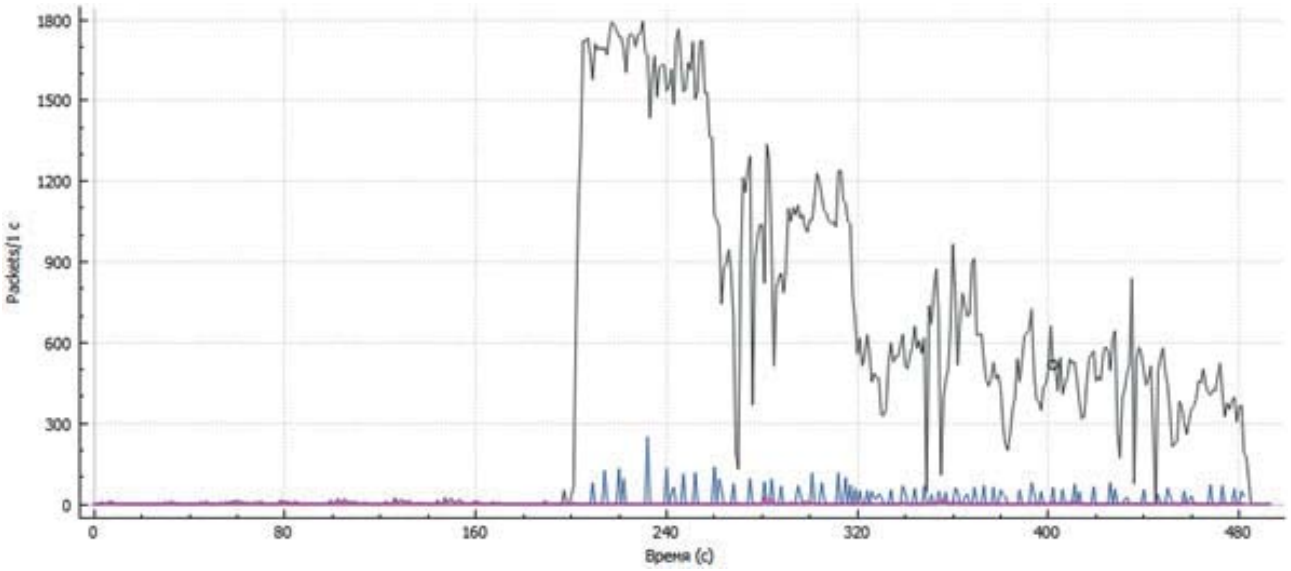
В завершение конфигурирования формируется список контроля доступа с именем SPISOK, которое было использовано при создании криптокарты:

```
RA(config)#ip access-list extended SPISOK
RA(config-ext-nacl)#permit ip 192.168.10.0 0.0.0.255 192.168.0.0 0.0.0.255
```

На каждой из моделей сети, представленных на рисунках 1, 2, было проведено исследование влияния степени загрузки канала связи на скорость передачи данных по VPN-соединению с различными типами шифрования и хеширования: aes/sha, aes/md5, 3des/sha, 3des/md5 [7]. Суть исследования состояла в том, что при подключении



а



б

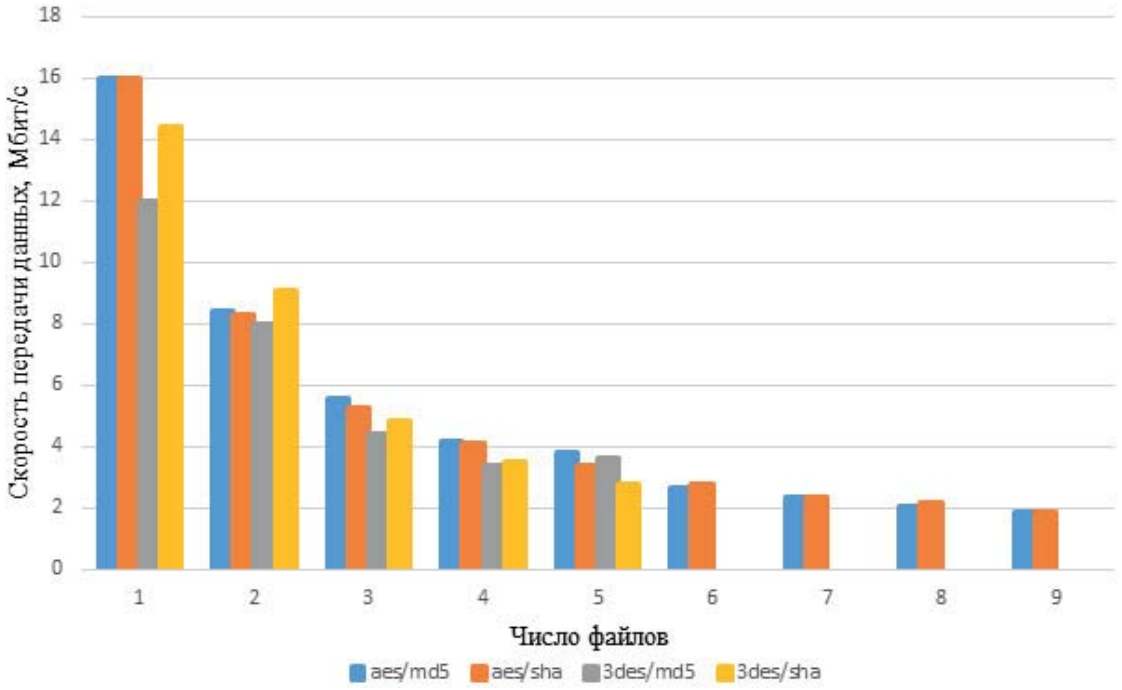
Рисунок 3. Скорость передачи пакетов для одного пользователя: *а* – VPN Client-to-Site; *б* – VPN Site-to-Site

ПК к серверу по виртуальной частной сети загружался с FTP-сервера один файл, фиксировалось показание скорости загрузки данного файла; затем проводилась одновременная загрузка от двух до девяти файлов одинакового размера с того же сервера, также фиксировались скорости загрузки всех файлов. В качестве FTP-сервера использовалась программа FileZilla [8] Server, подключение к которой со стороны клиента происходило с помощью файлового менеджера FileZilla Client.

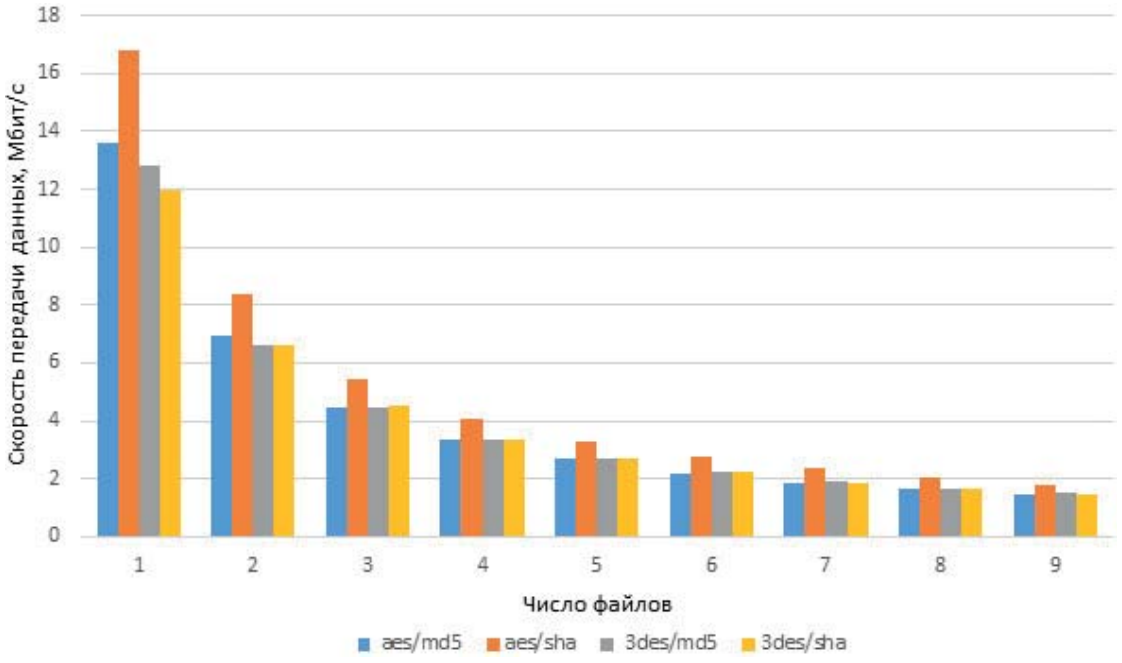
Во время подключения большого числа пользователей к VPN, каждый из них скачивал файлы с FTP-сервера, тем самым происходило увеличение нагрузки на канал связи. С помощью программы Wireshark [9] фиксировалось изменение скорости передачи файлов для одного пользователя для всех типов VPN. Данные результаты приведены на рисунках 3, *а* (VPN Client-to-Site) и *б* (VPN Site-to-Site).

На данных рисунках изображено изменение числа передаваемых пакетов в единицу времени (по оси X – время в секундах, по оси У – число передаваемых пакетов). Скорость передачи пакетов в VPN типа Client-to-Site при увеличении нагрузки на канал связи уменьшается плавно по экспоненциальному закону, тогда как при увеличении нагрузки на канал связи в VPN типа Site-to-Site скорость передачи пакетов уменьшается резкими рывками и в некоторые моменты времени достигает нулевого значения.

После загрузки были посчитаны средние скорости всех одновременно загруженных файлов. Результаты представлены в виде столбчатых диаграмм, которые приведены на рисунках 4, *а* (VPN



а



б

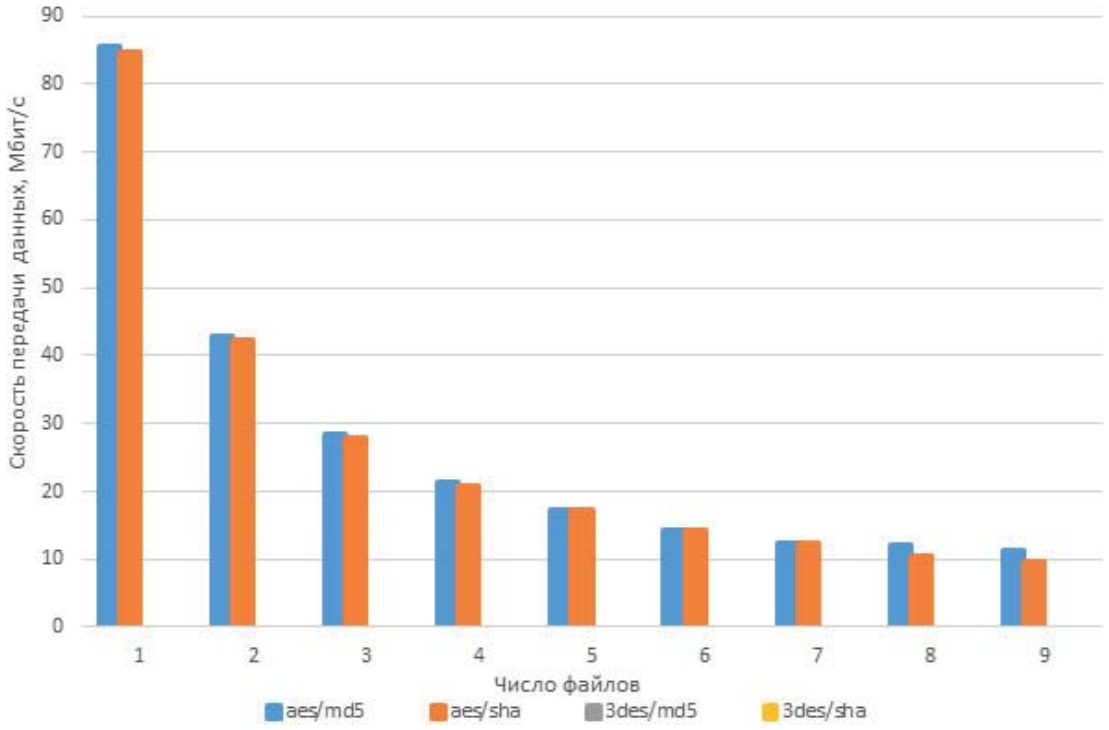
Рисунок 4. Результаты компьютерного моделирования: *а* – VPN Client-to-Site; *б* – VPN Site-to-Site

Client-to-Site) и *б* (VPN Site-to-Site). На приведенной диаграмме по оси X отложены столбцы, которые обозначают скорости передачи данных по VPN-соединению при одновременной загрузке от одного до девяти файлов одного размера.

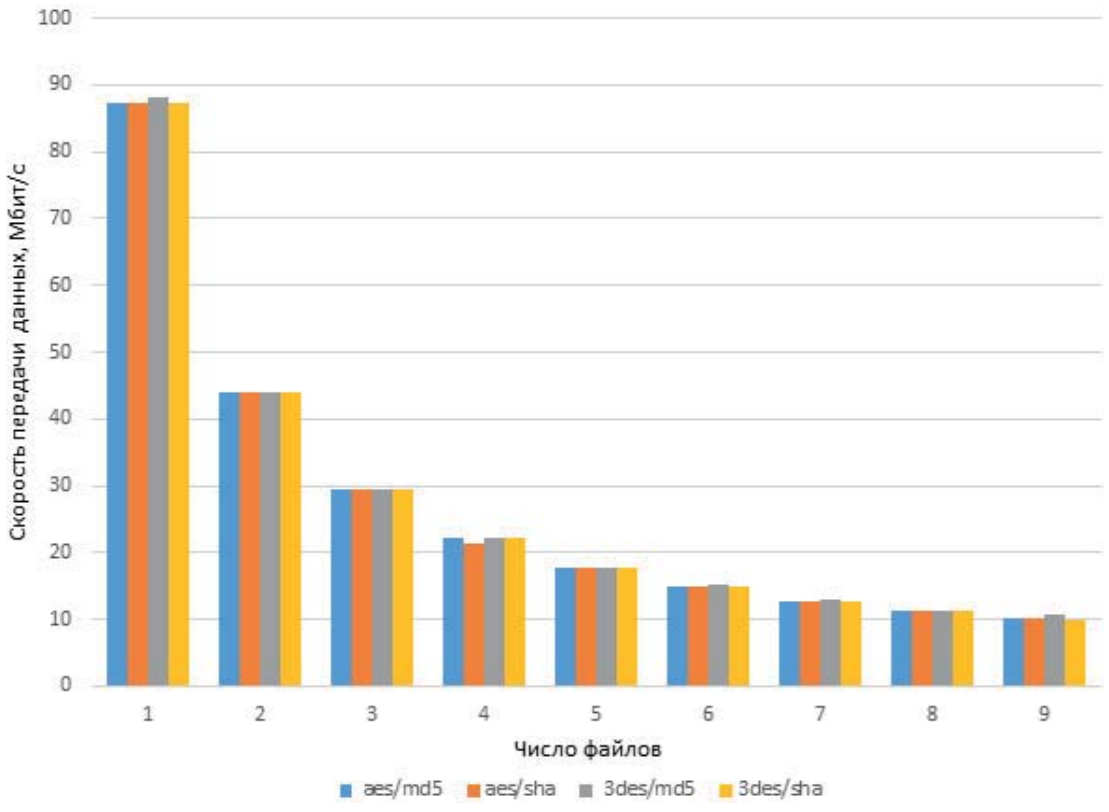
Из рисунков 4, *а* и *б* понятно, что наивысший показатель скорости передачи файлов показывает VPN-туннель с алгоритмами aes/sha. Также из рисунка 4, *а* видно, что при большой нагрузке на канал связи при алгоритмах 3des/md5 и 3des/sha происходит разрыв соединения.

Проверка достоверности результатов компьютерного моделирования проведена на физической модели сети. Для этого был создан программно-аппаратный комплекс на базе маршрутизаторов нового поколения с интегрированными услугами Cisco RV340 [10].

Эксперимент проводился так же, как и при компьютерном моделировании. Клиент подключался по VPN к FTP-серверу и скачивал один файл, скорость передачи этого файла фиксировалась; далее клиент увеличивал число скачива-



а



б

Рисунок 5. Результаты физического моделирования: *а* – VPN Client-to-Site; *б* – VPN Site-to-Site

емых файлов от двух до девяти, высчитывалась средняя скорость передаваемых файлов, и полученный результат фиксировался.

Результаты эксперимента на физической модели представлены в виде столбчатых диаграмм на рисунках 5, *а* (Client-to-Site) и *б* (Site-to-Site).

Анализ результатов

Из результатов эксперимента видно, что с увеличением нагрузки на канал связи скорость загрузки первого файла с FTP-сервера снижается.

Технология Client-to-Site имеет самые высокие скорости загрузки для типов шифрования/

хеширования aes/sha и aes/md5, но они не превышают скорость технологии Site-to-Site. Однако при сочетании алгоритмов шифрования/хеширования 3des/md5 и 3des/sha при большой нагрузке на канал связи, более пяти одновременно загружаемых файлов, VPN-туннель «разрушается» и дальнейшее его использование невозможно.

В VPN-соединении типа Site-to-Site параметры aes/sha поддерживают самую высокую скорость передачи файлов.

При физическом моделировании прослеживается та же закономерность, что и при компьютерном: с увеличением нагрузки на канал связи скорость загрузки файлов снижается. При совместном использовании типа шифрования 3des и всех типов хеширования в технологии Client-to-Site VPN-туннель работает нестабильно: соединение показывало предельно высокие скорости загрузки (выше 1 Гбайт/с), что приводило к отказу конечного оборудования (персонального компьютера). При всех остальных сочетаниях типов шифрования и хеширования значительной разницы в скорости передачи данных не наблюдается.

Заключение

Исходя из приведенных в работе результатов, можно сделать выводы:

– с увеличением нагрузки на канал связи скорость загрузки файлов снижается;

– для организации VPN рекомендуется применять алгоритмы шифрования и хеширования aes/sha, и, как видно из полученных результатов, при этом сочетании алгоритмов шифрования/хеширования VPN-туннель показывает стабильную работу под нагрузкой, а также имеет высокий показатель скорости по сравнению с другими сочетаниями;

– при компьютерном моделировании у всех технологий VPN наилучший показатель скорости загрузки файлов был с параметрами aes/sha;

– физическое моделирование подтвердило результаты моделирования и показало, что во всех рассмотренных типах VPN и при любом сочетании алгоритмов шифрования и хеширования нет существенной разницы в скорости передачи файлов, и поэтому следует использовать рекомендованные сочетания алгоритмов, а именно aes/sha, так как они обладают лучшей защищенностью.

Литература

1. Таненбаум Э., Уэзеролл Д. Компьютерные сети. СПб.: Питер, 2012. 41 с.
2. Олифер В., Олифер Н. Компьютерные сети. Принципы, технологии, протоколы. СПб.: Питер, 2016. 771 с.
3. Стандарт IETF (RFC 2401-2412). Архитектура безопасности для интернет-протокола. URL: https://datatracker.ietf.org/doc/html/rfc2401 (дата обращения: 12.05.2021).
4. Егоров А.Н. Моделирование компьютерных сетей. СПб.: ГУМРФ имени адмирала С.О. Макарова, 2015. URL: https://studfile.net/preview/5851940/page:35 (дата обращения: 12.05.2021).
5. Васин Н.Н., Аленников Е.М. Влияние алгоритмов шифрования на скорость передачи пакетов в пользовательской VPN // Проблемы техники и технологий телекоммуникаций (ПТиТТ-2020), IV Научный форум Телекоммуникации: теория и технологии (ТТТ-2020): сборник трудов XXII Международной научно-технической конференции. 2020. С. 250–251.
6. Васин Н.Н., Аленников Е.М., Субботская А.Ю. Моделирование виртуальных частных сетей: методические указания по выполнению лабораторной работы. Самара: ПГУТИ, 2020. 30 с. URL: http://eclib.psuti.ru/cgi-bin/irbis64r_12/cgiirbis_64.exe (дата обращения: 12.05.2021).
7. Что такое шифрование 3DES и как работает DES? URL: https://heritage-offshore.com/informacionnoj-bezopasnosti/chto-takoe-shifrovanie-3des-i-kak-rabotaet-des (дата обращения: 13.05.2021).
8. FileZilla – бесплатный FTP-клиент. URL: https://www.filezilla.ru (дата обращения: 14.05.2021).
9. Wireshark: офиц. сайт. URL: https://www.wireshark.org (дата обращения: 14.05.2021).
10. Cisco Small Business RV Series Routers. URL: https://www.cisco.com/c/en/us/support/routers/small-business-rv-series-routers/series.html (дата обращения: 17.05.2021).

Получено 31.05.2021

Васин Николай Николаевич, д.т.н., профессор кафедры сетей и систем связи (ССС) Поволжского государственного университета телекоммуникаций и информатики (ПГУТИ). 443010, Российская Федерация, г. Самара, ул. Л. Толстого, 23. Тел. +7 917 103-05-44. E-mail: vasin-nn@psuti.ru

Аленников Евгений Михайлович, магистрант кафедры ССС ПГУТИ. 443010, Российская Федерация, г. Самара, ул. Л. Толстого, 23. Тел. +7 917 111-42-08. E-mail: ealennikov@yandex.ru

Субботская Анна Юрьевна, магистрант кафедры ССС ПГУТИ. 443010, Российская Федерация, г. Самара, ул. Л. Толстого, 23. Тел. +7 999 171-03-16. E-mail: subotann@mail.ru

COMPARISON OF THE EFFECT OF ENCRYPTION AND HASHING ALGORITHMS ON DATA TRANSFER RATE OF CLIENT-TO-SITE AND SITE-TO-SITE VPN CONNECTIONS UNDER LOAD

Vasin N.N., Alennikov E.M., Subbotskaya A.Yu.
Povolzhskiy State University of Telecommunications and Informatics, Samara, Russian Federation
E-mail: vasin-nn@psuti.ru

Virtual private network (VPN) technology is currently the mainstay for the exchange of confidential information through Internet. The technologies used to protect traffic of such networks consume router resources and affect the processing speed. Use of routers to encrypt and decrypt data can affect the transfer rate of this data over such network, especially if such network carries not only VPN traffic, but also traffic of ordinary Internet users. This paper compares the impact of encryption and hashing algorithms on the process of transferring packets over two types of VPN connections: Client-to-Site and Site-to-Site connections. A study of the influence of encryption and hashing algorithms on the speed and performance of two VPN-connection technologies when loading a communication channel was carried out. This experiment was carried out on computer and physical models. The computer model of the network was created in the GNS3 network emulator, the physical model was assembled using the next generation routers with integrated services Cisco RV 340. The research results are presented in the form of graphs and diagrams.

Keywords: *VPN tunnel, encryption, hashing, computer model, physical model*

DOI: 10.18469/ikt.2021.19.3.09

Vasin Nikolai Nikolaevich, Povolzhskiy State University of Telecommunications and Informatics, 23, L. Tolstoy Street, Samara, 443010, Russian Federation; Professor of Communication Networks and Systems Department, Doctor of Technical Sciences. Tel. +7 917 103-05-44. E-mail: vasin-nn@psuti.ru

Alennikov Evgeny Mikhailovich, Povolzhskiy State University of Telecommunications and Informatics, 23, L. Tolstoy Street, Samara, 443010, Russian Federation; Student of Communication Networks and Systems Department. Tel. +7 917 111-42-08. E-mail: ealennikov@yandex.ru

Subbotskaya Anna Yurievna, Povolzhskiy State University of Telecommunications and Informatics, 23, L. Tolstoy Street, Samara, 443010, Russian Federation; Student of Communication Networks and Systems Department. Tel. +7 999 171-03-16. E-mail: subotann@mail.ru

References

1. Tanenbaum E., Uezeroll D. *Computer Networks*. Saint Petersburg: Piter, 2012, 41 p. (In Russ.)
2. Olifer V., Olifer N. *Computer Networks. Principles, Technologies, Protocols*. Saint Petersburg: Piter, 2016, 771 p. (In Russ.)
3. IETF standard (RFC 2401-2412). Security architecture for internet protocol. URL: https://datatracker.ietf.org/doc/html/rfc2401 (accessed: 12.05.2021). (In Russ.)
4. Egorov A.N. *Simulation of Computer Networks*. Saint Petersburg: GUMRF imeni admirala S.O. Makarova, 2015. URL: https://studfile.net/preview/5851940/page:35 (accessed: 12.05.2021). (In Russ.)
5. Vasin N.N., Alennikov E.M. Impact of encryption algorithms on the packet transfer rate in a custom VPN. *Problemy tehniki i tehnologij telekommunikatsij» (PTiTT-2020), IV Nauchnyj forum*

Telekommunikatsii: teorija i tehnologii (TTT-2020): Sbornik trudov XXII Mezhdunarodnoj nauchno-tehnicheskoj konferentsii, 2020, pp. 250–251. (In Russ.)
6. Vasin N.N., Alennikov E.M., Subbotskaja A.Yu. *Modeling Virtual Private Networks. Methodical Instructions for Performing Laboratory Work*. Samara: PGUTI, 2020, 30 p. URL: http://eclib.psuti.ru/cgi-bin/irbis64r_12/cgiirbis_64.exe (accessed: 12.05.2021). (In Russ.)
7. What is 3DES encryption and how does DES work? URL: https://heritage-offshore.com/informacionnoj-bezopasnosti/chto-takoe-shifrovanie-3des-i-kak-rabotaet-des (accessed: 13.05.2021). (In Russ.)
8. FileZilla is a free FTP client. URL: https://www.filezilla.ru (accessed: 14.05.2021). (In Russ.)
9. Wireshark official site. URL: https://www.wireshark.org (accessed: 14.05.2021).
10. Cisco Small Business RV Series Routers. URL: https://www.cisco.com/c/en/us/support/routers/small-business-rv-series-routers/series.html (accessed: 17.05.2021).

Received 31.05.2021

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ТЕХНОЛОГИЙ ПЕРЕДАЧИ И ОБРАБОТКИ ИНФОРМАЦИИ И СИГНАЛОВ

УДК 004.75

МЕТОД ОЦЕНКИ РЕСУРСОЕМКОСТИ РЕКОНФИГУРАЦИИ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ ПРИ ИЗМЕНЕНИИ ТРЕБОВАНИЙ НАЗНАЧЕНИЯ

Логинов И.В.
Академия ФСО России, Орел, РФ
E-mail: loginov_iv@bk.ru

Увеличение структурной и функциональной сложности инфокоммуникационных систем в результате научно-технического прогресса привело к формированию многофункциональных систем. Для таких систем в современных условиях характерно наличие динамики требований и реконфигурации под эти изменения. Непрерывная реконфигурация требует в процессе планирования выполнения оценок необходимых ресурсов. Целью исследования является разработка подхода к оцениванию ресурсоемкости реализации изменения требований назначения при неполноте описания реконфигурируемой инфокоммуникационной системы. Основная идея работы заключается в формировании оценок ресурсоёмкости реконфигурации на основе значений коэффициента изменения требований. Оценка выполняется на основе имеющихся данных о выполнении частных показателей системы требований – существующими функциональными компонентами с известными значениями ресурсоемкости. При этом вводятся поправочные коэффициенты, зависящие от вида изменения требований и типа ресурса, уточняемые в процессе изменения многофункциональной системы по критерию минимума ошибки оценивания. Практическая значимость работы заключается в разработке методики приближенного оценивания ресурсоемкости на основе нечеткого подхода с целью учета неопределенности исходных данных описания инфокоммуникационной системы.

Ключевые слова: *требования назначения, функциональная динамика, многофункциональные системы, инфокоммуникационные услуги, реконфигурация, неопределенность состояния*

Введение

Развитие инфокоммуникационных систем привело к существенному увеличению их структурной и функциональной сложности. Количество телекоммуникационных услуг, предоставляемых абонентам, значительно увеличивается. Изменение технических возможностей по предоставлению портфеля инфокоммуникационных услуг, с одной стороны, а предпочтения абонентов в получении современных сервисов, с другой стороны, определяют изменения требований назначения мультисервисных инфокоммуникационных систем. Основными причинами изменения требований назначения из-за внешних условий являются [1; 2]:

– внешние условия по отношению к организации-заказчику (требования рынка и регуляторов);

– изменение самой организации (организационно-штатные и нормативные изменения);

– возможности и ограничения поставщика инфокоммуникационных услуг (влияние технических и технологических решений и ограничений).