УДК 004.738.5:004.056.5
ББК 32.973.202
Д 58

Довгаль Виталий Анатольевич
Кандидат технических наук, доцент, доцент кафедры информационной безопасности и прикладной информатики факультета информационных систем в экономике и юриспруденции Майкопского государственного технологического университета, Майкоп, e-mail: urmia@mail.ru
Довгаль Дмитрий Витальевич
Студент факультета энергетики и нефтегазопромышленности Донского государственного технического университета, Ростов-на-Дону, e-mail: lanayamann@gmail.com

Обеспечение безопасности с помощью виртуализации сетевых функций

(Рецензирована)

Аннотация. *Рассматриваются главные задачи и возможности безопасности виртуализации сетевых функций (NFV), описывается дизайн архитектуры NFV и некоторые потенциальные проблемы и задачи безопасности NFV. Кроме того, проанализированы существующие продукты и решения в сфере безопасности NFV и некоторые многообещающие направления исследований в этой сфере.*
Ключевые слова: *виртуализация сетевых функций, программно-конфигурируемая сеть.*

Dovgal Vitaliy Anatolyevich
Candidate of Technical Sciences, Associate Professor, Associate Professor of Department of Information Security and Application Informatics of Faculty of Information Systems in Economy and Law, Maikop State University of Technology, Maikop, e-mail: urmia@mail.ru
Dovgal Dmitriy Vitalyevich
Student of Faculty of Energy Production and Oil-Gas Industry, Don State Technical University, Rostov-on-Don, e-mail: lanayamann@gmail.com

Security by means of virtualization of network functions

Abstract. *The paper describes the main tasks and the potentialities of security of network functions virtualization (NFV), the design of NFV architecture and some potential problems and tasks of NFV security. Besides, we analyzed the existing products and solutions in the sphere of NFV security and some promising directions of researches in this field.*
Keywords: *network functions virtualization, software defined networking.*

Введение

Виртуализация сетевых функций (NFV) – это решение, направленное на улучшение гибкости, эффективности и управляемости сетей с помощью эффективного использования виртуализации и технологий облачных вычислений для управления приборами сети с помощью программного обеспечения [1].

NFV позволяет уменьшить затраты на аппаратное обеспечение и способствует снижению потребления электроэнергии, улучшает эксплуатационную эффективность и оптимизирует конфигурацию сети. NFV позволяет уменьшить затраты провайдеров на приобретаемое аппаратное обеспечение, а также способствует снижению потребления электроэнергии, улучшает эксплуатационную эффективность и оптимизирует конфигурацию сети. Но главной проблемой NFV остается безопасность.

Для решения проблем, связанных с безопасностью NFV, были предложены различные подходы [2–5]. В этой статье будут обсуждены проблемы безопасности NFV и соответствующие решения и разъяснены предложенные архитектуры безопасности NFV.

Краткий обзор NFV

Как показано на рисунке 1, архитектурная платформа NFV включает NFV Management and Orchestrator (управление и организация NFV), NFVI (инфраструктура виртуализации сетевых функций) и VNF (виртуализированные сетевые функции). Инфраструктура NFV (NFVI) может быть использована в различных вариантах, таких как виртуализация сети мобильного ядра, виртуализация дома и виртуализация сетей доставки контента [6]. NFV

Management and Orchestration включает три функциональных блока: NFV Orchestrator, VNF Managers и Virtualized Infrastructure Manager. NFV Management and Orchestration осуществляет управление ресурсами NFVI и VFN во время всего жизненного цикла. Сервис, VNF и описание инфраструктуры – эти компоненты управляют всей системой NFV.

Среди трудностей внедрения NFV отметим проблему управления всеми виртуальными ресурсами и их интегрирование с обеспечением совместимости с существующими платформами. Требования внедрения были обозначены в спецификациях виртуализации NFV [7]. Для гарантии доступности услуг и сохранения устойчивости NFV должно быть включено автоматическое восстановление после отказов [8]. NFV может быть использована во многих случаях, таких как системы управления инцидентами (IMS), виртуализация домашних сетей и сетей предприятия, виртуализация сетей доставки контента и NFV с фиксированным доступом [9]. Облачные вычисления и стандартизация специализированных серверов внесли вклад в реализацию NFV.

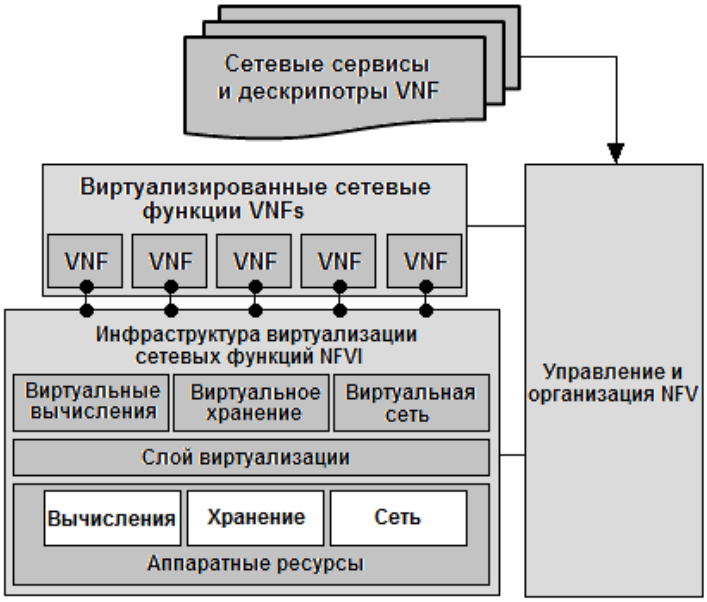

Рис. 1. Архитектурная платформа NFV

Программно-определяемые сети (Software Defined Networking, SDN) – это другой подход улучшения гибкости сетей с использованием разделения передающей и направляющих функций в различных плоскостях. NFV и SDN являются взаимодополняющими при построении программного решения для более масштабных, гибких и инновационных сетей, но они отличаются друг от друга.

Задачи и решения безопасности NFV

Основополагающими проблемами безопасности NFV являются авторизация и аутентификация пользователей или временных арендаторов. Часто безопасность NFV обсуждается в трех направлениях: безопасность внутри VNF, безопасность между VNF и безопасность вне VNF [6]. Безопасность и управление программным обеспечением являются главными задачами NFV. Способы решения проблем безопасности гипервизоров, передачи данных и систем взаимодействия остаются задачами повышенной сложности, которые необходимо решать при внедрении NFV в телекоммуникационных и мобильных сетях.

Несмотря на огромный потенциал NFV, безопасность и приватность остаются проблемами, которые необходимо решить [10]. В этом контексте выделяют следующие задачи: разделение сервисов для матриц данных и управления матриц, предписывающие правила и визуализирующие ресурсы для контролирующих функций, управление и контроль всей сети. Чтобы гарантировать безопасность в NFV, во время процесса настройки гибкие контролирующие сигналы должны идти через доверенные функциональные блоки, такие как NFV Orchestrator, VNF Managers и Virtualized Infrastructure Manager.

Предполагаемые платформы безопасности для NFV

Для обеспечения безопасности NFV предлагается и внедряется достаточно большое количество платформ и архитектур безопасности. Рассмотрим некоторые из них.

1. Администратор-политик для NFV – дополнительный программный компонент, позволяющий пользователям определить политику безопасности с помощью языков, политик высшего уровня (HLP) и политик среднего уровня (MLP). Администратор-политик генерирует необходимые конфигурации, чтобы удовлетворить пользовательские требования безопасности, а затем конфигурации отправляются оркестратору (решению по координации) для настройки различных VNF и обеспечения безопасности VNF. Интеграция менеджера политики с архитектурой NFV позволяет пользователям установить свои требования безопасности [11].

2. Архитектура SECURED обеспечивает безопасность пользователей при работе с приложениями [6]. Ее главные компоненты: модуль безопасности, менеджер политики безопасности, система аутентификации и приложение SECURED. Эти компоненты безопасности работают совместно, обеспечивая безопасность для NFV.

3. OpenNF – управляющая архитектура обеспечения эффективного и безопасного распределения потоков информации среди экземпляров сетевых функций в NFV [2]. OpenNF обеспечивает эффективный скоординированный контроль как состояния всех внутренних сетевых функций, так и состояния сетевой передачи. Это решает существующую проблему безопасного контроля сетевых функций, а также решает проблему состояния потока, связанную с издержками, а также использует минимум изменений для адаптации различных VNFs. Целью OpenNF является обеспечение безопасности и гибкости контроля VNFs в NFV с минимальными издержками.

4. Cisco Evolved Services Platform (CESP) – безопасное и малозатратное решение [12], гарантирующее эффективное и безопасное предоставление услуг с помощью включения в профили сервисов различных атрибутов и политик сервисов. Доступность VNFs и услуг для потребителей определяет каталог виртуальных функций, который расширяется за счет использования OpenStack для открытых архитектур.

5. VMware vCloud NFV – решение, обеспечивающее безопасность поставщикам коммуникационной услуги. Включает VMware vCloud Director for Service Providers (Communication Service Providers, CSPs) для сетей промышленного масштаба и VMware Integrated OpenStack для обеспечения качества обслуживания (QoS). Кроме того, решение содержит компоненты, удостоверяющие сетевые функции и сервисы для большого числа арендаторов, а также позволяющие восстановиться после атак [13].

6. Alcatel-Lucent CloudBand – платформа безопасности NFV, включающая централизованную систему управления CloudBand и многочисленные распределенные узлы CloudBand. Для обеспечения безопасности VNFs система управления CloudBand управляет ресурсами в NFVI и позволяет анализировать записанные ранее в реальном времени данные, такие как обнаружение аномалии и предсказание событий [14].

Несмотря на многочисленность предлагаемых платформ, разработанных для преодоления проблем безопасности в NFV, многие из потенциальных проблем все еще остаются не решенными:

1) компрометация VNF: обнаружение скомпрометированных компонентов оборудования и программного обеспечения сети NFV, поставленных различными поставщиками, и смягчение их воздействия остается сложной задачей в NVF;

2) распределенные атаки «отказ в обслуживании» (DDoS) могут нанести огромный ущерб сетям, поддерживающим NFV;

3) доверительное управление в NFV: NFV позволяет выйти на рынок сетевой инфраструктуры, предоставляя совместимое с NFV оборудование и программное обеспечение. Это приведет к появлению в NFV-поддерживаемой сети решений от большого количества поставщиков. Поэтому требуют исследования вопросы управления цепочки доверия и оценки степени доверия продуктов, предоставленных различными поставщиками. Кроме того, необходимо исследовать выбор программного обеспечения для адаптивной настройки VNFs с целью минимизации угроз безопасности сети.

Заключение. NFV снижает расходы на оборудование и улучшает эффективность работы, но содержит проблемы безопасности, которые необходимо решать при быстром развертывании NFV. Например, аутентификация пользователя, контроль привилегий пользователя и конфигурация сети могут быть предопределены до использования функций безопасности [15].

Примечания:

1. NFV: An Introduction, Benefits, Enablers, Challenges & Call for Action. NFV white paper. URL: http://portal.etsi.org/NFV/NFV_White_Paper.pdf
2. OpenNF: Enabling Innovation in Network Function Control / A. Gember-Jacobson, R. Viswanathan, C. Prakash, R. Grandl [et al.] // SIGCOMM '14. Aug. 2014. P. 163–174.
3. Toward a Telco Cloud Environment for Service Functions / J. Soares, C. Goncalves, B. Parreira [et al.] // IEEE Communications Magazine. Feb. 2015. Vol. 53, No. 2. P. 98–106.
4. OpenSCaaS: An Open Service Chain as a Service Platform Toward the Integration of SDN and NFV / W. Ding, W. Qi, J. Wang, B. Chen // IEEE Network. May/Jun. 2015. Vol. 29, No. 3. P. 30–35.
5. Virtualized Security at the Network Edge: A User-Centric Approach / D. Montero, M. Yannuzzi, A. Shaw [et al.] // IEEE Communications Magazine. April 2015. Vol. 53, No. 4. P. 176–186.
6. ETSI Group Specification: Network Functions Virtualization (NFV) NFV Security Problem Statement. URL: http://www.etsi.org
7. ETSI Group Specification: Network Functions Virtualization (NFV) Virtualization Requirements, October 2013. URL: http://www.etsi.org/deliver/etsi_gs/NFV/001_099/002/01.01.01_60/gs_NFV002v010101p.pdf
8. ETSI Group Specification: Network Functions Virtualization (NFV) Resiliency Requirements, January 2015. URL: http://www.etsi.org/deliver/etsi_gs/NFV-REL/001_099/001/01.01.01_60/gs_NFV-REL001v010101p.pdf
9. ETSI Group Specification: Network Functions Virtualization (NFV) Use Cases, October 2013. URL: http://www.etsi.org/deliver/etsi_gs/NFV/001_099/001/01.01.01_60/gs_NFV001v010101p.pdf
10. Elastic Network Functions: Opportunities and Challenges / R. Szabo, M. Kind, F.-J. Westphal [et al.] // IEEE Network. May/Jun. 2015. Vol. 29, No. 3. P. 15–21.
11. A novel approach for integrating security policy enforcement with dynamic network virtualization / C. Basile, A. Lioy, C. Pitscheider, F. Valenza, M. Vallini // NetSoft. April 2015. P. 1–5.
12. Cisco and/or its affiliates, Cisco Evolved Services Platform At-a-Glance, Oct. 2014. URL: https://www.cisco.com/c/dam/global/hr_hr/assets/ciscoconnect/2014/pdfs/2014_04_see_epn_mpls_4x3.pdf
13. VMware, Datasheet: VMware vCloud NFV, Sep. 2015. URL: https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/solutions/vmware-vcloud-nfv-datasheet.pdf
14. Alcatel-Lucent White Paper, «Providing Security in NFV: Challenges and Opportunities», May 2014. URL: http://www.tmcnet.com/tmc/whitepapers/documents/whitepapers/2014/10172-providing-security-nfv.pdf
15. Довгаль В.А., Довгаль Д.В. Анализ перспективных методов поведенческой биометрии для аутентификации пользователей // Вестник Адыгейского государственного университета. Сер. Естественно-математические и технические науки. 2017. Вып. 3 (206). С. 139–142. URL: http://vestnik.adygnet.ru

References:

1. NFV: An Introduction, Benefits, Enablers, Challenges & Call for Action. NFV white paper. URL: http://portal.etsi.org/NFV/NFV_White_Paper.pdf
2. OpenNF: Enabling Innovation in Network Function Control / A. Gember-Jacobson, R. Viswanathan, C. Prakash, R. Grandl [et al.] // SIGCOMM '14. Aug. 2014. P. 163–174.
3. Toward a Telco Cloud Environment for Service Functions / J. Soares, C. Goncalves, B. Parreira [et al.] // IEEE Communications Magazine. Feb. 2015. Vol. 53, No. 2. P. 98–106.
4. OpenSCaaS: An Open Service Chain as a Service Platform Toward the Integration of SDN and NFV / W. Ding, W. Qi, J. Wang, B. Chen // IEEE Network. May/Jun. 2015. Vol. 29, No. 3. P. 30–35.
5. Virtualized Security at the Network Edge: A User-Centric Approach / D. Montero, M. Yannuzzi, A. Shaw [et al.] // IEEE Communications Magazine. April 2015. Vol. 53, No. 4. P. 176–186.
6. ETSI Group Specification: Network Functions Virtualization (NFV) NFV Security Problem Statement. URL: http://www.etsi.org
7. ETSI Group Specification: Network Functions Virtualization (NFV) Virtualization Requirements, October 2013. URL: http://www.etsi.org/deliver/etsi_gs/NFV/001_099/002/01.01.01_60/gs_NFV002v010101p.pdf
8. ETSI Group Specification: Network Functions Virtualization (NFV) Resiliency Requirements, January 2015. URL: http://www.etsi.org/deliver/etsi_gs/NFV-REL/001_099/001/01.01.01_60/gs_NFV-REL001v010101p.pdf
9. ETSI Group Specification: Network Functions Virtualization (NFV) Use Cases, October 2013. URL: http://www.etsi.org/deliver/etsi_gs/NFV/001_099/001/01.01.01_60/gs_NFV001v010101p.pdf
10. Elastic Network Functions: Opportunities and Challenges / R. Szabo, M. Kind, F.-J. Westphal [et al.] // IEEE Network. May/Jun. 2015. Vol. 29, No. 3. P. 15–21.
11. A novel approach for integrating security policy enforcement with dynamic network virtualization / C. Basile, A. Lioy, C. Pitscheider, F. Valenza, M. Vallini // NetSoft. April 2015. P. 1–5.
12. Cisco and/or its affiliates, Cisco Evolved Services Platform At-a-Glance, Oct. 2014. URL: https://www.cisco.com/c/dam/global/hr_hr/assets/ciscoconnect/2014/pdfs/2014_04_see_epn_mpls_4x3.pdf
13. VMware, Datasheet: VMware vCloud NFV, Sep. 2015. URL: https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/solutions/vmware-vcloud-nfv-datasheet.pdf
14. Alcatel-Lucent White Paper, «Providing Security in NFV: Challenges and Opportunities», May 2014. URL: http://www.tmcnet.com/tmc/whitepapers/documents/whitepapers/2014/10172-providing-security-nfv.pdf
15. Dovgal V.A., Dovgal D.V Analysis of perspective methods of behavioral biometry for users authentication // The Bulletin of the Adyghe State University. Ser. Natural-Mathematical and Technical Sciences. 2017. Iss. 3 (206). P. 139–142. URL: http://vestnik.adygnet.ru