УДК 004.422.8 + 004.738.056.5 + 342.2/.7 : 004.056 Вестник УрФО № 4(14)/2014. Стр. 27–31

Шабуров А. С., Рашевский Р. Б.

О ПРАКТИЧЕСКОМ ПРИМЕНЕНИИ ТЕХНОЛОГИИ VMWARE VSHIELD APP ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ

Рассматриваются общие принципы работы семейства продуктов VMWare vShield App в части настройки и управления с использованием API. Приведен пример практического применения VMWare vShield App для сетевой защиты информационной системы персональных данных при реализации требований по защите среды виртуализации.

Ключевые слова: *информационная безопасность, авторизация, гипервизор, сетевая атака, информационная система персональных данных, среда виртуализации.*

Shaburov A. S., Rashevsky R. B.

ON PRACTICAL IMPLEMENTATION OF VMWARE VSHIELD APP TECHNOLOGY FOR ENSURING SECURITY OF PERSONAL DATA INFORMATION SYSTEMS

The authors dwell on general working principles of VMWare vShield App and settings and control with the use of API in particular. The authors give the examples of practical implementation of VMWare vShield App for network security of personal data information systems in the process of implementation of standards of virtualization security.

Keywords: *information security, authorization, hypervisor, network attack, personal data information systems, virtualization environment.*

Развитие корпоративных информационных систем в современных условиях предусматривает использование технологии виртуализации. Актуальность применения подобной технологии обусловлена, в первую очередь, необходимостью сокращения эксплуатационных расходов на информационную инфраструктуру. Вместе с тем, подобные инновации заставляют по-новому решать задачи защиты информации, размещаемой в облачном пространстве, а также предполагают выполнение требований по безопасности информации, регламентированных для различных информационных систем, в том числе информационных систем персональных данных (ИС ПДн) [1].

Уменьшение расходов на информационную инфраструктуру может осуществляться за счет размещения нескольких виртуальных серверов или рабочих станций на базе одного физического узла с установленным гипервизором. При этом применение виртуализации повышает гибкость и удобство развертывания и настройки новых узлов информационной инфраструктуры для сетевых инженеров и системных администраторов [2].

В связи со своей спецификой виртуальная инфраструктура требует несколько иных подходов к обеспечению информационной безопасности. Так, в случае обеспечения антивирусной защиты виртуальных серверов или рабочих станций использование классических антивирусных продуктов, предполагающих установку на каждый защищаемый узел, является нецелесообразным. Более рациональным будет использование антивирусного решения, устанавливаемого на гипервизор и выполняющего сканирование всех виртуальных серверов и рабочих станций, запущенных на физическом узле [3].

Применительно к обеспечению защиты от сетевых атак также более рациональным является использование решения, устанавливаемого на гипервизор. Такое решение позволит снизить использование аппаратных ресурсов физического узла, а также эффективно противостоять различным методикам сокрытия сетевого трафика.

На сегодняшний день лидером в области виртуализации является компания VMWare, имеющая широкую продуктовую линейку в области решений для виртуализации [4]. В целом обеспечение безопасности виртуальной инфраструктуры обеспечивается следующими программными продуктами: VMWare vShield Endpoint, VMWare vShield Edge и VMWare vShield App.

VMWare vShield Endpoint представляет собой специальные программные интерфейсы для организации антивирусной защиты виртуальной инфраструктуры на уровне гипервизора.

VMWare vShield Edge обеспечивает сетевую защиту виртуальной локальной сети, т. е. является аналогом аппаратного межсетевого экрана для виртуальной сети.

VMWare vShield App обеспечивает защиту отдельных виртуальных серверов или рабочих станций, а также групп серверов или рабочих станций средствами гипервизора, позволяя задавать правила фильтрации сетевого трафика.

Каждый из продуктов, входящих в состав продуктовой линейки VMWare vShield, имеет программный интерфейс управления (API) для настройки и управления [5].

API VMWare vShield App реализует модель взаимодействия REST, т. е. вызов тех или иных методов API, когда получение и передача данных выполняются с помощью HTTP-запросов. При этом поддерживаются четыре основных HTTP-метода: GET, POST, PUT, DELETE. Для обеспечения безопасности при работе с API используются защищенное соединение (SSL) и авторизация администратора.

В последней доступной на сегодняшний день версии API–5.5 для взаимодействия с программным интерфейсом необходимо отправить HTTP-запрос по URL-адресу https://<vsm-ip>/api/2.0/app/firewall/.

Организация взаимодействия с API предполагает прохождение процедуры авторизации, которая заключается в передаче пароля администратора в кодировке base64 в запросе. В соответствии с эталонной моделью HTTP-запросов в VMWare vShield API GET-запросы используются для получения текущей конфигурации и статистических данных, POST-запросы – для создания новых правил фильтрации, PUT-запросы – для изменения режима работы VMWare vShield App и DELETE-запросы – для удаления правил фильтрации (рис. 1).

В качестве примера рассмотрим виртуальный веб-сервер на базе UNIX-подобной операционной системы в составе ИС ПДн. Данный веб-сервер имеет два сетевых интерфейса, один из которых используется для доступа к веб-серверу из глобальной сети Ин-

```
   GET https://<vsm-ip>/api./2.0/app/firewall/
<dc-id>/config?list=config&precedence=DEFAULT
   Response Body:

      <VshieldAppConfiguration>
           <firewallConfiguration generationNumber="1312802020950"
timestamp="1312802020950" contextId="" provisioned="true">
                <layer3FirewallRule disabled="false"precedence="default"
id="1340">
                     <action>block</action>
                     <logged>false</logged>
                     <notes></notes>
                     <source/>
                     <destination/>
                </layer3FirewallRule>
                <layer2FirewallRule disabled="false"precedence="default"
id="1341">
                     <action>allow</action>
                     <logged>false</logged>
                     <notes></notes>
                     <destination/>
                </layer2FirewallRule>
           </firewallConfiguration>
      </VshieldAppConfiguration>
```

Рис. 1. Пример GET-запроса для получения правил, установленных по умолчанию, и ответ API на запрос

тернет, а второй – для подключения администраторов веб-сервера из внутренней сети. При этом основной задачей веб-сервера является взаимодействие по защищенному сетевому протоколу HTTPS для получения пользовательских данных из глобальной сети Интернет. Вместе с тем для обслуживания веб-сервера необходим удаленный доступ из локальной сети по протоколу SSH (рис. 2).

Для настройки правил фильтрации сетевого трафика в рассмотренном выше примере с двумя сетевыми интерфейсами предполагается воспользоваться API VMWare vShield App. На интерфейсе eth0 запретим всю сетевую активность, кроме входящих подключений по порту 443; на интерфейсе eth1 также запретим всю сетевую активность, кроме входящих подключений по порту 25.

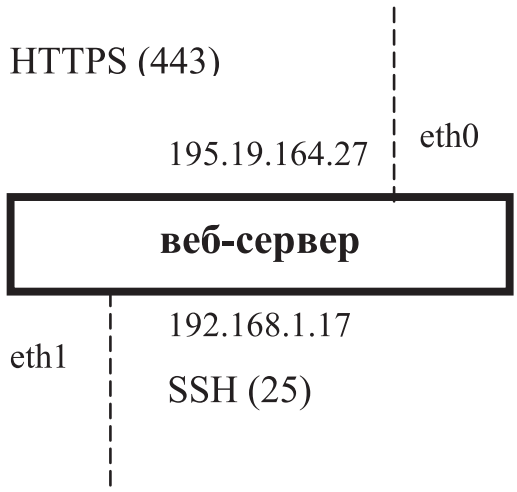


Рис. 2. Общая схема сетевых интерфейсов веб-сервера

Характерно, что поумолчанию весь сетевой трафик на обоих интерфейсах блокируется, т. е. VMWare vShield App работает в режиме «запрещено все, что явно не разрешено». Таким образом, для решения поставленной задачи достаточно создать дополнительные правила фильтрации сетевого трафика: для сетевого интерфейса eth0 необходимо разрешить входящие сетевые соединения по порту 443, а для сетевого интерфейса eth1 необходимо разрешить входящие сетевые соединения по порту 25.

Для добавления нового правила фильтрации сетевого трафика необходимо инициировать POST-запрос к API, в котором осуществить передачу нового правила, записанного в файле формата XML. После чего новое правило будет добавлено в список правил фильтрации VMWare vShield App (рис. 3).

Аналогичным образом добавляется правило для разрешения входящих сетевых соединений на интерфейс eth0 по порту 443.

```
      <VshieldAppConfiguration>
           <firewallConfiguration generationNumber="1312833020950"
timestamp="1312833020950" contextId="" provisioned="true">
                <layer3FirewallRule disabled="false"precedence="default" id="0">
                      <name>AllowSSH</name>
                     <action>allow</action>
                     <logged>true</logged>
                     <notes>Allows SSh traffic from ANY to eth1</notes>
                     <source/>
                     <destination>
                             <address>192.168.1.17</address>
                             <portinfo>25</portinfo>
                      </destination>
                </layer3FirewallRule>
           </firewallConfiguration>
      </VshieldAppConfiguration>
```

Рис. 3. XML-файл с правилом фильтрации сетевого трафика для разрешения входящих сетевых соединений

```
   GET https://<vsm-ip>/api./2.0/app/firewall/
   <dc-id>/config?list=config&precedence=DEFAULT
     Response Body:
      <VshieldAppConfiguration>
           <firewallConfiguration generationNumber="1312802020950"
timestamp="1312802020950" contextId="" provisioned="true">
                <layer3FirewallRule disabled="false"precedence="default"
id="1340">
                     <action>block</action>
                     <logged>false</logged>
                     <notes></notes>
                     <source/>
                     <destination/>
                </layer3FirewallRule>
                <layer3FirewallRule disabled="false"precedence="default"
id="1342">
                      <name>AllowSSH</name>
                     <action>allow</action>
                     <logged>true</logged>
                     <notes>Allows SSH traffic from ANY to eth1</notes>
                     <source/>
                     <destination>
                             <address>192.168.1.17</address>
                             <portinfo>25</portinfo>
                      </destination>
                </layer3FirewallRule>
                <layer3FirewallRule disabled="false"precedence="default"
id="1343">
                      <name>AllowHTTPS</name>
                     <action>allow</action>
                     <logged>true</logged>
                     <notes>Allows HTTPS traffic from ANY to eth0</notes>
                     <source/>
                     <destination>
                             <address>192.168.1.17</address>
                             <portinfo>443</portinfo>
                      </destination>
                </layer3FirewallRule>
                <layer2FirewallRule disabled="false"precedence="default"
id="1341">
                     <action>allow</action>
                     <logged>false</logged>
                     <notes></notes>
                     <destination/>
                </layer2FirewallRule>
           </firewallConfiguration>
      </VshieldAppConfiguration>
```

Рис. 4. GET-запрос с ответом для получения конфигурации правил VMWare vShield App

После добавления двух новых правил фильтрации сетевого трафика запросим текущую конфигурацию правил VMWare vShield App посредством GET-запроса к API и убедимся в том, что новые правила фильтрации были добавлены в конфигурацию VMWare vShield App (рис. 4).

Очевидно, все новые правила фильтрации сетевого трафика были корректно добавлены в конфигурации правил фильтрации VMWare vShield App.

Таким образом, проведенный анализ основных принципов функционирования VMWare vShield App API, а также рассмотренный пример практического применения программного интерфейса управления для создания новых правил фильтрации сетевого трафика и изменения конфигурации правил VMWare vShield App позволяют создавать на их основе защищенные виртуальные структуры, в том числе и для информационных систем персональных данных.

References

1. O.B. Ekimov, A.S. Shaburov, I.P. Isakov, P.V. Mazunin, A.N. Shlyakov. «O realizatsii trebovanii po zashchite personal'nykh dannykh v in-formatsionnoi sisteme permskogo filiala FGUP «RChTs PFO» [On implementation of Requirements for Personal Data Security in Information System of Perm Branch of Radio Frequency Center of Central Federal District]// Vestnik PNIPU. Elektrotekhnika, informatsionnye tekhnologii, sistemy uprav-leniya. – Perm', 2013. – No. 8. – p.144 – 155.

2. K. Kusek, V. Van Noi, A. Deniel. Administrirovanie VMWare vSphere 5 [Administration of VMWare vSphere 5] – Piter Publ. – St. Peters-burg, 2013.

3. P. Sarkar. VMWare vCloud Security – PACKT Publishing – Bir-mingham, 2014.

4. T.J. Bittman, M.A. Margevicius, P. Dawson. Gartner Magic Quadrant for x86 Server Virtualization Infrastructure – Gartner Inc. – Stamford, 2014.

5. VMWare vShield API Programming Guide – VMWare Inc. – Palo Al-to, 2014.

Шабуров А. С., к. т. н., доцент ПНИПУ. E-mail: shans@at.pstu.ru

Рашевский Р. Б. E-mail: oman@rashevskiy.com

Shaburov A. S., Perm National Research Polytechnic University, Cand. Sc. Engineering, associate professor. E-mail: shans@at.pstu.ru

Rashevsky R. B. E-mail: oman@rashevskiy.com