УДК 004.422.8+004.738].056.5

А.С. Шабуров, Р.Б. Рашевский

Пермский национальный исследовательский политехнический университет, Пермь, Россия

ПРАКТИЧЕСКОЕ ПРИМЕНЕНИЕ VMWARE VSHIELD APP ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ВИРТУАЛЬНОГО ВЕБ-СЕРВЕРА

Рассматриваются общие принципы работы семейства продуктов VMWare vShield App в части настройки и управления с использованием API, а также приведен пример практического применения VMWare vShield App для сетевой защиты виртуального сервера.

Ключевые слова: виртуализация, информационная безопасность, авторизация, гипервизор, сетевая атака.

A.S. Shaburov, R.B. Rashevskiy

Perm National Research Polytechnic University, Perm, Russian Federation

PRACTICAL APPLICATION OF VMWARE VSHIELD APP FOR SAFETY VIRTUAL WEB SERVER

The article deals with common principles and methods of VMWare vShield App product with regard to configuration and management using REST API as well as an example of practical application of VMWare vShield App for protecting virtual server against network attacks.

Keywords: virtualization, information security, authentication, hypervisor, network attack.

Введение. В современных условиях развитие корпоративных информационных систем 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. Кроме того, при создании корпоративных облачных сервисов предполагается выполнение требований информационной безопасности, регламентированных для информационных систем персональных данных, государственных информационных систем [1], что также требует поиска оптимальных

и эффективных решений. Уменьшение расходов на информационную инфраструктуру в первую очередь может осуществляться за счет размещение 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].

На сегодняшний день лидером в области виртуализации является компания VMWare, имеющая широкую продуктовую линейку в области решений для виртуализации. Специально разработанное программное обеспечение (ПО) включает продукты для создания виртуальной инфраструктуры, развертывания виртуальных серверов и рабочих станций, организации инфраструктуры виртуальных рабочих столов (VDI) и т.д. [3].

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 [4].

Применительно к обеспечению защиты от сетевых атак также более рациональным является использование решения, устанавливаемого на гипервизор. Во-первых, такое решение позволит снизить использование аппаратных ресурсов физического узла. Во-вторых, решение позволяет эффективно противостоять различным методикам сокрытия сетевого трафика, так как перехват и сканирование трафика проводятся средствами гипервизора, а не операционной системы, установленной на виртуальном сервере или рабочей станции.

В целом обеспечение безопасности виртуальной инфраструктуры обеспечивается продуктовой линейкой VMWare vShield, включающей ПО: VMWare vShield Endpoint, VMWare vShield Edge и VMWare vShield App. VMWare vShield Endpoint предоставляет собой специальные программные интерфейсы для организации антивирусной защиты виртуальной инфраструктуры на уровне гипервизора.

VMWare vShield 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, 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].

В рамках данной статьи предполагается рассмотреть общие принципы работы VMWare vShield App в части настройки и управления с использованием API, а также пример его практического применения для обеспечения сетевой защиты виртуального сервера. API VMWare vShield App реализует модель взаимодействия REST, т.е. вызов тех или иных методов API, 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 (см. ниже).

```
     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 disa-
bled="false"precedence="default" id="1340">
                       <action>block</action>
                       <logged>false</logged>
                       <notes></notes>
                       <source/>
                       <destination/>
                  </layer3FirewallRule>
```

```
                    <layer2FirewallRule disa-
bled="false"precedence="default" id="1341">
                          <action>allow</action>
                          <logged>false</logged>
                          <notes></notes>
                          <destination/>
                    </layer2FirewallRule>
              </firewallConfiguration>
        </VshieldAppConfiguration>
```

В качестве примера рассмотрим виртуальный веб-сервер на базе UNIX-подобной операционной системы, имеющий два сетевых интерфейса: один из которых используется для доступа в Интернет, а второй – для доступа к локальной сети. При этом основной задачей веб-сервера является взаимодействие по протоколу HTTP/HTTPS для передачи веб-контента в Интернет. Вместе с тем для обслуживания веб-сервера необходим удаленный доступ из локальной сети по протоколу SSH (рисунок).

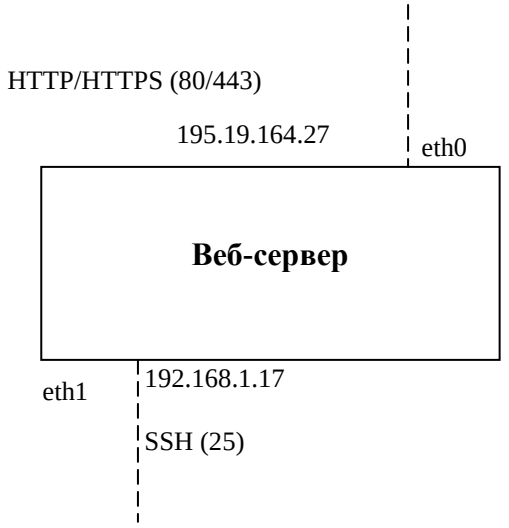

Рис. Общая схема сетевых интерфейсов веб-сервера

Воспользуемся API VMWare vShield App для настройки правил фильтрации сетевого трафика для рассмотренного выше виртуального веб-сервера с двумя сетевыми интерфейсами. На интерфейсе eth0 запретим всю сетевую активность, кроме входящих подключений по портам 80 и 443; на интерфейсе eth1 также запретим всю сетевую активность, кроме входящих подключений по порту 25.

Характерно, что по умолчанию 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 портам 80 и 443; 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 (см. ниже).

```
        <VshieldAppConfiguration>
             <firewallConfiguration
generationNumber="1312833020950" timestamp="1312833020950"
contextId="" provisioned="true">
                  <layer3FirewallRule disa-
bled="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>
```

Аналогичным образом добавляются оставшиеся два новых правила для разрешения входящих сетевых соединений на интерфейс eth0 по портам 80 и 443.

После добавления всех трех 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 (см. ниже).

```
     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 disa-
bled="false"precedence="default" id="1340">
                        <action>block</action>
                        <logged>false</logged>
                        <notes></notes>
                        <source/>
                        <destination/>
                  </layer3FirewallRule>
            <layer3FirewallRule disa-
bled="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 disa-
bled="false"precedence="default"    id="1343">
                  <name>AllowHTTP</name>
                        <action>allow</action>
                        <logged>true</logged>
                        <notes>Allows HTTP traffic from ANY to
eth0</notes>
                        <source/>
                        <destination>
                         <address>192.168.1.17</address>
                         <portinfo>80</portinfo>
                  </destination>
                  </layer3FirewallRule>
                  <layer3FirewallRule disa-
bled="false"precedence="default"    id="1344">
                  <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 disa-
bled="false"precedence="default" id="1341">
                         <action>allow</action>
                         <logged>false</logged>
                         <notes></notes>
                         <destination/>
                    </layer2FirewallRule>
               </firewallConfiguration>
          </VshieldAppConfiguration>
```

Как видим, все новые правила фильтрации сетевого 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 позволяет предположить возможность создания на их основе защищенных виртуальных структур различного назначения.

Библиографический список

1. О реализации требований по защите персональных данных в информационной системе Пермского филиала ФГУП «РЧЦ ПФО» / О.Б. Екимов, А.С. Шабуров, И.П. Исаков, П.В. Мазунин, А.Н. Шляков // Вестник Пермского национального исследовательского политехнического университета. Электротехника, информационные технологии, системы управления. – 2013. – № 8. – С.144 – 155.

2. Кусек К., Ван Ной В., Дэниел А.. Администрирование VMWare vSphere 5. – СПб.: Питер, 2013.

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

4. Sarkar P. VMWare vCloud Security. – PACKT Publishing. – Birmingham, 2014.

5. VMWare vShield API Programming Guide. – VMWare Inc. – Palo Alto, 2014.

References

1. Ekimov O.B., Shaburov A.S., Isakov I.P., Mazunin P.V., Shliakov A.N. O realizatsii trebovanii po zashchite personal'nykh dannykh v informatsionnoi sisteme Permskogo filiala Federal'nogo gosudarstvennogo unitarnogo predpriiatiia «Radiochastotnyi tsentr Privolzhskogo federal'nogo okruga» [About implementation of requirements for protection of personal information in information system of the Perm branch Federal State Unitary Enterprise Radio-frequency Center of the Volga Federal District]. *Vestnik Permskogo natsional'nogo issledovatel'skogo politekhnicheskogo universiteta. Elektrotekhnika, informatsionnye tekhnologii, sistemy upravleniia*, 2013, no. 8, pp.144 – 155.

2. Kusek K., Van Noi V., Deniel A. Administrirovanie VMWare vSphere 5 [Administration of VMWare vSphere 5]. Saint Petersburg: Piter, 2013.

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

4. Sarkar P. VMWare vCloud Security. Birmingham: PACKT Publishing, 2014.

5. VMWare vShield API Programming Guide. Palo Alto: VMWare Inc., 2014.

Сведения об авторах

Шабуров Андрей Сергеевич (Пермь, Россия) – кандидат технических наук, доцент кафедры автоматики и телемеханики Пермского национального исследовательского политехнического университета (614990, Пермь, Комсомольский пр., 29, e-mail: shans@at.pstu.ru).

Рашевский Роман Борисович (Пермь, Россия) – студент кафедры автоматики и телемеханики Пермского национального исследовательского политехнического университета (614990, Пермь, Комсомольский пр., 29, e-mail: roman@rashevskiy.com).

About the authors

Shaburov Andrey Sergeevich, (Perm, Russia) Ph.D. in Technical Sciences, Associate Professor of the Department of Automation and Telemechanics Perm National Research Polytechnic University (614990, Perm, 29, Komsomolsky pr., e-mail: shans@at.pstu.ru).

Rashevskiy Roman Borisovich (Perm, Russia) is student Perm National Research Polytechnic University (614990, Perm, 29, Komsomolsky pr., e-mail:roman@rashevskiy.com).

Получено 12.09.2014