ВЛИЯНИЕ СТРУКТУРНОЙ ДИНАМИКИ НА БЕЗОПАСНОСТЬ В ИНТЕЛЛЕКТУАЛЬНЫХ КОМПЬЮТЕРНЫХ СЕТЯХ

И.И. Прокопов

В современных компьютерных сетях важную роль играют виртуальные объекты, создаваемые на базе существующих в сети аппаратных средств с целью повышения функциональности и удобства обслуживания каких-либо сетевых объектов. Такие объекты создаются сравнительно легко в связи с широким распространением популярных платформ виртуализации в виде отдельных программных продуктов (VMware, VirtualBox, Virtual PC) и интегрированных в серверные платформы (Hyper-V). К виртуальным сетевым объектам можно отнести: виртуальные машины (хосты) на основе виртуальных операционных систем, виртуальные коммутаторы, виртуальные сетевые адаптеры. Имея несомненные достоинства, виртуальные объекты в ряде случаев порождают проблемы, связанные с изменением структуры сети как целостной системы, а также проблемы с безопасностью в сети.

Способы группирования виртуальных объектов в сети

Виртуальные узлы могут вносить различный вклад в изменение конфигурации сети в зависимости от способа группирования. Рассмотрим возможные способы подключения виртуального объекта к сети [1]:

1. Виртуальные узлы образуют свою сеть внутри хостовой системы и изолированы от физической сети (режим «внутренняя сеть» – «Local only»). В этом случае влияния на конфигурацию сети нет.

2. Режим «не подключен» – Not connected. Это случай полностью изолированного узла. Влияния на конфигурацию сети нет.

3. Режим «разделяемая сеть» – Shared Networking или NAT. Виртуальный узел подключен к общей сети хостового узла от его имени. В физической топологии сети в явном виде не доступен (не виден). Дает нагрузку на сеть, так как может служить клиентом для общих ресурсов сети, создавать трафик и оказывать влияние на соседние физические узлы.

4. Режим «сетевого моста» – Bridged Networking. Непосредственное соединение адаптера виртуальной машины с физическим адаптером ЭВМ. В этом случае в сети появляется полноправный узел со своими ресурсами и сетевыми характеристиками.

Матричная модель сети с виртуальными объектами

Любая сеть может быть охарактеризована набором своих параметров, которые определяют ее структуру, характеристики, возможность изменения, безопасность [2, 3].

Рассмотрим модель физической компьютерной сети в виде одномерного массива $\overline{H}$, состоящую из n физических узлов H_i, где i – порядковый номер узла в сети: $\overline{H} = \{H_1, H_2, H_3, \cdots, H_n\}$. В данном примере это одноранговая сеть.

При наличии виртуальных объектов на физических узлах данный вектор преобразуется в матрицу $\overline{HV}$, в которой каждый физический узел дополнен своими виртуальными узлами HV_{ij}, где i – номер физического узла сети, а j – номер виртуальной машины на данном физическом узле.

$$\overline{HV} = \begin{pmatrix} H_1 & HV_{11} & HV_{12} \cdots & HV_{1m} \\ H_2 & HV_{21} & HV_{22} \cdots & HV_{2m} \\ \cdots & & \cdots & \cdots \\ H_n & HV_{n1} & HV_{n2} \cdots & HV_{nm} \end{pmatrix}.$$

Данная матрица будет неровной и динамической, так как в общем случае количество виртуальных машин на каждом физическом узле может меняться случайным образом от нуля до $m = NV_{\max}$, где $NV_{\max}$ – максимально допустимое количество одновременно запущенных виртуальных машин на узле, которое определяется возможностями ЭВМ и платформы виртуализации. Первый столбец матрицы образуют сами физические хосты. Включение и выключение физических хостов также может происходить случайным образом, и соответственно будут появляться и исчезать целиком строки матрицы, т. е. элемент H_i является независимым элементом строки, а элементы HV_{ij} все зависимы от него полностью. Между собой элементы HV_{ij} независимы. Таким образом, наличие вектора-строки матрицы полностью определяется наличием его первого элемента H_i.

В зависимости от режима работы виртуального сетевого адаптера строки матрицы также могут изменяться. В случае режима NAT происходит свертка строки матрицы соответствующего физического хоста до первого элемента строки (случай, когда все виртуальные машины используют функцию NAT). Если часть виртуальных машин используют режим моста, а часть – NAT, то происходит укорачивание соответствующей строки матрицы. Также укорачивание происходит при использовании изолированных виртуальных машин в режимах только внутренней сети и отключенном (от любой сети) режиме. С точки зрения внешнего наблюдения (мониторинга)

определить причину изменения матрицы конфигурации сети не всегда возможно, так как например выключение (выгрузка) виртуальной машины и переход ее в состояние сетевого отключения практически неразличимы.

Изолированные или отключенные от сети виртуальные машины потенциально могут изменить свой статус, появившись в сети после изменения настроек конфигурации соответствующей платформы. Время их появления (старта выгруженной и перезапуска изолированной систем) будет примерно одинаковым с разницей в ΔT секунд, требуемых на выгрузку изолированной машины. Интервал ΔT определяется типом и настройками ОС виртуальной машины, а также способом прекращения ее работы: форсированное завершение, стандартный режим выключения, с сохранением состояния. Интервал может колебаться от 10–15 секунд до 3–4 минут. Та же ситуация будет при переводе виртуальной машины из режима NAT в режим моста.

Топологическая модель сети с виртуальными объектами

Рассмотрим модель сети в виде графа соединений двух типов хостов и сетей (см. рисунок). Для различения виртуальных и физических хостов обозначим их соответственно темными и светлыми.

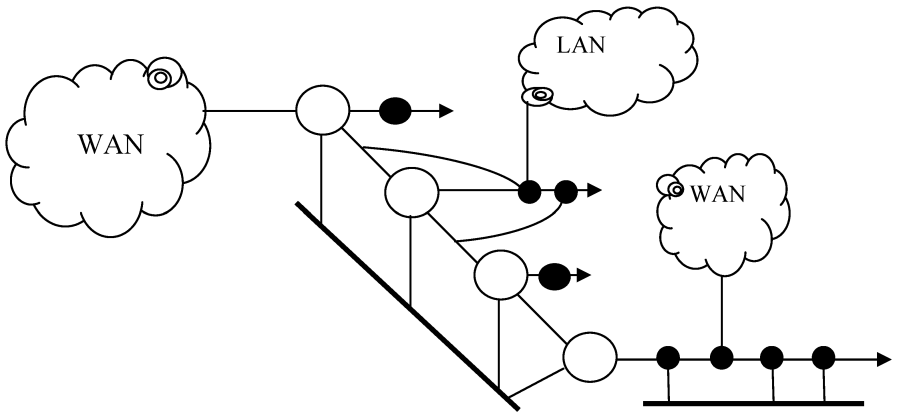

Схема соединения физических, виртуальных хостов и сетей

Возможны подключения к одной и той же сети разными способами через разные маршруты – к локальной сети хостовых машин, к глобальной сети, к локальным внешним сетям [4]. В связи с этим возникает проблема интерпретации понятия «периметр сети». Это понятие является одним из основополагающих при организации защиты сети, а также при ее расширении. Возможно образование петель, так как администратор виртуальной машины может не знать топологии всей сети в целом.

Влияние виртуальных узлов на управляемость и безопасность в сети

1. Каждый виртуальный узел может представлять собой точку подсоединения к исходной физической сети других узлов или даже сетей. Это возможно в том случае, если имеется возможность подключения к двум или более сетевым адаптерам на одной физической ЭВМ. При этом вирту-

альный хост выполняет функции шлюза, соединяющего контролируемую сеть и неконтролируемую. Таким образом, граница сети нарушается и может приобретать различные очертания. Матрица сети преобразуется и получает третье измерение – сети, подсоединенные к элементам HV_{ij}, а сам элемент превращается в вектор. Матрица становится трехмерным массивом с неровными границами и по второму и по третьему измерению.

$$\overline{HV}=\begin{pmatrix} H_1 & HV_{11} & \{HV_{12}, HS_{121}, HS_{122} \cdots\} \cdots & HV_{1m} \\ H_2 & & HV_{21} \quad HV_{22} \cdots & \{HV_{2m}, HS_{2m1}, HS_{2m2} \cdots\} \\ \cdots & & \cdots & \cdots \\ H_n & & HV_{n1} \quad HV_{n2} \cdots & \{HV_{nm}, HS_{nm1}, HS_{nm2} \cdots\} \end{pmatrix}.$$

Но так как любая строка матрицы, содержащая несанкционированные шлюзы, зависит от первого элемента строки (физический хост), то защита может осуществляться средствами хостовой ОС и аппаратуры ЭВМ.

2. Виртуальная машина может представлять опасность для сети, так как устанавливается и администрируется пользователем физического хоста, который может не выполнить настройку политики безопасности в сети.

3. Любая корпоративная сеть является управляемой. Управление структурой и безопасностью сети основано на использовании информации о характеристиках узлов, которая либо заранее известна, либо получается в процессе мониторинга.

Выводы

• Модель сети с виртуальными объектами может быть представлена в виде многомерного неровного динамического массива (минимум трехмерного) – конфигурационной матрицы сети.

• Изменение состояния сети происходит в ряде случаев случайным образом.

• При обеспечении безопасности сети необходимо учитывать структурную динамику сети с учетом влияния виртуальных узлов.

Библиографический список

1. http://dlc.sun.com.edgesuite.net/virtualbox/4.0.4/UserManual.pdf

2. Брэгг, Р. Безопасность сетей. Полное руководство / Р. Брэгг, М. Родс-Оусли, К. Страссберг; пер. с англ. – М.: Изд-во «ЭКОМ», 2006. – 912 с.: ил.

3. Охтилев, М.Ю. Интеллектуальные технологии мониторинга и управления структурной динамикой сложных технических объектов / М.Ю. Охтилев, Б.В. Соколов, Р.М. Юсупов. – М.: Наука, 2006. – 410 с.

4. Хилл, Б. Полный справочник по Cisco.: пер. с англ. / Б. Хилл. – М.: Издательский дом «Вильямс», 2008. – 1088 с.