УДК 681.3.066

ПРОЕКТИРОВАНИЕ ЛОКАЛЬНОЙ СЕТИ ДЛЯ ЛАБОРАТОРИИ ПО АНАЛИЗУ ЗАЩИТЫ СЕТЕЙ.

Беда И.А., Погребной А.В., Ракитина Я.В. Рожковский А.Н.
Научный руководитель — к-т.ф.м.н., профессор Шитов Ю.А.
Сибирский федеральный университет

В настоящее время вопросы безопасности информации в сетях является актуальной задачей. Для противодействия атакам используются различные схемы защиты сетей. Для того, чтобы оперативно создавать новые схемы защиты, а также дорабатывать уже существующие, необходимы инструменты, с помощью которых возможно моделировать различные сетевые инфраструктуры с различным оборудованием, и на этих инструментах отрабатывать схемы защиты. Далее смоделированные схемы защиты подвергать различным атакам и, при необходимости, модернизировать их.

Именно для исследования подобных задач на кафедре ПМКБ института космических и информационных технологий (ИКИТ) СФУ в рамках лаборатории по анализу защиты сетей была спроектирована и реализована локальная сеть.

Локальная сеть была спроектирована на основе технологии виртуализации. Технология виртуализации позволяет запускать на одной физической машине несколько виртуальных. Такая возможность технологии виртуализации достигается с помощью использования специального программно-аппаратного комплекса. С аппаратной стороны это реализуется поддержкой процессором VMX расширения. VMX (Virtual Machine eXtensions) — это расширение процессора, добавляющее к основному набору инструкций, инструкции управления виртуальными машинами. Таким образом, такие процессы, как создание виртуальной машины, переключение контекста между виртуальными машинами, реализуются на аппаратном уровне, что увеличивает быстродействие системы. С программной стороны для использования технологии виртуализации необходима программа, которая, используя VMX, создает и управляет виртуальными машинами. Такая программа называется гипервизором. Гипервизор также обеспечивает изоляцию виртуальных машин друг от друга, защиту и безопасность, разделение ресурсов между различными запущенными виртуальными машинами и управление ресурсами.

С помощью технологии виртуализации возможно реализовать для каждого пользователя свою сетевую инфраструктуру, а также динамически ее изменять. Но при работе нескольких пользователей вычислительной мощности одного сервера не достаточно. Поэтому необходимо использовать кластер серверов. Кластер — группа серверов, объединённых высокоскоростными каналами связи и представляющих с точки зрения пользователя единый аппаратный ресурс. С учетом выше сказанного была выбрана логическая схема локальной сети, которая приведена на рисунке 1.

Рис. 1. Логическая схема сети

На этой схеме:

сервер управления кластером — сервер, который распределяет задачи между узлами кластера. Отвечает за трансляцию сетевых адресов и портов. Засчет чего с точки зрения пользователя кластер выглядит как единый ресурс.

Хранилище данных — дисковый массив, разделяемый между всеми узлами кластера. Так как дисковый массив является разделяемым, то он должен обеспечивать высокую скорость доступа к данным. На нем хранятся образы виртуальных машин.

Узлы кластера — серверы, подчиненные серверу управления. Узлы кластера получают задачи от сервера.

Коммутатор — высокоскоростное устройство, с помощью которого осуществляется связь между узлами кластера и сервером управления. Также через него осуществляется связь рабочих станций с виртуальными машинами, работающими на узлах кластера.

Рабочие станции — компьютеры, осуществляющие работу с кластером. С рабочих станций пользователи подключаются к серверу управления и запускают необходимые виртуальные машины для создания сетевых инфраструктур.

Для реализации лаборатории было предоставлено следующее оборудование:

- Сервер Depo Storm 3 шт.
  intel xenon, 8Гб RAM, 2x500 HDD SATA.
- Cisco 3560

8 портов Fast Ethernet, 1 порт Gigabit Ethernet

- Cisco 2960

24 порта Gigabit Ethernet.

- Рабочие станции 12шт.
  Intel core2duo, 1Гб RAM, 320 HDD
  монитор, клавиатура, мышь.

На основе этого оборудования была спроектирована локальная сеть, приведенная на рисунке 2.

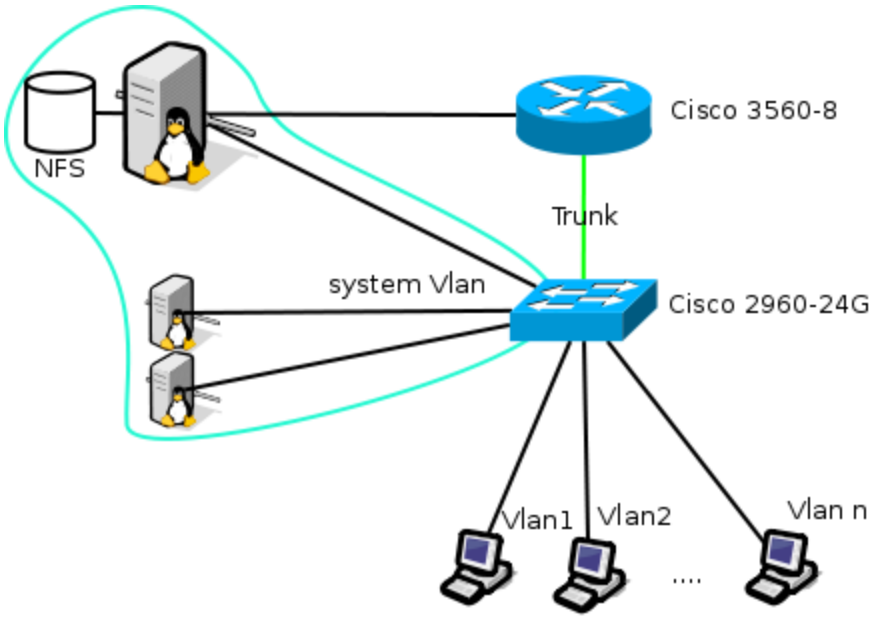

Рис. 2. Реальная схема сети

Сопоставим логическую и реальную схемы сети.

В качестве сервера управления используется сервер Depo Storm под управление операционной системы Linux. На сервере реализовано хранилище данных на основе двух дисковых массивов. Первый дисковый массив представляет собой отказоустойчивый raid1 из двух дисков, на который установлена операционная система, а также хранятся резервные копии. Второй дисковый массив состоит из четырех дисков объединенных в высокоскоростной raid0. Этот дисковый массив разделяется между узлами кластера. Доступ к нему осуществляется по протоколу NFS.

NFS (Network File System) — протокол сетевого доступа к файловым системам. NFS позволяет подключать удалённые файловые системы через сеть. Протокол NFS был выбран, потому что он осуществляет доступ только к тем частям файла, к которым обратился процесс, и делает этот доступ прозрачным. Это означает то, что любое приложение без дополнительных модификаций может работать с файлом, находящимся на NFS так, будто этот файл находится на локальном жестком диске (диске физически подключенном к компьютеру).

Также на втором дисковом массиве находится корневой раздел узлов кластера. Узлы кластера загружаются по сети с помощью PXE. Preboot Execution Environment (PXE) — среда для загрузки компьютеров с помощью сетевой карты без использования жёстких дисков, компакт-дисков и других устройств, применяемых при загрузке операционной системы. Сетевая загрузка происходит с помощью pxelinux. Pxelinux — файл, входящий в набор загрузчиков syslinux, который может загружать по сети и передавать управление ядру Linux. Для загрузки pxelinux и ядра Linux используется протокол tftp. TFTP (Trivial File Transfer Protocol) — простой протокол передачи файлов, основанный на протоколе UDP, который не содержит возможностей аутентификации и используется для первоначальной загрузки бездисковых ЭВМ.

Сетевая загрузка для узлов кластера была выбрана для возможности оперативного расширения кластера. Так как операционная система загружается по сети, а доступ к необходимым файлам осуществляется через NFS, то любой компьютер с поддержкой PXE может использоваться в качестве узла кластера. Также достоинством сетевой загрузки является то, что для добавления нового узла не нужно останавливать работу кластера.

Для нормальной работы NFS необходим высокоскоростной канал связи. В качестве этого канала связи используется Gigabit Ethernet на витой паре. В качестве коммутатора для этого канала связи используется Cisco 2960. На коммутаторе выделен отдельный системный VLAN, в котором и происходит обмен информацией между узлами кластера и сервером управления. VLAN (Virtual Local Area Network) — виртуальная локальная компьютерная сеть, представляющая собой группу устройств, которые взаимодействуют так, как если бы они были физически подключены к одному коммутатору. Также VLAN позволяет изолировать друг от друга несколько групп устройств, подключенных к одному коммутатору.

Каждой рабочей станцией выделен отдельный VLAN. Для настройки параметров TCP/IP рабочих станций на коммутаторе Cisco 3560 настроен dhcp сервер. DHCP (Dynamic Host Configuration Protocol) — это сетевой протокол, позволяющий компьютерам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети TCP/IP. Для каждого VLAN выделена отдельная подсеть, а на dhcp сервере выделен отдельный диапазон адресов. Таким образом, для сервера каждая рабочая станция будет находиться в отдельной сети, что упростит настройку трансляции адресов и портов до виртуальных машин. Трансляция адресов и портов необходима для того, чтобы каждая рабочая станция работала с виртуальными машинами независимо от других.

Рабочие станции подключены к Cisco 2960. Каждый порт которой, за исключением портов объединенных в системный vlan для серверов, принадлежит отдельному vlan. Соединение по транковому порту с Cisco 3560 обеспечивает передачу пакетов от dhcp серверов на Cisco 3560 до рабочих станций. Транковым (trunk) портом в терминологии Cisco называется порт, передающий тегированный трафик нескольких VLAN.

Рассмотрим платформу виртуализации кластера. В качестве гипервизора используется kvm(qrmu-kvm). KVM (Kernel-based Virtual Machine) — это программное решение, обеспечивающее виртуализацию в среде Linux на платформе x86(x86_64), которая поддерживает аппаратную виртуализацию на базе Intel VT, либо AMD SVM. Сетевой доступ к виртуальным машинам в qemu-kvm осуществляется по протоколу VNC. VNC (Virtual Network Computing) — система удалённого доступа к рабочему столу компьютера, использующая протокол RFB (Remote FrameBuffer). Управление осуществляется путём передачи нажатий клавиш на клавиатуре и движений мыши с одного компьютера на другой и ретрансляции содержимого экрана через компьютерную сеть.

Таким образом, на кафедре ПМКБ института космических и информационных технологий (ИКИТ) СФУ в рамках лаборатории по анализу защиты сетей была спроектирована и реализована локальная сеть, позволяющая моделировать различные сетевые инфраструктуры. Моделирование происходит на кластере серверов таким образом, будто каждый пользователь работает с отдельным сервером.