КОМПЕТЕНЦИЯ «СЕТЕВОЕ И СИСТЕМНОЕ АДМИНИСТРИРОВАНИЕ»

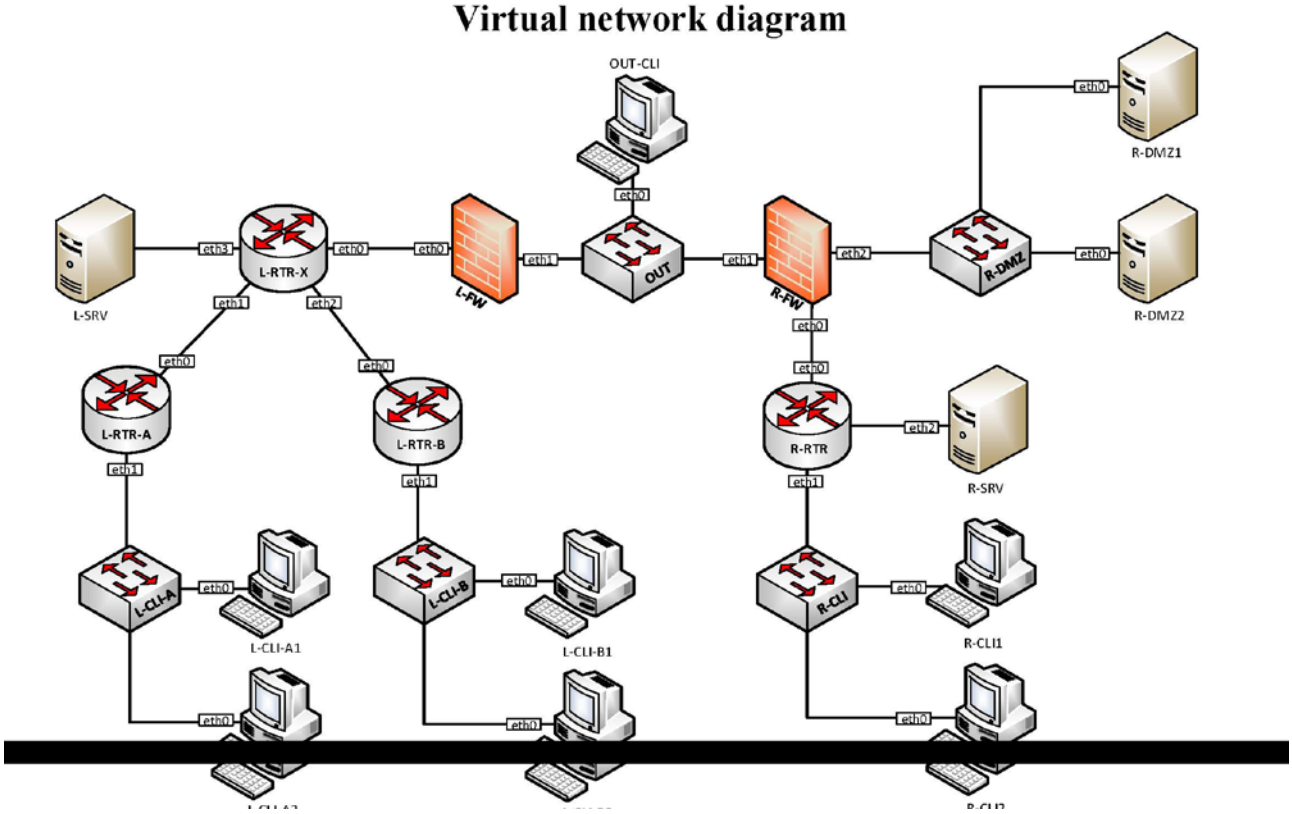
ЗАДАНИЕ ДЛЯ ДЕМОНСТРАЦИОННОГО ЭКЗАМЕНА

МОДУЛЬ А: LINUXISLAND

Разработано экспертами WSR:
Фучко М.М.
Горбачев А.П.

Дата: 09.09.16
Версия: 5

Linux Island.
Virtual network diagram



Базовая конфигурация

1) Задайте имена всех машин в соответствии с сетевой диаграммой
2) Настройте IP-адресацию согласно таблице 1
3) На клиентской машине OUT-CLI создайте скрипты для подключения с помощью удаленного доступа:
    a. Подключение к сетям организаций Left и Right выполняется путем выполнения скриптов connect_left и connect_right
    b. Отключение удаленного доступа (к любой организации) должен выполнять скрипт disconnect_any
    c. Все скрипты должны быть расположены в /opt/vpn
    d. Скрипты должны вызываться из любого каталога простым введением имени скрипта
4) На клиентских машинах обеих организаций создайте скрипты для подключения соответствующих файловых хранилищ:
    a. Монтирование должно осуществляться через вызов скрипта mount_share
    b. Скрипт должен располагается в /opt/scripts клиентской машины
    c. Скрипт должен вызываться без указания пути
    d. Вызываться должен экземпляр скрипта, находящийся в /opt/scripts

Конфигурация маршрутизации и виртуальных частных сетей

1) Настройте защищенный канал передачи данных между машинами L-FW и R-FW с помощью технологии IPSEC:
    a. Параметры политики первой фазы IPSec:
        i. Проверка целостности SHA-1
        ii. Шифрование 3DES
        iii. Группа Диффи-Хелмана — 7
        iv. Аутентификация по общему ключу WSR-2017
    b. Параметры преобразования трафика для второй фазы IPSec:
        i. Протокол ESP

ii. Шифрование DES
iii. Проверка целостности SHA-1

c. В качестве трафика, разрешенного к передаче через IPsec-туннель, должен быть указан только GRE-трафик между машинами машинамиL-FW и R-FW

2) Настройте GRE-туннель между машинами L-FW и R-FW:
   a. Используйте следующую адресацию внутри GRE-туннеля:
      i. L-FW: 10.5.5.1/30
      ii. R-FW: 10.5.5.2/30
3) Настройте динамическую маршрутизацию по протоколу OSPF с использованием пакета Quagga:
   a. Анонсируйте все сети, необходимые для достижения полной связности
   b. Используйте зону с номером 0
   c. Применение статических маршрутов не допускается
   d. В обмене маршрутной информацией участвуют машины L-RTR-X, L-RTR-A, L-RTR-B, R-RTR, L-FW и R-FW
   e. Соседство и обмен маршрутной информацией между машинами L-FW и R-FW должно осуществляться исключительно через настроенный GRE-туннель
4) Настройте удаленный доступ к организациям Left и Right.
   a. Используйте пакет OpenVPN
   b. Используйте общие настройки для обеих организаций:
      i. Сгенерируйте необходимую ключевую информацию на каждом сервере
      ii. Используйте TLS шифрование
      iii. Серверную часть ключевой информации хранить в /opt/vpn/keys/
      iv. Используйте сжатие
   c. Для организации Left:
      i. В качестве сервера выступает машина L-SRV
      ii. Используйте протокол TCP
      iii. Тип устройства TAP
      iv. Порт 1159
      v. Используйте пул IP-адресов для подключаемых клиентов 10.2.2.0/24
      vi. Необходимо обеспечить достижимость службы OpenVPN для внешних клиентов
   d. Для организации Right:
      i. В качестве сервера выступает машина R-FW
      ii. Используйте протокол UDP
      iii. Тип устройства TUN
      iv. Порт 1029
      v. Используйте пул IP-адресов для подключаемых клиентов 10.9.8.0/24
   e. Обеспечьте возможность удаленного доступа с машины OUT-CLI до сетей организаций Right и Left:
      i. Ключевая информация должна быть расположена в /opt/vpn/keys
      ii. Вызываться должна копия скрипта, находящаяся в /opt/vpn
      iii. Машины одной организации не должны быть доступны при подключении к другой организации
      iv. Машина OUT-CLI должна быть достижима со всех машин каждой организации при подключении к одной из них через удаленный доступ

Конфигурация сетевых сервисов

1) Настройте службу DHCP на машинах L-RTR-A, R-RTR в соответствии с требованиями:
   a. Клиентам сетей L-CLI-A, L-CLI-B, R-CLI, R-SRV динамически назначаются сетевые адреса
      i. Диапазон от 50 до 150 соответствующей сети
      ii. Домен соответствующей организации
      iii. Шлюз по умолчанию через интерфейс роутера в данной сети

iv. Адрес DNS-сервера соответствующей организации
v. Автоматическое обновление записей DNS-сервера организации при выдаче адреса

b. Для узла R-SRV средствами службы DHCP должен быть зарезервирован статический адрес в соответствии с таблицей 1.

2) Настройте службу DNS для организации Left на сервере L-SRV:
   a. Задайте имя зоны wsr.left
   b. Разместите файлы зон в /var/wsr/
   c. Обеспечьте прямое и обратное разрешение имен
   d. На всех машинах организации Left реализуйте автоматическое разрешение имен в соответствии с таблицей 2
   e. При запросе на разрешение имен зоны wsr.right должно происходить автоматическое обращение к соответствующей службе организации Right
3) Настройте службу DNS для организации Right на сервере R-DMZ1
   a. Задайте имя зоны wsr.right
   b. Разместите файлы зон в /var/wsr/
   c. Обеспечьте прямое и обратное разрешение имен
   d. На всех машинах организации Right реализуйте автоматическое разрешение имен в соответствии с таблицей 3
   e. Реализуйте разрешение имен машин организации Right при разрешении их из сети организации Left в соответствии с таблицей 4.
   f. Реализуйте разрешение имен машин организации Right при разрешении их из сети OUT в соответствии с таблицей 5.Для обратного разрешения доступны только внешние адреса
   g. При запросе на разрешение имен зоны wsr.left должно происходить автоматическое обращение к соответствующей службе организации Left
   h. Автоматически добавляемые имена доступны для разрешения только из организации Right
4) Настройте трансляцию сетевых адресов в соответствии с таблицей 8.
   a. Настройте трансляцию портов для всех машин каждой организации во внешний адрес соответствующего межсетевого экрана
   b. Обеспечьте достижимость VPN-шлюза организации Left из сети OUT путем трансляции соответствующего порта на L-FW

Конфигурация веб- и почтовых служб

1) На машине R-DMZ2 установите и настройте веб-сервер apache:
   a. Организуйте структуру файлов и соответствующих URL в соответствии с таблицей 6.
   b. Настройте права доступа и содержание веб страниц в соответствии с таблицей 7.
   c. При доступности SSL-соединения настройте автоматический переход по протоколу HTTPS при попытке доступа по протоколу HTTP.
   d. Используйте сертификат, подписанный удостоверяющим центром. При доступе по протоколу HTTPS с клиентских машин каждой организации сертификат должен рассматриваться как доверенный.
   e. Настройте веб-сервер таким образом, чтобы из ответов сервера нельзя было узнать версию веб-сервера и версию ОС.

Конфигурация файловых служб

1) На сервере R-SRV создайте каталог /opt/nfs/. Организуйте доступ к данному каталогу по протоколу NFS:
   a. Настройте доступ на чтение и запись для клиентов сетей R-CLI и R-SRV
   b. Настройте доступ только для чтения для всех остальных машин организации Right

2) На сервере L-SRV создайте каталог /opt/samba/. Организуйте доступ к данному каталогу по протоколу Samba:
   a. Создать разделяемый ресурс Share
   b. Разрешить доступ учетной записи (логин smbuser, пароль smbpass) с правами на чтение и запись
   c. Файлы должны создаваться с маской 0700
   d. Разрешить гостевой доступ с правами «только на чтение».
3) Настройте клиентские машины каждой организации
   a. Все машины должны иметь доступ к файловому хранилищу своей организации
   b. Хранилище должно монтироваться в /opt/share соответствующей клиентской машины вызовом скрипта mount_share

Конфигурация служб мониторинга и журналирования

1) На сервере R-SRV установите и настройте сбор системных сообщений с помощью пакета rsyslog
   a. Настроить сбор syslog сообщений с межсетевого экрана R-FW в папку /opt/logs/r-fw.log.
   b. Настроить сбор syslog сообщений с маршрутизатора R-RTR в папку /opt/logs/r-rtr.log
   c. Настройте журналирование любых системных сообщений, кроме сообщений уровня отладки

Конфигурация параметров безопасности и служб аутентификации

1) Для клиентских машин организации Left:
   a. Настройте sudo следующим образом:
      i. Для пользовательских учетных записей запретите запуск команды visudo через sudo
      ii. Ввод всех остальных команд через sudo должен быть разрешен с вводом пароля
   b. Запретите вход под учетной записью администратора на первой консоли с 18-00 до 07-00
   c. Запретите удаленный вход к данным машинам по протоколу ssh под учетной записью администратора
2) Для клиентских машин организации Right:
   a. Установите парольную политику:
      i. Длина не менее 8 символов
      ii. Должны использоваться буквы разного регистра
      iii. В пароле обязательно должна быть как минимум одна цифра
   b. Установите запрет на вход с первой консоли под учетной записью администратора
3) Настройте ограничения сетевого трафика
   a. Разрешите VPN-подключения из сети OUT
   b. Разрешите необходимый трафик к серверам R-DMZ1 и R-DMZ2 по транслированным IP-адресам
   c. Разрешите необходимый трафик для создания IPSec и GRE туннелей между организациями
   d. Запретите весь остальной трафик

Таблица 1. Сети и IP-адресация

Имя	Сеть	Хосты	Состав
OUT	10.10.10.0/24	10.10.10.5 10.10.10.100 10.10.10.200	OUT-CLI L-FW R-FW

R-DMZ	192.168.10.0/24	192.168.10.1 192.168.10.100 192.168.10.200	R-FW R-DMZ-1 R-DMZ-2
R-SRV	192.168.20.0/24	192.168.20.1 192.168.20.100	R-RTR R-SRV
R-CLI	192.168.30.0/24	192.168.30.1 DHCP DHCP	R-RTR R-CLI1 R-CLI2
R-CORE	192.168.100.0/30	192.168.100.1 192.168.100.2	R-FW R-RTR
L-CORE	172.16.10.0/30	172.16.10.1 172.16.10.2	L-FW L-RTR-X
L-CLI-A	172.16.100.0/24	172.16.100.1 DHCP DHCP	L-RTR-A L-CLI-A1 L-CLI-A2
L-CLI-B	172.16.200.0/24	172.16.200.1 DHCP DHCP	L-RTR-B L-CLI-B1 L-CLI-B2
L-SRV	172.16.20.0/24	172.16.20.1 172.16.20.100	L-RTR-X L-SRV
L-RTR-A	172.16.50.0/30	172.16.50.1 172.16.50.2	L-RTR-X L-RTR-A
L-RTR-B	172.16.55.0/30	172.16.55.1 172.16.55.2	L-RTR-X L-RTR-B

Таблица 2. Сопоставление имен машин организации Left

Машина	DNS-имя
L-SRV	srv.wsr.left; wsr.left; access.wsr.left.(для NAT)
L-RTR-A	rtr-a.wsr.left
L-RTR-B	rtr-b.wsr.left
L-RTR-X	rtr-x.wsr.left
L-FW	fw.wsr.left; tunnel.wsr.left

Таблица 3. Сопоставление имен машин организации Right при разрешении их из сети организации Right:

Машина	DNS-имя
R-SRV	srv.wsr.right
R-RTR	rtr.wsr.right
R-DMZ1	dmz1.wsr.right;dns.wsr.right
R-DMZ2	dmz2.wsr.right;web.wsr.right
R-FW	fw.wsr.right; tunnel.wsr.right

Таблица 4. Сопоставление имен машин организации Right при разрешении их из сети организации Left:

Машина	DNS-имя
R-SRV	srv.wsr.right
R-RTR	----
R-DMZ1	dmz1.wsr.right;dns.wsr.right
R-DMZ2	dmz2.wsr.right;web.wsr.right
R-SRV	srv.wsr.right

Таблица 5. Сопоставление имен машин организации Right при разрешении их из внешней сети:

Машина	DNS-имя
R-SRV	------
R-RTR	------
R-DMZ1	dns.wsr.right
R-DMZ2	web.wsr.right
R-FW	access.wsr.right;

Таблица 6. Структура файлов и URL:

URL	Путь к файлу
web.wsr.right	/opt/www/hello_right.html
web.wsr.right	/opt/www/authorized_left.html
web.wsr.right	/opt/www/hello_vpn.html
web.wsr.right	/opt/www/out.html

Таблица 7. Права доступа и содержание веб-страниц:

Группа	SSL	Аутентификация	Текст	Файл
Left	Нет	Через RADIUS-сервер	Hello, Left!	authorized_left.html
Out	Да	Нет	Hm, outsider.	out.html
VPN	Да	По сертификату	Hello, Teleworker!	hello_vpn.html
Right	Нет	Нет	Hello, Right!	hello_right.html

Таблица 8. Трансляция сетевых адресов

Машина	Адрес
R-DMZ1	10.10.10.210
R-DMZ2	10.10.10.220
L-SRV	10.10.10.190