**Skill**

**"IT NETWORK SYSTEM ADMINISTRATION"**

**Test project**

**module A:**

**Linux ISLAND**

**Developed by WSR experts:**

**Fuchko M.M.**

**Mukhametov R.A.**

**Silaev N.O.**

**Date: 20.06.18**

**Version: 3**

## CONTENTS

This Test Project proposal consists of the following documentation/files:

1. NC18\_TP39\_Module-A\_RU.docx

## INTRODUCTION

Open source systems knowledge is became essential nowadays for people who want to build a successful career in any IT engineering field. This test project contains a lot of challenges from real life experience, primarily IT integration and IT outsourcing. If you are able to complete this project with the high score, you are definitely ready to serve network infrastructure for any multi-branch enterprise.

## DESCRIPTION OF PROJECT AND TASKS

Current test project is designed using a variety of network technologies with which you should be familiar within the LPIC and Red Hat certification tracks. Tasks are broken down into following configuration sections:

* Basic configuration
* Network services configuration
* Monitoring and logging services
* Remote access services configuration
* Web and Email services configuration
* Storage services configuration
* Authentication and security services configuration

All sections are independent but all together they build very complex network infrastructure. Some tasks are pretty simple and straightforward, but some may be tricky. You may see that some technologies are expected to work on top of other technologies. For example, dynamic routing is expected to run on top of configured VPN tunnel between organizations. It is important to understand that if you are cannot come up with any solution in the middle of such technology stack it doesn’t mean that the rest of your work will not be graded at all. For example, in order to configure remote access, a GRE tunnel must be created inside an IPsec tunnel. If, for example, you were unalbe to configure IPsec, but you did configure GRE, you would still receive points for configuring remote access.

## Instructions for the competitor

It is very important to read the whole test project first. Bring your attention that not all tasks are written in chronological order. Some sections may require configuration from other sections below them. For example, task 6 in «Basic configuration» section asks you to automate VPN access which is obviously will not work before you apply all necessary configurations from the “Routing & VPN” section that comes right after. This is your responsibility to divide your time and choose what have to be done first and what’s next. As mentioned above, do not waste your time if you’re stuck with some tasks. You can use a temporary solution (if you have technology stack dependency) and continue to work with other tasks so may go back afterwards and fix things that are not working properly if you still have time. In addition, we recommend you to check all your previous work when you complete following modules.

**Access to all virtual machines is using the following account root:toor**.

**The ISP virtual machine is pre-configured. Administrative access to this virtual machine is not available during the task completion. If you would try to recover access, you will face trouble.**

LEFT organization includes the following virtual machines: L-SRV, L-FW, L-RTR-A, L-RTR-B, L-CLI-A, L-CLI-B.

RIGHT organization includes the following virtual machines: R-DMZ, R-FW, R-RTR, R-CLI.

## EQUIPMENT, MACHINERY, INSTALLATIONS AND MATERIALS REQUIRED

It is expected that all Test Projects can be done by Competitors based on the equipment and materials specified in the Infrastructure List.

**CentOS 17.08** is used as the operating system.

You will have access to the CentOS-7-x86\_64-Everything-1708.iso

You will also have acces to the AdditionalPackages.iso disk, where additional required packages are located.

## MARKING SCHEME

Each sub criterion has approximately the same weight. Aspects within each section have different weights depending on aspects count and their complexity.

Marking scheme is designed in the way that every configuration aspect is graded only once. For example, in the “Basic configuration” section you are required to configure hostnames for all devices but it will be checked on only one device and graded only once. The same configuration aspect may be checked and graded more than once if it’s done with different configuration options for different devices or for different device classes.

Detailed description of the marking process will be developed by the experts, participating in marking the test project during the competition, and it will be added as an additional document. These details are subject to 30% changes as well as the aspects in marking scheme.

**Host configuration**

1. Configure hostnames according to the **diagram**.
2. Install the following software to **ALL** virtual machines:
   1. tcpdump package
   2. ftp client
   3. lftp client
   4. net-tools package
   5. vim editor
   6. lynx
   7. dhclient
   8. bind-utils
   9. nfs-utils
3. Create the **/etc/hosts** file according to the **diagram** (except the address of host L-CLI-A). This file will be used during assessment in case the DNS services are unavailable. IP addresses will not be used during assessment.
4. If DNS services are working correctly, the DNS replies must have higher priority.

**Network services configuration**

1. Configure IP addresses on ALL hosts according to the **diagram**.
2. Configure dynamic host configuration protocol server for L-CLI-A and L-CLI-B
   1. Use L-RTR-A as the DHCP server for LEFT organization
      1. Use 172.16.100.60 — 172.16.100.75 as the address pool for the L-RTR-A network
      2. Use 172.16.200.60 — 172.16.200.75 as the address pool for the L-RTR-B network
      3. Use L-SRV address as the DNS server address.
   2. Configure the DHCP server so L-CLI-B would always receieve a fixed address according to the **diagram.**
   3. Use the respective router's LAN IP address as the default gateway address.
   4. Use the DNS-suffix **skill39.wsr**
   5. DNS entries of A type for corresponding hosts should be updated upon recieving address from the DHCP server.
3. Configure domain name resolution service on L-SRV
   1. The server must service **skill39.wsr** zone
   2. Name resolution should be configured according to **Table 1**
   3. Configure R-DMZ as the secondary DNS server for **skill39.wsr** zone
      1. Use R-DMZ address as the DNS server for R-CLI
   4. Queries for names outside **skill39.wsr** zone should be forwarded to the ISP DNS server.
   5. Configure support for reverse zone lookups.
   6. Place the zone files in **/opt/dns/**
   7. L-FW server should forward external DNS queries from OUT-CLI to L-SRV.
      1. It is important to resolve only [www.skill39.wsr](http://www.skill39.wsr/) to the external address of R-FW
   8. Delegate the subdomain ext.skill39.wsr to ISP server.
4. Configure an internet gateway on L-FW to organize shared internet access. Configure network address translation for internal network addresses to the address of the outside interface.
   1. Make DNS service on L-SRV available on the external address of L-FW.

**Monitoring and logging services**

1. Configure LDAP server to perform centralized account management
   1. Use L-SRV as the server
   2. Configure the accounts according to **Table 2**
   3. Create the OUs according to **Table 2**
   4. L-CLI-A and L-CLI-B should use LDAP authentication
   5. Only OU "Admin" and "Guest" should be able to authenticate on clients
2. Configure centralized home directory storage for LDAP users
   1. Use L-SRV as the home directory server
   2. Store home directories in /opt/homes/
   3. Configure a storage quota of 10MB
   4. Use NFS to access the directories
3. Configure L-SRV to collect logs from hosts L-CLI-A, L-CLI-B, L-FW and L-SRV
   1. Logs should be stored in **/opt/logs/**
   2. Logging should be performed according to **Table 3.**
   3. Log file size should not exceed **10Kb**.
   4. Log rotation should be configured

**Remote access services configuration**

1. Configure an OpenVPN remote access server on L-FW:
   1. Use L-FW as the server
   2. Tunnel configuration
      1. TUN device
      2. UDP protocol
      3. Compression enabled
      4. Server port 1122
   3. Key information should be generated on L-FW
   4. Authentication should be performed using LDAP server on L-SRV
      1. Only LDAP users in the "VPN" OU should have access to VPN service
   5. Use network 5.5.5.0/24 as the address pool for connecting clients
      1. Ensure that fixed address are assigned according to the **diagram.**
   6. Store all necessary information (except the configuration files) in **/opt/vpn**
2. Configure OpenVPN remote access client on OUT-CLI:
   1. Remote connection should be established by running a script named **start\_vpn.sh**
      1. The script should accept the following parameters (in the order listed):
         1. OpenVPN username
         2. Clear-text password
      2. Automated VPN disconnect is not required
      3. This script should be placed in **/opt/vpn** directory.
      4. One should be able to start the script from any directory without specifying the path
      5. Locate the script at the following path **/opt/vpn/start\_vpn.sh**
3. Configure a secure connection between L-FW and R-FW using IPsec:
   1. Phase 1 parameters:
      1. Integrity check using SHA-1
      2. 3DES encryption
      3. DH group – 7
      4. Shared key authentication using key WSR-2018
   2. Phase 2 parameters:
      1. Protocol – ESP
      2. DES encryption
      3. Integrity check using SHA-1
   3. Only GRE traffic between L-FW and R-FW should be allowed to use the IPsec tunnel
4. Configure a GRE tunnel between L-FW and R-FW:
   1. Use following addresses for GRE tunnel:
      1. L-FW: 10.5.5.1/30
      2. R-FW: 10.5.5.2/30
5. Configure dynamic routing using OSPF with Quagga:
   1. Advertise all networks, that are required to achieve full connectivity
   2. Use area 0
   3. Using static routes is prohibited
   4. L-RTR-A, L-RTR-B, R-RTR, L-FW and R-FW participate in the exchange of routing information
   5. Adjacency and exchange of routing information between L-FW and R-FW should be performed exclusively through the configured GRE tunnel
   6. Advertise the networks on local interfaces of L-RTR-A and L-RTR-B.
6. On L-FW configure remote access using SSH protocol:
   1. The access is available only to users **ssh\_p** and **ssh\_c**
      1. Use the password **ssh\_pass**
   2. SSH server should be avaliable on port **1022**
7. Configure SSH remote access client on OUT-CLI:
   1. Connection to the L-FW server should be performed automatically to the correct port, without explicitly stating the port number when using the connection command.
   2. For all other servers port **22** should be used by default
   3. Access to L-FW using the **ssh\_p** account should be performed using public key authentication.

**Web and Email services configuration**

1. On R-DMZ install and configure the Apache web server:
   1. Configure a website www.skill39.wsr for external users
      1. Use the /var/www/html/out directory
      2. Use port 8088
   2. Configure a website intra.skill39.wsr for internal users
      1. Use the /var/www/html/intra directory
      2. The access should be available only to "webusers" OU
2. Configure HAProxy on R-FW
   1. www.skill39.wsr website should be available from the external network on the external address of R-FW
   2. Configure SSL

**Storage services configuration**

1. Create an LVM volume on R-RTR and create a directory /opt/lvm on it
   1. Create virtual drives for the LVM volume manually
   2. Configure hourly automatic snapshot creation with a name <Date>.<Time>
      1. Ensure that at least one snapshot will be present by the time of assessment
2. Configure a distributed DFS storage
   1. Locate the DFS root on L-SRV, directory /opt/dfs/
   2. Shared client resources should be mounted to /opt/dfs
      1. Use client hostname as the name of shared resource
   3. Use real linking
   4. Configure shared access for clients to the /opt/smb directory
   5. Use LDAP for user authentication
      1. Access is allowed only to the "Guest" OU

**Authentication and security services configuration**

1. Configure a CA on R-FW using OpenSSL.
   1. Use **/etc/ca** as the root CA directory
   2. Use the following CA attributes:
      1. Country - RU
      2. Organization - WorldSkills Russia
      3. Use WSR CA as CN
   3. Issue a root CA certificate
   4. All operating systems should trust this CA
2. Configure **iptables** firewall on L-FW and R-FW
   1. Deny direct traffic from networks to **Internal**
   2. Allow remote connections using OpenVPN on the external interface of L-FW
   3. Allow all necessary traffic to establish IPsec and GRE tunnels between organizations
   4. Allow SSH connections to the corresponding port
   5. VPN clients should have full access to the **Internal** network
   6. Allow necessary traffic to the servers L-SRV and R-DMZ using translated IP addresses
   7. Restrict access to www.skill39.wsr site when using Remote-access VPN. Allow access only to intra.wsr.right
   8. All other services should not be allowed
      1. Configure actions for inbound (coming from external network) ICMP requests as you see fit

**Table 1** - DNS names

|  |  |
| --- | --- |
| **Host** | **DNS name** |
| L-CLI-A | A: l-cli-a.skill39.wsr |
| L-CLI-B | A: l-cli-b.skill39.wsr |
| L-RTR-A | A: l-rtr-a.skill39.wsr |
| L-RTR-B | A: l-rtr-b.skill39.wsr |
| L-SRV | A: l-srv.skill39.wsr  CNAME: server.skill39.wsr  CNAME: center.skill39.wsr |
| L-FW | A: l-fw.skill39.wsr  CNAME: vpn.skill39.wsr |
| R-FW | A: r-fw.skill39.wsr  CNAME: www.skill39.wsr |
| R-DMZ | A: r-dmz.skill39.wsr  CNAME: intra.skill39.wsr |
| R-RTR | A: r-rtr.skill39.wsr |
| R-CLI | A: r-cli.skill39.wsr |

**Table 2** - LDAP accounts

|  |  |  |  |
| --- | --- | --- | --- |
| **OU** | **CN** | **Password** | **Access** |
| Admin | tux | toor | Full on all hosts |
| Guest | user1 – user99 | P@ssw0rd | only to client hosts |
| VPN | vpn1 – vpn99 | Passw0rd | only for VPN |
| webuser | webuser1 – webuser99 | P@ssword | only to access intra.skill39.wsr site |

**Table 3** – Logging configuration

|  |  |  |
| --- | --- | --- |
| **Source** | **Logging level** | **File** |
| All hosts | critical | /opt/logs/<HOSTNAME>/crit.log |
| L-SRV | auth.\* | /opt/logs/<HOSTNAME>/auth.log |
| L-FW | \*.err | /opt/logs/<HOSTNAME>/error.log |
| R-RTR | alert | /opt/logs/<HOSTNAME>/alert.log |
| All except L-FW | \*.err | /opt/logs/err.log |

\*<HOSTNAME> - name of the directory for the logged host

\*\* The directory /opt/logs/ must not contain any files except those listed in the table

## Virtual network diagram

