**Module Cisco**

**Seleksi Calon Competitor**

**World Skills Competition 2021 Shanghai**

# DESCRIPTION OF PROJECT AND TASKS

This Cisco module test project applies a judgment assessment system. This is to provide comfort to competitors working in accordance with the level of ability and mastery of the technology. The better and more complex the technology, the higher the judgment point. To facilitate the judgment marking process, you must write down each technology or protocol selection you use in the task section below.

Network Virtualization:

* Url: <https://172.30.33.52/>
* Username: *{Private Message}*
* Password: *{Private Message}*

Server:

* IP & Port esxi: 10.220.24.100
* username: competitor
* password: 7vinowkH-yfight
* Linux: root / Skill39
* Windows 10 : competitor / Skill39

# BASIC CONFIGURATION

* Configure IP & Hostname according to the appendix.
* See the network topology to understand IP addressing, services and network diagram.
* If no IP Address is specified for a host, you are allowed to use all host IPs in that subnet.
* Configure domain name **selection-tc1.id** for ALL network devices on the topology
* Create an encrypted password using md5 so that the network device when entering special EXEC mode for each switch with password **lOck0N1**.
* Create user **compet** with password **wss2021** on ALL devices
  + Only scrypt hash of the password should be stored in configuration.
  + User should have maximum privileges.
* Configure new AAA model for BR.
  + Configure AAA model with AUTHRTR as authentication list name.
  + Remote console (vty) authentication should use local username database.
  + After successful authentication on vty line users should automatically land in privileged mode.
  + Enable login authentication on local console.
  + After successful authentication on local console user should land in user mode with minimal privileges (privilege level 1).
* Configure RADIUS authentication for all remote consoles (vty) on HQ router.
  + Authentication sequence:
    - RADIUS server
    - Local username database
  + Use “cisco1” as the shared key.
  + Use port numbers 1812 for authentication and 1813 for accounting.
  + IP address of the RADIUS server is 18.31.192.10
  + Configure automatic authorization — after successful authentication on RADIUS server user should automatically land in privileged mode with maximal privileges.
  + Test RADIUS authentication using radius/cisco1 credentials.
* Configure **compet** as a privileged mode password for RO1 and RO2.
  + Password should be stored in configuration in plain text (not in hash).
  + Configure privileged mode authorization on RO1 and RO2. For example:

|  |
| --- |
| #connect to RO1 using SSH or Console  Username: **compet**  Password: **wss2021**  Type help or '?' for a list of available commands.  HQ> enable  Password: **wss2021**  HQ# |

* Configure current local time zone (GMT +7) on HQ1 router.

# SWITCHING CONFIGURATION

* Configure VLAN distribution feature on **SW1**. When adding any new VLAN to **SW1**, this VLAN should be automatically distributed to **SW2, SW3** and **SW4**. VLAN database should contain the following VLANs:
* **VLAN 11** with name **CENTRAL-HOSTS**
* **VLAN 12** with name **CENTRAL-VOICE**
* **VLAN 13** with name **EDGE**
* Configure all trunking and access interfaces for the VLANs to work as expected.
* **SW1** should be the root bridge for all **VLANs** and **SW2** should take over in case **SW1** fails.
* Configure link aggregation between **SW2** and **SW3**.

|  |
| --- |
| ***How did you implement link aggregation?***  □ Not implemented  □ Static (L2)  □ Static (L3)  **□** LACP  **□** PAgP  □ Other (please specify): |

* Turn on security mechanism that prevents STP root change on **SW2** port which is connected to **FW1**. In case a superior BPDU arrives on this port, the port should transfer to root-inconsistent state.
* Configure port on **SW3** switch which is connected to **FW1** so that it goes to Forwarding state without waiting for STP recalculation.

# PUBLIC INTERNET

1. **google.com** must be accessible on public internet from any client virtual machine.

***How did you implement routing on the public internet?***

□ Not implemented

□ Static \ Default routes

□ RIP v1/2

□ OSPF

□ EIGRP

**□** BGP

□ Other (please specify):

# ENTERPRISE ROUTING DOMAIN

1. Ensure end-to-end connectivity between all virtual machines inside enterprise routing domain.
2. All traffic between sites must be encrypted with IPsec while traversing via public internet.
3. Serial links must serve as a routing failover to branch networks and internet access in case of public internet is down. Implement a secure layer 2 protocol on this link.
4. Implement secure remote access for **LEE** so he can securely access all services inside enterprise routing domain. Add A record **vpn.selection-tc1.id** with IP address of VPN termination device to **Google** DNS server.
5. **BR2** should act as stateless failover for all traffic from **BRANCH** towards the internet and enterprise routing domain and vice versa. In case of **BR1** failure **BR2** should take over all roles of **BR1** so all network services will continue normal operation.

***How did you implement site-to-site VPN(s) between SHA, KVX, YKS, HKG-01 and HKG-02?***

□ Not implemented

□ Full mesh GRE

□ Hub-and-spoke GRE

□ Full mesh IPsec

□ Hub-and-spoke IPsec

□ DMVPN Phase 1

□ DMVPN Phase 2

□ DMVPN Phase 3

□ Other (please specify):

***How did you implement site-to-site VPN(s) between TOF and the rest of enterprise routing domain?***

□ Not implemented

□ Hub-and-spoke IPsec

□ Point-to-Point IPsec (specify peer):

□ Other (please specify):

***Specify components that are used for IPsec***

*Internet Key Exchange protocol: □ IKE v1 □ IKE v2*

*Authentication: □ Pre-shared key □ RSA*

*Payload security: □ AH □ ESP*

*Other \ Details (please specify):*

***How did you implement routing inside enterprise routing domain?***

□ Not implemented

□ Static routes

□ RIP

□ OSPF

□ EIGRP

□ BGP

□ Other \ Details (please specify):

***How did you implement remote access VPN?***

□ Not implemented

□ PPTP

□ L2TP

□ IPsec

□ AnyConnect

□ Other (please specify):

***Which entry point(s) is used for remote access VPN?***

*□ Not implemented*

*□ RO1*

*□ RO2*

*□ FW1*

*□ FW2*

*□ BR1*

*□ BR2*

*□ Other \ Details (please specify):*

# SECURITY CONFIGURATION

* Configure role-based access control on **RO1** router:
* Create **user1, user2, user3** with **Skill39** password.
* Create view-context “**show\_view**”:
* Include “**show version**” command
* Include all unprivileged commands of “**show ip \***”
* Include “**who**” command
* **user1** should land in this context after successful authentication on local or remote console.
* Create view-context “**ping\_view**”:
* Include “**ping**” command
* Include “**traceroute**” command
* **user2** should land in this context after successful authentication on local or remote console.
* Create **superview-context** that **combines these 2 contexts**. **user3** should land in this **superview-context** after successful authentication on local or remote console.
* Make sure that users cannot issue any other commands within contexts that are assigned to them (except show banner and show parser, which are implicitly included in any view).
* Implement **layer 2 security features** on the switches at the **Bandung** site.

# BACKUP CONFIGURATION

* Configure logging of system messages on FW2 Firewall and RO1 Router. All logs including informational messages should be sent to the NetOps server (location /var/log/fw2.log and /var/log/ro1.log).
* Configure configuration backup on RO1 router:
  + Backup copy of running configuration should be automatically saved on NetOps server using TFTP each time configuration is saved (copied to startup);
  + Use following naming convention for backup files: .cfg
  + Location for configuration backup files is /srv/tftp/ on NetOps server

**Make sure all configurations are saved, after completion CML will be turned off. The marking process will be carried out from the first time the device turns on.**

# NETWORK DIAGRAM

