SIMOS

Implementing Cisco Secure Mobility Solutions (SIMOS v1.0)

Remote Lab Administration Guide

Global Knowledge

Contents

1. Overview

The purpose of the Remote Lab Administration Guide is to assist in the setup and configuration of the classroom for connecting to the Remote Lab for Implementing Cisco Secure Mobility Solutions (SIMOS v1.0).

This guide is not a substitute for Cisco Course Administration Guide (CAG) and should be used in conjunction with CAG. It's imperative that Instructor goes through the entire guide to familiarize himself with the remote lab setup.

This guide does not include any access details. All access details will be included in the Remote Lab Administrator's email.

2. Course Version

This course is the original release of SIMOS v1.0

3. Students per Pod

Each Pod can accommodate 2 students.

4. Remote Lab Description

The remote lab is accessed via RDP to the following location.

rlabs.globalknowledge.ae:443

Login using the credentials provided in the access details email from Remote Lab Support Team.

Please refer the attached **GK MEA Remote Lab Access Procedure** for connecting to the remote lab.

Upon successful authentication, a new window opens up the lab topology for this lab. You can gain access to the consoles of the different devices in the lab by simply clicking (left Click) the device that you would like to access.

Once a device is clicked, a new tab is added to the lab interface which gives access to the selected device.

Access to the console connections is exclusive. If you are unable to access the console of a particular device you can always clear the console lines to that device

by selecting **Clear line of the device** option obtained by right clicking the (tab name)/(device from topology) .

General administrative tasks listed below can be carried out by right clicking the respective Device from the topology/tab name.

For Devices

- Close console connection to the device
- Change font of the terminal
- Clear line of the device
- Send Ctrl Break
- Power Management

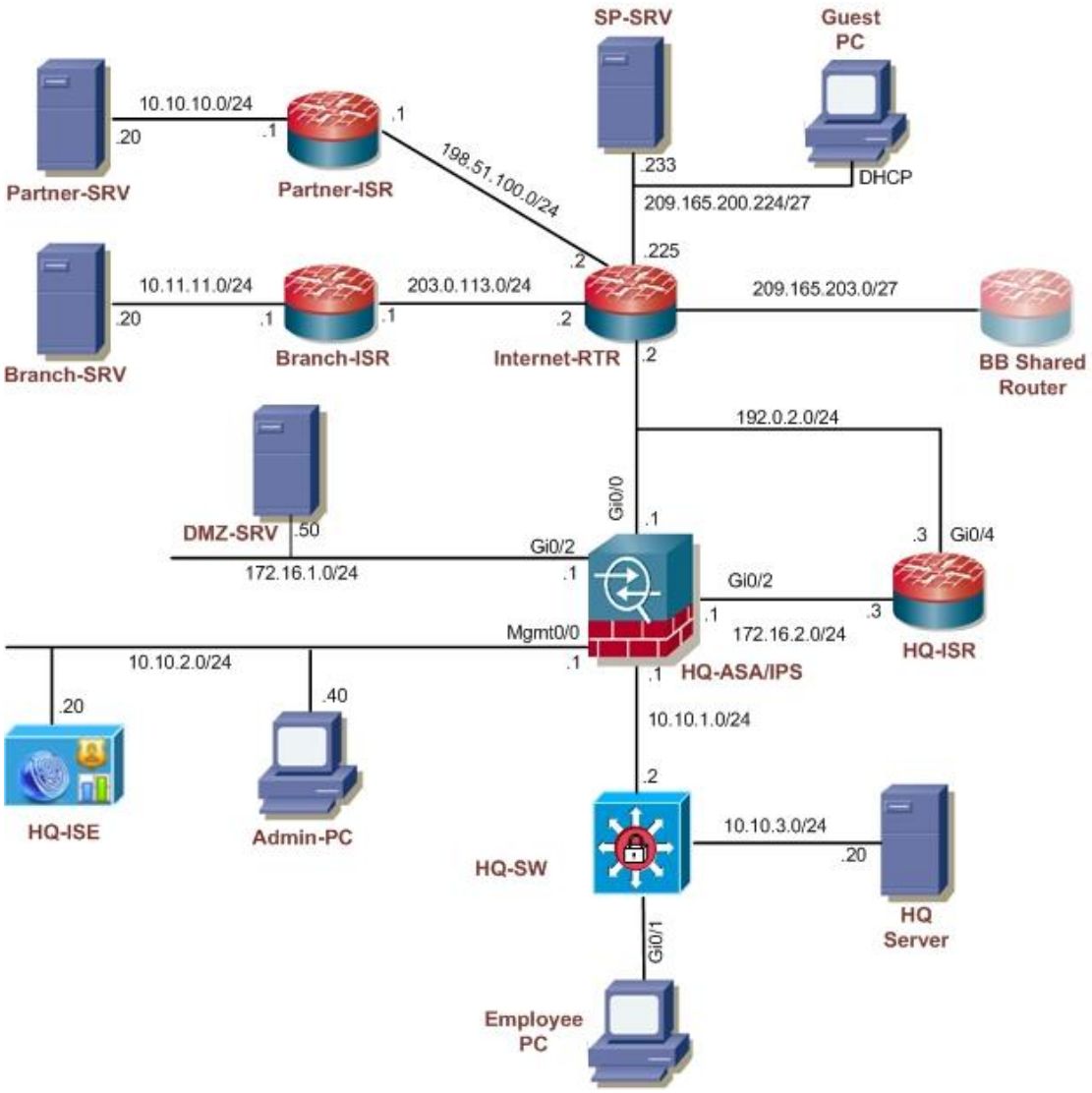
For Server/Client PC's

- Send Ctrl Alt Del to Server/PC
- Close console connection to Server/PC
- Power Management

A helpful tips section is also provided towards the bottom right corner of the topology that lists the Known issues/work around that the remote lab developer has come across during the preparation of this lab.

5. Remote Lab Topology

The network topology diagram for Implementing Cisco Secure Mobility Solutions (SIMOS v1.0) remote lab is as per Cisco Topology mentioned in the lab guide.



Each Pod is provided with the following equipments and VMs:

- HQ-ASA
- HQ-ISR
- HQ-SW
- Partner-ISR
- Branch-ISR
- Internet-RTR
- Employee PC
- Guest PC
- Admin PC
- HQ Server

- Branch Server
- Partner Server
- SP Server
- DMZ Server
- HQ-ISE

6. Lab Exercise Tips

This section provides additional tips/workaround for certain tasks mentioned in the Cisco Lab guide. Please refer to these tips before contacting the remote lab support team.

6.1. General Guidelines

Note: All Pods are using same IP addressing scheme

Credentials for the Servers/PCs in the network are as follows:

Equipments/Servers/PCs	Username	Password
HQ-ASA	admin	Ci5coAdmin Enable: cisco
HQ-IPS	cisco	Ci5coAdmin
Employee PC	student	Ci5coAdmin
Guest PC	student	Ci5coAdmin
Admin PC	student	Ci5coAdmin
HQ Server	administrator	Ci5coAdmin
Partner Server	administrator	Ci5coAdmin
Branch Server	administrator	Ci5coAdmin
SP Server	administrator	Ci5coAdmin
DMZ Server	root	Ci5coAdmin
HQ-ISE	admin	Ci5coAdmin

6.2. Lab 2-1: Implement Site-to Site Secure Connectivity on the Cisco ASA

- Task3 : Step4: Verify the IP address obtained on Employee PC and use http:// IP address of Employee PC

6.3. Lab 2-2: Implement Cisco IOS Static VTI Point-to-Point Tunnel

- No Change

6.4. Lab 2-3: Implement DMVPN

- No Change

6.5. Lab 3-1: Implement Site-to-Site Secure Connectivity using Cisco IOS Flex VPN

- No Change

6.6. Lab 3-2: Implement Hub-to-Spoke Secure Connectivity using Cisco IOS Flex VPN

- Task1 : Step2: Internet Router is already synchronized with NIST Internet Time Server (time.nist.gov). It is not required to configure NTP as Cisco NTP server (64.103.34.15). Also ensure all other Routers (HQ-ISR, Branch ISR and Partner ISR) should be synchronized via NTP to the Internet-RTR .

6.7. Lab 3-3: Implement Spoke-to-Spoke Secure Connectivity using Cisco IOS Flex VPN

- No Change

6.8. Lab 4-1: Implement ASA Basic Clientless SSL VPN

- No Change

6.9. Lab 4-2: Configure Application Access for Cisco ASA Clientless SSL VPN

- No Change

6.10. Lab 4-3: Implement Local and External AAA for Clientless SSL VPNs

- Task1 : Step1: A) www.secure-x.public will not be accessible due to the default behavior of ASA that it will not permit inside resources using public dns through the outside interface. Instead of using public dns, use internal name of the sever dmz.secure-x.local here.
- Task3 : Step2: A) : Instead of using public dns www.secure-x.public, use internal name of the sever dmz.secure-x.local

6.11. Lab 5-1: Implement ASA Basic AnyConnect SSL VPN

- No Change

6.12. Lab 5-2: Configure Advanced Authentication for Cisco AnyConnect SSL VPN

- No Change

6.13. Lab 5-3: Implement AnyConnect IPSec/IKEv2

- No Change

6.14. Lab 6-1: Implement Host Scan and DAP

- No Change

7. Remote Lab Support

- Please note that our primary form of support is through email. Our email id is remotelabsupport@globalknowledge.ae

- In order to have an interactive communication with the instructors, we are also available on Skype and our Skype name is gkrlsmea. In case you cannot find us on Skype, please send an email on remotelabsupport@globalknowledge.ae, we will login in Skype at the earliest for you.