SENSS

Implementing Cisco Edge Network Security Solutions (SENSS 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 Edge Network Security Solutions (SENSS 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

SENSS v1.0 is a new course

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

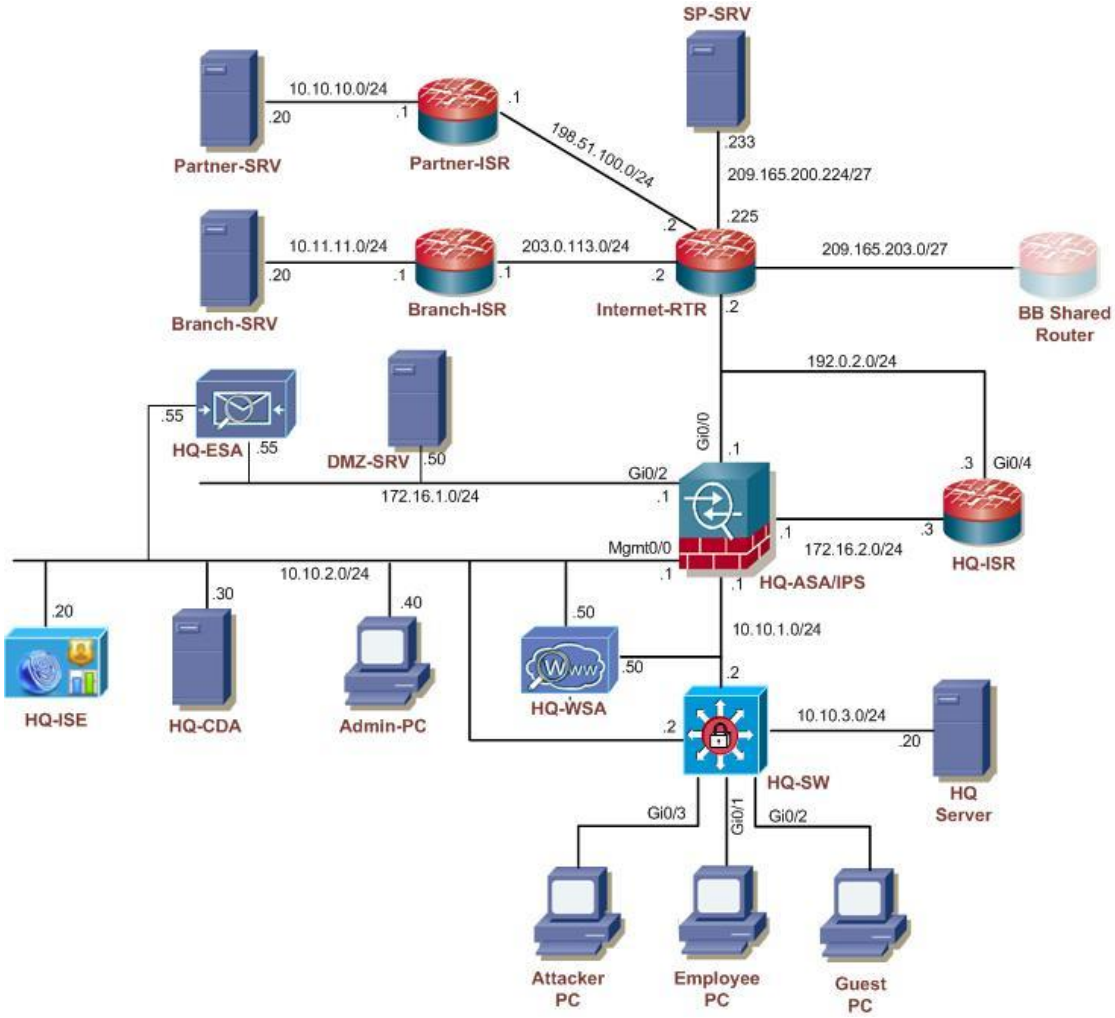
For Server/Client PC's

- 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 Edge Network Security Solutions (SENSS 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
- Branch-ISR
- Partner-ISR
- HQ-SW
- Internet-RTR
- Employee PC
- Guest PC
- Attacker PC
- Admin PC
- HQ Server
- Partner Server
- SP Server

- DMZ Server
- HQ-CDA
- HQ-ISE
- Branch Server
- HQ-ESA
- HQ-WSA

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
Employee PC	student	Ci5coAdmin
Guest PC	student	Ci5coAdmin
Attacker PC	root	Ci5coAdmin
Admin PC	student	Ci5coAdmin
HQ Server	administrator	Ci5coAdmin
Partner Server	administrator	Ci5coAdmin
SP Server	administrator	Ci5coAdmin
DMZ Server	root	Ci5coAdmin
HQ-CDA	admin	Ci5coAdmin
HQ-ISE	admin	Ci5coAdmin
Branch Server	administrator	Ci5coAdmin
HQ-ESA	admin	Ci5coAdmin
HQ-WSA	admin	Ci5coAdmin

6.2. Lab 2-1: Configure Control and Management Plane Security Controls

- Task1 : Step22: In the Lab Answer Keys there is an error in the match subcommand of Class map. ''name'' is missing in the ''match access-group name SNMP_MGMT''

- Task2 : Step15: Select the ***inside*** interface while adding the SNMPv3 host.
- Task2 : Step17: The SNMP entity address should be the IP address of the HQ-ASA inside interface (10.10.1.1).
- Task3 : Step10: The username/password for ISE web login is admin/Ci5coAdmin. The password is erroneously mentioned in the Lab Guide.

6.3. Lab 2-2: Configure Traffic Telemetry Methods

- Task1 : Step16: It takes around 10-15 minutes to show the interface instance in Scrutinizer.

6.4. Lab 2-3: Configure Layer 2 Data Plane Security Controls

- Task1 : Step11: The Employee-PC administrator username/ password is administrator/Ci5coAdmin
- Task2 : Step6: Telnet needs to be enabled on HQ-ISR router for testing the features in this lab module

6.5. Lab 2-4: Configure Layer 3 Data Plane Security Controls

- Task1 Step1: If the Attacker-PC is not getting IP address from DHCP, try restarting the network service on Attacker PC using the command **"/etc/init.d/networking restart"**

6.6. Lab 3-1: Configure Cisco ASA NAT

- No Change

6.7. Lab 3-2: Configure Cisco IOS Software NAT

- Task2 : Step6: Navigate to http://sp-srv.sp-public. Wrong screen shot is shown in the Lab Guide

6.8. Lab 4-1: Configure Basic Cisco ASA Access Policies

- No Change

6.9. Lab 4-2: Configure Advanced Cisco ASA Access Policies

- No Change

6.10. Lab 4-3: Configure Cisco ASA Botnet Traffic Filter

- Task1 : Step9: The Malware site mentioned in the Lab Guide http://bot-sparta.no-ip.org is not available anymore. Alternatively the delegates can try accessing the other Malware sites.

  For eg: *http://englischtraining.com;*

  http://lightpo.ru; http://creation-societe.biz

6.11. Lab 4-4: Configure Cisco ASA Identity Firewall

- Task1 : Step4: The password for adding AD server is *Ci5coAdmin*. It is erroneously mentioned as Cis5oAdmin in the Lab Guide
- Task1 : Step12: The below step is required to carry out on ASA to show the registered devices in CDA.

  ASDM: *Firewall ->Identity Options* -> Under *Active Directory Agent* -> Select *CDA* as the Agent Group, then click apply to send the configuration to ASA.

6.12. Lab 5-1: Configure Basic Cisco IOS Zone-Based Policy Firewall Access Policies

- No Change

6.13. Lab 5-2: Configure Advanced Cisco IOS Zone-Based Policy Firewall Access Policies

- 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.