SASAA

# Implementing Advanced Cisco ASA Security (SASAA v 2.1)

## 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 Advanced Cisco ASA Security (SASAA v2.1).

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 updated release of Implementing Advanced Cisco ASA Security (SASAA v2.0)

# 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.

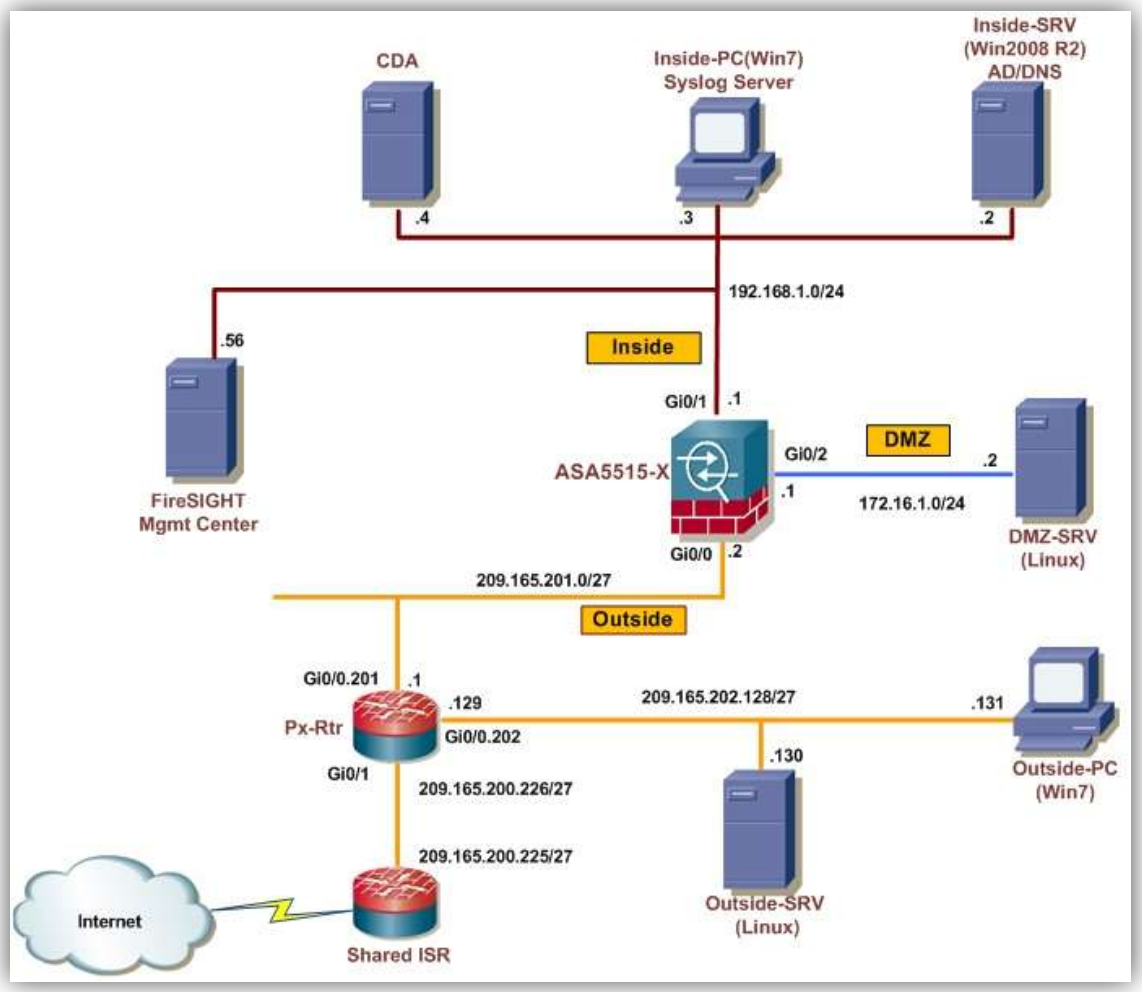
# 5. Remote Lab Topology

The network topology diagram for Implementing Advanced Cisco ASA Security (SASAA v2.0) remote lab is as per Cisco Topology mentioned in the lab guide.

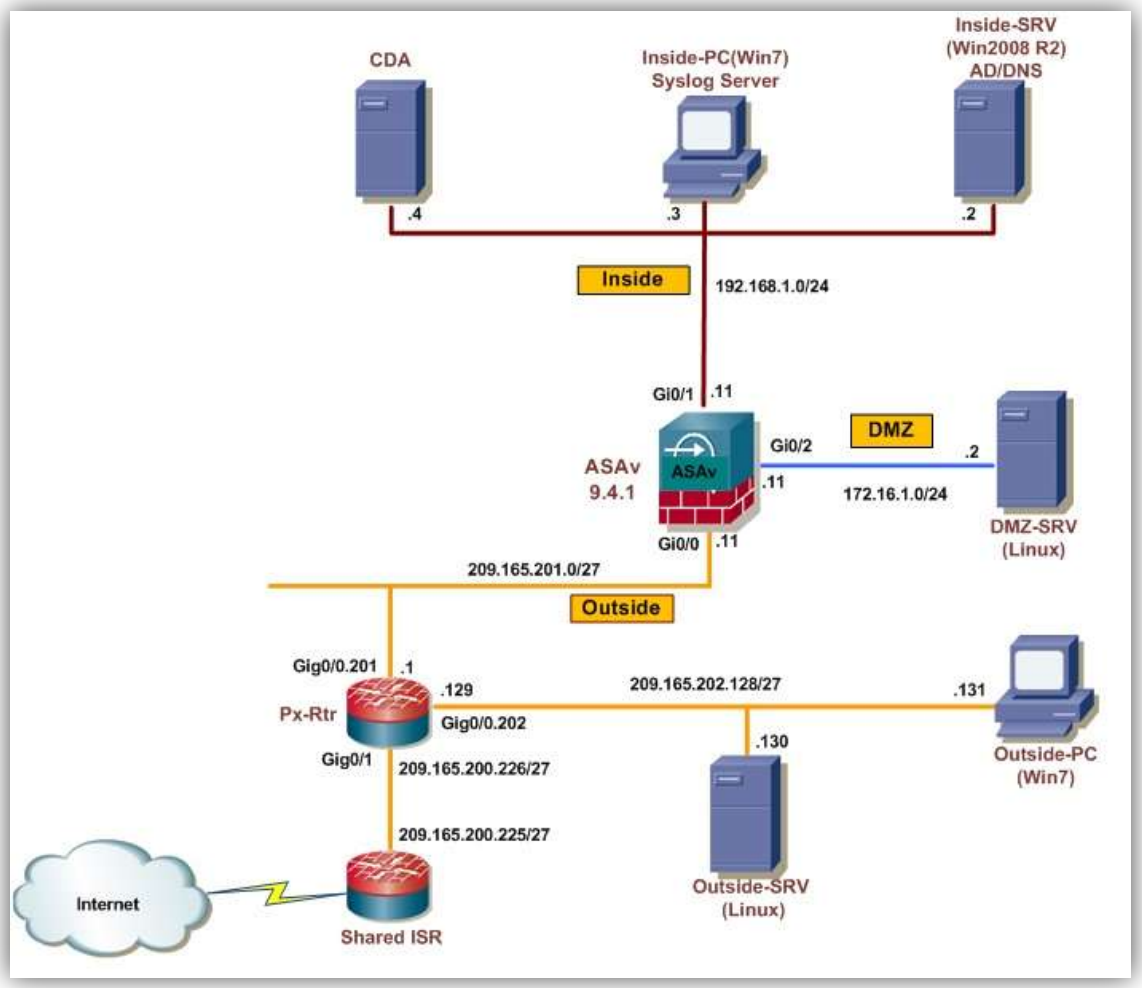
There are three Topologies in this lab and those are

- Base Topology
- ASAv Topology ( Non Clustering lab Virtual ASA Topology)
- Clustering Topology

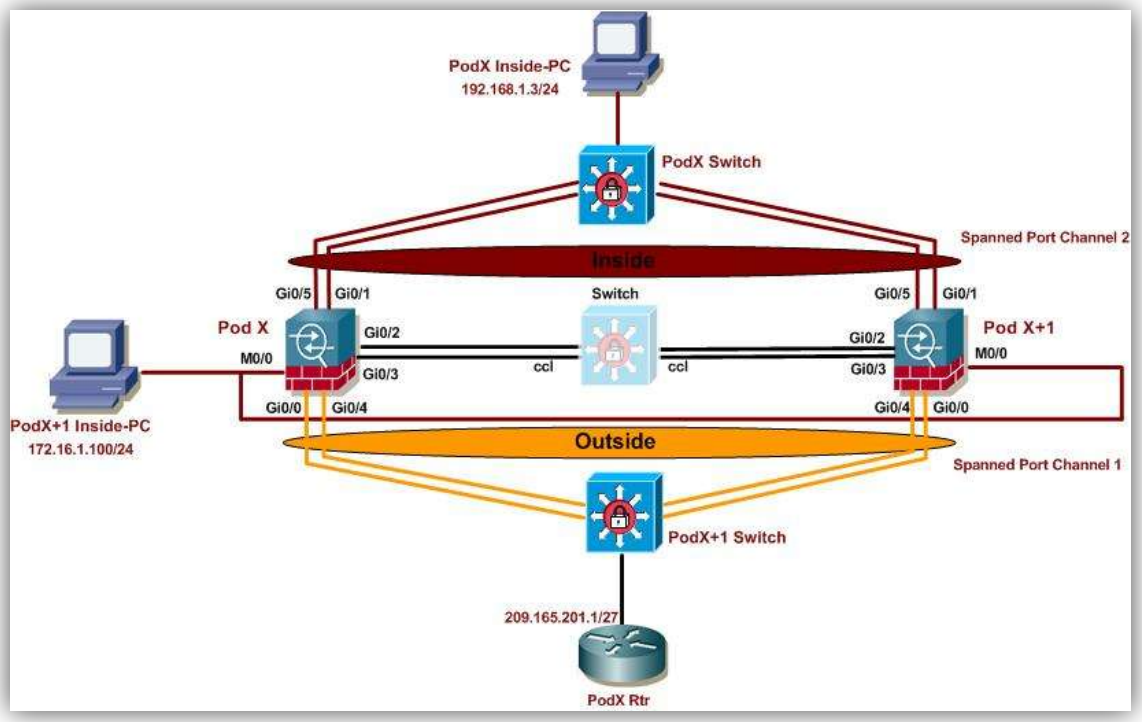
**Base Topology**



## Virtual ASA (ASAv) Topology (For Lab 1)




## Clustering Topology (For Lab 9)



Each Pod is provided with the following equipments and VMs:

- ASA 5515-X
- Px-Rtr
- Shared-ISR
- Px-Sw
- Inside PC
- Inside-Server
- DMZ-Server
- Outside-PC
- Outside-Server
- ASAv
- CDA
- Firepower Management Center

# 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

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

| Equipments/Servers/PCs | Username | Password |
|---|---|---|
| HQ-ASA | - | **enable:** C!sco!23 |
| Inside PC | Inside-pc\student | Ci5coAdmin |
| DMZ Server | root | Ci5coAdmin |
| Inside Server | administrator | Cisco123 |
| Outside PC | student | Ci5coAdmin |
| Outside Server | root | Ci5coAdmin |
| Inside PC (secure-x ) | It1 | cisco |
| Inside PC (secure-x ) | sales1 | cisco |
| Inside PC (secure-x ) | marketing1 | cisco |
| Inside PC (secure-x ) | engineer1 | cisco |
| Inside PC (secure-x ) | contractor1 | cisco |
| Inside PC (secure-x ) | employee1 | cisco |
| Inside PC (secure-x ) | student | cisco |

Note: All Pods are using same IP addressing scheme

## 6.2. Lab 1: Remote Lab Environment Access

- The lab devices and VMs are accessible by clicking the Device/VM icons on the Topology

## 6.3. Lab 2: Setup and Test the ASAv

- Virtual ASA can be accessed by left clicking the ASAv icon (ASAv Topology). No enable password is set on ASAv.
- **Task 1 Step 1:** There is an error in the running config shown for the Outside interface. The IP address should be 209.165.201.11. It is erroneously shown as 207.165.201.11
- **Task 1 Step 6:** The ASAv is not licensed. It is ok to perform the lab without the license.

- **Task 1 Step 8:** The ASAv software and ASDM versions are 9.4(1) and 7.4(1). Also, due to the way the VMs are organized and presented in the User Interface, you do not have access to view the Virtual Machine Properties to see the MAC Address of the VM Network Adapter.

## 6.4. Lab 3: Implement New Features in ASA 9.3 and 9.4

- **Task 1 Step 1:** The Rest API image **asa-restapi-111-lfbff-k8.SPA** is present on Disk0:/ of the ASAv. Please note that the filename extension of the Rest API image "SPA" is in Uppercase.
- **Task 1 Step 4:** The URL given for accessing the REST API online documentation is incorrectly mentioned in the LG as https://192.168.1.11/doc whereas it should be https://192.168.1.11/doc/

## 6.5. Lab 4: Configure the Cisco CDA

- Make sure that default gateway of Inside PC is changed to 192.168.1.1 from 192.168.1.11 as required in the previous lab module.
- **Task1 Step14:** Base Server where the Inside server VM hosted is synchronized to ntp server time.nist.gov and Inside server time is configured to sync with the base server . No need to use w32tm/resync command as the Inside server time is already sync with time.nist.gov . Also note Inside server is set to the UTC time zone.

## 6.6. Lab 5: Configure ASA IDFW

- No Change

## 6.7. Lab 6: Cisco ASA Firepower Services Module Installation

- **Task 1 Step 5**: ASA SFR CLI, use the command

```
system install FTP://192.168.1.3/asasfr-sys-6.0.0-1005.pkg
```

## 6.8. Lab 7: Cisco Firepower Management Center Configuration

- **Task 7 Step 8:** In the search box type in 209.165.202.130 instead of 209.165.202.131
- **Task 5 Step 7:** Windows host is detected as Printer

## 6.9. Lab 8: Cisco ASA CWS

- **Task 1 Step 1:** To disable service policy that redirects traffic from ASA to ASA Firepower

  ```
  no service-policy asasfr_policy interface inside
  no service-policy asasfr_policy interface dmz
  ```

- **Task 1 Step 1:** Please use the Primary & Backup proxy as below

  **Primary:** Access13.cws.sco.cisco.com port 8080

  **Backup:** proxy1363.scansafe.net port 8080

- **Task 1 Step 2:** Please use the license Key as mentioned below:

  AA965633510873872C3BE36318EE4720

- **Task 1 Step 8:** Please refer to the ***Access details mail*** for Cisco ScanCenter login credentials. This user account has full read only access in the Cisco ScanCenter.

- Scansafe account will be locked out and deactivated if 10 unsuccessful login attempts are made. Kindly ensure to use the right username and password mentioned in the *Access details mail* for the scansafe login. In case you use the right username and password but are still unable to login, it might be due to an account lock-out scenario, in this case, please contact Remote Lab Support Team to re-activate the account

## 6.10. Lab 9: Cisco ASA Cluster Configuration

**Note: Before starting Lab 9, please contact the Remote Lab Support team, such that prior physical changes can be made to the Pod to carry out Lab 9**

- The Cluster Topology is used for carrying out this task.

# 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.