



## Lab 5.2.1 Install and Configure CSACS 3.3 for Windows

### Objective

In this lab, the students will complete the following tasks:

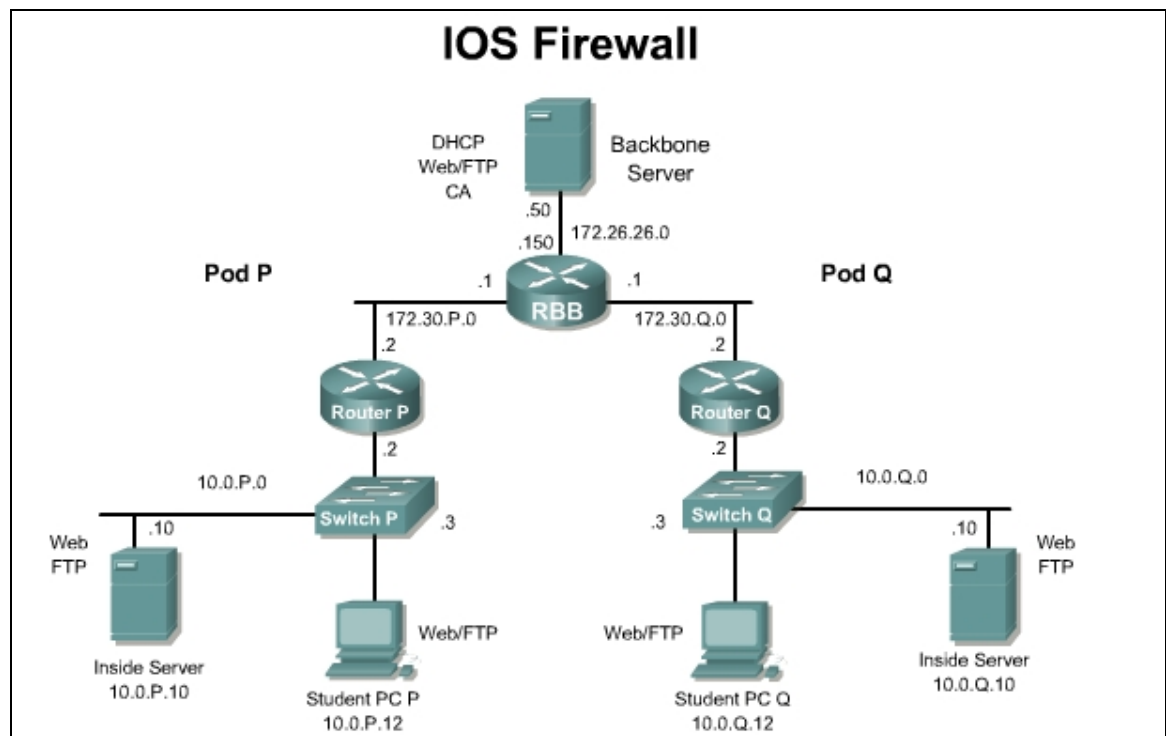
- Install Cisco Secure Access Control Server (CSACS) for Windows 2000
- Take a tour of CSACS for Windows

### Scenario

Cisco Secure Access Control Server for Windows 2000/NT Servers (Cisco Secure ACS) network security software helps administrators authenticate users by controlling dial-in access to a network access server (NAS) device, an access server, Cisco PIX Security Appliance, switch, wireless access point, or router. Cisco Secure ACS operates as a Windows NT or Windows 2000 service and controls the authentication, authorization, and accounting (AAA) of users accessing networks.

### Topology

This figure illustrates the lab network environment.



## Preparation

Begin with the standard lab topology and verify the starting configuration on the pod router. Test the connectivity between the pod routers. Access the perimeter router console port using the terminal emulator on the student PC. If desired, save the router configuration to a text file for later analysis. Refer back to the *Student Lab Orientation* if more help is needed.

## Tools and resources

In order to complete the lab, the following is required:

- Standard IOS Firewall lab topology
- Console cable
- HyperTerminal
- Cisco Secure Access Control Server (CSACS) version 3.3 or later for Windows 2000

## Additional materials

The following websites provide additional information on CSACS:

- [http://www.cisco.com/en/US/products/sw/secursw/ps2086/products\\_ganda\\_item09186a0080094bac.shtml](http://www.cisco.com/en/US/products/sw/secursw/ps2086/products_ganda_item09186a0080094bac.shtml)
- [http://www.cisco.com/en/US/products/sw/secursw/ps2086/products\\_white\\_paper09186a0080115464.shtml](http://www.cisco.com/en/US/products/sw/secursw/ps2086/products_white_paper09186a0080115464.shtml)
- [http://www.cisco.com/en/US/products/sw/secursw/ps2086/prod\\_configuration\\_examples\\_list.html](http://www.cisco.com/en/US/products/sw/secursw/ps2086/prod_configuration_examples_list.html)

## Step 1 Install CSACS 3.3 for Windows 2000

Complete the following steps to install CSACS on the Windows 2000 server. This procedure assumes that the Windows 2000 server is operational.

- a. Log in to Windows 2000 server using the administrator account. The instructor will provide the correct username and password combination for the administrator account.
- b. Open the CSACS folder on the PC. Begin the CSACS installation by double-clicking the **Setup.exe** file. The CSACS for Windows NT/2000 installation wizard starts. Ignore any warning messages concerning memory requirements.
- c. Click **Accept** to acknowledge the terms of the CAACS license agreement. Click **Next** to close the 'Welcome' window. Check all items listed in the 'Before You Begin' window and click **Next**. Click **Next** to accept the default settings in the 'Choose Destination Location' window.
- d. Complete the following substeps within the Authentication Database Configuration window:
  - i. Check the **Also Check the Windows User Database** option.
  - ii. Check the **Yes refer to "Grant dialin permission to user" setting** check box.
  - iii. Click **Next**.
- e. Check all of the check boxes within the Advanced Options window and click **Next**. It is important to check all of the check boxes as this will determine the ACS options that will be available for configuration later.
- f. Accept the default settings within the Active Service Monitoring window by clicking **Next**.
- g. Accept default settings within the CiscoSecure ACS Service Initiation window by clicking **Next**. Setup then starts the CiscoSecure service.
- h. Click **Finish**. A web browser will start with the Cisco Secure ACS v3.3 homepage.
- i. Click on the **Interface Configuration** button, Click the **Advanced Options** text link.

Check the **Network Device Groups** box and click the **Submit** button.

- j. Click on the **Network Configuration** button.
- k. Click on the **(Not Assigned)** text link in the Network Device Groups window.
- l. Click on the top **Add Entry** button in the AAA Clients section. Complete the following sub steps within the Add AAA Server window:
  - i. Select **TACACS+ (Cisco IOS)** from the Authenticate Users Using scroll box.
  - ii. Enter the name of the pod router to be used as the NAS in the AAA Client Hostname box. For example, Router1, Router2, and so on.
  - iii. Enter the IP address (10.0.P.2) of the pod router inside interface in the Access Server IP Address box.
  - iv. Enter **secretkey** (one word and all lowercase) in the TACACS+ or RADIUS key box.
  - v. Finish adding the pod router as the AAA client by clicking the **Submit+Restart** button.
- m. Click on the Network Configuration button.
- n. Click on the (Not Assigned) text link under Network device Group.
- o. Click the Add Entry button in the AAA Servers section. Complete the following sub steps within the Cisco Secure ACS Add AAA Server window:
  - i. Enter a name for the student PC, for example **studentP**, in the AAA Server Name box (where P = pod number).
  - ii. Enter the IP Address of the student PC (**10.0.P.12**) in the AAA Server IP Address box (where P = pod number).
  - iii. Enter **secretkey** (one word and all lowercase) in the Key field.
  - iv. Make sure that **Cisco Secure ACS** is selected for the AAA Server Type.
  - v. Make sure that **inbound/outbound** is selected for Traffic Type.
- p. Finish adding the PC as the AAA Server by clicking the **Submit+Restart** button.
- q. Close the Internet Explorer window containing the Cisco Secure ACS main window.
- r. Close any open windows.
- s. Using Windows Task Manager (**Ctrl+Alt+Delete > Task Manager**) check to see if the following services are now running on the Windows 2000 server PC:
  - CSAdmin.exe
  - CSAuth.exe
  - CSDBSync.exe
  - CSLog.exe
  - CSMon.exe
  - CSRadius.exe
  - CSTacacs.exe

If these services are not listed as running, restart the Windows 2000 server PC and repeat this step.

If all of the tasks are running, CSACS 3.3 for Windows 2000 has been successfully installed.

## Step 2 Take a Grand Tour of CSACS for Windows

Complete the following steps to become familiar with the CSACS for Windows administration interface, and to change some global settings.

- a. Start the ACS configuration manager by double-clicking the **ACS Admin** desktop icon.
- b. Select the **Cisco Systems** icon at the top of the left frame.
  1. What is displayed in the right frame? What is the release version?  

---
- c. Examine the user setup functions by completing the following substeps:
  - i. Select **User Setup** in the left frame.
  - ii. Enter **aaauser** in the User text box. Then click on the **Add/Edit** button.
  - iii. Enter the password **aaapass** in the **Password** and **Confirm Password** fields of the **User Setup** section.
  - iv. Press the **Submit** button.
  - v. Select the **List All Users** button.
    1. How many users are configured?  

---
- d. Examine the group setup functions by completing the following substeps:
  - i. Select **Group Setup** in the left frame.
    1. What group is shown in the Group window?  

---
  - ii. Select the **Users in Group** button in the center frame.
    1. How many users are in the group?  

---
- e. Select **Network Configuration** in the left frame:
  1. How many AAA Clients are configured?  

---
- f. Examine the system configuration functions by completing the following substeps:
  - i. Select **System Configuration** in the left frame.
  - ii. Select the **Service Control** text link in the System Configuration window and answer the following question.
    1. What is the status of the Cisco Secure service, level of detail for logging, and frequency of the new file generation?  

---
  - iii. Select **Cancel** to return to the select list.
  - iv. Select the **Logging** text link in the System Configuration window and answer the following question.
    1. What log targets are enabled?  

---
  - v. Select **Cancel** to return to the select list.

- vi. In the System Configuration window, select **Local Password Management** and then review the Password Validation Options, answer the following, and then select Cancel to return to the select list.

1. What is the purpose of the password validation options?

---

- vii. Select the **Cisco Secure Database Replication** text link in the System Configuration window, answer the following, and then select **Cancel** to return to the select list.  
If this option does not appear, click Interface Configuration > Advanced Options and then check the CiscoSecure Database Replication checkbox and the Distributed System Settings checkbox.

1. What is the purpose of **Cisco Secure** Replication Setup?

---

- viii. Select the **ACS Backup** text link in the System Configuration window, answer the following, and then select **Cancel** to return to the select list.

1. Where can the ACS user and group databases be backed up?

---

- ix. Select the **ACS Restore** text link in the System Configuration window, answer the following, and then select **Cancel** to return to the select list.

1. What components can be backed up and restored?

---

- x. Select the **ACS Service Management** text link in the System Configuration window, answer the following, and then select **Cancel** to return to the select list.

1. How can a system administrator be notified of events that are logged?

---

- g. Examine the interface configuration functions by completing the following substeps:

- i. Select **Interface Configuration** in the left frame.
- ii. Select the **User Data Configuration** text link in the Interface Configuration window, answer the following, and then select **Cancel** to return to the select list.

1. How are user-defined fields useful?

---

- iii. Select the **Advanced Option** text link in the Interface Configuration window, perform the following task, and answer the following question.

- iv. Ensure that all of the options are checked.

1. What is the purpose of selecting advanced options?

---

---

---

- v. Select **Submit** to return to the select list.

- vi. Select the **TACACS+ (Cisco IOS)** text link in the Interface Configuration window, perform the following tasks, and answer the following questions.

If this option is not present, a AAA client needs to be added. This is done on the Network Configuration page. Click the **Add Entry** Button and enter the AAA Client Hostname, AAA

Client IP Address, and the Key **secretkey**. Click the **Submit+Restart** button to finish adding the client.

- vii. In the TACACS+ Services window, ensure PPP IP, PPP LCP, PPP Multilink, and Shell (exec) are selected.. These services will be available when clicking the Edit Settings button on the Group Setup page.
- viii. In the Advanced Configuration Options window, ensure that all four of the boxes are checked. When the Advanced TACACS+ Features option is checked, TACACS+ options can be enabled for individual users on the User Setup page.
- ix. Select **Submit** to return to the select list.

- 1. Where are the TACACS+ services and advanced configuration objects applied in this window?

---

---

- h. Click on the **Administration Control** button in the left frame.

- 1. What administrator accounts are configured?

---

- 2. What is the purpose of administrator control?

---

---

- i. Examine the external user database functions by completing the following substeps:

- i. Select **External User Databases** in the left frame.
  - ii. Select the **Unknown User Policy** text link in the External User Databases window and answer the following questions

- 1. What two options are available if a user is not found in the Cisco Secure database?

---

---

- 2. Which one is the default?

---

- 3. What external databases can be checked for the unknown user?

---

---

- j. Select **Cancel** to return to the select list.

- i. Select the **Database Group Mappings** text link in the External User Databases window. Select **Cancel** to return back to the select list.

- ii. Select the **Database Configuration** text link in the External User Databases window, answer the following, and then select **Cancel** to return to the select list.

- 1. What can be configured in the External User Database Configuration window?

---

- k. Examine the reports and activity functions by completing the following substeps:
    - i. Select Reports and Activity in the left frame.
    - ii. Select the **Administration Audit** text link in the Reports and Activity window, and answer the following question.
      - 1. What appears in the Administration Audit.csv file?
- 
- l. Select **Online Documentation** in the left frame.
    - i. Take a moment to browse the new features, software requirements, and troubleshooting sections of the online documentation.