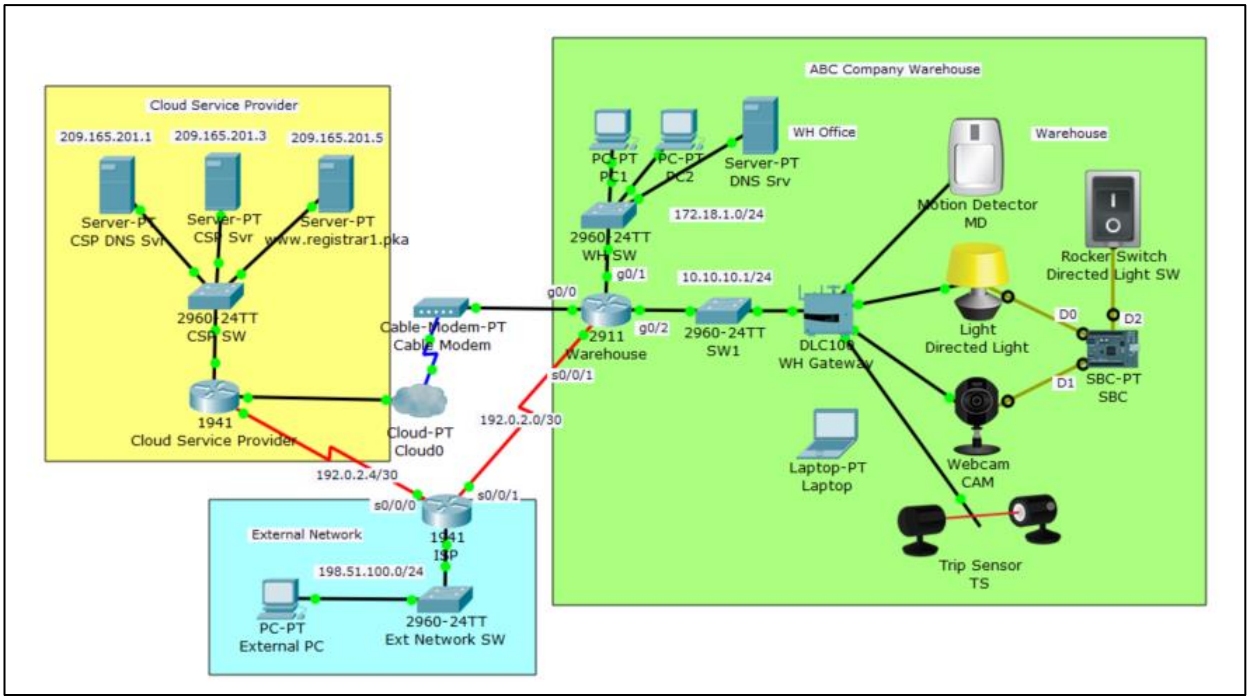
Packet Tracer – Securing Cloud Services in the IoT

Topology



Objectives

Deploy Basic Security Measures for IoT Systems with Cloud Services.

Background / Scenario

ABC Compnay is developing IoT systems in their main warehouse. The objective is to deploy some physical security devices around the warehouse so that, when the warehouse is closed, these devices will monitor the doors and windows. When an intruder is detected, the lights are turned on and web cameras will start recording.

The security is an important aspect in addition to the function of IoT systems with cloud services.

In this Packet Tracer activity you will complete configuration tasks:

- Register four IoT devices in the ABC Company warehouse: a motion detector, a directed light, a webcam, and a trip sensor. Add conditions in the registration server so that when either the motioin detector or the trip sensor is activated, the directed light and webcam will turn on.
- Configure the warehouse router to require strong authentication for console and remote access.
- Configure ACLs to restrict network traffic between the registration server and the ABC Company warehouse.
- Configure the web server in the cloud service provider network to ensure that data communication is secure.

Required Resources

- Packet Tracer 7.1 or newer.

Step 1 – Register IoT Devices to the Registration Server

- Add a user to the registration server www.registrar1.pka with a strong password:
  1. Use a PC in the WH office. Under **Desktop** tab, open **Web Browser**, type www.registrar1.pka and select **Go**. The Registration Server Login window displays.
  2. Click **Sign up now** and create your own account with a strong password (ensure a password is at least 8 characters long with combination of capital characters, lower case characters, and numbers).
  3. What is your username and password? ______________________________
- Register IoT devices to the registration server:
  1. Within the warehouse, click on **Motion Detector**. Under the **Config** tab, select **Remote Server** in the IoT Server section. Enter www.registrar1.pka as the server address and click **Connect**. Enter the username/password you just created.
  2. Does Motion Detector appear in the registration server? ________________
  3. Repeat steps 1 and 2 to register the Light, Webcam, and Trip Sensor.

Step 2 – Add Conditions in the Registration Server

You will add conditions in the registration server so that when either the Motion Detector or Trip Sensor is activated, the directed light and the webcam are turned on.

- Log in to the registration server using the username/password you created.

  Do you see four IoT devices listed? ______________________________
- Click **Conditions** and add following three conditions:
  1. Name it LightsOn1, if MD status On is true, then set Directed Light status to On AND set CAM status On to true.
  2. Name it LightsOn2, if TS status On is true, then set Directed Light status to On AND set CAM status On to true.
  3. Name it LightsOff, if both MD status On is false AND TS status On is false, then set Directed Light status to Off AND set CAM status On to false.
  4. Test the conditions.

     Hold the ALT key and move the mouse over Motion Detector. Are Directed Light and Webcam turned on?

     ____

     Move the mouse away and wait for a few seconds. Are Directed Light and Webcam turned off?

     ____

Step 3 – Configure Strong Authentication to Network Devices

- You will configure strong authentication for a wireless connection on the WH gateway device:

1. Within the warehouse, click on the **WH Gateway** device. Under the **Config** tab, **Wireless** option, set the SSID to ***WhGateway1***, set Authentication to **WPA2-PSK** with Pass Phrase as ***IoTWh001***. Leave Encryption Type as AES.
2. Click on the **Laptop**. Under the **Config** tab, **Wireless0** option, set the SSID to ***WhGateway1***, set Authentication to **WPA2-PSK** with Pass Phrase as ***IoTWh001***. Leave Encryption Type as AES.

   Does the laptop connect to WH Gateway successfully?

- On the warehouse router, configure a banner to display a warning message for unlawful access. Although a banner message is not a security measure by itself, it may function as a deterrence to intruders. Set an encrypted password to enter the Exec mode. Set up a local user account for the console line and remote access.

  1. Click the Warehouse 2911 router, then click the **CLI** tab and enter these commands:

     ```
     Warehouse> enable
     Warehouse# config terminal
     Warehouse(config)# banner login %Login with valid password%
     Warehouse(config)# banner motd %Authorized Access Only! Unauthorized access is
     subject to Federal Prosecution.%
     Warehouse(config)#
     ```

  2. Set a secure Exec mode password:

     ```
     Warehouse(config)# enable secret AbcWh001
     Warehouse(config)# exit
     ```

  3. Set a local username for the console line and VTY lines access:

     ```
     Warehouse# configure terminal
     Warehouse(config)# username WhAdmin secret AbcLine001
     Warehouse(config)# line console 0
     Warehouse(config-line)# login local
     Warehouse(config-line)# exit
     Warehouse(config)# line vty 0 4
     Warehouse(config-line)# login local
     Warehouse(config-line)# end
     Warehouse#
     ```

Step 4 – Configure Access Lists to Restrict Traffic between ABC Company IoT devices and the Cloud Service Provider Network

- On the warehouse router, configure and apply access list 10 to allow traffic from only the DNS server and the registration server to enter the ABC Company warehouse IoT devices network:

  ```
  Warehouse# configure terminal
  Warehouse(config)# access-list 10 permit host 172.18.1.5
  Warehouse(config)# access-list 10 permit host 209.165.201.5
  Warehouse(config)# interface g0/2
  Warehouse(config-if)# ip access-group 10 out
  Warehouse(config-if)# end
  Warehouse#
  ```

- On the Cloud Service Provider router, configure and apply an access list 110 to allow traffic from only the ABC Company warehouse IoT devices network to access the registration server:

  ```
  CSP# configure terminal
  ```

```
CSP(config)# access-list 110 permit ip host 209.165.200.226 host 209.165.201.5
CSP(config)# access-list 110 deny ip any host 209.165.201.5
CSP(config)# access-list 110 permit ip any any
CSP(config)# interface g0/0
CSP(config-if)# ip access-group 110 out
CSP(config-if)# end
CSP#
```

In the ACL 110, why is the warehouse router interface IP address selected as the source in the ACL 110?

____

____

Step 5 – Configure Secure Web Communication to the Web Server in the Cloud Service Provider Network

- The ABC Company uses the web server in the cloud service provider for part of its operation. Configure the web server in the cloud service provider network to be accessed only via HTTPS:
  1. Click **CSP Svr**, then click the **Services** tab.
  2. Click **HTTP** on the left pane. Make certain that HTTP is off and HTTPS is on.

Step 6 – Test

- From the laptop in the warehouse network, access the registration server. Trigger either the motion detector or trip sensor, and observe the action of the directed light and webcam
- From PC1 or PC2, open the web browser. Can it access the registration server? No.
- From PC1 or PC2, open the web browser. Can it access the web server 209.165.201.3 via HTTP?
- From PC1 or PC2, open the web browser. Can it access the web server 209.165.201.3 via HTTPS?

Reflection

What security measures are implemented?

____

____

____

What other security measures should be considered when deploying IoT solutions with cloud computing?

____

____

____