Packet Tracer - Server Firewalls and Router ACLs

Addressing Table

Device	Private IP Address	Public IP Address	Subnet Mask	Site
Web Server	N/A	209.165.201.10	255.255.255.0	Internet

Objectives

Part 1: Connect to the Web Server

Part 2: Prevent Unencrypted HTTP Sessions

Part 3: Access the Firewall on the Email Server

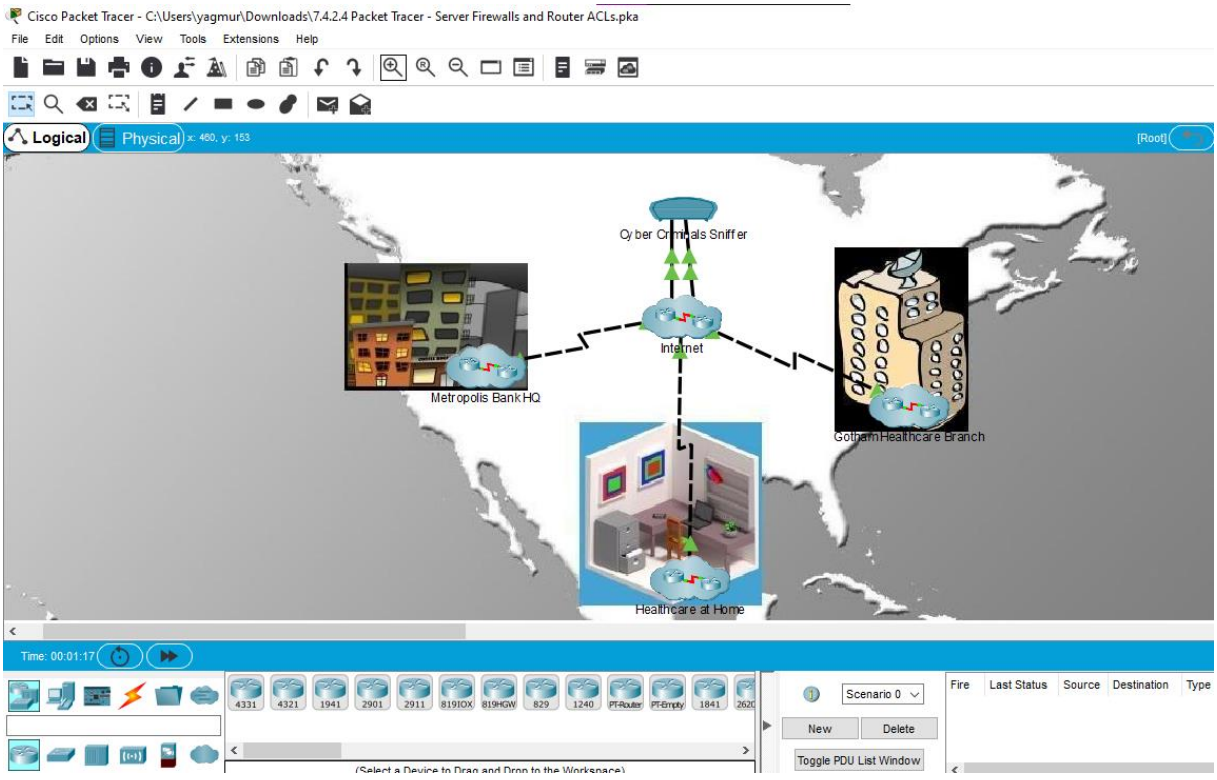
Background

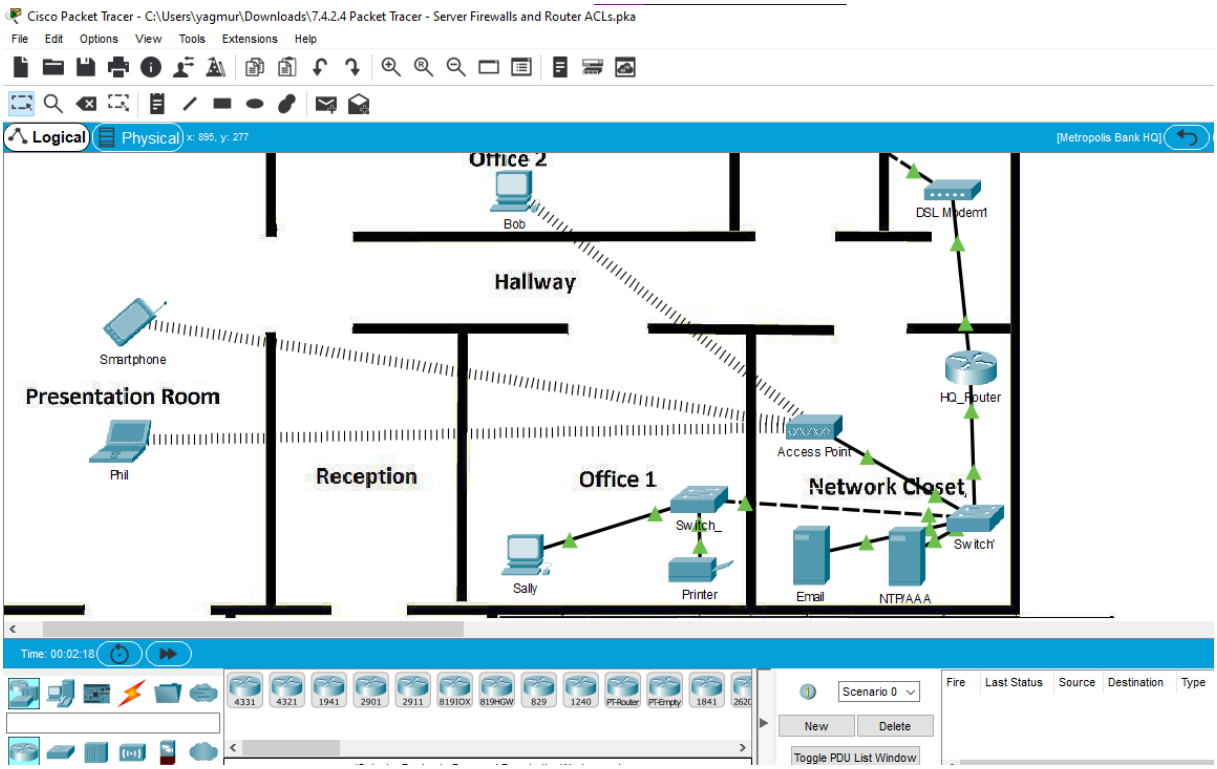
In this activity, you will access a user within the Metropolis site and connect using HTTP and HTTPS to a remote Web Server. The IP addressing, network configuration, and service configurations are already complete. You will use a client device in the Metropolis site to test connectivity to a remote Web Server and then secure the Metropolis site by preventing unencrypted web sessions from connecting to the outside world.

Part 1: Connect to the Web Server

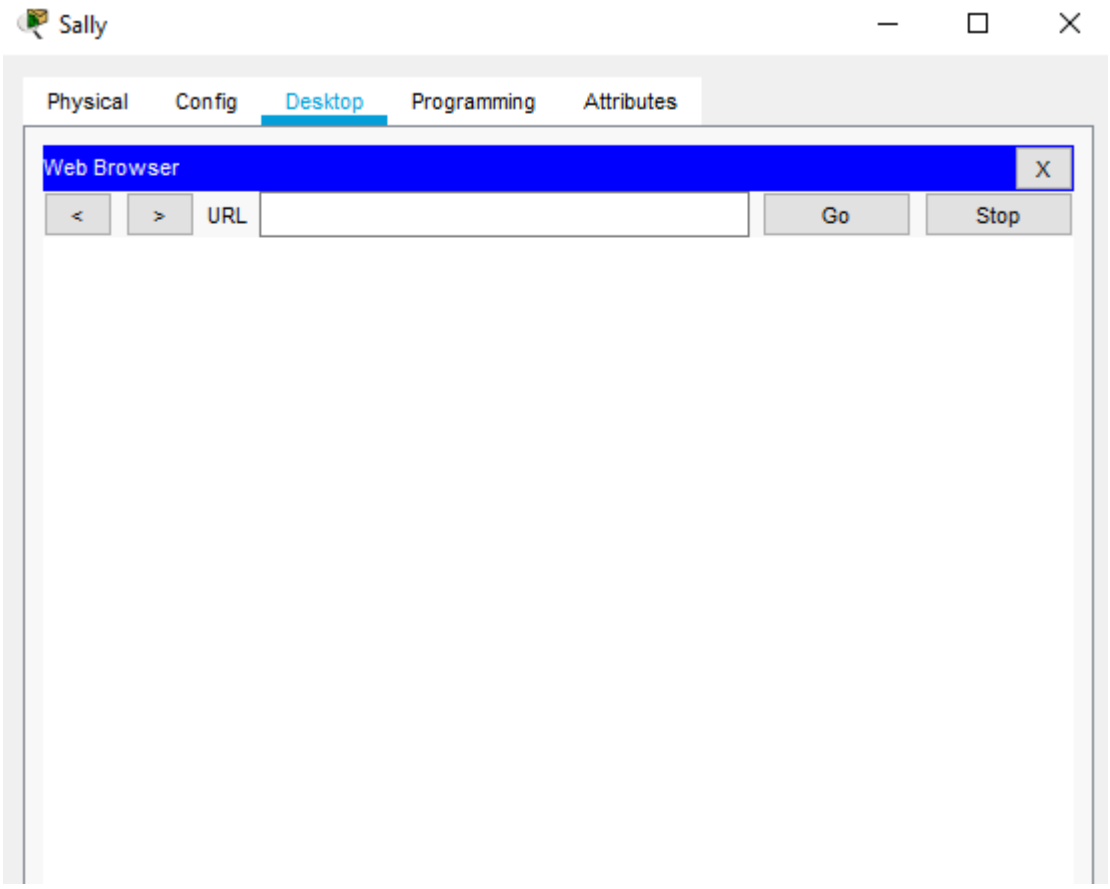
Step 1: Access the HQ Internet Web Server on Sally's PC using HTTP.

a. Click the **Metropolis Bank HQ** site and then click the PC **Sally**.





b. Click the **Desktop** tab and then click **Web Browser**.



c. Enter the URL of **http://www.cisco.corp** and click **Go**.

d. Click the link **Login Page**.

Why would a user be concerned when submitting information using this website?

The webpage is accepting user authentication information via insecure unencrypted HTTP.

Step 2: Access the HQ Internet Web Server on Sally's PC using HTTPS.

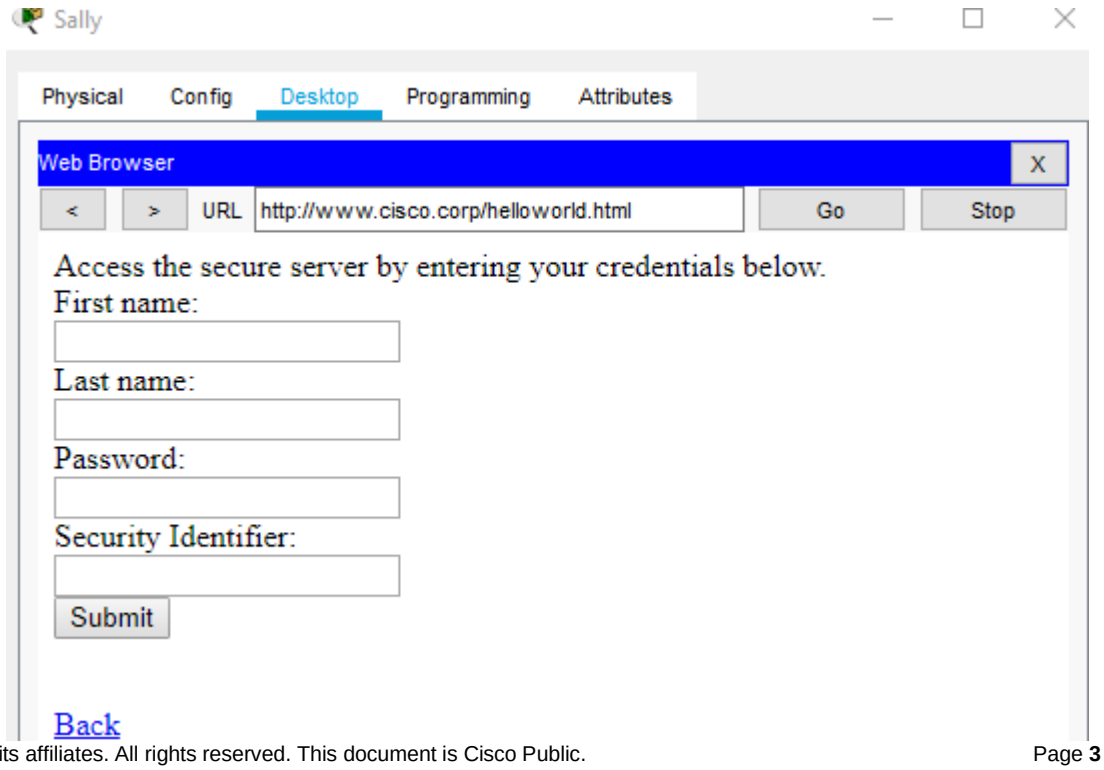
a. Access the **Web Browser** on Sally's computer.

b. Enter the URL of **https://www.cisco.corp** and click Go.

c. Click on the link **Login Page**.

Why would a user be less concerned when submitting information using this website?

The webpage is securing the user authentication information with SSL/TLS via encrypted HTTPS.



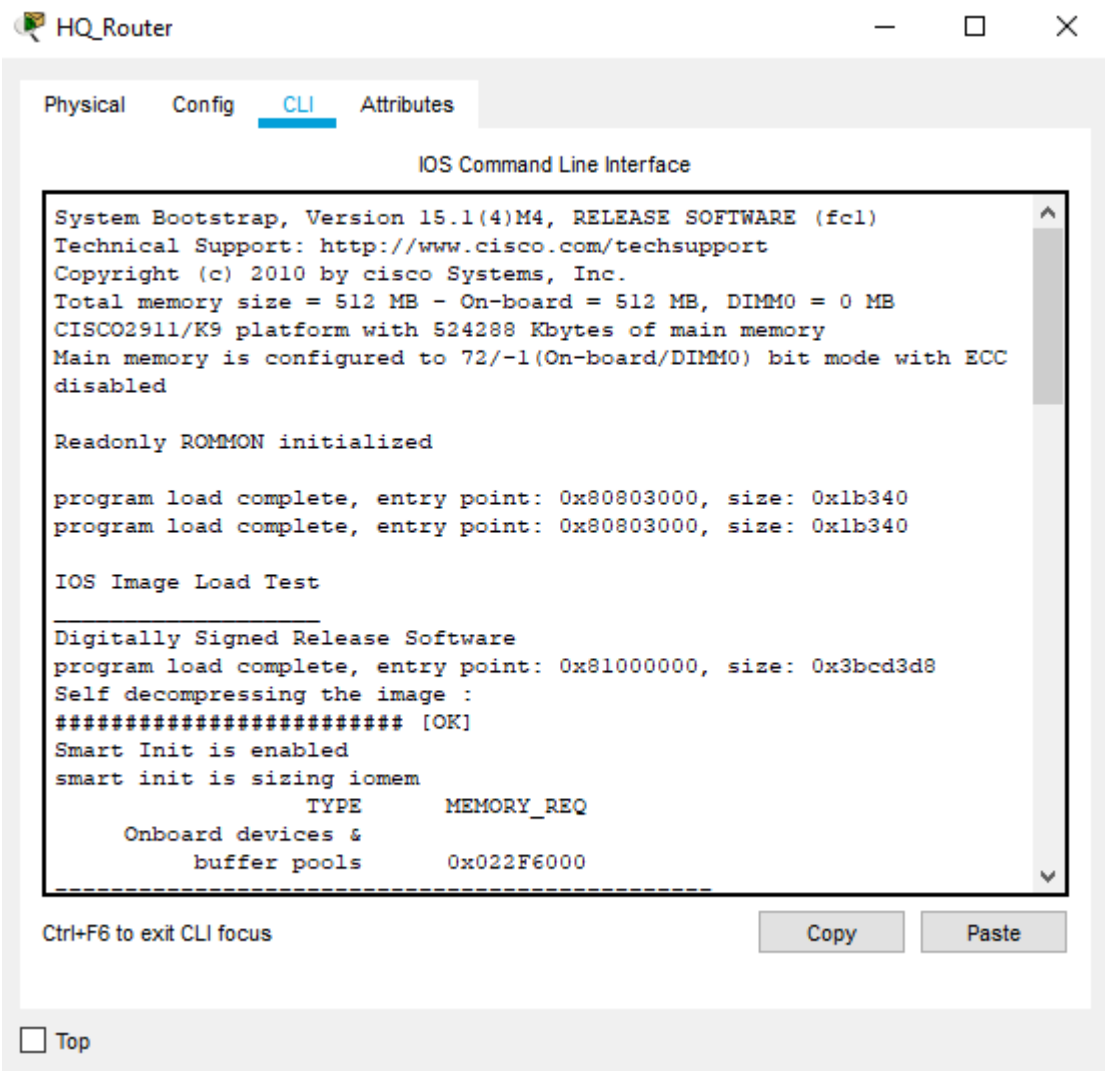
d. Close **Sally's** computer.

Part 2: Prevent Unencrypted HTTP Sessions

Step 1: Configure the HQ_Router.

a. Within the **Metropolis Bank HQ** site, click the **HQ_Router**.

b. Click the **CLI** tab and press **Enter**.



c. Use the password **cisco** to login to the router.

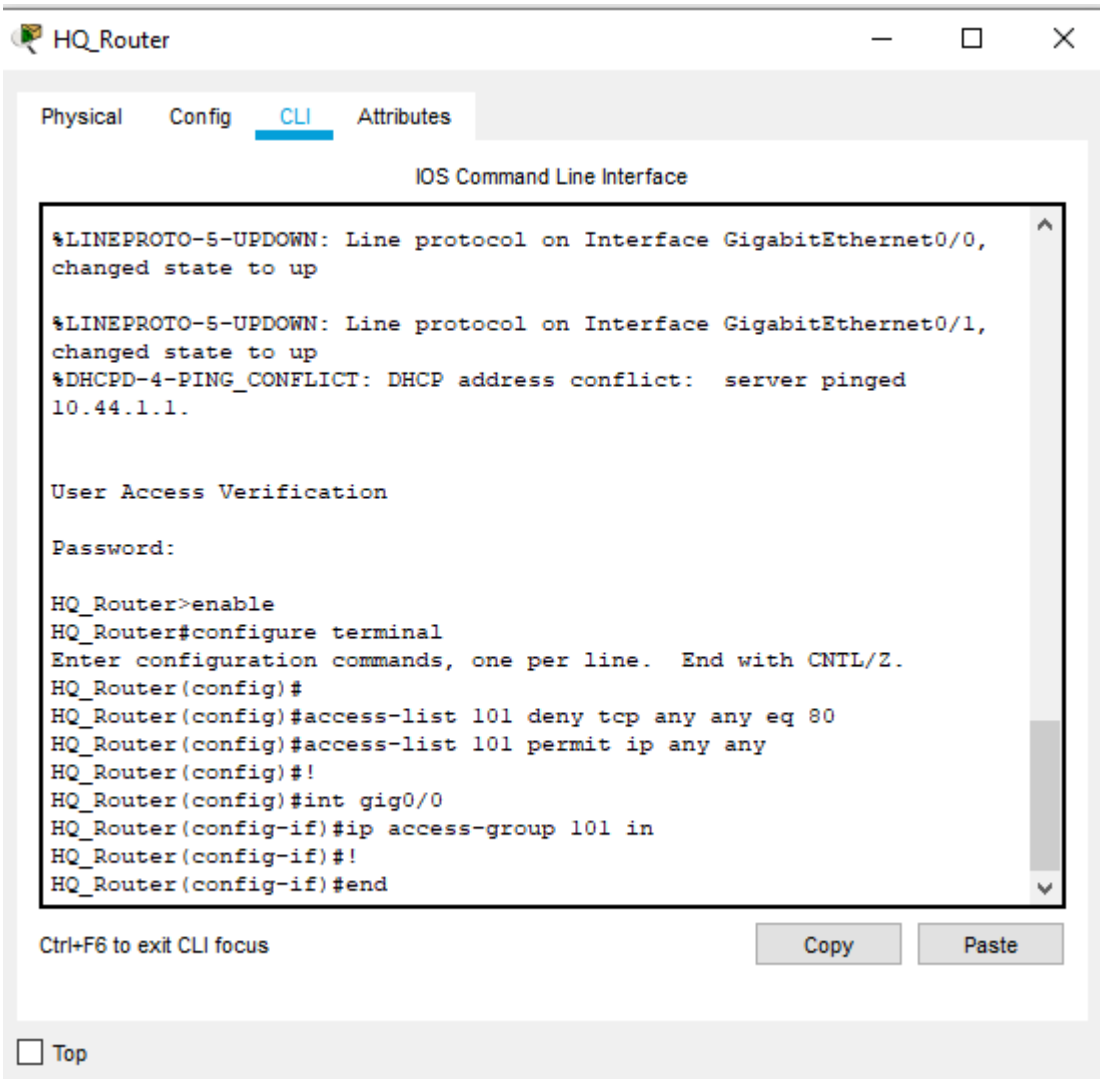
d. Use the **enable** command and then **configure terminal** command to access the global configuration mode.

In order to prevent unencrypted HTTP traffic from traveling through the HQ router, network administrators can create and deploy access control lists (ACLs).

The following commands are beyond this course but are used to demonstrate the ability to prevent unencrypted traffic from moving through the HQ_Router.

e. Within the global configuration mode **HQ_Router**(config)# copy the following access-list configuration below and paste it into the **HQ_Router**.

```
!
access-list 101 deny tcp any any eq 80
access-list 101 permit ip any any
!
int gig0/0
ip access-group 101 in
!
end
```



f. Close the **HQ_Router**.

Step 2: Access the HQ Internet Web Server on Sally's PC using HTTP.

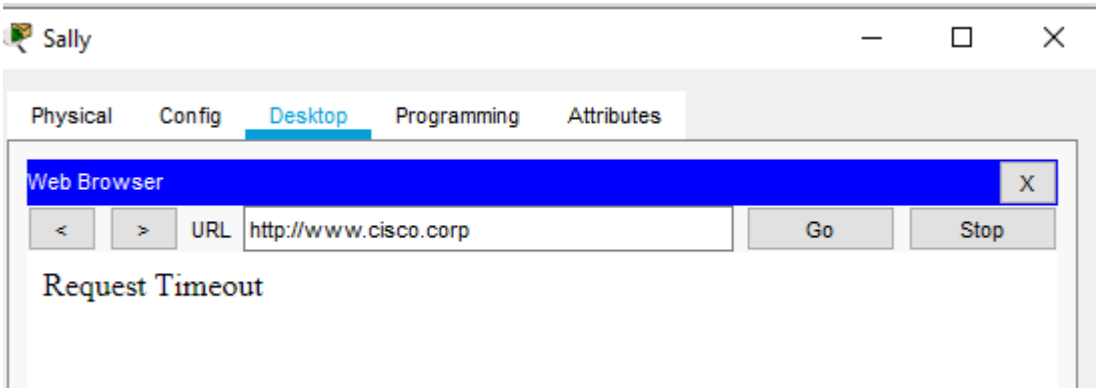
a. Within the **Metropolis Bank HQ** site, click the PC **Sally**.

b. Click the **Desktop** tab and then click **Web Browser**.

c. Enter the URL of **http://www.cisco.corp** and click **Go**.

Is Sally's computer able to access the HQ Internet Web Server using HTTP?

No, the HTTP request is not connecting to the server.



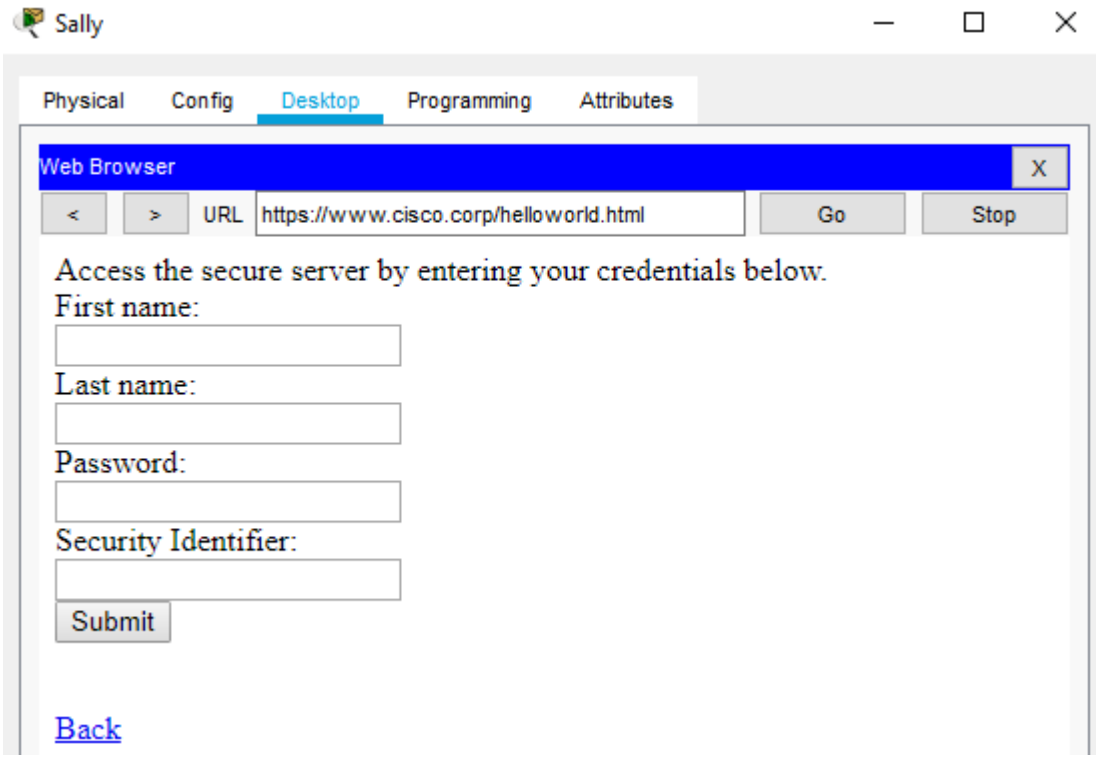
Step 3: Access the HQ Internet Web Server on Sally's PC using HTTPS.

a. Access the **Web Browser** on Sally's computer.

b. Enter the URL of **https://www.cisco.corp** and click Go.

Is Sally's computer able to access the HQ Internet Web Server using HTTP?

Yes, the HTTPS request is connecting to the server.



c. Close **Sally's** computer.

Part 3: Access the Firewall on the Email Server

a. Within the **Metropolis Bank HQ** site, click the **Email** server.

b. Click the **Desktop** tab and then click on **Firewall**. There are no firewall rules implemented.

In order to prevent non-email related traffic from being sent or received from the Email server, network administrators can create firewall rules directly on the server, or as previously shown, they can use access control lists (ACLs) on a network device like a router.