Packet Tracer – Skills Integration Challenge (Instructor Version)

**Instructor Note**: Red font color or gray highlights indicate text that appears in the instructor copy only.

Addressing Table

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Device | Interface | IP Address | Subnet Mask | Default Gateway |
| HQ\_Router | G0/0 | 10.44.1.1 | 255.255.255.0 | N/A |
| G0/1 | 209.165.201.2 | 255.255.255.248 | N/A |
| VPN server | NIC | 209.165.201.19 | 255.255.255.248 | N/A |
| HQ\_Wireless | LAN | 10.44.0.254 | 255.255.255.0 | 10.44.1.1 |
| FTP/Web server | NIC | 10.44.1.252 | 255.255.255.0 | 10.44.1.1 |
| BackupFiles server | NIC | 10.44.2.10 | 255.255.255.0 | 10.44.2.1 |

Scenario

This culminating activity includes many of the skills that you have acquired during this course. You will configure a wireless router, upload and download files using FTP, connect securely to a remote site using a VPN, and secure a Cisco IOS router.

Implementation

**Note:** You only have access to the Metropolis HQ site. You can access all the servers and PCs within this site for testing purposes.

Implement to following requirements:

**Sally’s Computer – Metropolis Bank HQ**

* Upload the **secure.txt** file to the **FTP/Web** server using FTP:
* User **sally** with password **ftpaccess**
* The file to upload is **secure.txt**
* Use the IP address of the **FTP/Web server** located in the addressing table.
* Connect **Sally’s** computer to the **Gotham Healthcare Branch** site via a client-to-site VPN:
* Use the IP address of the VPN server located in the addressing table and ping the VPN server
* Connect the client-to-site VPN with user **sally** and password **vpnsally**
* Use the group **VPNGROUP** and key **123**
* Using the VPN connection, download the **data.txt** file from the **BackupFiles** server using FTP:
* Use the IP address of the **BackupFiles** server located in the addressing table.
* User **sally** with password **securesally**
* The file to download is **data.txt**

**Phil’s Laptop – Metropolis Bank HQ**

* Configure the **HQ\_Wireless** router.
* Use the IP address of the **HQ\_Wireless** router located in the addressing table.
* Use the Web Browser to configure the **HQ\_Wireless** router from **Phil’s** laptop.
* User **admin** with password **p@ssword**
* Change the SSID from **Default** to **HQwifi**
* Set the SSID to be viewable (broadcasted) to wireless clients.
* Configure wireless security of **WPA2 Personal** with the passphrase of **cisco321**.
* Secure the **HQ\_Router**.
* Use the IP address of **HQ\_Router** router located in the addressing table.
* Use the Command prompt to ssh to **HQ\_Router** with the user **phil** and password **securessh**
* Use the **enable** command and password **cisco.**
* Configure a banner motd message that includes the phrase **Authorized Access Only**
* Activate the Cisco IOS resilient configuration feature and reload the router.

**Gina’s Laptop – Metropolis Bank HQ**

* Connect **Gina’s** laptop to the wireless network.
* Connect to the SSID of **HQwifi**
* Use the Pre-shared Key of **cisco321**
* Verify that the laptop uses **DHCP**

Suggested Scoring Rubric

Packet Tracer scores 100 points.

1. Final Config for HQ\_Router

enable

config t

banner motd "Authorized Access Only"

secure boot-image

exit