# Packet Tracer – Configuring VPN Tunnel Mode

## Addressing Table

| Device | Private IP Address | Subnet Mask | Site |
|---|---|---|---|
| File Backup Server | 10.44.2.254 | 255.255.255.0 | Gotham Healthcare Branch |

## Objectives

**Part 1: Sending Unencrypted FTP Traffic**

**Part 2: Configuring the VPN Tunnel between Metropolis and Gotham**

**Part 3: Sending Encrypted FTP Traffic**

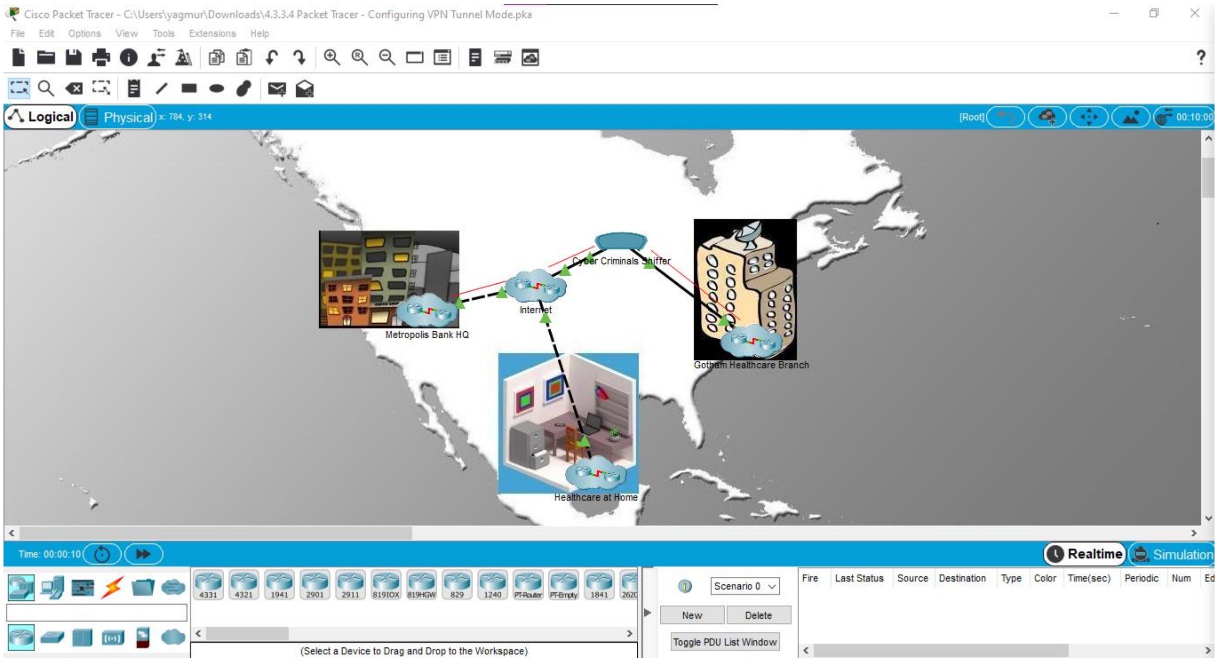
## Background

In this activity, you will observe the transfer of unencrypted FTP traffic between two geographic sites. You will then configure a VPN tunnel between two geographic sites and send encrypted FTP traffic. The IP addressing, network configuration, and service configurations are already complete. You will use the client devices in the differing geographic regions to transfer FTP data securely and insecurely.

# Part 1: Sending Unencrypted FTP Traffic

## Step 1: Access the Cyber Criminals Sniffer.

a. Click the **Cyber Criminals Sniffer** and click the **GUI** tab.

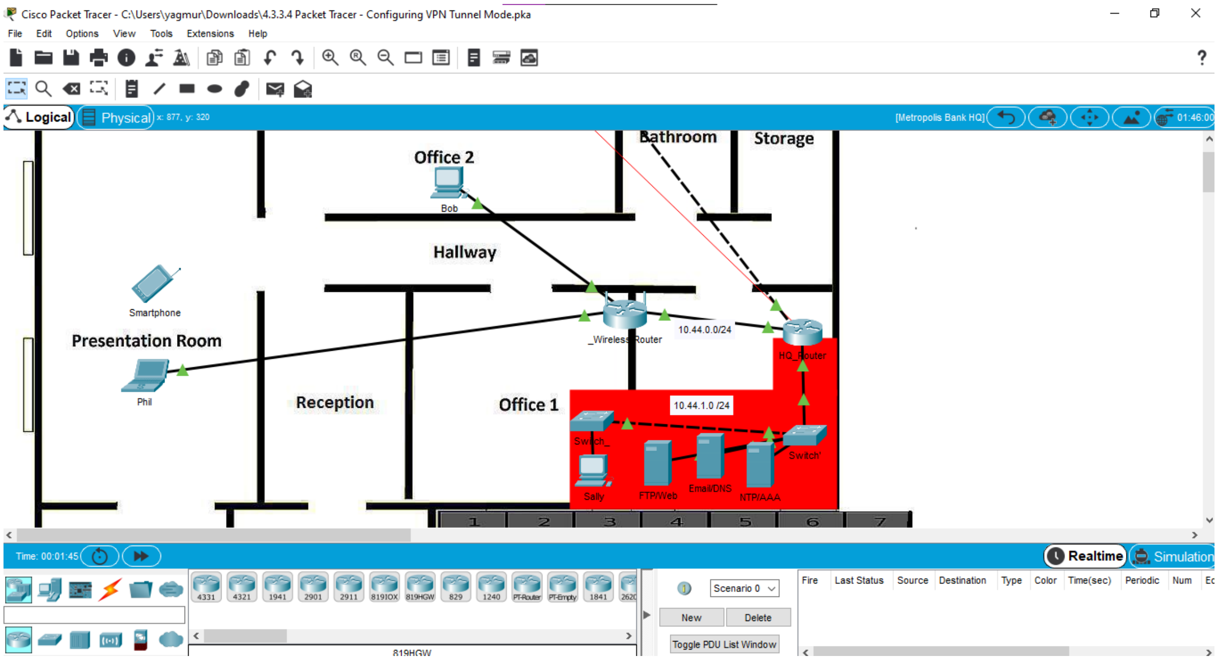

Cisco Packet Tracer - C:\Users\yagmur\Downloads\4.3.3.4 Packet Tracer - Configuring VPN Tunnel Mode.pka
File Edit Options View Tools Extensions Help
Logical
Physical
x: 784, y: 314
[Root]
00:10:00
Cyber Criminals Sniffer
Internet
Metropolis Bank HQ
Gotham Healthcare Branch
Healthcare at Home
Time: 00:00:10
Realtime
Simulation
4331 4321 1941 2901 2911 819IOX 819HGW 829 1240 PT-Router PT-Empty 1841 2620
Scenario 0
New
Delete
Toggle PDU List Window
Fire Last Status Source Destination Type Color Time(sec) Periodic Num Ed
(Select a Device to Drag and Drop to the Workspace)

b. Click the **Clear** button to remove any possible traffic entries viewed by the sniffer.

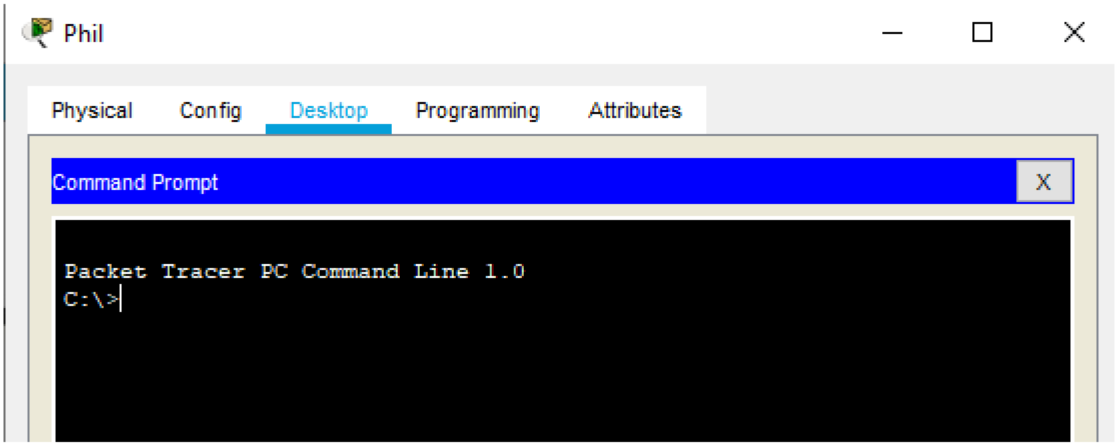
c. Minimize the **Cyber Criminals Sniffer**.

## Step 2: Connect to the FTP Backup server using an insecure FTP connection.

a. Click the **Metropolis Bank HQ** site and click **Phil's** laptop.

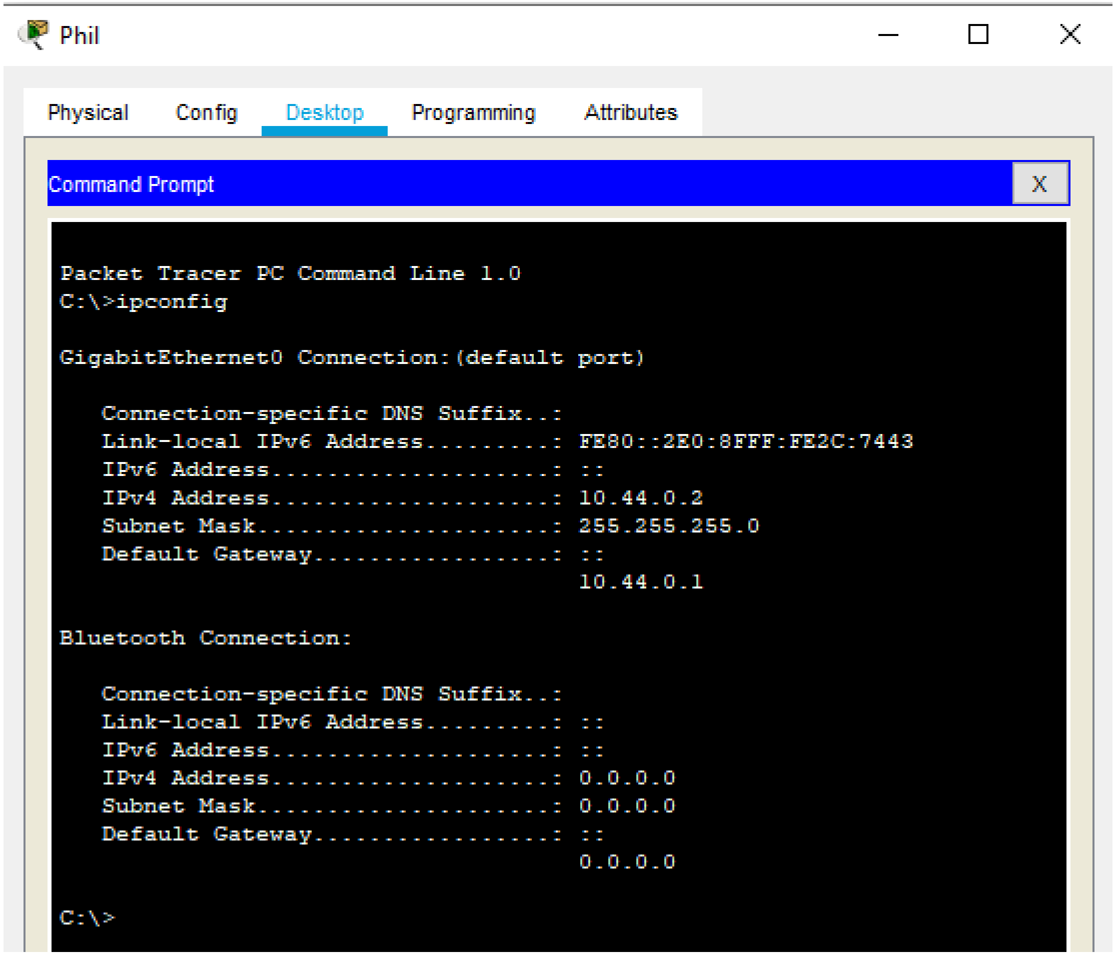


b. Click the **Desktop** tab and click on **Command Prompt**.



```
Packet Tracer PC Command Line 1.0
C:\>
```

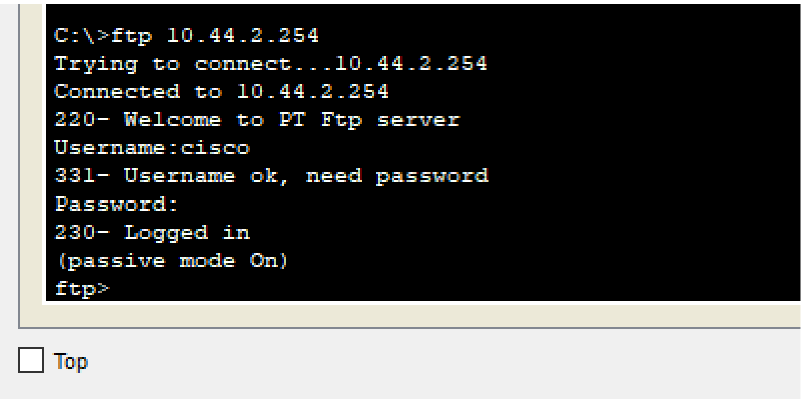
c. Use the **ipconfig** command to view the current IP address of **Phil's** PC.



```
Packet Tracer PC Command Line 1.0
C:\>ipconfig

GigabitEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.........: FE80::2E0:8FFF:FE2C:7443
   IPv6 Address....................: ::
   IPv4 Address....................: 10.44.0.2
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.................: ::
                                     10.44.0.1

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.........: ::
   IPv6 Address....................: ::
   IPv4 Address....................: 0.0.0.0
   Subnet Mask.....................: 0.0.0.0
   Default Gateway.................: ::
                                     0.0.0.0

C:\>
```

d. Connect to the **File Backup** server at **Gotham Healthcare Branch** by entering **ftp 10.44.2.254** in the command prompt.

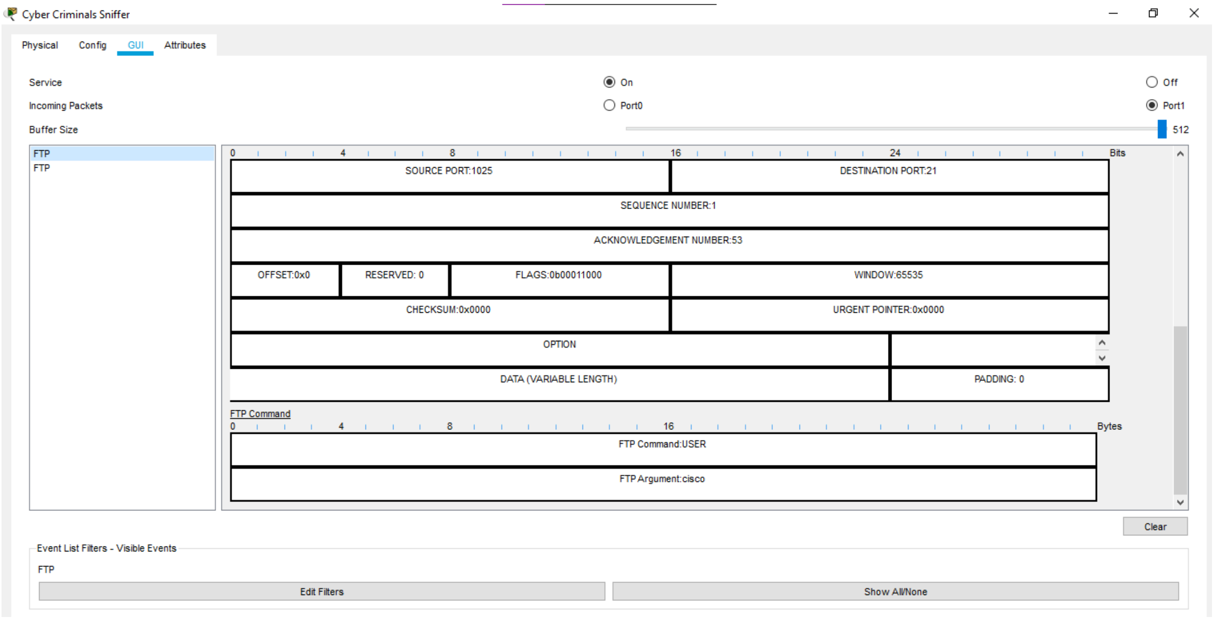
Enter the username of **cisco** and password of **cisco** to login to the **File Backup** server.



```
C:\>ftp 10.44.2.254
Trying to connect...10.44.2.254
Connected to 10.44.2.254
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>
```

## Step 3: View the traffic on the Cyber Criminals Sniffer.

a. Maximize the **Cyber Criminals Sniffer** that was previously minimized.



Service ● On ○ Off

Incoming Packets ○ Port0 ● Port1

Buffer Size 512

SOURCE PORT:1025 | DESTINATION PORT:21

SEQUENCE NUMBER:1

ACKNOWLEDGEMENT NUMBER:53

OFFSET:0x0 | RESERVED: 0 | FLAGS:0b00011000 | WINDOW:65535

CHECKSUM:0x0000 | URGENT POINTER:0x0000

OPTION

DATA (VARIABLE LENGTH) | PADDING: 0

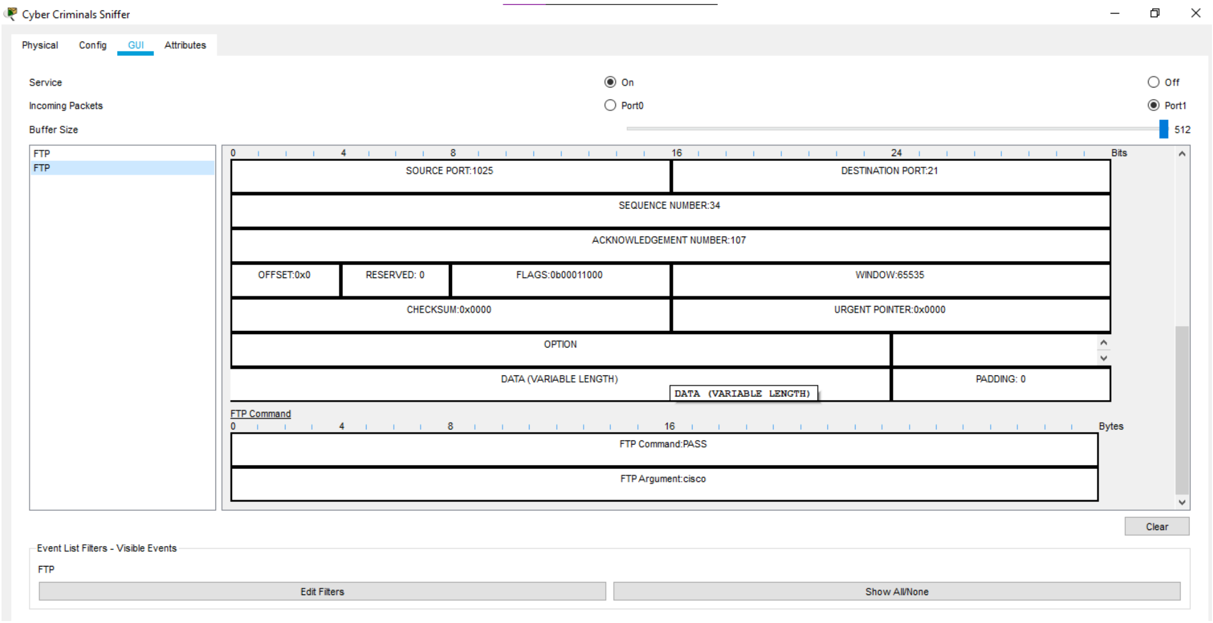
FTP Command

FTP Command:USER

FTP Argument:cisco

Event List Filters - Visible Events

FTP



Service ● On ○ Off

Incoming Packets ○ Port0 ● Port1

Buffer Size 512

SOURCE PORT:1025 | DESTINATION PORT:21

SEQUENCE NUMBER:34

ACKNOWLEDGEMENT NUMBER:107

OFFSET:0x0 | RESERVED: 0 | FLAGS:0b00011000 | WINDOW:65535

CHECKSUM:0x0000 | URGENT POINTER:0x0000

OPTION

DATA (VARIABLE LENGTH) | PADDING: 0

DATA (VARIABLE LENGTH)

FTP Command

FTP Command:PASS

FTP Argument:cisco

Event List Filters - Visible Events

FTP

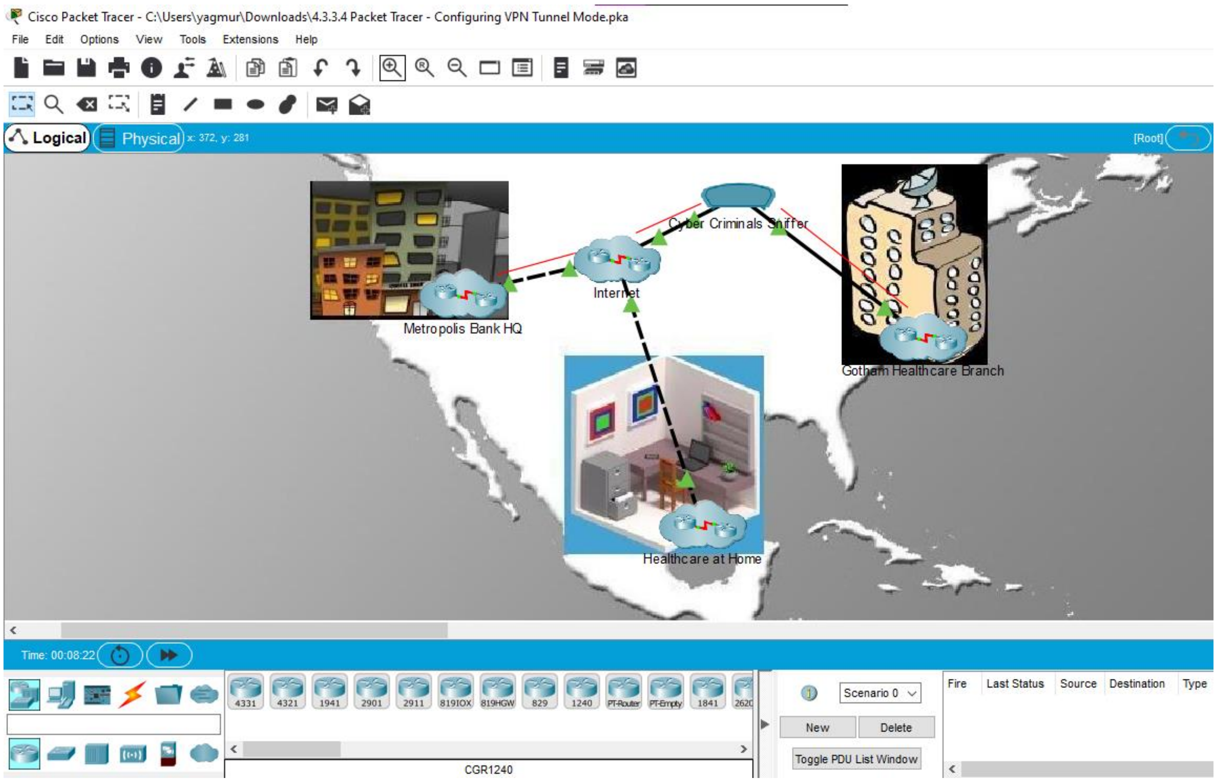
b. Click the **FTP** messages displayed on the sniffer and scroll to the bottom of each one.

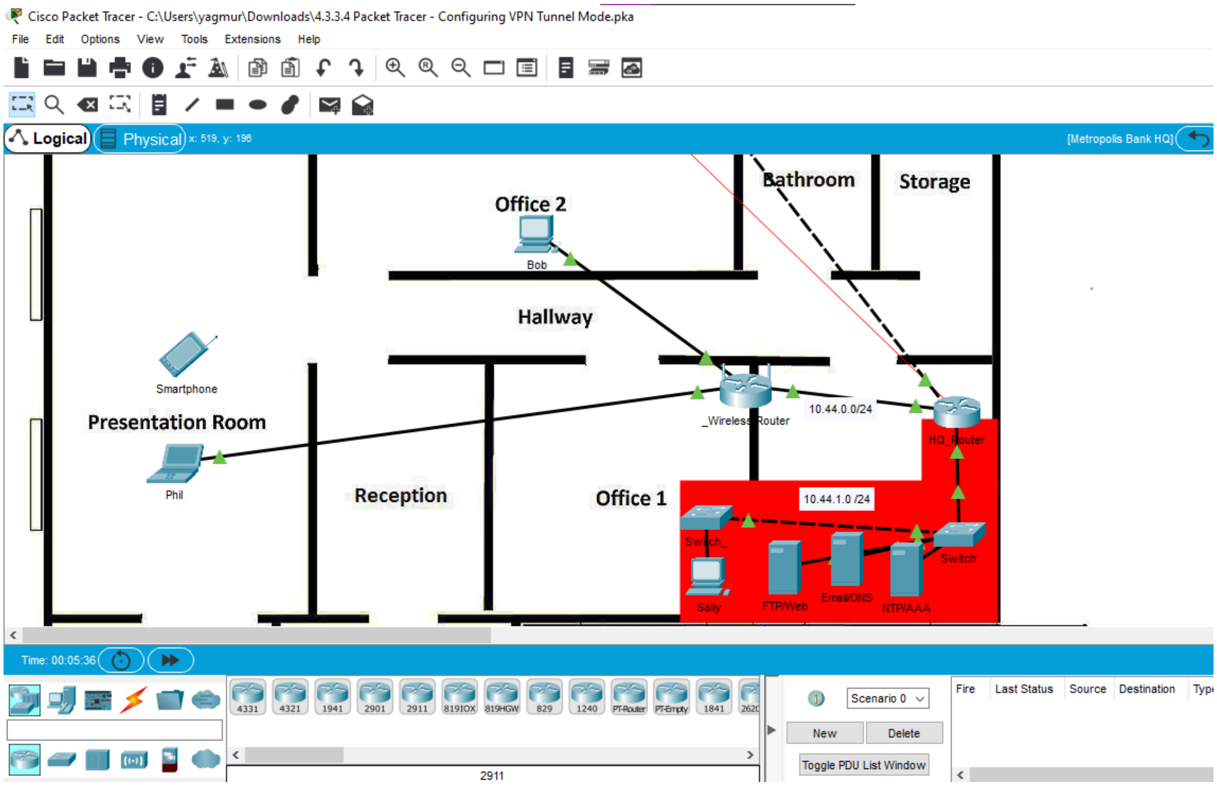
**What information is displayed in clear text?**

*USER cisco PASS cisco*

## Part 2: Configuring the VPN Tunnel between Metropolis and Gotham

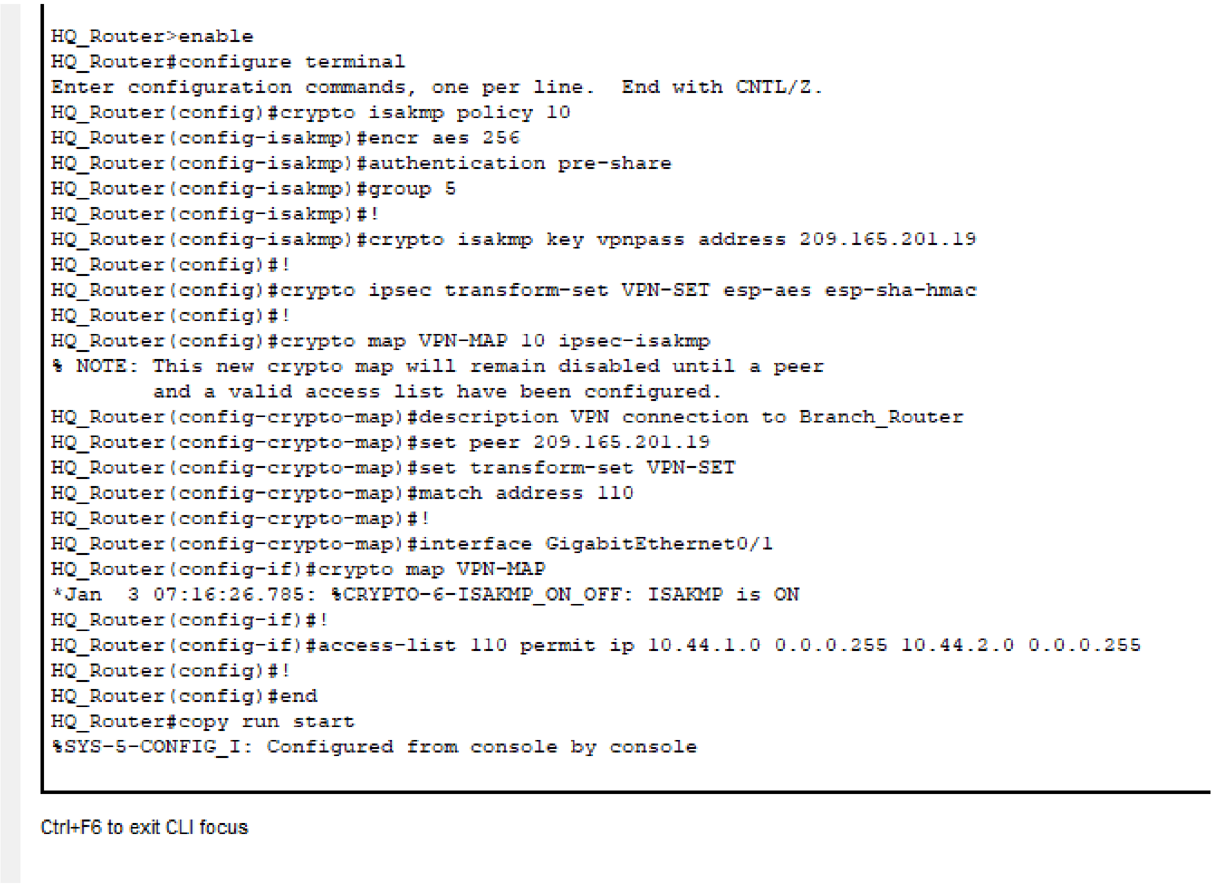
a. Within the **Metropolis Bank HQ** site, click the **HQ_Router**.





b. Copy the IPSec VPN site-to site configuration below and paste it into **HQ_Router**.

```
enable
configure terminal
crypto isakmp policy 10
 encr aes 256
 authentication pre-share
 group 5
!
crypto isakmp key vpnpass address 209.165.201.19
!
crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
!
crypto map VPN-MAP 10 ipsec-isakmp
 description VPN connection to Branch_Router
 set peer 209.165.201.19
 set transform-set VPN-SET
 match address 110
!
interface GigabitEthernet0/1
crypto map VPN-MAP
!
access-list 110 permit ip 10.44.1.0 0.0.0.255 10.44.2.0 0.0.0.255
!
end
copy run start
```



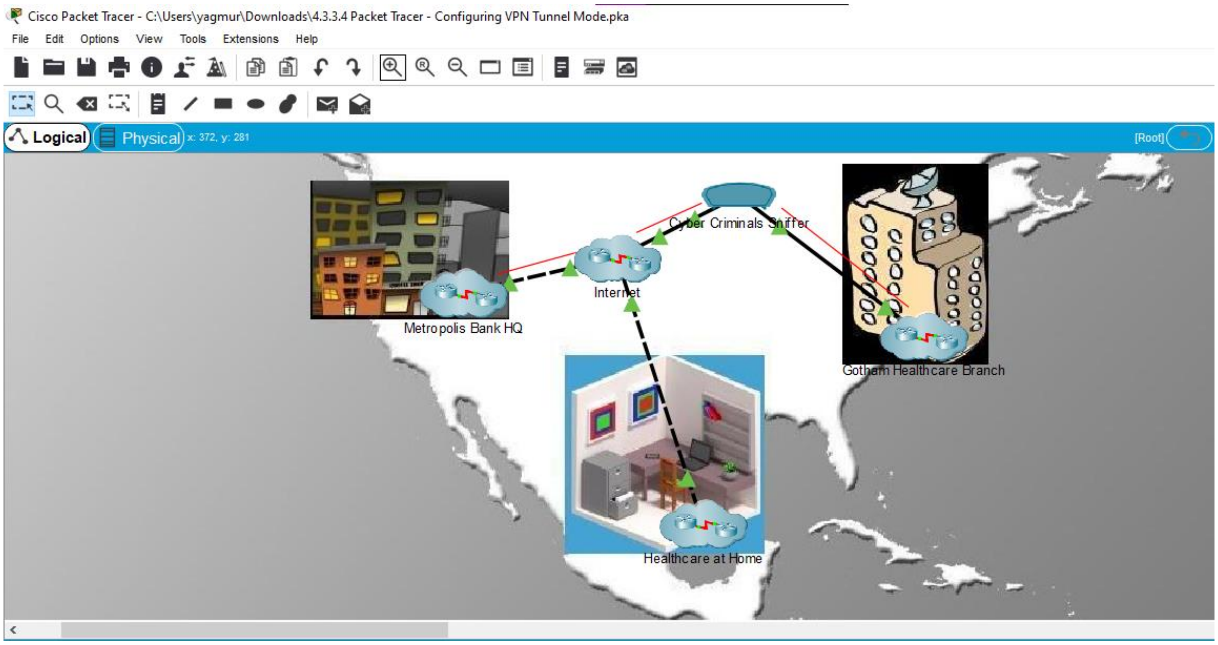
```
HQ_Router>enable
HQ_Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
HQ_Router(config)#crypto isakmp policy 10
HQ_Router(config-isakmp)#encr aes 256
HQ_Router(config-isakmp)#authentication pre-share
HQ_Router(config-isakmp)#group 5
HQ_Router(config-isakmp)#!
HQ_Router(config-isakmp)#crypto isakmp key vpnpass address 209.165.201.19
HQ_Router(config)#!
HQ_Router(config)#crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
HQ_Router(config)#!
HQ_Router(config)#crypto map VPN-MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
HQ_Router(config-crypto-map)#description VPN connection to Branch_Router
HQ_Router(config-crypto-map)#set peer 209.165.201.19
HQ_Router(config-crypto-map)#set transform-set VPN-SET
HQ_Router(config-crypto-map)#match address 110
HQ_Router(config-crypto-map)#!
HQ_Router(config-crypto-map)#interface GigabitEthernet0/1
HQ_Router(config-if)#crypto map VPN-MAP
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
HQ_Router(config-if)#!
HQ_Router(config-if)#access-list 110 permit ip 10.44.1.0 0.0.0.255 10.44.2.0 0.0.0.255
HQ_Router(config)#!
HQ_Router(config)#end
HQ_Router#copy run start
%SYS-5-CONFIG_I: Configured from console by console
```

c. The required mirror configuration of the IPSec VPN has already been implemented on the **Branch_Router** of the **Gotham Healthcare Branch** site.

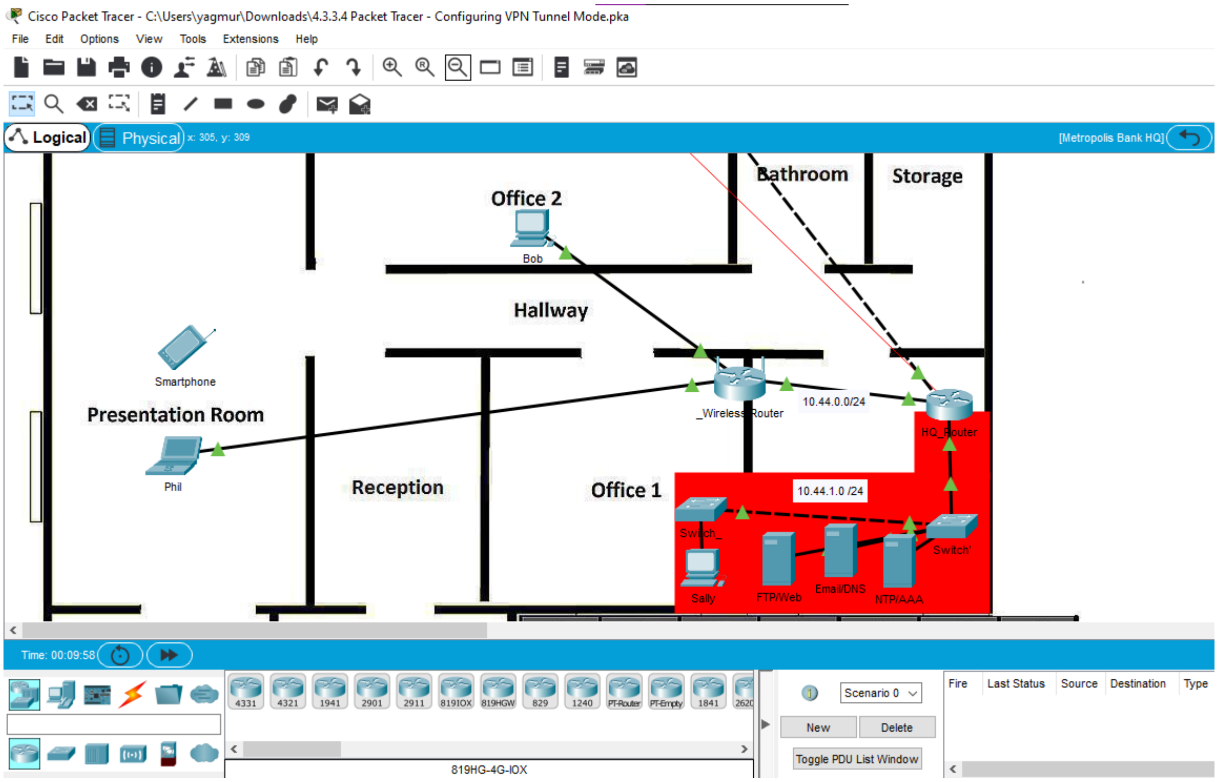
## Part 3: Sending Encrypted FTP Traffic

### Step 1: Send FTP traffic from Sally's PC to the File Backup server.

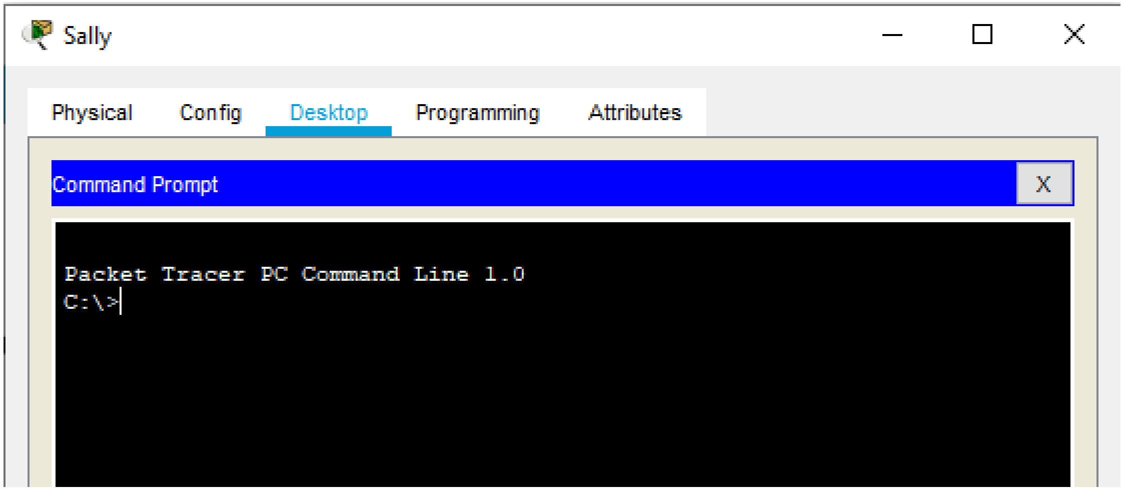
a. Within the **Metropolis Bank HQ** site, click **Sally's** computer.



Cisco Packet Tracer - C:\Users\yagmur\Downloads\4.3.3.4 Packet Tracer - Configuring VPN Tunnel Mode.pka
File Edit Options View Tools Extensions Help
Logical
Physical
x: 372, y: 281
[Root]
Cyber Criminals Sniffer
Internet
Metropolis Bank HQ
Gotham Healthcare Branch
Healthcare at Home

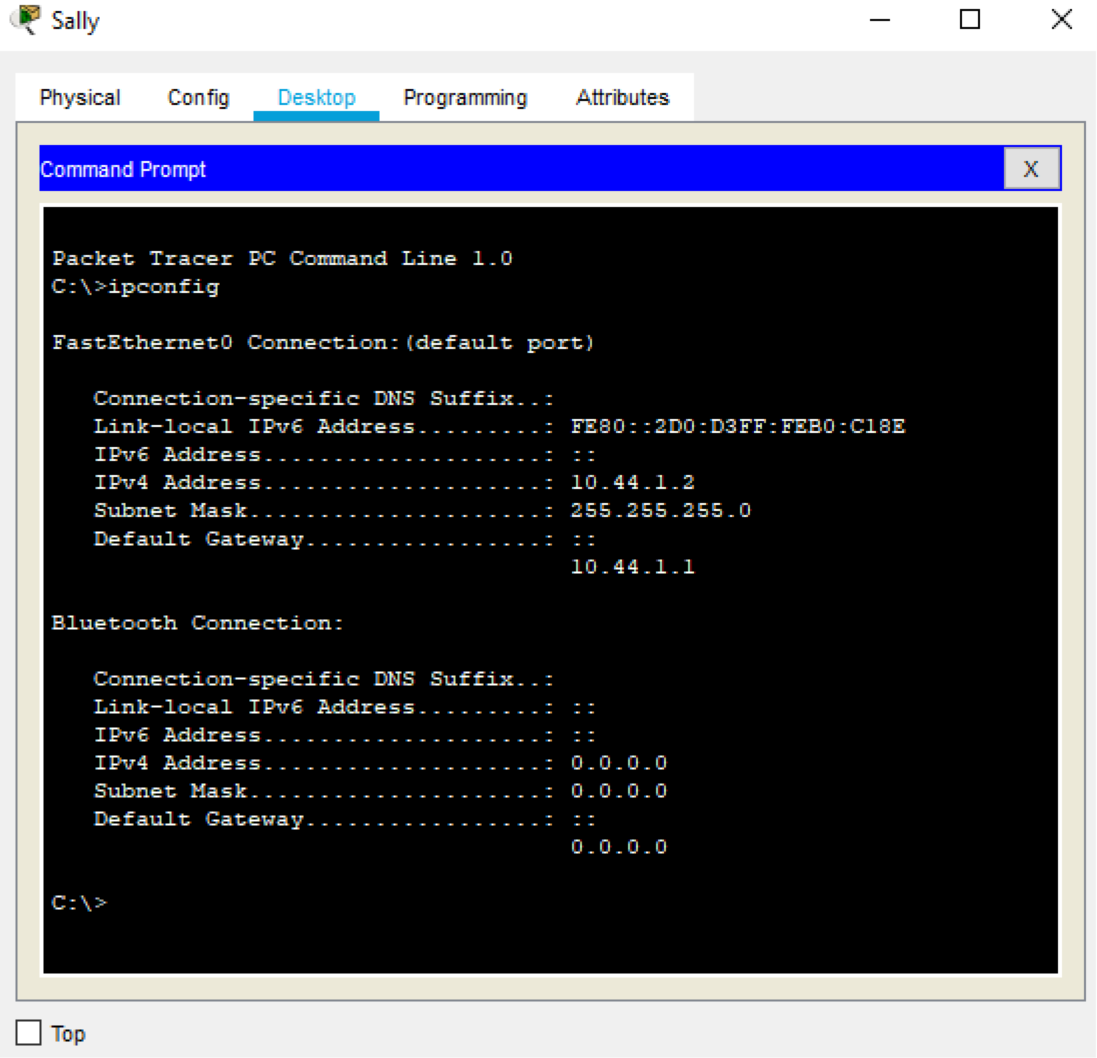


b. Click the **Desktop** tab and then click **Command Prompt**.



```
Packet Tracer PC Command Line 1.0
C:\>
```

c. Use the **ipconfig** command to view the current IP address of **Sally's** PC.

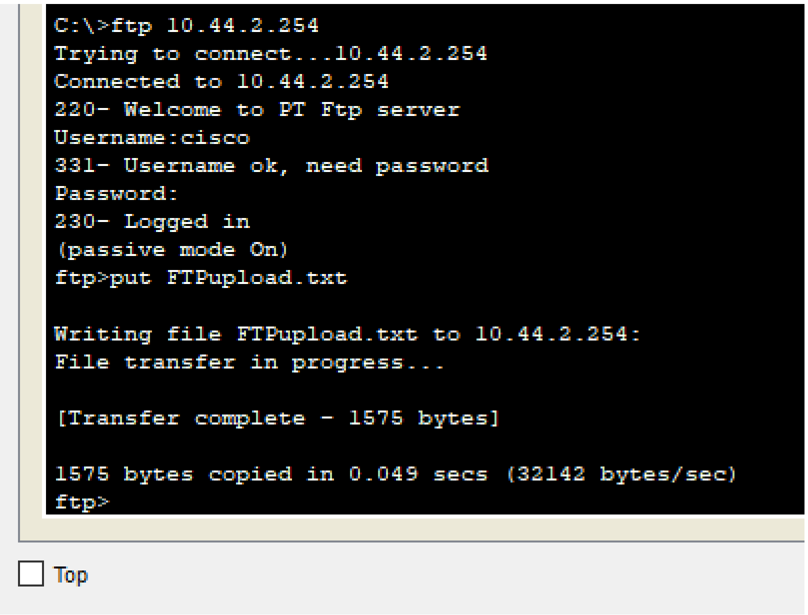


```
Packet Tracer PC Command Line 1.0
C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.........: FE80::2D0:D3FF:FEB0:C18E
   IPv6 Address....................: ::
   IPv4 Address....................: 10.44.1.2
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.................: ::
                                     10.44.1.1

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.........: ::
   IPv6 Address....................: ::
   IPv4 Address....................: 0.0.0.0
   Subnet Mask.....................: 0.0.0.0
   Default Gateway.................: ::
                                     0.0.0.0

C:\>
```

d. Connect to the **File Backup** server at **Gotham Healthcare Branch** by entering **ftp 10.44.2.254** in the command prompt. (It may take 2-5 attempts)

e. Enter the username of **cisco** and password of **cisco** to login to the **File Backup** server

f. Use the **put** command to upload the file **FTPupload.txt** to the **File Backup** server.

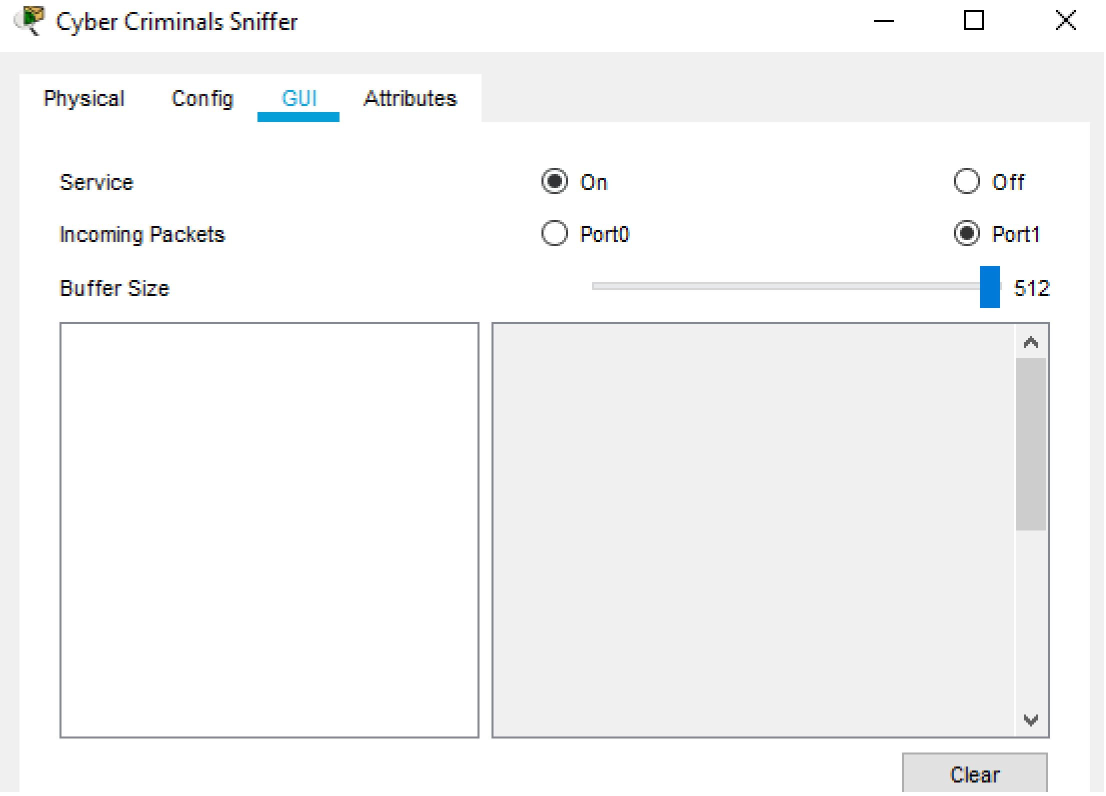


```
C:\>ftp 10.44.2.254
Trying to connect...10.44.2.254
Connected to 10.44.2.254
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>put FTPupload.txt

Writing file FTPupload.txt to 10.44.2.254:
File transfer in progress...

[Transfer complete - 1575 bytes]

1575 bytes copied in 0.049 secs (32142 bytes/sec)
ftp>
```

## Step 2: View the traffic on the Cyber Criminals Sniffer

a. Maximize the **Cyber Criminals Sniffer** that was previously minimized.

b. Click the **FTP** messages displayed on the sniffer.



Service ● On ○ Off

Incoming Packets ○ Port0 ● Port1

Buffer Size 512

**Are there any FTP messages sourced from the IP of Sally's computer? Explain.**

*No, the IPSec VPN is using encryption and the Cyber Criminals Sniffer cannot decrypt the traffic to view it.*