

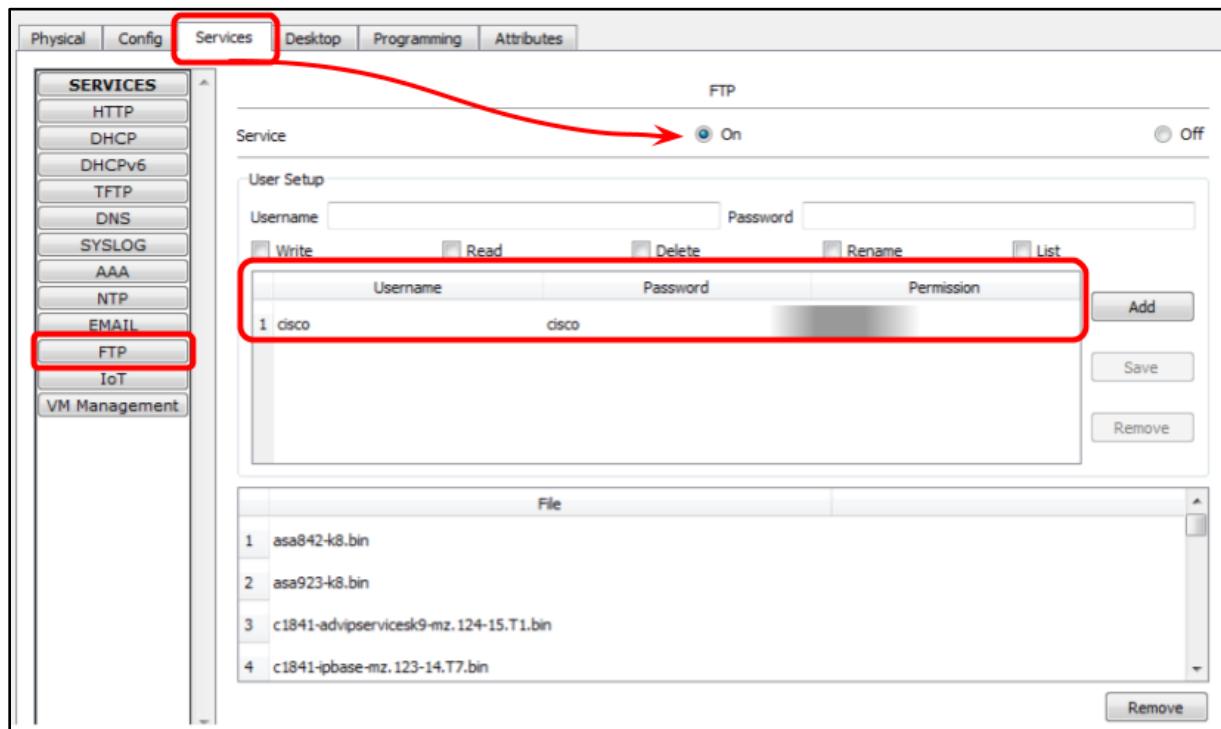
## CYB 220 Module Four Activity Worksheet

**Directions:** Complete the guided tutorial activity using the Module Four Activity Student File available in the learning environment. Follow the steps outlined below in Packet Tracer. You will be asked to provide screenshots or answers to the questions as instructed. Complete this template by replacing the bracketed text with the relevant information.

### Part I: FTP Server

#### FTP Access Configuration

Step 1: In the Services Tab of the **FTP\_Server\_Public**, ensure the FTP services are on. Notice that this service has a default admin account. (The username and password are both **cisco**). You will use this account for any testing.



**Question 1:** What are the permissions for the default FTP user **cisco**?

The default permissions are: Read, Write, Delete, Rename and List

Step 2: From Server1\_Admin, access the Command Prompt (from the Desktop tab). Use the **FTP <IP Address>** command, and log in with the default Cisco FTP account credentials:

```
Packet Tracer PC Command Line 1.0
C:\>FTP 10.1.10.5
Trying to connect...10.1.10.5
Connected to 10.1.10.5
220- Welcome to PT Ftp server
Username:
```

Use the `dir` command (for directory) for a list of all the files hosted on the FTP server.

**Question 2:** What is file number 8 in the FTP directory?

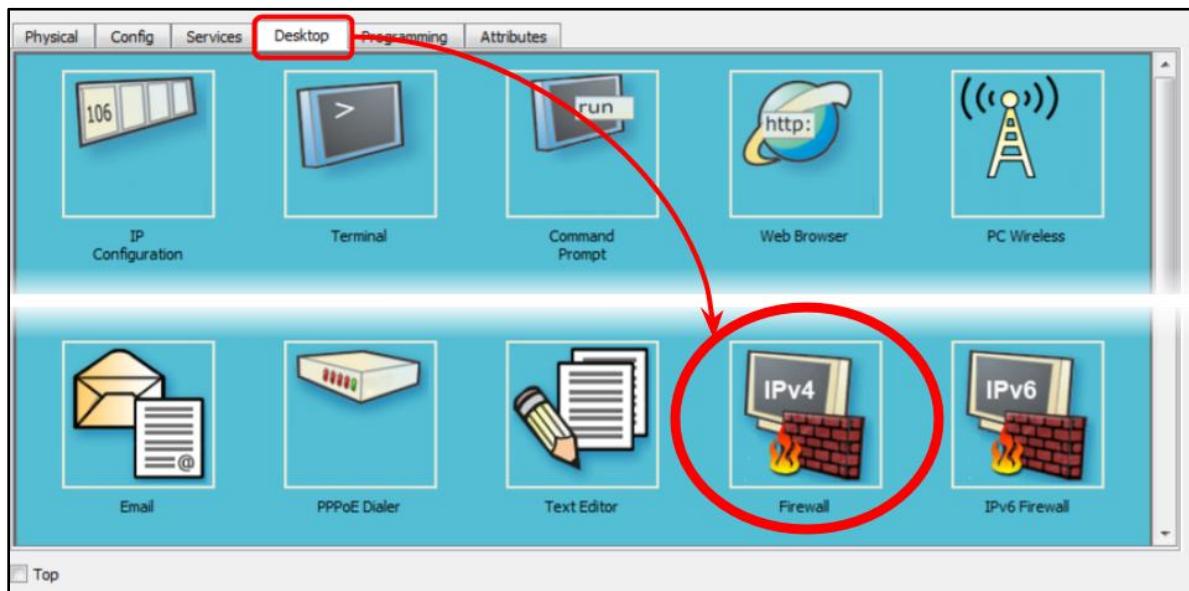
File number 8 is: c2600-ipbasek9-mz.124-8.bin

## Part II: Host-Based Firewall

Type the command `ftp>quit` before starting Part II.

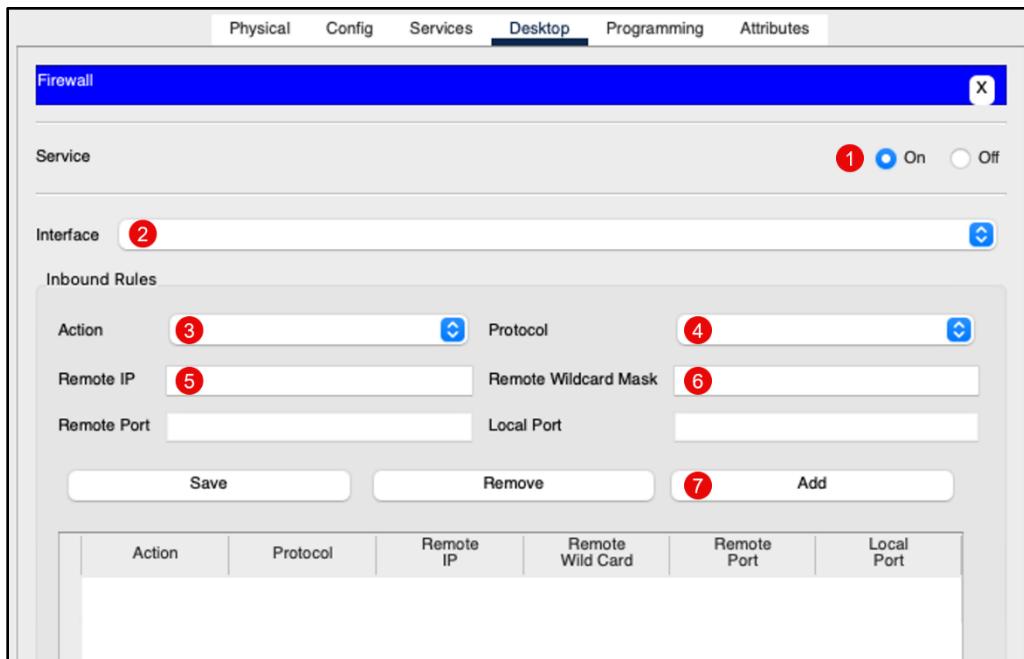
### ***Configure the Firewall on the FTP\_Server\_Public***

Step 1: From the Desktop Tab, open the IPv4 Firewall application:

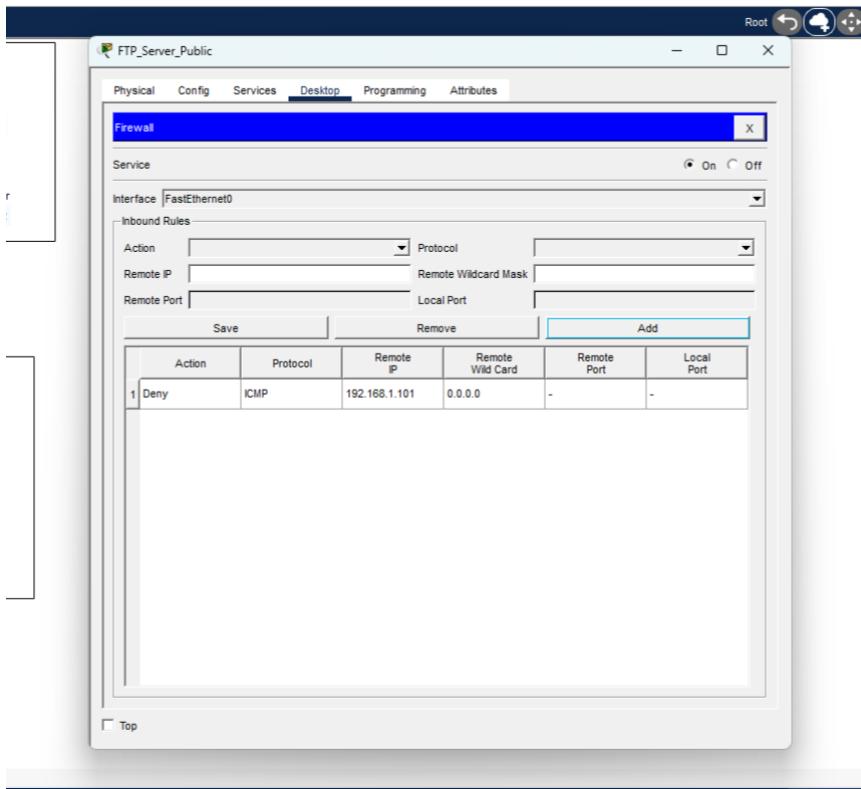


Step 2: Add a firewall rule according to the following settings:

1. Service: "On"
2. Interface: FastEthernet0
3. Action: "Deny"
4. Protocol: "ICMP"
5. Remote IP: 192.168.1.101
6. Remote Wildcard Mask: 0.0.0.0
7. Click "Add."



**Screenshot 1:** Add a screenshot of the proper firewall rule in place.





### ***Test the Firewall Rule***

Step 1: From Server1\_Admin (192.168.1.101), use FTP in the command prompt to attempt to connect to the FTP server (10.1.10.5).

**Question 3:** This connection is prevented if your firewall configuration is correct. What is the error message you receive when this connection is unable to be made?

The error message is: %Error opening ftp://10.1.10.5/ (Timed out)

### ***Modify the Firewall Rules***

Step 1: From PC1\_End\_Users (in the End User network), ping the FTP server (10.1.10.5). You should receive a “Request timed out” message. Why? The Firewall Service is configured in a *default-deny* stance. By activating the Firewall Service and applying at least one *Inbound Rule*, all other traffic is denied unless *allowed by exception* using another rule.

Step 2: To allow specific traffic, you will need to add another rule to the FTP Server host-based firewall. Imagine you would like only the hosts in the End\_User network to access the FTP services on the FTP Server. You have the options following this paragraph available to be applied. Feel free to test each out in Packet Tracer before answering Question 4.



Option One:

Action	Protocol	Remote IP	Remote Wildcard	Remote Port	Local Port
Allow	IP	192.168.2.101	0.0.0.0	any	21

Option Two:

Action	Protocol	Remote IP	Remote Wildcard	Remote Port	Local Port
Allow	IP	192.168.0.0	0.0.255.255	any	21

Option Three:

Action	Protocol	Remote IP	Remote Wildcard	Remote Port	Local Port
Allow	IP	192.168.2.96	0.0.0.15	any	21

Option Four:

Action	Protocol	Remote IP	Remote Wildcard	Remote Port	Local Port
Allow	IP	192.168.2.0	0.0.0.255	any	21

**Question 4:** Which option is the best to allow only the hosts in the End\_User network to access the FTP services on the FTP Server? Why did you recommend this rule?

I chose option 4 because it allows traffic from that subnet but not the others like option 2 would. Option 1 and option 3 only allow a specific IP address.

Before moving on to Part III, be sure you have configured your selected rule on the FTP server before moving forward to the next question.

### Part III: Standard Access List

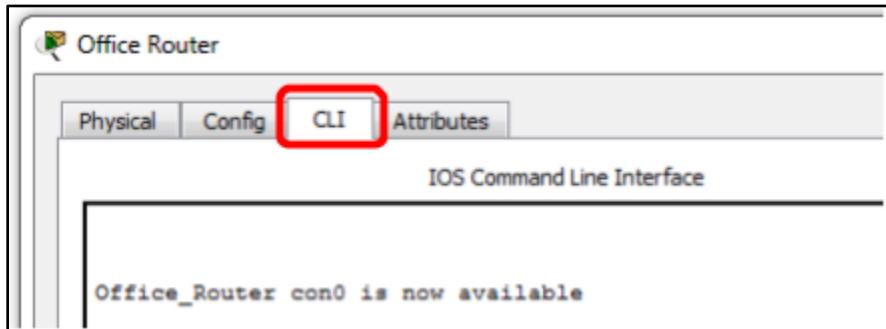
#### ***Create the Standard Access List Control List***

Standard access control lists (ACLs) can be configured in two ways:

1. Numbered access list using the command #access-list <#1-99>
2. Named access list using the command IP access-list standard <#1-99 or name>

Once created, both will function identically; however, named access lists provide the advantage of being editable. With a numbered list, you must first delete the entire ACL, then recreate it with any edits you require. In this tutorial, you will use the named ACL to allow us to explore the results of making changes.

Step 1: Go to the CLI tab in the Office Router:

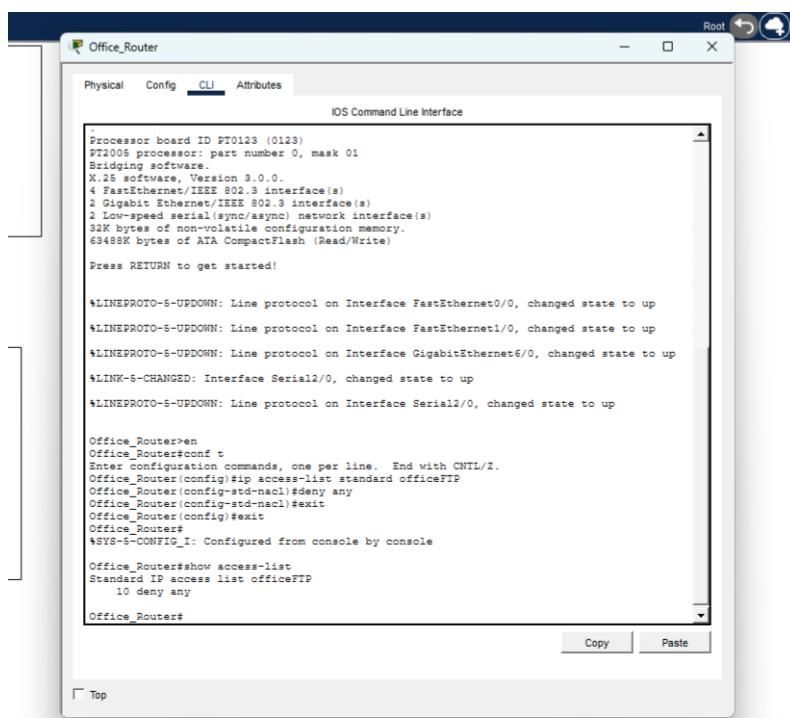


Step 2: Create the Standard Access List:

```
Office_Router>enable
Office_Router#configure terminal
Office_Router(config)#ip access-list standard officeFTP
Office_Router(config-std-nacl)#deny any
Office_Router(config-std-nacl)#exit
Office_Router(config)#exit
Office_Router#
%SYS-5-CONFIG_I: Configured from console by console

Office_Router#show access-lists
```

**Screenshot 2:** Add a screenshot of your configured access list.



The screenshot shows the "CLI" tab selected in the "Office\_Router" interface. The command-line interface displays the configuration steps for creating a standard access list named "officeFTP". It shows the configuration of a deny rule for any source IP address and exits back to the configuration mode. Finally, the "show access-lists" command is run to verify the configuration, which lists the "Standard IP access list officeFTP" with one rule: "10 deny any".

```
Processor board ID PTO123 (0123)
PT2005 processor part number 0, mask 01
Bridging software.
X.25 software, Version 3.0.0
4 FastEthernet/IEEE 802.3 interface(s)
2 Gigabit Ethernet/IEEE 802.3 interface(s)
2 Low-speed serial(sync/async) network interface(s)
32K bytes of non-volatile configuration memory.
63488K bytes of ATA CompactFlash (Read/Write)

Press RETURN to get started!

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet6/0, changed state to up
%LINK-5-CHANGED: Interface Serial2/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0, changed state to up

Office_Router>
Office_Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Office_Router(config)#ip access-list standard officeFTP
Office_Router(config-std-nacl)#deny any
Office_Router(config-std-nacl)#exit
Office_Router(config)#exit
Office_Router#
%SYS-5-CONFIG_I: Configured from console by console

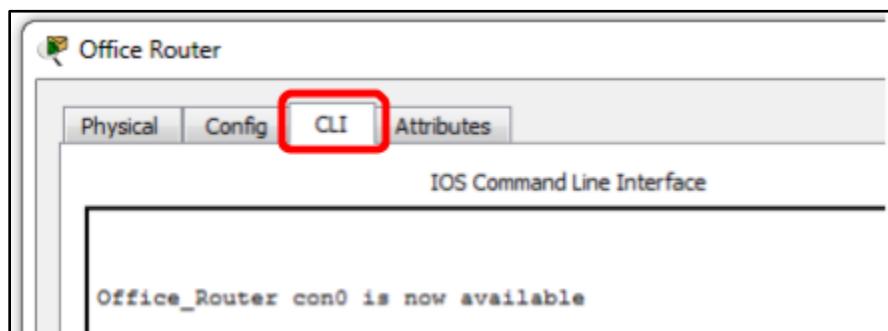
Office_Router#show access-list
Standard IP access list officeFTP
  10 deny any

Office_Router#
```

**Apply the Standard Access Control List Named Office to the Gigabit Ethernet 6/0 Interface**

Routers/firewall appliances filter traffic with access control lists (ACLs) assigned to a specific interface. The processing and filtering of traffic is affected by whether the ACL is designated as inbound or outbound. In this tutorial, the standard ACL, officeFTP, will be applied to the g6/0 interface as an outbound ACL. Before forwarding traffic out of the g6/0 interface, the router checks the source IP address against the ACL. If the packet source is from a “deny” address, the packets are discarded. If they are from a “permit” address, they are forwarded.

Step 1: Go to the CLI tab in the Office Router:



Step 2: Apply the standard access control list to a specific interface.

```
Office_Router#configure terminal
Office_Router(config)#interface g6/0
Office_Router(config-if)#ip access-group officeFTP out
Office_Router( config-if)#exit
Office_Router(config)#exit
%SYS-5-CONFIG_I: Configured from console by console
```

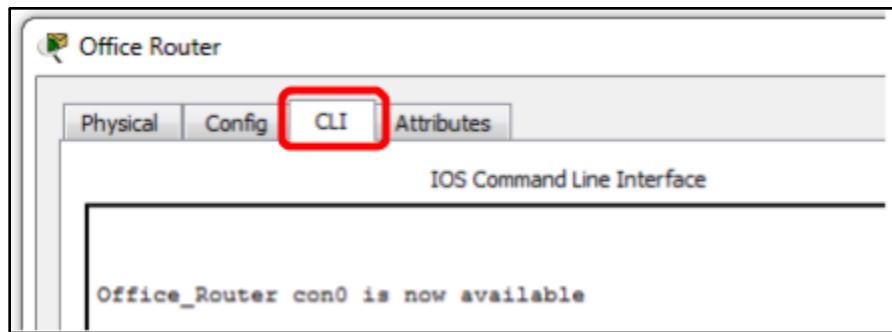
Step 3: From PC1\_End\_Users, use the command C:\>ftp 10.1.10.5 to access the FTP Server.

**Question 5:** Explain the interaction between the FTP's host-based firewall and the router's access list.

The router's access list is set to deny all traffic; therefore, any attempt to connect to the FTP using the address 10.1.10.5 would fail because the router blocks the traffic from reaching the server.

**Modify the Standard ACL on Gig6/0:**

Step 1: Go to the CLI tab in the Office Router:



Step 2: Add a new rule to the standard ACL.

```
Office_Router>enable
Office_Router#configure terminal
Office_Router(config)#ip access-list standard officeFTP
Office_Router(config-std-nacl)#permit 192.168.2.0 0.0.0.255
Office_Router(config-std-nacl)#exit
Office_Router(config)#exit
%SYS-5-CONFIG_I: Configured from console by console
```

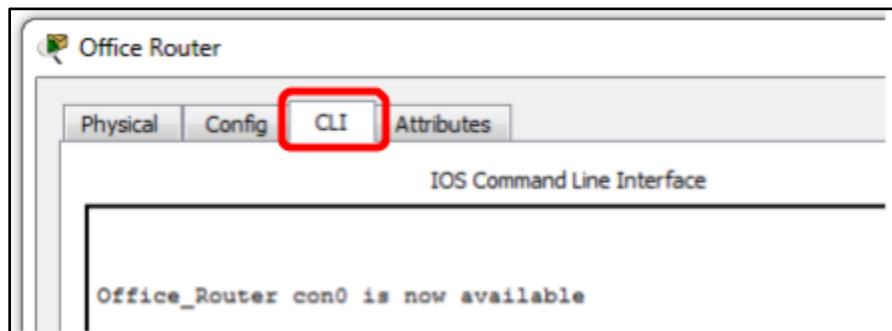
Step 3: From PC1\_End\_Users, use the command C:\>ftp 10.1.10.5 to access the FTP Server.

**Question 6:** Explain why the connection times out despite adding the “permit” statement for the End\_User network to the ACL.

The outbound application of the ACL officeFTP is on interface g6/0. Thus, the amount of data that may leave the router via this port is limited

#### **Edit the Standard ACL on Gig6/0**

Step 1: Go to the CLI tab in the Office Router:

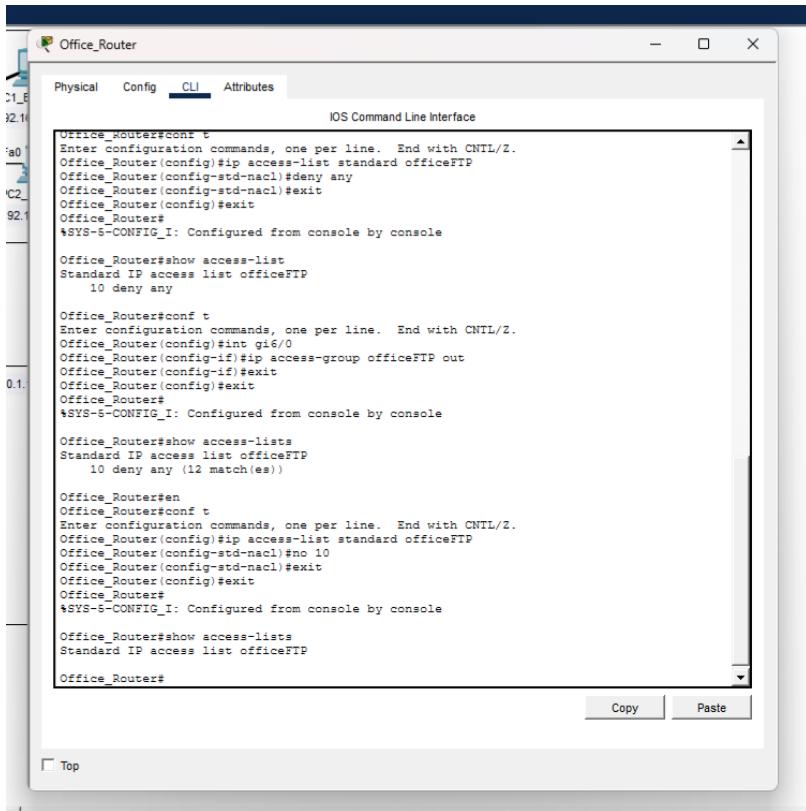


Step 2: Edit the standard ACL.

```
Office_Router>enable
Office_Router#configure terminal
Office_Router(config)#ip access-list standard officeFTP
Office_Router(config-std-nacl)#no 10
```

```
Office_Router(config-std-nacl)#exit
Office_Router(config)#exit
%SYS-5-CONFIG_I: Configured from console by console
Office_Router#show access-lists
```

**Screenshot 3:** Add a screenshot of your configured access list.



The screenshot shows the Cisco IOS CLI interface with the title bar "Office\_Router". The "CLI" tab is selected. The main window displays the following configuration commands:

```
Office_Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Office_Router(config)#ip access-list standard officeFTP
Office_Router(config-std-nacl)#deny any
Office_Router(config-std-nacl)#exit
Office_Router(config)#exit
Office_Router#
%SYS-5-CONFIG_I: Configured from console by console

Office_Router#show access-lists
Standard IP access list officeFTP
 10 deny any

Office_Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Office_Router(config)#int g6/0
Office_Router(config-if)#ip access-group officeFTP out
Office_Router(config-if)#exit
Office_Router(config)#exit
Office_Router#
%SYS-5-CONFIG_I: Configured from console by console

Office_Router#en
Office_Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Office_Router(config)#ip access-list standard officeFTP
Office_Router(config-std-nacl)#no 10
Office_Router(config-std-nacl)#exit
Office_Router(config)#exit
Office_Router#
%SYS-5-CONFIG_I: Configured from console by console

Office_Router#show access-lists
Standard IP access list officeFTP
 10 deny any (12 match(es))

Office_Router#
```

At the bottom of the window are "Copy" and "Paste" buttons. Below the window, there is a checkbox labeled "Top".

### FTP Server Access

Step 1: Use the command `C:\>ftp 10.1.10.5` to access the FTP server from:

- PC1\_End\_Users
- Kiosk1\_Remote\_Access

**Question 7:** Explain the effects of editing the office FTP ACL. Why are the two hosts above permitted or denied access to the FTP server?

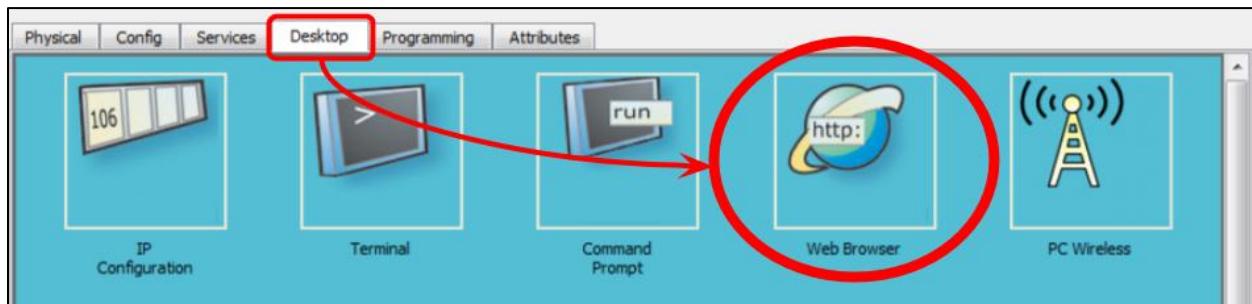
The PC1 is allowed access because the rule 10 was eliminated on the router but the ftp server still has a firewall rule to deny traffic from any except the end user subnet.

### Part IV: Extended Access Control List

Extended Access Control List (ACL) was implemented to filter specific protocols without the need to call out specific hosts/network addresses.

**Show Kiosk1\_Remote\_Access Initially Has Access to Server1\_Admin File Server:**

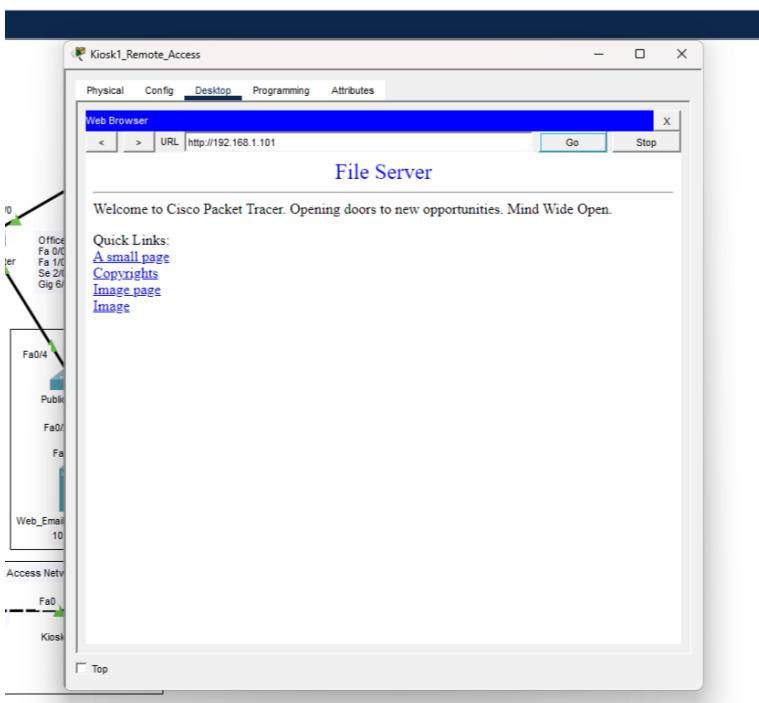
Step 1: Use the Desktop Menu to access the Web Browser:



Step 2: Navigate to File server on Server1\_Admin (192.168.1.101).



**Screenshot 4:** Add a screenshot of your results attempting to access the file server.



**Configure Remote\_Router Extended ACL for SMTP/POP3 Traffic to Email Server**

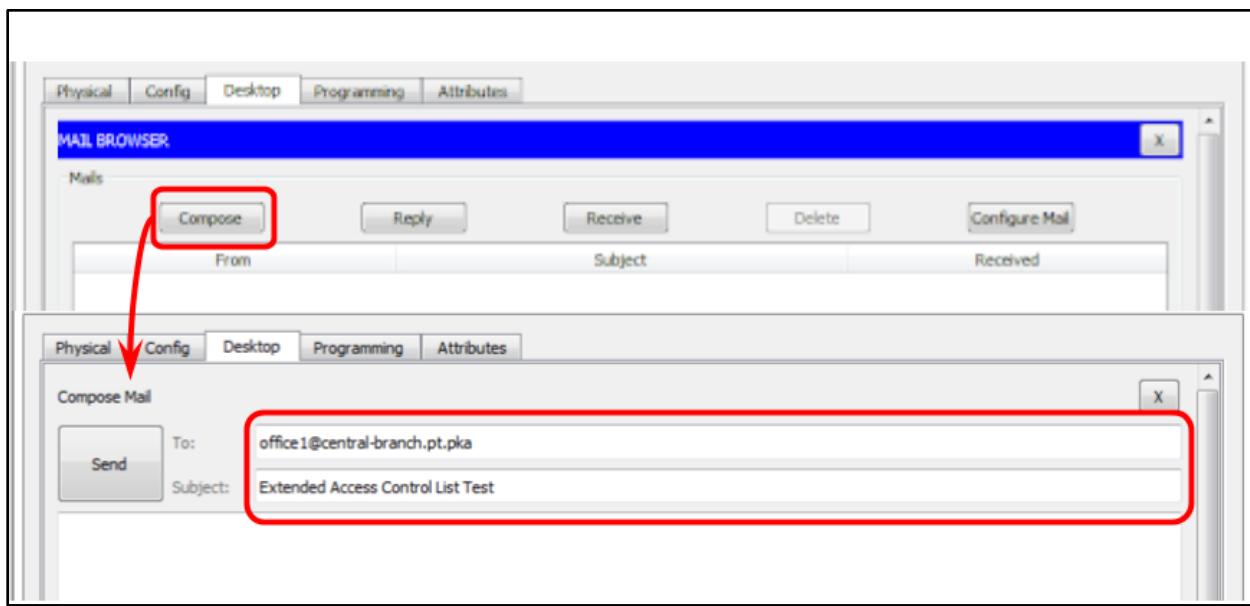
Step 1: In the Remote\_Router CLI tab, add:

```
Remote_Router>enable
```

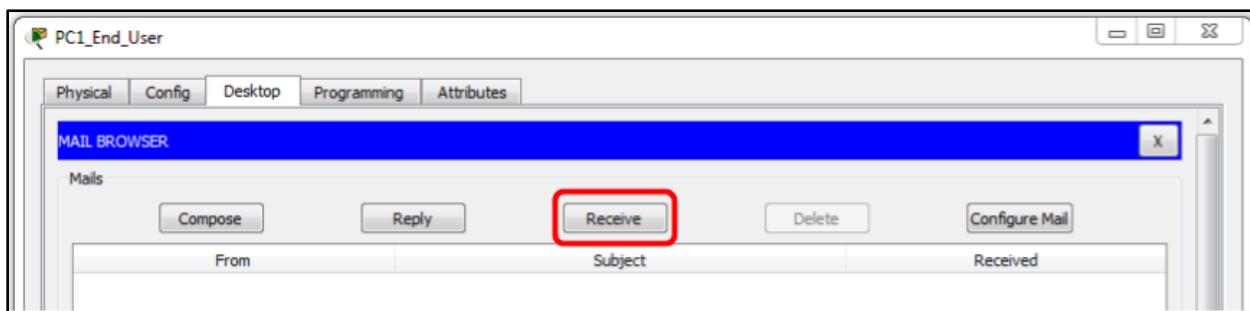
```
Remote_Router#configure terminal
Remote_Router(config)#ip access-list extended email
Remote_Router(config-ext-nacl)#permit tcp 192.168.3.2 0.0.0.0 host
10.1.10.6 eq smtp
Remote_Router(config-ext-nacl)#permit tcp 192.168.3.2 0.0.0.0 host
10.1.10.6 eq pop3
Remote_Router(config-ext-nacl)#exit
Remote_Router(config)interface g0/0/1
Remote_Router(config-if)#ip access-group email in
Remote_Router(config)#exit
%SYS-5-CONFIG_I: Configured from console by console
```

Step 3: Compose email from Kiosk1 to PC1\_End\_User (office1@central-branch.pt.pka).

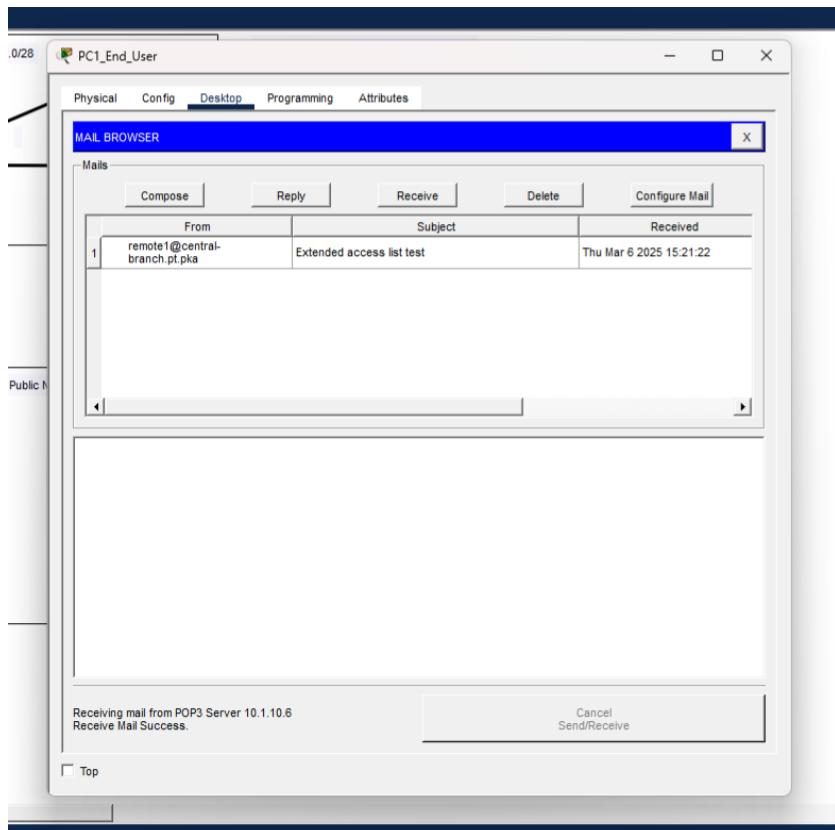




Step 4: Confirm PC1\_End\_User's inbox contains the received email from Kiosk1.

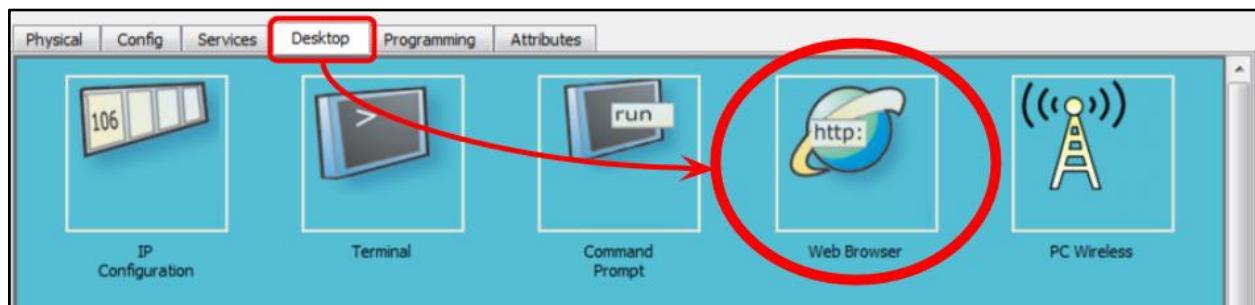


Screenshot 5: Add a screenshot of PC1\_End\_User's inbox containing the received email.

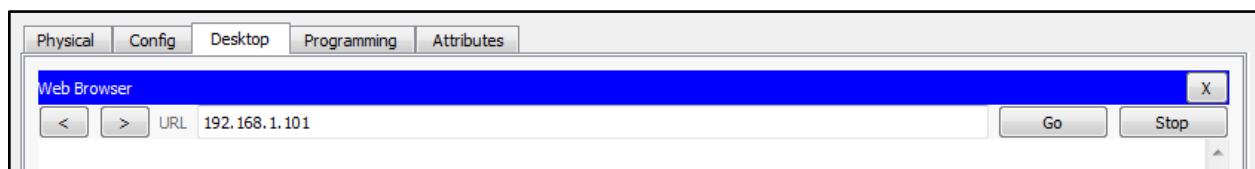


#### Step 5: Verify That the ACL Has Prevented Access to the File Server

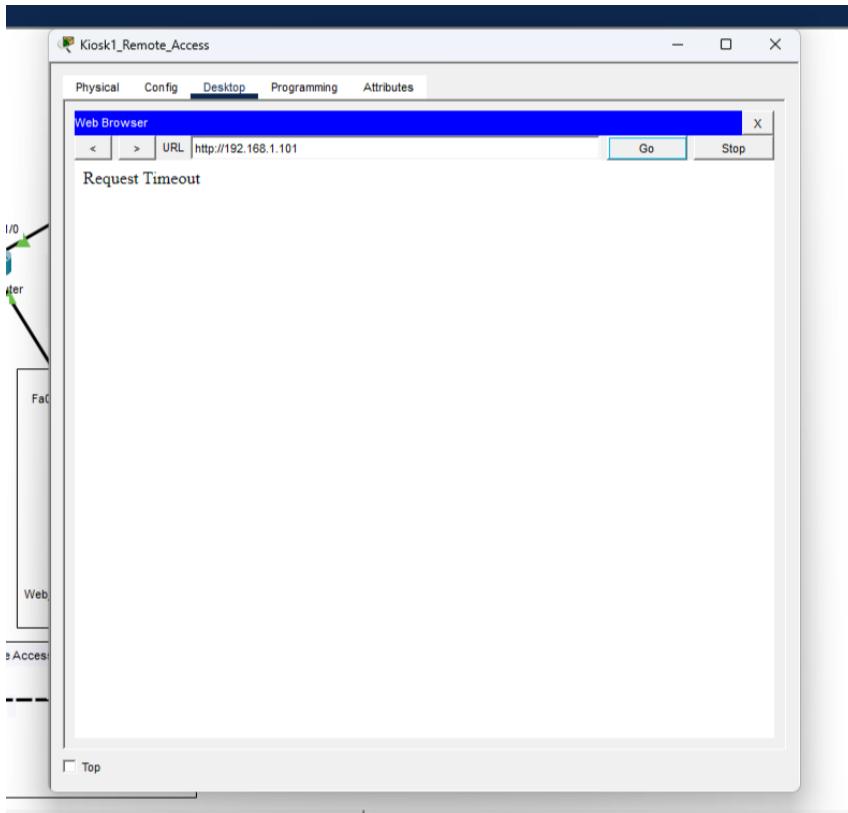
a. Use the Desktop Menu to access the Web Browser:



b. Navigate to the file server on Server1\_Admin (192.168.1.101).



**Screenshot 6:** Add a screenshot of the file server.



**Question 8:** How would you configure the Extended ACL for scalability? In other words, how could you set up the extended ACL to avoid having to modify the ACL every time you add a new host?

You would set up the extended ACL by subnets so as new users go on in the same subnet they will automatically be allowed access.