Network Security Practices

CY5150

Lab 3 - Firewall Lab

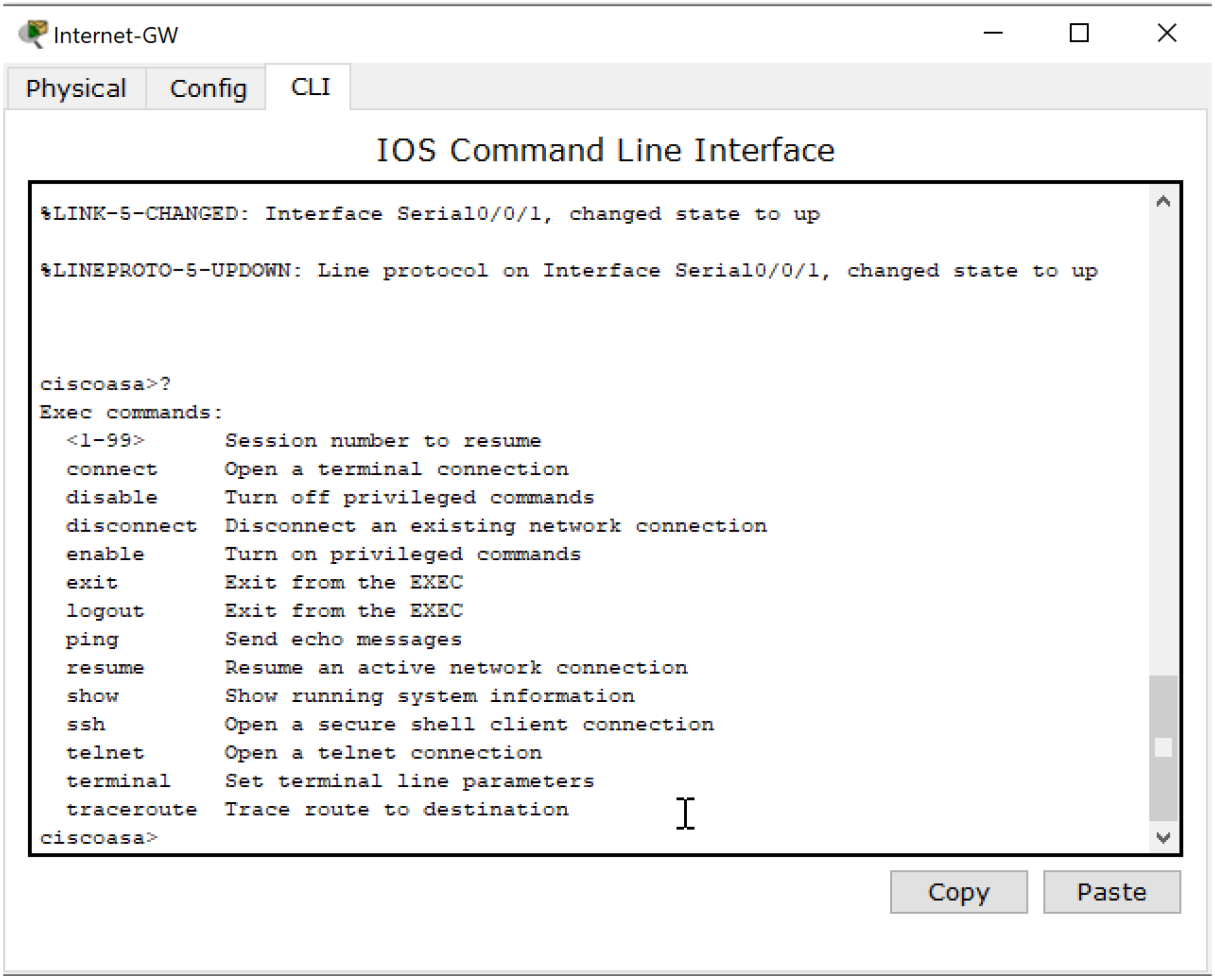
Submitted By:
Sonam Ghatode(001305171)

Table of Contents

Configuring Privilege Access:

- **What does *?* command do?**

  Entering a ? gives a list of available commands for the user.



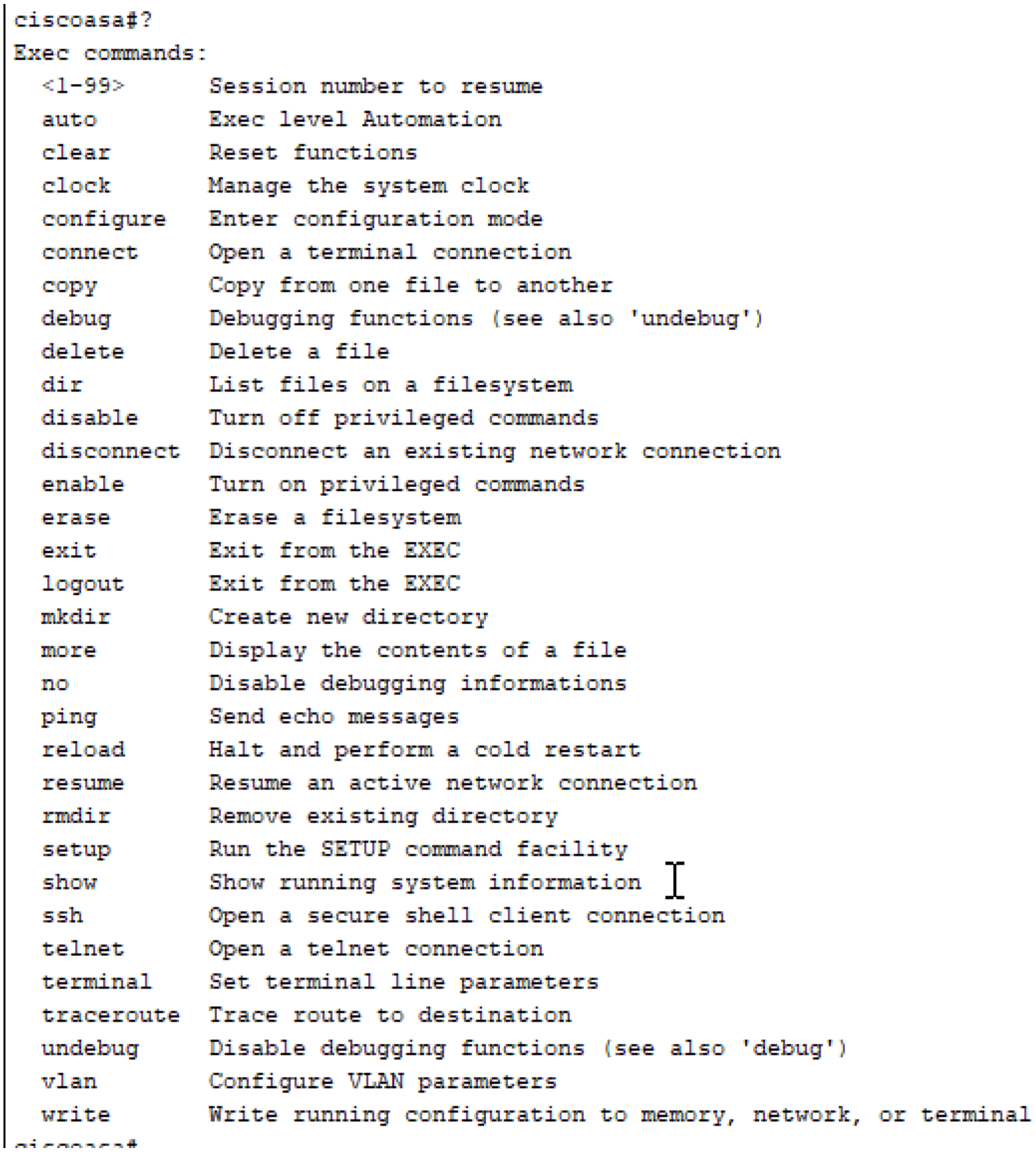
```
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up



ciscoasa>?
Exec commands:
  <1-99>      Session number to resume
  connect     Open a terminal connection
  disable     Turn off privileged commands
  disconnect  Disconnect an existing network connection
  enable      Turn on privileged commands
  exit        Exit from the EXEC
  logout      Exit from the EXEC
  ping        Send echo messages
  resume      Resume an active network connection
  show        Show running system information
  ssh         Open a secure shell client connection
  telnet      Open a telnet connection
  terminal    Set terminal line parameters
  traceroute  Trace route to destination
ciscoasa>
```

- **How many privilege levels are there and what is the highest privilege level?**

  By default, there are 3 levels of privileges: **zero, user** and **privileged** with **privileged level** being the highest privilege level(15)**.** To provide flexibility, routers can be configured with 16 levels of privileges.

- **What's changed in *?* command?**

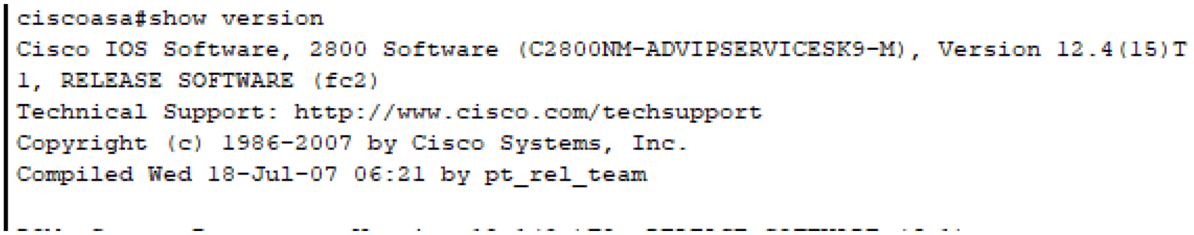
  After entering the privileged level, more commands were available for use.



```
ciscoasa#?
Exec commands:
  <1-99>      Session number to resume
  auto        Exec level Automation
  clear       Reset functions
  clock       Manage the system clock
  configure   Enter configuration mode
  connect     Open a terminal connection
  copy        Copy from one file to another
  debug       Debugging functions (see also 'undebug')
  delete      Delete a file
  dir         List files on a filesystem
  disable     Turn off privileged commands
  disconnect  Disconnect an existing network connection
  enable      Turn on privileged commands
  erase       Erase a filesystem
  exit        Exit from the EXEC
  logout      Exit from the EXEC
  mkdir       Create new directory
  more        Display the contents of a file
  no          Disable debugging informations
  ping        Send echo messages
  reload      Halt and perform a cold restart
  resume      Resume an active network connection
  rmdir       Remove existing directory
  setup       Run the SETUP command facility
  show        Show running system information
  ssh         Open a secure shell client connection
  telnet      Open a telnet connection
  terminal    Set terminal line parameters
  traceroute  Trace route to destination
  undebug     Disable debugging functions (see also 'debug')
  vlan        Configure VLAN parameters
  write       Write running configuration to memory, network, or terminal
```

- **What is the version of the software that is running on this device?**

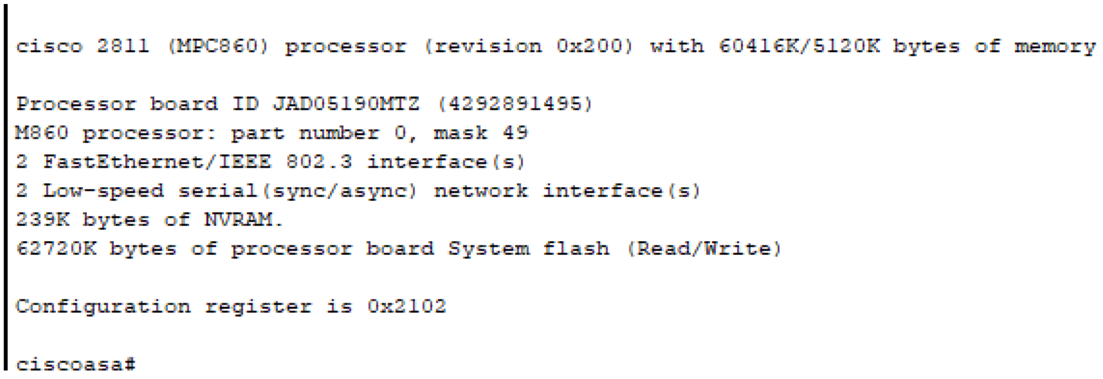
  The software that is running on this device and it's version is **Cisco IOS Software, 2800 Software (C2800NM-ADVIPSERVICESK9-M), Version 12.4(15)T1, RELEASE SOFTWARE (fc2).**



```
ciscoasa#show version
Cisco IOS Software, 2800 Software (C2800NM-ADVIPSERVICESK9-M), Version 12.4(15)T
1, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 18-Jul-07 06:21 by pt_rel_team
```

- **What processor does the device have?**

  The device had a **cisco 2811 (MPC860) processor (revision 0x200)(M860 processor).**.



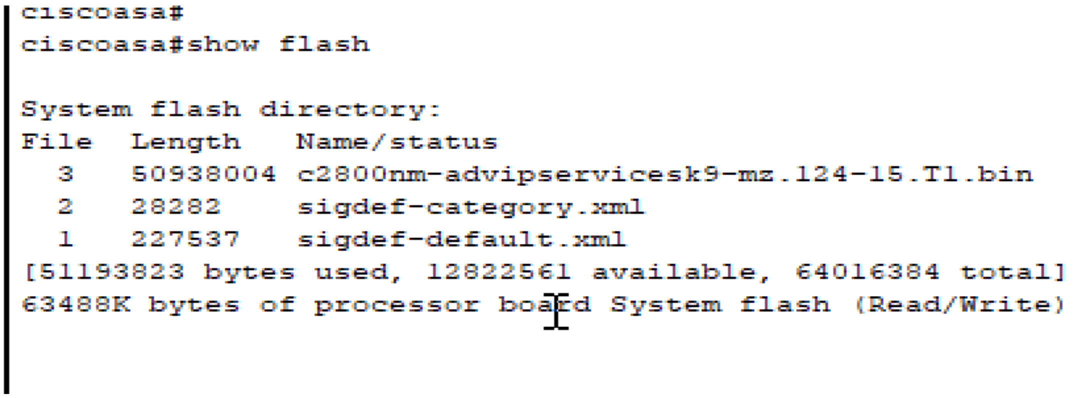
```
cisco 2811 (MPC860) processor (revision 0x200) with 60416K/5120K bytes of memory

Processor board ID JAD05190MTZ (4292891495)
M860 processor: part number 0, mask 49
2 FastEthernet/IEEE 802.3 interface(s)
2 Low-speed serial(sync/async) network interface(s)
239K bytes of NVRAM.
62720K bytes of processor board System flash (Read/Write)

Configuration register is 0x2102

ciscoasa#
```

- **What are the different types of memory in the device and what are their total sizes?**

  The device has **processor memory of 60416K/5120K bytes, NVRAM of 239 bytes** and **processor board System Flash 62720K bytes**.

- **How much flash space is used vs. available?**

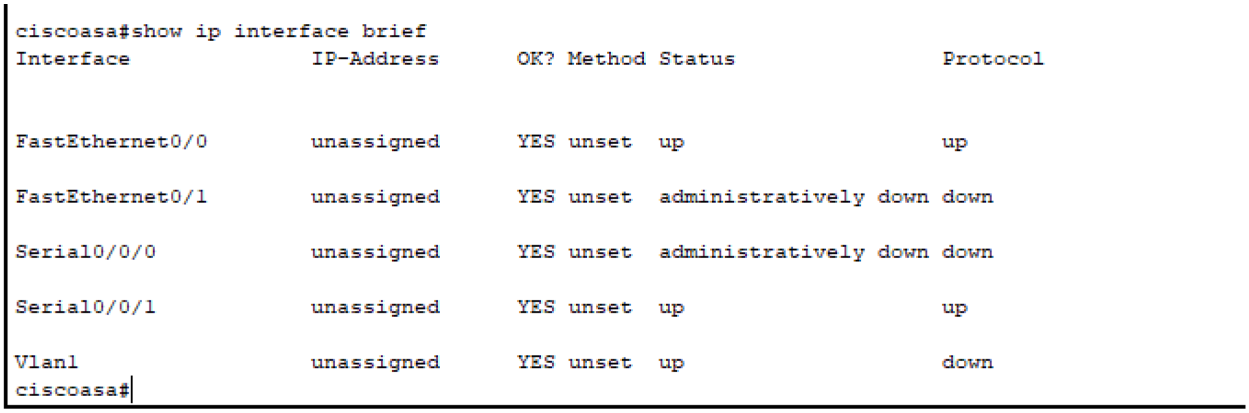
  Following is the Flash space used vs. available: **51193823 bytes used, 12822561 available, 64016384 total.**



```
ciscoasa#
ciscoasa#show flash

System flash directory:
File  Length   Name/status
  3   50938004 c2800nm-advipservicesk9-mz.124-15.T1.bin
  2   28282    sigdef-category.xml
  1   227537   sigdef-default.xml
[51193823 bytes used, 12822561 available, 64016384 total]
63488K bytes of processor board System flash (Read/Write)
```

- **How many and what types of interfaces does the device have?**

  The device has 5 interfaces: **2 Fast Ethernet, 2 Serial, and 1 VLAN interface.**



```
ciscoasa#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol


FastEthernet0/0        unassigned      YES unset  up                    up

FastEthernet0/1        unassigned      YES unset  administratively down down

Serial0/0/0            unassigned      YES unset  administratively down down

Serial0/0/1            unassigned      YES unset  up                    up

Vlan1                  unassigned      YES unset  up                    down
ciscoasa#
```

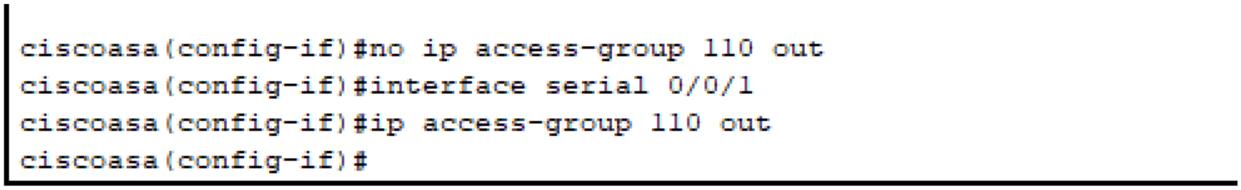
- **What is the difference between password and secret?**

  The difference between password and secret is that enabling password allows the user to access privileged levels of networking devices and enabling secret provides additional security layer over enable password command. Enable secret is more secure than enable password. Other difference is that the password is stored in plaintext while secret is stored as MD-5 hash.

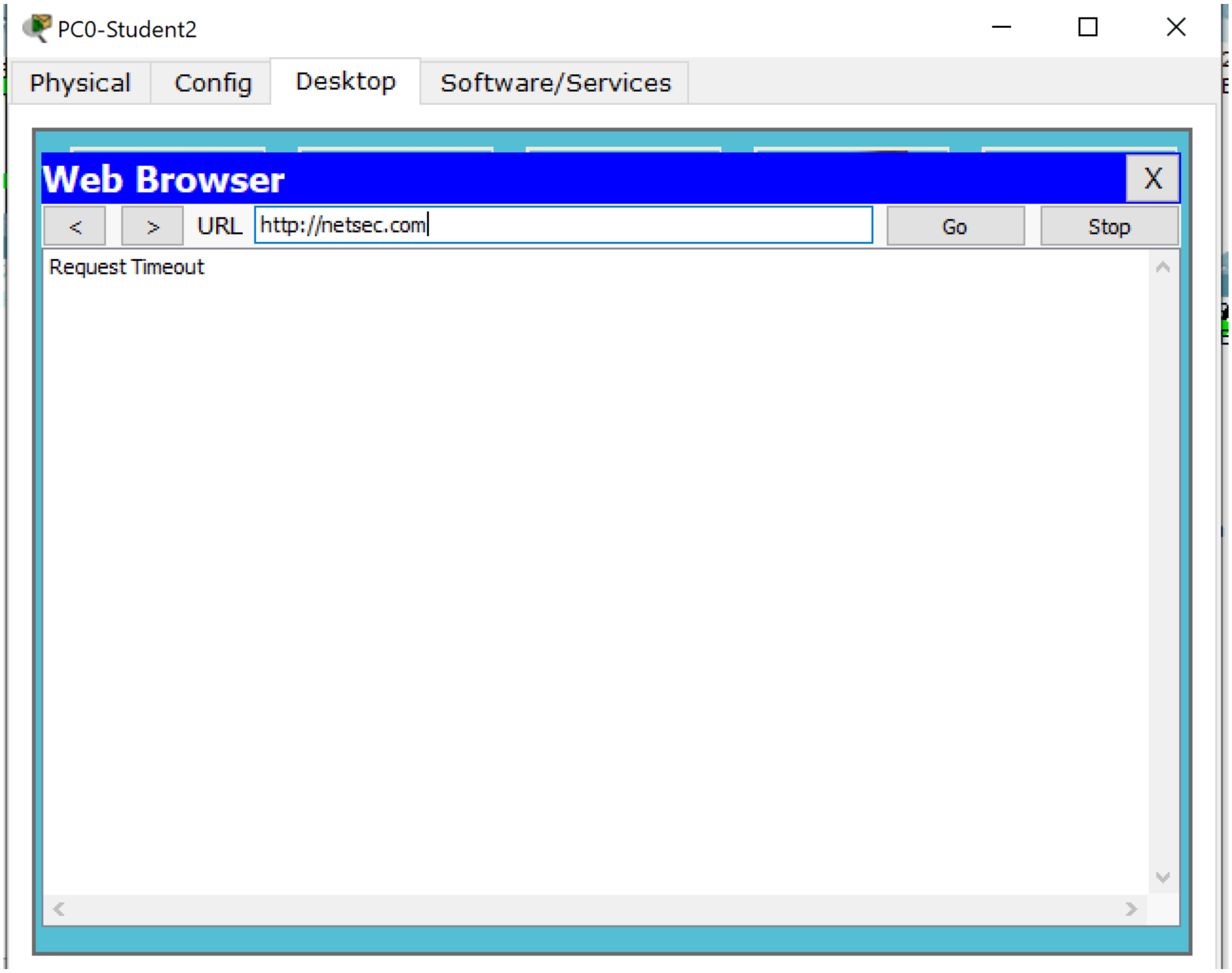
Restricting network traffic (ACLs):

- **Which combinations of interface & direction meets the required criteria of blocking HTTP traffic destined to WAN hosts?**

  The interface **Serial interface ip access-group out and Fastethernet 0/0 ip access-group in** meets the required criteria of blocking HTTP traffic destined to WAN hosts.



```
ciscoasa(config-if)#no ip access-group 110 out
ciscoasa(config-if)#interface serial 0/0/1
ciscoasa(config-if)#ip access-group 110 out
ciscoasa(config-if)#
```



http://netsec.com

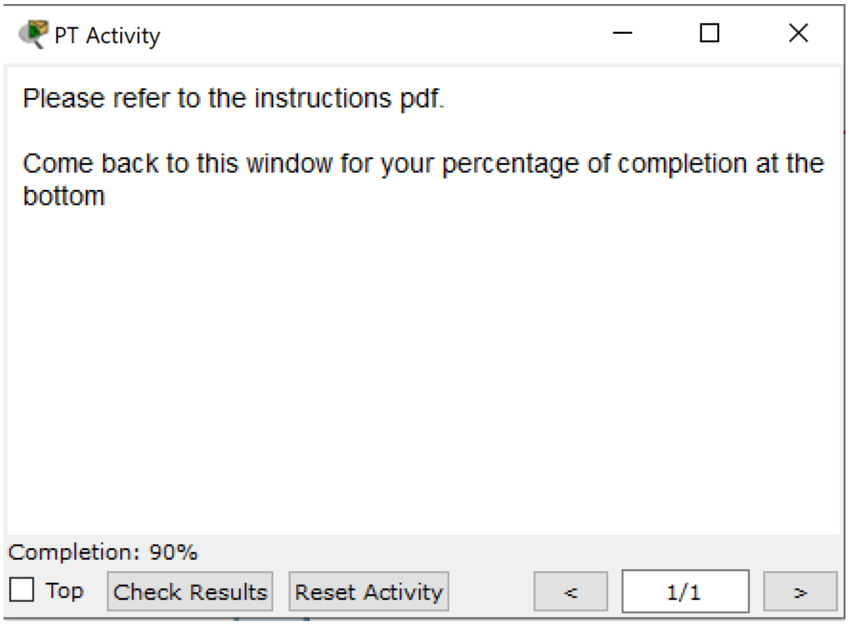
Request Timeout

Default deny stance:

- **Is FTP service listed as allowed in the ACL?**

  FTP service is not allowed in the ACL.

Screenshot of PT activity:



Please refer to the instructions pdf.

Come back to this window for your percentage of completion at the bottom

Completion: 90%

Start-up Configuration:

```
Using 2311 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname ciscoasa
!
!
!
enable password gohuskies
!
!
ip dhcp excluded-address 10.5.5.1 10.5.5.99
ip dhcp excluded-address 10.5.5.121 10.5.5.255
!
ip dhcp pool LAN
 network 10.5.5.0 255.255.255.0
 default-router 10.5.5.1
 dns-server 10.7.7.20
!
!
```

```
!
username adminssh password 0 adminssh01
!
!
!
!
!
ip domain-name netsec.com
!
!
spanning-tree mode pvst
!
!
!
!
interface FastEthernet0/0
 ip address 10.5.5.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/0/0
 no ip address
 clock rate 2000000
 shutdown
!
interface Serial0/0/1
 ip address 10.1.1.1 255.255.255.252
 ip access-group 115 out
 clock rate 2000000
!
interface Vlan1
 no ip address
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.1.1.2
!
!
```

```
access-list 110 deny tcp any any eq www
access-list 110 permit ip any any
access-list 100 permit icmp any any echo
access-list 100 permit icmp any any echo-reply
access-list 100 permit tcp any any eq www
access-list 100 permit tcp any any eq pop3
access-list 100 permit tcp any any eq smtp
access-list 100 permit udp any any eq domain
access-list 100 permit udp any eq bootpc any eq bootps
access-list 100 deny ip any any
access-list 120 deny tcp 10.5.5.100 0.0.0.3 host 10.7.7.11 eq www
access-list 120 permit icmp any any echo
access-list 120 permit icmp any any echo-reply
access-list 120 permit tcp any any eq www
access-list 120 permit tcp any any eq pop3
access-list 120 permit tcp any any eq smtp
access-list 120 permit udp any any eq domain
access-list 120 permit udp any eq bootpc any eq bootps
access-list 120 deny ip any any
access-list 115 permit tcp host 10.5.5.101 host 10.7.7.11 eq www
access-list 115 deny tcp 10.5.5.100 0.0.0.3 host 10.7.7.11 eq www
access-list 115 permit icmp any any echo
access-list 115 permit icmp any any echo-reply
access-list 115 permit tcp any any eq www
access-list 115 permit tcp any any eq pop3
access-list 115 permit tcp any any eq smtp
access-list 115 permit udp any any eq domain
access-list 115 permit udp any eq bootpc any eq bootps
access-list 115 deny ip any any
!
!
!
!
!
line con 0
line vty 0 4
 login local
 transport input ssh
!
!
!
end
```

Bonus (additional 5%) - Zone Based Firewall:

To create a Zone Based Firewall on the Border router, it was observed that Intranet is at interface Fastethernet 0/0, internet at Fastethernet 0/1 and DMZ at Fastethernet 1/0. Zones were created first, following the attaching of interfaces to the security zones. Zone-pairs were created with zone combinations, class maps were created to classify the traffic and policy maps were created to filter out the traffic. Class-map that specify access-list for intranet-internet connection was associated with zone-pair intranet-internet, similarly class-map that specify access-list for intranet-DMZ connection was associated with zone-pair intranet-DMZ and class-map that specify access-list for internet-DMZ connection was associated with zone-pair internet-DMZ. Access-lists in each class-map specified the protocols and rules. After access-list and class-map association, these class and default policies(drop, pass) were created according to the given problem. Following is the start-up configuration for the same:

```
Using 2691 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
!
!
!
!
!
!
!
!
!
!
!
!
!
spanning-tree mode pvst
!
class-map type inspect match-all inout-class
 match access-group name inout
class-map type inspect match-all outin-class
 match access-group name outin
class-map type inspect match-all indmz-class
 match access-group name indmz
```

```
class-map type inspect match-all outdmz-class
 match access-group name outdmz
!
policy-map type inspect inout-pmap
 class type inspect inout-class
  drop
 class type inspect class-default
  drop
!
policy-map type inspect outin-pmap
 class type inspect outin-class
  drop
 class type inspect class-default
  drop
!
policy-map type inspect outdmz-pmap
 class type inspect outdmz-class
  drop
 class type inspect class-default
  drop
!
policy-map type inspect indmz-pmap
 class type inspect indmz-class
  drop
 class type inspect class-default
  drop
!
!
!
zone security intranet
zone security internet
zone security dmz
zone-pair security indmz source intranet destination dmz
 service-policy type inspect indmz-pmap
zone-pair security inout source intranet destination internet
 service-policy type inspect inout-pmap
zone-pair security outdmz source internet destination dmz
 service-policy type inspect outdmz-pmap
zone-pair security outin source internet destination intranet
 service-policy type inspect outin-pmap
!
interface FastEthernet0/0
 ip address 10.0.1.2 255.255.255.0
 zone-member security intranet
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 10.0.2.1 255.255.255.0
 zone-member security internet
 duplex auto
 speed auto
!
interface FastEthernet1/0
 ip address 10.0.3.1 255.255.255.0
 zone-member security dmz
 duplex auto
 speed auto
!
interface Vlan1
 no ip address
 shutdown
!
ip classless
ip route 192.168.1.0 255.255.255.0 10.0.1.1
ip route 192.168.2.0 255.255.255.0 10.0.2.2
!
!
ip access-list extended inout
 permit icmp 192.168.1.0 0.0.0.255 any
 permit udp 192.168.1.0 0.0.0.255 any
 permit tcp 192.168.1.0 0.0.0.255 any
ip access-list extended outin
 permit icmp any 192.168.1.0 0.0.0.255 echo-reply
 permit tcp any 192.168.1.0 0.0.0.255 established
 permit udp any 192.168.1.0 0.0.0.255
ip access-list extended indmz
 permit tcp 192.168.1.0 0.0.0.255 10.0.3.0 0.0.0.255 eq www
 permit icmp 192.168.1.0 0.0.0.255 10.0.3.0 0.0.0.255
 permit icmp 10.0.3.0 0.0.0.255 192.168.1.0 0.0.0.255 echo-reply
 permit tcp 10.0.3.0 0.0.0.255 192.168.1.0 0.0.0.255
ip access-list extended outdmz
 permit tcp any 10.0.3.0 0.0.0.255 eq www
 permit tcp 10.0.3.4 0.0.0.25 any eq www
!
!
```

```
!
!
!
line con 0
line vty 0 4
 login
!
!
!
end
```

References:

[1]https://community.cisco.com/t5/security-documents/ios-zone-based-firewall-step-by-step-basic-configuration/ta-p/3142774