



Assessment I

Name: Syed Asghar Abbas Zaidi	Student ID: 07201
-------------------------------	-------------------

1 Objective

The Objectives of this lab are:

- Configure basic device hardening and secure network management
- Configure port security and disable unused switch ports
- Configure an IOS IPS
- Configure a Zone-based Policy Firewall (ZPF) to implement security policies

2 Background/Scenario

This culminating challenge includes many of the skills that you have acquired during this course. The routers and switches are preconfigured with the basic device settings, such as IP addressing and routing. You will use the CLI to configure various IOS features, such as device hardening, secure network management, and Zone-Based Policy Firewall (ZPF). Additionally, you will configure port security, disable unused switch ports, and implement an IOS IPS to strengthen network security.

3 Topology

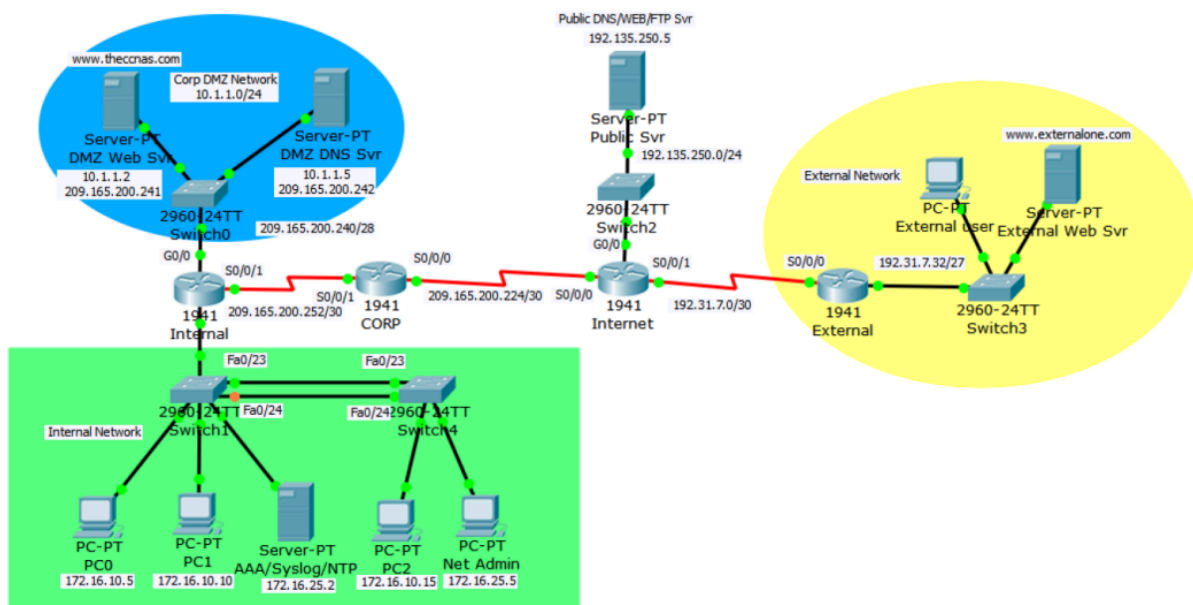


Figure 1: Topology

4 Addressing Table



Device	Interface	IP Address	Subnet Mask	Gateway	DNS Server
Internet	S0/0/0	209.165.200.225	255.255.255.252	N/A	
	S0/0/1	192.31.7.1	255.255.255.252	N/A	
	G0/0	192.135.250.1	255.255.255.0	N/A	
Public Svr	NIC	192.135.250.5	255.255.255.0	192.135.250.1	
External	S0/0/0	S0/0/0	255.255.255.252	N/A	
	G0/0	192.31.7.62	255.255.255.224	N/A	
External Web Svr	NIC	192.31.7.35	255.255.255.224	192.31.7.62	192.135.250.5
External User	NIC	192.31.7.33	255.255.255.224	192.31.7.62	192.135.250.5
CORP	S0/0/0	209.165.200.226	255.255.255.252	N/A	
	S0/0/1	209.165.200.254	255.255.255.252	N/A	
Internal	S0/0/1	209.165.200.253	255.255.255.252	N/A	
	G0/0	10.1.1.254	255.255.255.0	N/A	
	G0/1.10	172.16.10.254	255.255.255.0	N/A	
DMZ DNS Svr	NIC	10.1.1.5	255.255.255.0	10.1.1.254	192.135.250.5
DMZ Web Svr	NIC	10.1.1.2	255.255.255.0	10.1.1.254	10.1.1.5
PC0	NIC	172.16.10.5	255.255.255.0	172.16.10.254	10.1.1.5
PC1	NIC	172.16.10.10	255.255.255.0	172.16.10.254	10.1.1.5
AAA/NTP/Syslog Svr	NIC	172.16.25.2	255.255.255.0	172.16.25.254	10.1.1.5
PC2	NIC	172.16.10.15	255.255.255.0	172.16.10.254	10.1.1.5
Net Admin	NIC	172.16.25.5	255.255.255.0	172.16.25.254	10.1.1.5

Table 1: Addressing Table

Task 1: Configure Basic Device Hardening for the CORP and the Internal Routers.

- Configure the CORP and the Internal routers to only accept passwords with a minimum length of **10** characters.
- Configure an encrypted privileged level password of **ciscoclass**.
- Enable password encryption for all clear text passwords in the configuration file.
- Configure the console port and all vty lines with the following requirements:
Note: Both the CORP and the Internal routers are already configured with the username **CORPADMIN** and password **Ciscoccnas**.
 - Use the local database for login.
 - Disconnect after being idle for **20** minutes.
- Disable the CDP protocol on the CORP router on the link to the Internet router.

CORP:



```
CORP>
CORP>
CORP>en
CORP#config t
Enter configuration commands, one per line. End with CNTL/Z.
CORP(config)#security password min-length 10
CORP(config)#end
CORP#
%SYS-5-CONFIG_I: Configured from console by console
write memory
Building configuration...
[OK]
CORP#enable secret ciscoclass
CORP#
^
% Invalid input detected at '^' marker.

CORP#config t
Enter configuration commands, one per line. End with CNTL/Z.
CORP(config)#enable secret ciscoclass
CORP(config)#service password-encryption
CORP(config)#line console 0
CORP(config-line)#login local
CORP(config-line)#exec-timeout 20 0
CORP(config-line)#line vty 0 15
CORP(config-line)#exec-timeout 20 0
CORP(config-line)#exit
CORP(config)#s0/0/0
CORP(config)#
^
% Invalid input detected at '^' marker.

CORP(config)#int s0/0/0
CORP(config-if)#no cdp enable
```

INTERNAL:

```
Internal>en
Internal#config t
Enter configuration commands, one per line. End with CNTL/Z.
Internal(config)#security password min-length 10
Internal(config)#end
Internal#
%SYS-5-CONFIG_I: Configured from console by console
write memory
Building configuration...
[OK]
Internal#config t
Enter configuration commands, one per line. End with CNTL/Z.
Internal(config)#service password-encryption
Internal(config)#line console 0
Internal(config-line)#login local
Internal(config-line)#exec-timeout 20 0
Internal(config-line)#line vty 0 15
Internal(config-line)#login local
Internal(config-line)#exec-timeout 20 0
```

Task 2: Configure Secure Network Management for the CORP Router.

- Configure the IOS login enhancement for all vty lines with the following requirements:
 - Disable logins for **30** seconds after **3** failed login attempts within **60** seconds

```
CORP(config-if)#login block-for 30 attempts 3 within 60
```



Task 3: Configure Secure Network Management for the Internal Router.

- a. Configure the Internal router:
 - as an NTP client to the AAA/NTP/Syslog server
 - to update the router calendar (hardware clock) from the NTP time source
 - to timestamp log messages
 - to send logging messages to the AAA/NTP/Syslog server
- b. Configure the IOS login enhancement for all vty lines with the following requirements:
 - Disable logins for **30** seconds after **3** failed login attempts within **60** seconds.
 - Log any failed or successful login to the syslog server.
- c. Configure the Internal router to accept SSH connections. Use the following guidelines:

Note: Internal is already configured with the username **SSHAccess** and the secret password **ciscosshaccess**.

 - The domain name is **theccnas.com**.
 - RSA encryption key pair using a modulus of **1024**
 - SSH version **2**, timeout of **90** seconds, and **2** authentication retries
 - All vty lines accept only SSH connections.
- d. Configure the Internal router with server-based AAA authentication and verify its functionality:

Note: The AAA server is already configured with RADIUS service, a username **CORPSYS**, and the password **LetSysIn**.

 - The key to connect to the RADIUS server is **corpradius**.
 - AAA authentication uses the RADIUS server as the default for console line and vty lines access.
 - The local database is used as the backup if the RADIUS server connection cannot be established



```
Internal(config)#ntp server 172.16.25.2
Internal(config)#ntp update-calendar
Internal(config)#service timestamps log datetime msec
Internal(config)#logging host 172.16.25.2
Internal(config)#login block-for 30 attempts 3 within 60
Internal(config)#login block-for 30 attempts 3 within 60
Internal(config)#login on-failure log
Internal(config)#login on-success log
Internal(config)#ip domain-name theccnas.com
Internal(config)#crypto key generate rsa
The name for the keys will be: Internal.theccnas.com
Choose the size of the key modulus in the range of 360 to 4096 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

Internal(config)#ip ssh version 2
*Oct 18 11:0:12.25: %SSH-5-ENABLED: SSH 1.99 has been enabled
Internal(config)#ip ssh time-out 90
Internal(config)#ip ssh authentication-retries 2
Internal(config)#line vty 0 15
Internal(config-line)#transport input ssh
Internal(config-line)#exit
Internal(config)#aaa new-model
Internal(config)#radius-server host
% Incomplete command.
Internal(config)#radius-server host 172.16.25.2 key corpradius
Internal(config)#

Internal>en
Internal#config t
Enter configuration commands, one per line. End with CNTL/Z.
Internal(config)#aaa authentication login default group radius local
Internal(config)#line console 0
Internal(config-line)#login authentication default
Internal(config-line)#line vty 0 15
Internal(config-line)#login authentication default
Internal(config-line)#|
```

Task 4: Configure ACLs on the Internal Router to Implement Secure Management Access.

- Create ACL 12 to implement the security policy regarding the access to the vty lines:
 - Only users logged on to the Net Admin PC are allowed access to the vty lines.

```
Internal(config)#access-list 12 permit host 172.16.25.5
Internal(config)#line vty 0 15
Internal(config-line)#access-class 12 in
Internal(config-line)#|
```

Task 5: Configure Device Hardening for Switch1 and Switch4

- Access Switch1 and Switch4 with username **CORPADMIN**, password **Ciscoccnas**, and the enable secret password of **ciscoclass**.
- Configure Switch1 to protect against STP attacks.
 - Configure PortFast on FastEthernet ports 0/1 to 0/22.



- Enable BPDU guard on FastEthernet ports 0/1 to 0/22.
- c. Configure Switch1 port security and disable unused ports.
 - Set the maximum number of learned MAC addresses to **2** on FastEthernet ports 0/1 to 0/22. Allow the MAC address to be learned dynamically and to be retained in the running-config. Shutdown the port if a violation occurs.
 - Disable unused ports (Fa0/2-4, Fa0/6-10, Fa0/13-22).
- d. Configure the trunk link on Fa0/23 and Fa0/24 on both Switch1 and Switch4
 - Disable DTP negotiation on the trunking ports.
 - Set the native VLAN as VLAN 50 for the trunk links.

Switch 1:

Cause of so many fastport messages, my previous commands got drowned, but basically i did this
configure terminal
interface range fastEthernet0/1-22
spanning-tree portfast
(and then I was getting this output, and for rest, screenshots are attached as normal)

```
Switch1
Physical Config CLI Attributes
IOS Command Line Interface

host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/9 but will only
have effect when the interface is in a non-trunking mode.
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/10 but will only
have effect when the interface is in a non-trunking mode.
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/11 but will only
have effect when the interface is in a non-trunking mode.
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/12 but will only
have effect when the interface is in a non-trunking mode.
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/13 but will only
have effect when the interface is in a non-trunking mode.
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/14 but will only
have effect when the interface is in a non-trunking mode.
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/15 but will only
have effect when the interface is in a non-trunking mode.
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
```



Switch1

Physical Config CLI Attributes

```
%Portfast has been configured on FastEthernet0/16 but will only
have effect when the interface is in a non-trunking mode.
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/17 but will only
have effect when the interface is in a non-trunking mode.
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/18 but will only
have effect when the interface is in a non-trunking mode.
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/19 but will only
have effect when the interface is in a non-trunking mode.
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/20 but will only
have effect when the interface is in a non-trunking mode.
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/21 but will only
have effect when the interface is in a non-trunking mode.
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/22 but will only
have effect when the interface is in a non-trunking mode.
Switch1(config-if-range)#spanning-tree bpduguard enable
Switch1(config-if-range)#int range f0/1 - 22
Switch1(config-if-range)#switchport port-security
Switch1(config-if-range)#switchport port-security maximum 2
Switch1(config-if-range)#switchport port-security mac-address sticky
Switch1(config-if-range)#switchport port-security violation shutdown
```



```
Switch1(config-if-range)#exit
Switch1(config)#int range f0/2-4,f0/6-10,f/13-22
                                     ^
% Invalid input detected at '^' marker.

Switch1(config)#int range f0/2-4,f0/6-10,f0/13-22
Switch1(config-if-range)# shutdown

%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/7, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/8, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/9, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/10, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/13, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/14, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/15, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/16, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/17, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/18, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/19, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/20, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/21, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/22, changed state to administratively down
Switch1(config-if-range)#exit
Switch1(config)#int range f0/23-24
Switch1(config-if-range)#switchport mode trunk
```




```
Switch1
Physical Config CLI Attributes
IOS Command Line Interface

Switch1(config-if-range)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/23, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/23, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/24, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/24, changed state to up
Switch1(config-if-range)#switchport nonnegotiate
^
% Invalid input detected at '^' marker.

Switch1(config-if-range)#switchport nonegotiate
Switch1(config-if-range)#exit
Switch1(config)#vlan 50
Switch1(config-vlan)#int range f0/23-24
Switch1(config-if-range)#switchport mode trunk
Switch1(config-if-range)#no switchport mode trunk
Command rejected: An interface must be configured to the Access or Trunk modes to be configured to NoNegotiate.
Command rejected: An interface must be configured to the Access or Trunk modes to be configured to NoNegotiate.
Switch1(config-if-range)#switchport trunk native vlan 50
Switch1(config-if-range)#
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/23 (50), with Switch4 FastEthernet0/23 (1).
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/24 (50), with Switch4 FastEthernet0/24 (1).
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/23 (50), with Switch4 FastEthernet0/23 (1).
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/24 (50), with Switch4 FastEthernet0/24 (1).
%SPANTREE-2-RECV_PVID_ERR: Received BPDU with inconsistent peer vlan id 1 on FastEthernet0/23 VLAN50.
%SPANTREE-2-BLOCK_PVID_LOCAL: Blocking FastEthernet0/23 on VLAN0050. Inconsistent local vlan.
%SPANTREE-2-RECV_PVID_ERR: Received BPDU with inconsistent peer vlan id 1 on FastEthernet0/24 VLAN50.
%SPANTREE-2-BLOCK_PVID_LOCAL: Blocking FastEthernet0/24 on VLAN0050. Inconsistent local vlan.

%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/23 (50), with Switch4 FastEthernet0/23 (1).
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/24 (50), with Switch4 FastEthernet0/24 (1).
%SPANTREE-2-UNBLOCK_CONSIST_PORT: Unblocking FastEthernet0/23 on VLAN0001. Port consistency restored.
%SPANTREE-2-UNBLOCK_CONSIST_PORT: Unblocking FastEthernet0/23 on VLAN0050. Port consistency restored.
%SPANTREE-2-UNBLOCK_CONSIST_PORT: Unblocking FastEthernet0/24 on VLAN0001. Port consistency restored.
%SPANTREE-2-UNBLOCK_CONSIST_PORT: Unblocking FastEthernet0/24 on VLAN0050. Port consistency restored.
```

Switch 4:



```
Switch4
Physical Config CLI Attributes
IOS Command Line Interface

User Access Verification
Username:
Username: CORPADMIN
Password:

Switch4>en
Password:
Switch4#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch4(config)#int range f0/23-24
Switch4(config-if-range)#switchport mode trunk

Switch4(config-if-range)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/23, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/23, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/24, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/24, changed state to up
%SPANTREE-2-RECV_FVID_ERR: Received BPDU with inconsistent peer vlan id 50 on FastEthernet0/23 VLAN1.
%SPANTREE-2-BLOCK_FVID_LOCAL: Blocking FastEthernet0/23 on VLAN0001. Inconsistent local vlan.
%SPANTREE-2-RECV_FVID_ERR: Received BPDU with inconsistent peer vlan id 50 on FastEthernet0/24 VLAN1.
%SPANTREE-2-BLOCK_FVID_LOCAL: Blocking FastEthernet0/24 on VLAN0001. Inconsistent local vlan.

%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/23 (1), with Switch1 FastEthernet0/23 (50).
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/24 (1), with Switch1 FastEthernet0/24 (50).
switchport mode trunk
Switch4(config-if-range)#switchport mode trunk
Switch4(config-if-range)#
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/23 (1), with Switch1 FastEthernet0/23 (50).
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/24 (1), with Switch1 FastEthernet0/24 (50).

Switch4(config-if-range)#switchport nonegotiate
Switch4(config-if-range)#exit
Switch4(config)#vlan 50
Switch4(config-vlan)#int range f0/23-24
Switch4(config-if-range)#switchport trunk native vlan 50
Switch4(config-if-range)##SPANTREE-2-UNBLOCK_CONSIST_PORT: Unblocking FastEthernet0/23 on VLAN0050. Port consistency restored.
%SPANTREE-2-UNBLOCK_CONSIST_PORT: Unblocking FastEthernet0/23 on VLAN0001. Port consistency restored.
```

Task 6: Configure an IOS IPS on the Internal Router.

- On the Internal router, if asked to login, then login as **CORPSYS** with password **LetSysIn**. The enable secret password is **ciscoclass**.
- Use the IPS signature storage location at **flash:**.
- Create an IPS rule named **corpips**.
- Configure the IOS IPS to use the signature categories. Retire the **all** signature category and unretire the **ios_ips basic** category.
- Apply the IPS rule to the Gi0/0 interface in the **out** direction.
- Modify the **ios_ips basic** category. Unretire the **echo request** signature (signature **2004**, subsig **0**); **enable** the signature; modify the signature **event-action** to produce an alert and deny packets that match the signature.



```
User Access Verification
Username: CORPSYS
Password:
% Login invalid

Username:
*Oct 18, 12:15:03.1515: SEC_LOGIN-5-LOGIN_FAILED: Login failed [user: CORPSYS] [Source: 0.0.0.0] [localport: 0] [Reason: Login Authentication Failed] at 12:15:03 UTC Thu Oct 18 2018

Username: CORPSYS
Password:
Internally
*Oct 18, 12:15:24.1515: SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: CORPSYS] [Source: 0.0.0.0] [localport: 0] at 12:15:24 UTC Thu Oct 18 2018

Internal>en
Internal#conf term
Enter configuration commands, one per line. End with CNTL/Z.
Internal(config)#ip ips config location flash:
Internal(config)#ip ips name corpips
Internal(config)#
Internal(config)#ip ips signature-category
Internal(config-ips-category)#category all
Internal(config-ips-category)#category all
Internal(config-ips-category-action)#retired true
Internal(config-ips-category-action)#exit
Internal(config-ips-category)#category ios ips basic
Internal(config-ips-category)#category ios ips basic
^
% Invalid input detected at '^' marker.

Internal(config-ips-category)#category ios ips basic
Internal(config-ips-category-action)#retired false
Internal(config-ips-category-action)#exit
Internal(config-ips-category)#exit
Do you want to accept these changes? [confirm]
Applying Category configuration to signatures ...
%IPS-6-ENGINE_BUILDING: atomic-ip - 288 signatures - 6 of 13 engines
%IPS-6-ENGINE_READY: atomic-ip - build time 30 ms - packets for this engine will be scanned




Internal(config)#int g0/0
Internal(config-if)#ip ips corpips
% Incomplete command.
Internal(config-if)#ip ips corpips out
Internal(config-if)#
*Oct 18, 12:17:50.1717: %IPS-6-ENGINE_BUILDS_STARTED: 12:17:50 UTC Oct 18 2018
*Oct 18, 12:17:50.1717: %IPS-6-ENGINE_BUILDING: atomic-ip - 3 signatures - 1 of 13 engines
*Oct 18, 12:17:50.1717: %IPS-6-ENGINE_READY: atomic-ip - build time 8 ms - packets for this engine will be scanned
*Oct 18, 12:17:50.1717: %IPS-6-ALL_ENGINE_BUILDS_COMPLETE: elapsed time 8 ms
Internal(config-if)#exit
Internal(config)#ip ips signature-definition
Internal(config-sigdef)#signature 2004 0
Internal(config-sigdef-sig)#status
Internal(config-sigdef-sig-status)#retired false
Internal(config-sigdef-sig-status)#enabled true
Internal(config-sigdef-sig-status)#exit
Internal(config-sigdef-sig)#event-action produce-alert
^
% Invalid input detected at '^' marker.

Internal(config-sigdef-sig)#engine
Internal(config-sigdef-sig-engine)#event-action produce-alert
Internal(config-sigdef-sig-engine)#event-action deny-packet-inline
Internal(config-sigdef-sig-engine)#exit
Internal(config-sigdef-sig)#exit
Internal(config-sigdef)#exit
Do you want to accept these changes? [confirm]
%IPS-6-ENGINE_BUILDS_STARTED:
%IPS-6-ENGINE_BUILDING: atomic-ip - 303 signatures - 3 of 13 engines
%IPS-6-ENGINE_READY: atomic-ip - build time 480 ms - packets for this engine will be scanned
%IPS-6-ALL_ENGINE_BUILDS_COMPLETE: elapsed time 648 ms

Internal(config)#
```

- g. Verify that IPS is working properly. Net Admin in the internal network cannot ping DMZ Web Svr. DMZ Web Svr, however, can ping Net Admin.

Attach ping results below:

Fire	Last Status	Source	Destination	Type
	Failed	Net Admin	DMZ Web Svr	ICMP
	Failed	Net Admin	DMZ Web Svr	ICMP
	Failed	Net Admin	DMZ Web Svr	ICMP



Task 7: Configure ZPF on the CORP Router.

- a. Access the CORP router with username **CORPADMIN**, password **Ciscoccnas**, and the enable secret password of **ciscoclass**.
- b. Create the firewall zones.
 - Create an internal zone named **CORP-INSIDE**.
 - Create an external zone named **INTERNET**.
- c. Define a traffic class to allow traffic from the Internal network to access services in the Internet.
 - Create a class map using the option of **class map type inspect** with the **match-any** keyword. Name the class map **INSIDE_PROTOCOLS**.
 - Match the protocols, **http, tcp, udp, icmp, dns** Specify firewall policies to allow internal hosts to access Internet.
 - Create a policy map named **INSIDE_TO_INTERNET**.
 - Use the **INSIDE_PROTOCOLS** class map.
 - Specify the action of **inspect** for this policy map.
- d. Define a traffic class to allow traffic from the Internet to access services in the DMZ network.
 - Create a class map using the option of **class map type inspect** with the **match-any** keyword. Name the class map **DMZ_WEB**.
 - Match the protocols, **http** and **dns**
- e. Specify firewall policy to allow Internet traffic to access DMZ services.
 - Create a policy map named **INTERNET_TO_DMZWEB**.
 - Use the **DMZ_WEB** class map.
 - Specify the action of **pass** for this policy map.
- f. Apply the firewall.
 - Create a pair of zones named **IN_TO_OUT_ZONE** with the source as **CORP-INSIDE** and destination as **INTERNET**.
 - Specify the policy map **INSIDE_TO_INTERNET** for handling the traffic between the two zones.
 - Create a pair of zones named **INTERNET_TO_DMZ_ZONE** with the source as **INTERNET** and destination as **CORP-INSIDE**.
 - Assign interfaces to the appropriate security zones.



```
CORP
Physical Config CLI Attributes

User Access Verification
Username: CORPADMIN
Password:

CORP>en
Password:
CORP#conf term
Enter configuration commands, one per line. End with CNTL/Z.
CORP(config)#zone security CORP-INSIDE
CORP(config-sec-zone)#exit
CORP(config)#zone security INTERNET
CORP(config-sec-zone)#class-map type inspect match-any INSIDE_PROTOCOLS
CORP(config-cmap)#match protocol http
CORP(config-cmap)#match protocol tcp
CORP(config-cmap)#match protocol udp
CORP(config-cmap)#match protocol icmp
CORP(config-cmap)#match protocol dns
CORP(config-cmap)#exit
CORP(config)#policy-map type inspect INSIDE_TO_INTERNET
CORP(config-pmap)#class type inspect INSIDE_PROTOCOLS
CORP(config-pmap-c)#inspect
CORP(config-pmap-c)#exit
CORP(config-pmap)#exit
CORP(config)#class-map type inspect match-any DMZ_WEB
CORP(config-cmap)#match protocol http
CORP(config-cmap)#match protocol dns
CORP(config-cmap)#exit
CORP(config)#policy-map type inspect INTERNET_TO_DMZWEB
CORP(config-pmap)#class type inspect DMZ_WEB
CORP(config-pmap-c)#pass
CORP(config-pmap-c)#exit
CORP(config-pmap)#exit
CORP(config)#zone-pair security IN_TO_OUT source CORP-INSIDE destination INTERNET
CORP(config-sec-zone-pair)#service-policy type inspect INSIDE_TO_INTERNET
CORP(config-sec-zone-pair)#exit
CORP(config)#zone-pair security INTERNET_TO_DMZ_ZONE source INTERNET destination CORP-INSIDE
CORP(config-sec-zone-pair)#service-policy type inspect INTERNET_TO_DMZWEB
CORP(config-sec-zone-pair)#exit
CORP(config)#int s0/0/0
CORP(config-if)#zone-member security INTERNET
CORP(config-if)#int s0/0/1
CORP(config-if)#zone-member security CORP-INSIDE
CORP(config-if)#
CORP(config-if)#
```

g. Verify the ZPF configuration.

- The External user can access the URLs <http://www.theccnas.com> and <http://www.externalone.com>.

CAN'T VERIFY CAUSE I DON'T HAVE ACCESS TO WEB BROWSER. UNLIKE PING






WHICH I CAN DO DIRECTLY THROUGH PDU WINDOW!

- The External user cannot ping the DMZ Web Svr.

Fire	Last Status	Source	Destination	Type
	Failed	External user	DMZ Web Svr	ICMP
	Failed	External user	DMZ Web Svr	ICMP
	Failed	External user	DMZ Web Svr	ICMP

- The PCs in the internal network can ping and access the External Web Svr URL.

Fire	Last Status	Source	Destination	Type
	Successful	PC0	External Web Svr	ICMP
	Successful	PC0	External Web Svr	ICMP
	Successful	PC0	External Web Svr	ICMP

PT Activity: 02:26:49

Cryptography and Network Security - Assessment I

In this practice Packet Tracer Skills Based Assessment, you will:

- configure basic device hardening and secure network management
- configure port security and disable unused switch ports
- configure an IOS IPS
- configure a Zone-based Policy Firewall (ZPF) to implement security policies

Topology

Time Elapsed: 02:26:49

Completion: 88%

☐ Top ☐ Dock 1/1



Assessment Rubric
Assessment I - Skills Integration Challenge I

Name: Syed Asghar Abbas Zaidi	Student ID: 07201
--------------------------------------	--------------------------

Points Distribution

Task No.	LR 2 Simulation	LR5 Results/Plots	LR9 Report
Task 1	10		
Task 2	5		
Task 3	10		
Task 4	10		
Task 5	10		
Task 6	10	/5	
Task 7	20	/10	
Total	/75	/15	/10
CLO Mapped	CLO 1-4	CLO 1-4	CLO 1-4

CLO	Total Points	Points Obtained
1-4	100	100
Total	100	

For description of different levels of the mapped rubrics, please refer the provided Lab Evaluation Assessment Rubrics and Affective Domain Assessment Rubrics.



Lab Evaluation Assessment Rubric

#	Assessment Elements	Level 1: Unsatisfactory Points 0-1	Level 2: Developing Points 2	Level 3: Good Points 3	Level 4: Exemplary Points 4
LR2	Program/Code / Simulation Model/ Network Model	Program/code/simulation model/network model does not implement the required functionality and has several errors. The student is not able to utilize even the basic tools of the software.	Program/code/simulation model/network model has some errors and does not produce completely accurate results. Student has limited command on the basic tools of the software.	Program/code/simulation model/network model gives correct output but not efficiently implemented or implemented by computationally complex routine.	Program/code/simulation /network model is efficiently implemented and gives correct output. Student has full command on the basic tools of the software.
LR5	Results & Plots	Figures/ graphs / tables are not developed or are poorly constructed with erroneous results. Titles, captions, units are not mentioned. Data is presented in an obscure manner.	Figures, graphs and tables are drawn but contain errors. Titles, captions, units are not accurate. Data presentation is not too clear.	All figures, graphs, tables are correctly drawn but contain minor errors or some of the details are missing.	Figures / graphs / tables are correctly drawn and appropriate titles/captions and proper units are mentioned. Data presentation is systematic.
LR9	Report	All the in-lab tasks are not included in report and / or the report is submitted too late.	Most of the tasks are included in report but are not well explained. All the necessary figures / plots are not included. Report is submitted after due date.	Good summary of most the in-lab tasks is included in report. The work is supported by figures and plots with explanations. The report is submitted timely.	Detailed summary of the in-lab tasks is provided. All tasks are included and explained well. Data is presented clearly including all the necessary figures, plots and tables.