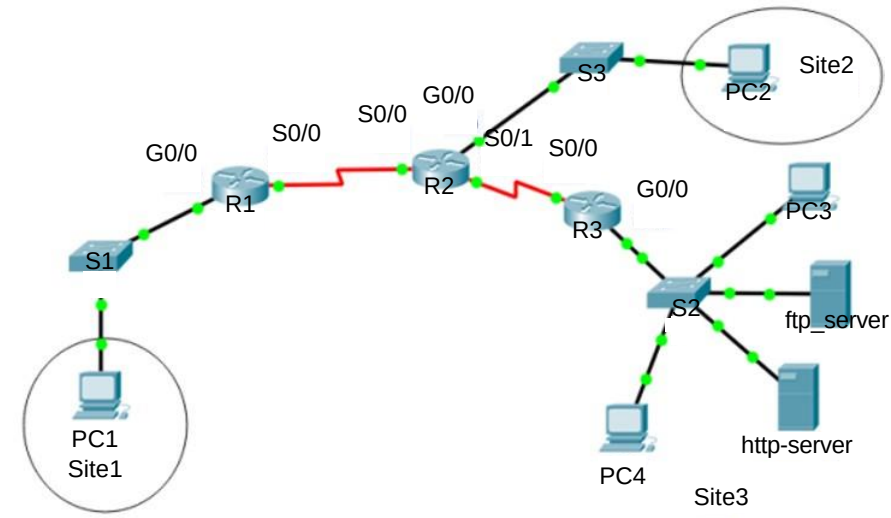
Exercises for application

EXERCISE 6.–

Topology



For a color version of this figure, see www.iste.co.uk/sadiqui/computer.zip

Addressing table

Device	Interface	IP address	Subnet mask	Gateway
R1	G0/0	192.168.0.1	/24	–
	S0/0	192.168.100.1	/30	–
R2	G0/0	192.168.1.1	/24	–
	S0/0	192.168.100.2	/30	–
	S0/1	192.168.200.1	/30	–
R3	G0/0	192.168.2.1	/24	–
	S0/0	192.168.200.2	/30	–
PC1	NIC	192.168.0.2	/25	192.168.0.1
PC2	NIC	192.168.1.2	/26	192.168.1.1
PC3	NIC	192.168.2.4	/24	192.168.2.1
PC4	NIC	192.168.2.5	/24	192.168.2.1
ftp_server	NIC	192.168.2.2	/24	192.168.2.1
http-server	NIC	192.168.2.3	/24	192.168.2.1

Objectives

– Securing passwords;

– configuring an IPv4 ACL;

– configuring an IPv6 ACL.

Software to be used

Packet tracer.

Part A: establishing the basic device configuration.

1. Configure the basic device settings.

1.1. Configure the host names as shown in the topology.

1.2. Apply the IP addresses to the device interfaces according to the addressing table.

1.3. Set the clock value to 128 000 for the serial interface.

2. Configure the routing using the OSPF protocol.

2.1. Enable OSPF on both routers using the value 1 as the process ID.

2.2. Set the RID value to 1.1.1.1 for R1, 2.2.2.2 for R2 and 3.3.3.3 for R3.

2.3. Add all networks to the OSPF protocol.

2.4. Test connectivity between all network elements.

Part B: securing passwords

1. Set a minimum password length of 8 characters.

2. Set the password "Ci$c0ena" for the privileged mode.

3. Configure the console, auxiliary ports and virtual access lines.

3.1. Set "Ci$c0con" as the console port password and set the inactivity interval to 5 minutes.

3.2. Set "Ci$c0vty" as the password on the VTY lines and set the inactivity interval to 2 minutes.

3.3. Disable the auxiliary port.

4. Encrypt all passwords;

R1(config)# **service password-encryption**

Part C: configuring an IPv4 ACL

1. Review the valid range of numbers for numbered extended ACLs.

……

2. On R3, create a numbered extended ACL that authorizes access to the http-server from station PC1. To do this create an ACL with the following options:

– the extended list number is **100**

– the action to be defined is **permit**;

– the protocol to be used is **TCP**;

– the source is a **host** with the IP address **192.168.0.2** (PC1);

– the destination is a **host** with the IP address **192.168.2.2** (http-server);

– the port to be used is **80**.

Write the ACL to be used:

……

3. Add a rule to the extended ACL already created to allow denial of access to the http-server from the "site 2" network. To do this, configure ACL 100 with the following options:

– the action to be defined is **deny**;

– the protocol to be used is **TCP**;

– the source is **network** with the network address **192.168.1.0 / 26** (site 2);

– the **generic mask** is obtained by subtracting mask 255.255.255.255 from the network mask:

255.255.255.255 – 255.255.255.192 = **0.0.0.63**

– the destination is a **host** with the IP address **192.168.2.3** (http-server);

– the port to be used is **80**.

Write the command to be used:

.....

4. Add a rule to the previous ACL allowing all IP traffic with the http-server. To do this, configure the ACL 100 with the following options:

– the action to be defined is **permit**;

– the protocol to be used is **IP**;

– the source to be used is **any**;

– the destination is a **host** with the IP address **192.168.2.3** (http-server).

Write the command to be used:

.....

5. Add a rule to the previous ACL allowing the denial of ICMP traffic between PC1 and PC4. To do this, configure ACL 100 with the following options:

– the action to be defined is **permit**;

– the protocol to be used is **ICMP**;

– the source to use is a **host** with the IP address **192.168.0.2** (PC1);

– the destination is a **host** with the IP address **192.168.2.4** (PC4).

Write the command to be used:

.....

6. Apply the access control list 100 to the G0/0. / 0 interface.

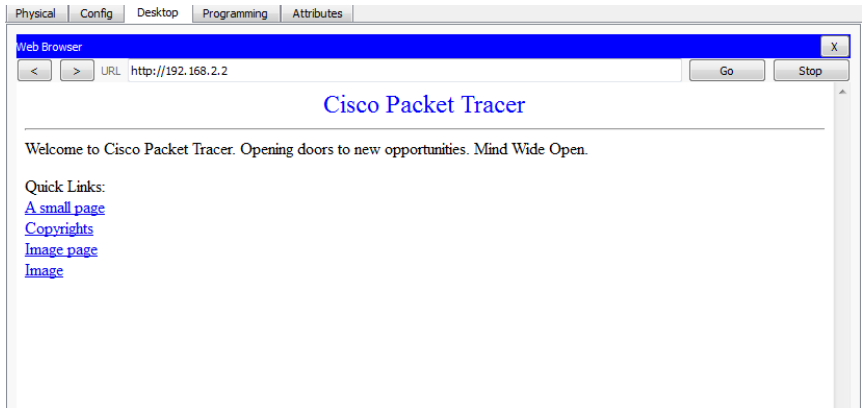
Write the command to be used:

.....

NOTE.– As a general rule, extended ACLs should be placed near the source. However, as ACL 100 affects traffic coming from two networks, “Site 1” and “Site 2”, the best placement would be on the output of interface G0/0.

7. Test the ACL created previously.

– Check that it is possible to access the **http** service from **PC1**.



– Check that the **http** service cannot be accessed from **PC2**.

– Check that it is possible to send a **ping** request to **http-server** from **PC2**.

– Check that it is not possible to send a **ping** request to **PC3** from **PC1**.

– Check that it is possible to send a **ping** request to **PC4** from **PC1.**

8. Delete the created ACL.

R3(config)#**no access-list 100**

9. On R3, create and test an extended ACL named "ACL_HTTP" which makes it possible to fulfil the security requirements stated earlier.

9.1. Create the extended ACL.

R3(config)#**ip access-list extended ACL_HTTP**
R3(config-ext-nacl)#

9.2. Allow http access from PC1 to http-server

R3(config-ext-nacl)# **permi tcp host 192.168.0.2 host 192.168.2.3 eq www**

9.3. Block http traffic from network “site 2” to the http-server.

R3(config-ext-nacl)# **deny tcp 192.168.1.0 0.0.0.63 host 192.168.2.3 eq www**

9.4. Allow all IP traffic with the http-server.

R3(config-ext-nacl)#**permit ip any host 192.168.2.3**

9.5. Display the ACL_HTTP ACL rules.

R3#**sh IP access-lists ACL_HTTP**

9.6. Applying the ACL_HTTP ACL to the G0/0. / 0 interface.

R3#**IP access-group ACL_HTTP out**

9.7. Test the effect of ACL_HTTP ACL.

10. On R3, create an extended ACL named “ACL_FTP” which makes it possible to fulfil the following security requirements:

– allow **ftp** access from **PC2** to **ftp_server**;

– block **ftp** traffic from “site 1” network to **ftp_server_http**;

– allow all **IP** traffic with **ftp_server**.

10.1. Display the ACL_FTP ACL rules.

10.2. Apply the ACL_FTP ACL to the G0/ 0 interface.

10.3. Test the effect of the ACL_FTP ACL.

PC2:\>**ftp 192.168.2.3**
Trying to connect...192.168.2.3
Connected to 192.168.2.3
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:**** (cisco)
230- Logged in
(passive mode On)
ftp>

Part D: configuring an IPv6 ACL

IPv6 addressing table

Device	Interface	IP address	Gateway
R1	G0/0	2001:DB8:AAAA:A::1/64	–
	S0/0	2001:DB8:AAAA:D::1/64	–
R2	G0/0	2001:DB8:AAAA:B::1/64	–
	S0/0	2001:DB8:AAAA:D::2/64	–
	S0/1	2001:DB8:AAAA:E::1/64	–
R3	G0/0	2001:DB8:AAAA:C::1/64	–
	S0/0	2001:DB8:AAAA:E::2/64	–
PC1	NIC	2001:DB8:AAAA:A::2/64	FE80::1
PC2	NIC	2001:DB8:AAAA:B::2/64	FE80::1
PC3	NIC	2001:DB8:AAAA:C::4/64	FE80::1
PC4	NIC	2001:DB8:AAAA:C::5/64	FE80::1
ftp_server	NIC	2001:DB8:AAAA:C::2/64	FE80::1
http-server	NIC	2001:DB8:AAAA:C::3/64	FE80::1

1. Create a new template with the same topology as in the previous exercise

2. Configure the basic parameters on R1, R2 and R3.

2.1. Configure the host name as indicated in the topology.

2.2. Apply the IP addresses to the router's interfaces according to the addressing table.

NOTE.– The local link addresses of the routers will be set to FE80: 1/64.

2.3. Set the clock value to 128 000 for the serial interface.

3. Configure the routing using the OSPF protocol.

3.1. Enable OSPF on both routers using the value 1 as the process ID.

3.2. Set the RID to 1.1.1.1 for R1, to 2.2.2.2 for R2 and to 3.3.3.3 for R3.

3.3. Add all networks to the OSPF protocol.

3.4. Test connectivity between all network elements.

4. On R3, create and activate an extended ACL named "ACL_HTTP" which makes it possible to meet all the security requirements defined in Part 1.

Write the command to be used:

……

……

……

5. On R3, create an extended ACL called "ACL_FTP" which makes it possible to meet the security requirements defined in Part 1.

……

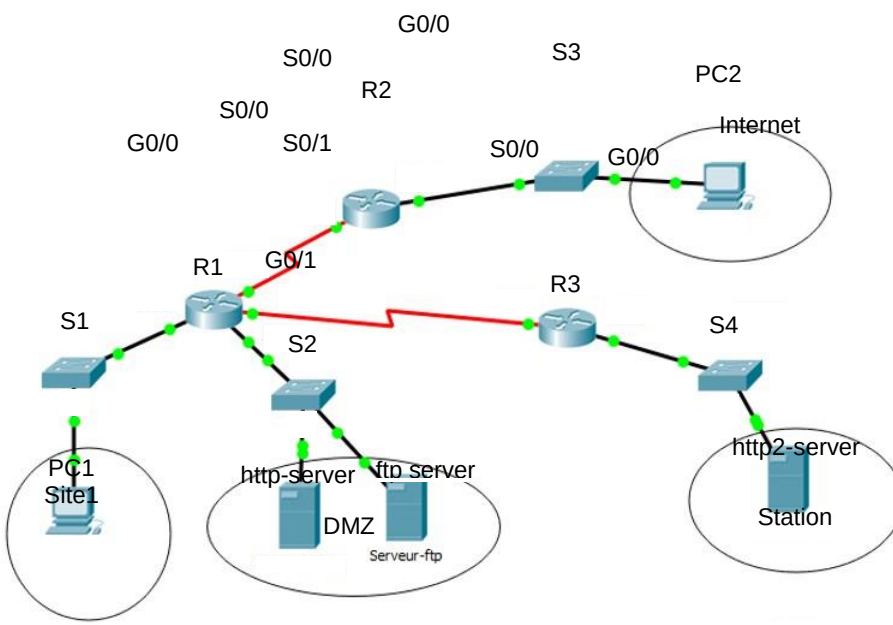
……

……

6. Test the effect of the ACLs created.

EXERCISE 7.–

Topology



For a color version of this figure, see www.iste.co.uk/sadiqui/computer.zip

Addressing table

Device	Interface	IP address	Subnet mask	Gateway
R1	G0/0	192.168.0.1	/24	–
	G0/1	192.168.1.1	/24	–
	S0/0	192.168.100.1	/30	–
	S0/1	192.168.200.1	/30	–
R2	G0/0	192.168.10.1	/24	–
	S0/0	192.168.100.2	/30	–
R3	G0/0	192.168.20.1	/24	–
	S0/0	192.168.200.2	/30	–
PC1	NIC	192.168.0.2	/24	192.168.0.1
PC2	NIC	192.168.10.2	/24	192.168.10.1
ftp_server	NIC	192.168.1.2	/24	192.168.1.1
http-server	NIC	192.168.1.3	/24	192.168.1.1
http2-server	NIC	192.168.20.2	/24	192.168.20.1

Objectives

Configuring a zone-based firewall.

Software to be used

Packet tracer.

Part A: establishing the basic device configuration.

1. Configure the basic device settings.

1.1. Configure the host names as shown in the topology.

1.2. Apply the IP addresses to the device interfaces according to the addressing table.

1.3. Set the clock value to 128 000 for the serial interface.

2. Configure the routing using the OSPF protocol.

2.1. Enable OSPF on the routers using the value 1 as the process ID.

2.2. Set the RID value to 1.1.1.1 for R1, to 2.2.2.2 for R2 and to 3.3.3.3 for R3.

2.3. Add all networks to the OSPF protocol.

2.4. Test connectivity between all network elements.

Part B: configuring a zone-based firewall

1. Review the definition of the DMZ zone.

.....

.....

2. Creating security zones on R1.

2.1. Create the internal zone with the name IN-ZONE.

```
R1(config)# zone security IN-ZONE
R1(config-sec-zone) exit
```

2.2. Create the DMZ zone with the name DMZ-ZONE.

```
R1(config)# zone security DMZ-ZONE
R1(config-sec-zone) exit
```

2.3. Create the external zone with the name OUT-ZONE.

```
R1(config)# zone security OUT-ZONE
R1(config-sec-zone) exit
```

2.4. Create the external zone with the name HEAD-ZONE.

```
R1(config)# zone security HEAD-ZONE
R1(config-sec-zone) exit
```

3. Create Class-Maps to identify authorized traffic.

3.1. Create a CMAP-IN-TO-DMZ Class-Map.

R1(config)#**class-map type inspect match-any CMAP-IN-TO-DMZ**

3.2. Allow http and ftp and icmp protocols.

R1(config-cmap)#**match protocol http** R1(config-cmap)#**match protocol ftp** R1(config-cmap)#**match protocol icmp** R1(config-cmap)#**exit**
R1(config)#**exit**

3.3. Create a CMAP-IN-TO-HEAD Class-Map.

R1(config)#**class-map type inspect match-any CMAP-IN-TO-HEAD**

3.4. Allow http and icmp protocols.

R1(config-cmap)#**match protocol http** R1(config-cmap)#**match protocol icmp** R1(config-cmap)#**exit**
R1(config)#**exit**

3.5. Create a CMAP-OUT-TO-DMZ Class-Map.

R1(config)#**class-map type inspect match-any OUT -TO-DMZ**

3.6. Allow only the http protocol.

R1(config-cmap)#**match protocol http**
R1(config-cmap)#**exit**
R1(config)#**exit**

4. Create the Policy-Maps for applying the access rules to the Class-Map.

4.1. Review the definition of the three rules applied to inter-zone traffic.

–**Pass**:.....

– **Inspect**:.....

– **Drop**:.....

4.2. Create a Policy-Map to apply the Class-Map CMAP-IN-TO-DMZ.

R1(config)# **policy-map type inspect PMAP-IN-TO-DMZ**
R1(config-pmap)# **class type inspect CMAP-IN-TO-DMZ**
R1(config-pmap-c)# **pass**

4.3. Similarly, create the following Policy-Maps:

– **PMAP-OUT-TO-DMZ** for the Class-Map **CMAP-OUT-TO-DMZ**;

– **PMAP- IN-TO-HEAD** for the Class-Map **CMAP- IN-TO-HEAD.**

5. Define the zone pairs.

5.1. Create a zone pair that applies the PMAP-IN-TO-DMZ policy between IN-ZONE and DMZ-ZONE.

R1(config)#**zone-pair security IN-to-DMZ source IN-ZONE destination DMZ-ZONE**
R1(config-sec-zone-pair)# **service-policy type inspect PMAP-IN-TO-DMZ**

5.2. Similarly, create the following zone pairs:

– **OUT-to-DMZ** that applies the **PMAP-OUT-TO-DMZ** strategy;

– **IN-to-HEAD** that applies the **PMAP-IN-TO-HEAD** strategy.

6. Assign the interfaces to the zones.

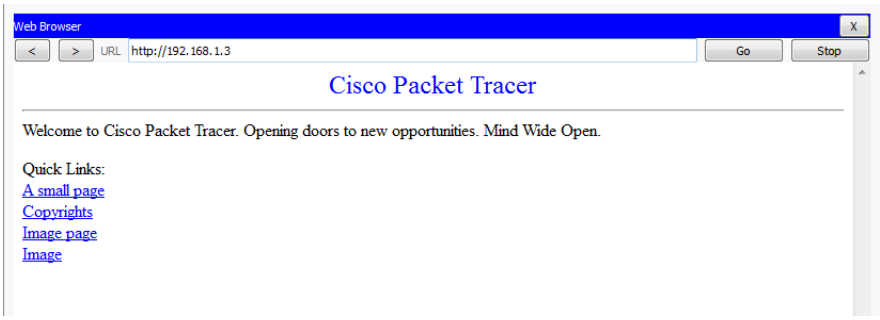
R1(config)#interface G0/0
R1(config-if)#zone-member security **IN-ZONE**
R1(config)#interface G0/1
R1(config-if)#zone-member security **DMZ-ZONE**
R1(config)#interface S0/0
R1(config-if)#zone-member security **OUT-ZONE**
R1(config)#interface S0/1
R1(config-if)#zone-member security **HEAD-ZONE**

7. Verify the configuration of R1.

Using the "show running-config" command, verify all the parameters of your configuration.

8. Test the configuration of your firewall.

– Ensure that it is possible to access the **http-server** from **PC1** and **PC2**.



– Check that it is possible to access **http2-server** only from PC1**.**

– Check that it is possible to access the ftp-server service only from **PC1**.

PC1:\>**ftp 192.168.1.3**

– Check that it is possible to send a **ping** request to **http-server** from **PC1**.

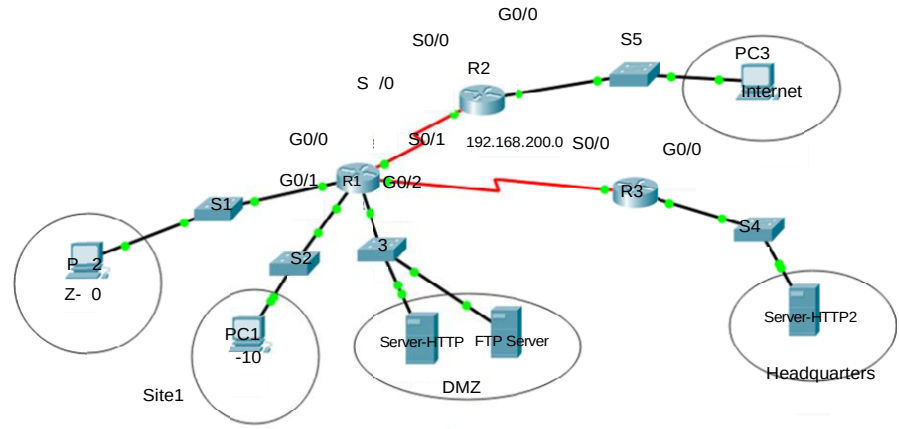
– Check that it is not possible to send a **ping** request to **http-server** from **PC2**.

Check that it is possible to send a **ping** request to **PC2** from **PC1**

6.8. Exercises for application

EXERCISE 8.–

Topology



For a color version of this figure, see www.iste.co.uk/sadiqui/computer.zip

Addressing table

Device	Interface	IP address	Subnet mask	Gateway
R1	G0/0	192.168.0.1	/25	–
	G0/1	192.168.0.129	/25	–
	G0/2	192.168.1.1	/24	–
R1	S0/0	192.168.100.1	/30	–
	S0/1	192.168.200.1	/30	–
R2	G0/0	192.168.10.1	/24	–
	S0/0	192.168.100.2	/30	–
R3	G0/0	192.168.20.1	/24	–
	S0/0	192.168.200.2	/30	–
PC1	NIC	192.168.0.2	/25	192.168.0.1
PC2	NIC	192.168.0.130	/25	192.168.0.129
PC3	NIC	192.168.10.2	/24	192.168.10.1
FTP_server	NIC	192.168.1.2	/24	192.168.1.1
Server-HTTP	NIC	192.168.1.3	/24	192.168.1.1
Server-HTTP2	NIC	192.168.20.2	/24	192.168.20.1

Objectives

Configuring a zone-based firewall.

Software to be used

Packet tracer.

Part A: setting up the basic device configuration

1. Configure the basic device settings.

1.1. Configure the host names as shown in the topology.

1.2. Apply the IP addresses to the device interfaces according to the addressing table.

1.3. Set the clock value to 128 000 for the serial interfaces.

2. Configure the routing using the OSPF protocol.

2.1. Enable OSPF on the routers using the value 1 as the process ID.

2.2. Set the RID value to 1.1.1.1 for R1, to 2.2.2.2 for R2 and to 3.3.3.3 for R3.

2.3. Add all networks to the OSPF protocol.

2.4. Test connectivity between all network elements.

Part B: configuring a zone-based firewall

1. Create security zones on R1.

Create the following security zones:

Name of the security zone	Description
IN-ZONE-Z10	Network for Service 1
IN-ZONE-Z20	Network for Service 2
DMZ-ZONE	Network for the DMZ zone
OUT-ZONE	Internet network
HEAD-ZONE	The headquarters network

2. Create ACLs that define the internal traffic to be monitored.

2.1. Create a numbered ACL that authorizes http, FTP and icmp streams.

R1(config)# **access-list 101 permit tcp 192.168.0.0 0.0.0.127 host 192.168.1.2 eq www**
R1(config)# **access-list 101 permit tcp 192.168.0.0 0.0.0.127 host 192.168.1.2 eq ftp**
R1(config)# **access-list 101 permit icmp 192.168.3.0 0.0.0.127 any**

2.2. Creates a numbered ACL that allows the FTP stream.

R1(config)# **access-list 102 permit tcp any host 192.168.1.2 eq ftp**
R1(config)# **access-list 102 permit icmp any host 192.168.1.2**

2.3. Create a numbered ACL that allows http and icmp streams towards the headquarters.

R1(config)# **access-list 103 permit tcp 192.168.0.0 0.0.0.255 host 192.168.20.2 eq www**
R1(config)# **access-list 103 permit icmp 192.168.0.0 0.0.0.255 host 192.168.20.2**

3. Create Class-Maps to identify authorized traffic.

3.1. Create a CMAP-IN-TO-DMZ Class-Map and identify authorized traffic.

R1(config)#class-map type inspect match-any CMAP-IN-TO-DMZ
R1(config-cmap)# **match access-group 101**
R1(config-cmap)# **exit**

3.2. Create a CMAP-IN-TO-HEAD Class-Map and identify authorized traffic.

R1(config)#class-map type inspect match-any CMAP-IN-TO-HEAD
R1(config-cmap)# **match access-group 103**
R1(config-cmap)# **exit**

3.3. Create a CMAP-OUT-TO-DMZ Class-Map.

R1(config)#class-map type inspect match-any OUT -TO-DMZ

R1(config-cmap)# **match access-group 102**
R1(config-cmap)# **exit**

4. Create the Policy-Map to apply the Class-Maps.

4.1. Create a Policy-Map to apply the CMAP-IN-TO-DMZ Class-Map.

R1(config)# policy-map type inspect PMAP-IN-TO-DMZ
R1(config-pmap)# class type inspect CMAP-IN-TO-DMZ
R1(config-pmap-c)# pass

4.2. Similarly, create the following Policy-Maps:

PMAP-OUT-TO-DMZ for the **CMAP-OUT-TO-DMZ Class-Map**

PMAP- IN-TO-HEAD for the **CMAP-IN-TO-HEAD Class-Map**

5. Define the zone pairs.

Create the following zone pairs:

Name of the zone pair	Source	Destination	Strategy to apply
IN-to-DMZ	IN-ZONE-Z10	DMZ-ZONE	PMAP-IN-TO-DMZ
OUT-to-DMZ	OUT-ZONE	DMZ-ZONE	PMAP-OUT-TO-DMZ
IN1-to-HEAD	IN-ZONE-Z10	HEAD-ZONE	PMAP- IN-TO-HEAD
IN2-to-HEAD	IN-ZONE-Z20	HEAD-ZONE	PMAP- IN-TO-HEAD

6. Assign the interfaces to the zones.

Name of the interface	Name of the security zone
G0/0	IN-ZONE-Z20
G0/1	IN-ZONE-Z10
G0/2	DMZ-ZONE
S0/0	OUT-ZONE
S0/1	HEAD-ZONE

7. Verify the configuration of R1.

Using the “show running-config” command, verify all the parameters of your configuration.

8. Test the configuration of your firewall.

– Check that it is possible to access the **Server-HTTP** from **PC2** and **PC3**.

– Check that it is only possible to access **Server-http2** from PC1.

– Check that it is only possible to access the **Server-ftp** service from PC1.

PC1:\>**ftp 192.168.1.3**

– Check that it is possible to send a **ping** request to **Server-HTTP** from **PC1**.

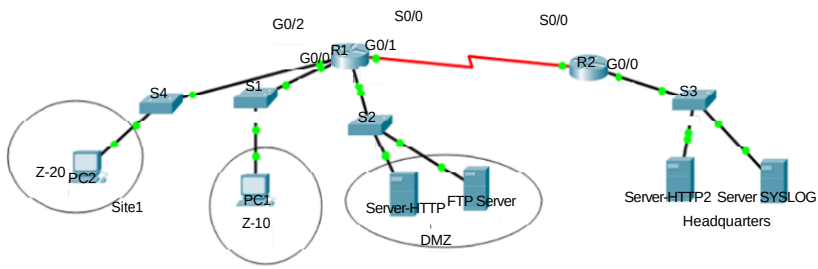
– Check that it is possible to send a **ping** request from **PC1** from to **PC3**.

9. Modify the parameters of your R1 firewall.

Add the modifications required to **authorize** and **inspect** the traffic between Z-20 and the **http-Server.**

EXERCISE 9.–

Topology



For a color version of this figure, see www.iste.co.uk/sadiqui/computer.zip

Addressing table

Device	Interface	IP address	Subnet mask	Gateway
R1	G0/0	192.168.0.1	/25	–
	G0/2	192.168.0.129	/25	–
	G0/1	192.168.1.1	/24	–
	S0/0	192.168.100.1	/30	–
R2	G0/0	192.168.10.1	/24	–
	S0/0	192.168.100.2	/30	–
PC1	NIC	192.168.0.2	/25	192.168.0.1
PC2	NIC	192.168.0.130	/25	192.168.0.129
FTP_server	NIC	192.168.1.2	/24	192.168.1.1
Server-HTTP	NIC	192.168.1.3	/24	192.168.1.1
Server-HTTP2	NIC	192.168.10.2	/24	192.168.10.1
Server-SYSLOG	NIC	192.168.10.3	/24	192.168.10.1

Objectives

– Configure a zone-based firewall;

– configure an IPS using the CLI command.

Software to be used

Packet tracer.

Part A: establishing the basic device configuration.

1. Configure the basic device settings.

1.1. Configure the host names as shown in the topology.

1.2. Apply the IP addresses to the device interfaces according to the addressing table.

1.3. Set the clock value to 128 000 for the serial interfaces.

1.4. Set the system date and time.

2. Configure the routing using the OSPF protocol.

2.1. Enable OSPF on the routers using the value 1 as the process ID.

2.2. Set the RID value to 1.1.1.1 for R1 and 2.2.2.2 for R2.

2.3. Add all networks to the OSPF protocol.

2.4. Test connectivity between all network elements.

Part B: configuring a zone-based firewall

1. Create security zones on R1.

Create the following security zones:

Name of the security zone	Description
IN-ZONE-Z10	Network for Service 1
IN-ZONE-Z20	Network for Service 2
DMZ-ZONE	Network for the DMZ zone
HEAD-ZONE	The headquarters network

2. Create ACLs that define the internal traffic to be monitored.

2.1. Create a numbered ACL (101) that authorizes the http, FTP and icmp streams between Z-10 and the DMZ-zone servers.

2.2. Create a numbered ACL (102) that allows the FTP flow between Z-20 and the FTP server for the DMZ.

2.3. Create a numbered ACL (103) that allows all http and icmp streams towards the headquarters.

3. Create Class-Maps to identify authorized traffic.

3.1. Create a CMAP-IN-TO-DMZ Class-Map and identify authorized traffic.

3.2. Create a CMAP-IN-TO-HEAD Class-Map and identify authorized traffic.

3.3. Create a CMAP-OUT-TO-DMZ Class-Map.

4. Create the Policy-Map to apply the Class-Maps.

4.1. Create a Policy-Map to apply the CMAP-IN-TO-DMZ Class-Map.

4.2. Similarly, create the following Policy-Maps:

PMAP-OUT-TO-DMZ for the **CMAP-OUT-TO-DMZ Class-Map**

PMAP- IN-TO-HEAD for the **CMAP- IN-TO-HEAD Class-Map**

5. Define the zone pairs.

Create the following zone pairs:

Name of the zone pair	Source	Destination	Strategy to apply
IN-to-DMZ	IN-ZONE-Z10	DMZ-ZONE	PMAP-IN-TO-DMZ
IN1-to-HEAD	IN-ZONE-Z10	HEAD-ZONE	PMAP-IN-TO-HEAD
IN2-to-HEAD	IN-ZONE-Z20	HEAD-ZONE	PMAP-IN-TO-HEAD

6. Assign the interfaces to the zones.

Name of the interface	Name of the security zone
G0/0	IN-ZONE-Z10
G0/2	IN-ZONE-Z20
G0/1	DMZ-ZONE
S0/0	HEAD-ZONE

7. Verify the configuration of R1.

Using the “show running-config” command, verify all the parameters of your configuration.

8. Test the configuration of your firewall.

Part C: configuring an IPS using CLI commands

1. Review the definition of an IPS signature.

……

……

2. Create a configuration directory.

R2# **mkdir ipsDir**

R2# **config terminal**

R2(config)#**ip ips config location ipsDir**

3. Create an IPS rule.

R2(config)#**ip ips name ipsRule**

4. Enable logging to the Syslog server.

R2(config)#**service timestamps log datetime msec**
R2(config)#**logging on**
R2(config)#**logging 192.168.10.3**
R1(config)#**ip ips notify log**

5. Configure the IPS to use the signature categories.

5.1. Remove all signatures

R2(config)#**ip ips signature-category** R2(config-ips-category)#**category all** R2(config-ips-category-action)#**retired true** R2(config-ips-category-action)#**exit**

5.2. Only activate the signatures from the category "ios_ips basic".

R2(config-ips-category)#**category ios_ips basic** R2(config-ips-category-action)#**retired false** R2(config-ips-category-action)#**exit**
R2(config-ips-category)#**exit**
Do you want to accept these changes? [confirm]

6. Apply the IPS rule to an interface.

R2(config)#**interface S0/0**
R2(config-if)#**ip ips ipsRule in**

7. Modify the signature parameters.

7.1. Display the information associated with the signature "ICMP Echo Request" (IDsig: 2004, IDsubsig: 0).

```
R2#show ip ips signature sigid 2004 subid 0
…
Action=(A)lert, (D)eny, (R)eset, Deny-(H)ost, Deny-(F)low
Trait=alert-traits          EC=event-count          AI=alert-interval
GST=global-summary-threshold  SI=summary-interval   SM=summary-mode
SW=swap-attacker-victim       SFR=sig-fidelity-rating Rel=release
 SigID:SubID En  Cmp   Action Sev   Trait   EC   AI   GST   SI  SM SW
SFR Rel
 ----------- --  ----  ------ ---   -----  ---- ---- -----  --- -- -- --- ---
 2004:0     N* Nr    A     INFO     0     1    0    200   30  FA  N 100 S1
    sig-name: ICMP Echo Request
    sig-string-info: My Sig Info
    sig-comment: Sig Comment
    Engine atomic-ip params:
        fragment-status: icmp-
        type: 8
        l4-protocol: icmp
```

7.2. Select the signature “ICMP Echo Request”.

```
R2(config)#ip ips signature-definition
R2(config-sigdef)#signature 2004 0
```

7.3. Enable the signature.

```
R2(config-sigdef-sig)#status
R2(config-sigdef-sig-status)#retired  false
R2(config-sigdef-sig-status)#enabled  true
R2(config-sigdef-sig-status)#exit
```

7.4. Change the action for the signature to “produce-alert”.

```
R2(config-sigdef-sig)#engine
R2(config-sigdef-sig-engine)#event-action produce-alert
R2(config-sigdef-sig-engine)#exit
```

R2(config-sigdef-sig)#**exit**

R2(config-sigdef)#**exit**

Do you want to accept these changes? [confirm]

8. Check the IPS configuration is done.

R2#**show ip ips all**

IPS Signature File Configuration Status

Configured Config Locations: ipsDir

Last signature default load time:

…

IPS Syslog and SDEE Notification Status

Event notification through syslog is enabled

IPS Signature Status

Total Active Signatures: 1

Total Inactive Signatures: 0

IPS Packet Scanning and Interface Status

IPS Rule Configuration

IPS name ipsRule

IPS fail closed is disabled

..

Interface Configuration

Interface Serial0/0

Inbound IPS rule is not set

Outgoing IPS rule is ipsRule

IPS Category CLI Configuration:

Category all

Retire: True

Category ios_ips basic

Retire: False

9. Check that your configuration works.

9.1. Review the definition of an IDS.

……

……

9.2. Send out a "ping" from PC2 to Server-http2.

9.3. Check that the following message was added to the Server-SYSLOG:

%IPS-4-SIGNATURE: Sig:2004 Subsig:0 Sev:25 [192.168.0.2 -> 192.168.10.2:0] RiskRating:25

9.4. Why can R2 be considered as an IDS and not an IPS?

……

……

9.5. Modify the "ICMP Echo Request" signature to refuse ICMP packets.

R2(config)#ip ips **signature-definition** R2(config-sigdef)#**signature 2004 0** R2(config-sigdef-sig)#**engine**
R2(config-sigdef-sig-engine)#**event-action produce-alert** R1(config-sigdef-sig-engine)#**event-action deny-packet-inline** R2(config-sigdef-sig-engine)#**exit**
R2(config-sigdef-sig)#**exit** R2(config-sigdef)#**exit**
Do you want to accept these changes? [confirm]

9.6. Send out a "ping" from PC2 to Server-http2. Why was this command unsuccessful?

……..

9.7. Verify that a message has been added to the Server-SYSLOG.

9.8. Why can we now consider R2 as an IPS?

……..

……..