



Configure OSPF on All routers

For all routers execute the following commands

Enable secret tyit1819

Hostname R1

Username admin1 secret adminit2019

AAA new-model  
AAA authentication login default local

Line console 0

Login authentication default

Exit

End

Exit

En

Config t

Ip domain-name tyit.com

Crypto key generate RSA

AAA authentication login SSH-LOGIN local

Line vty 0 4

Login authentication SSH-LOGIN

End

**Part 1: Enable IOS IPS**

**Step 1: Enable the Security Technology package.**

Licence boot module c1900 technology-package securityk9

Yes

Do copy run start

Exit

Reload

Show version

**Step 2: Verify network connectivity.**

On command prompt of PC-A

Ping 192.168.3.2 (pinging)

On command prompt of PC-C

Ping 192.168.1.2 (pinging)

**Step 3: Create an IOS IPS configuration directory in flash.**

On **R1**

R1# mkdir ipsdir

Create directory filename [ipsdir]? <**Enter**> Created

**Step 4: Configure the IPS signature storage location. On R1**

R1(config)# **ip ips config location flash:ipsdir**

**Step 5: Create an IPS rule.**

R1(config)# **ip ips name iosips**

**Step 6: Enable logging.**

R1(config)# **ip ips notify log**

Enable the timestamp service if it is not enabled.

R1(config)# **service timestamps log datetime msec**

R1(config)# **logging host 192.168.1.50**

**Step 7: Configure IOS IPS to use the signature categories.**

R1(config-ips-category)# **category all**

R1(config-ips-category-action)# **retired true**

R1(config-ips-category-action)# exit

R1(config-ips-category)# **category ios\_ips basic**

R1(config-ips-category-action)# **retired false**

R1(config-ips-category-action)# exit

R1(config-ips-cateogry)# exit

Do you want to accept these changes? [confirm] **<Enter>**

**Step 8: Apply the IPS rule to an interface**

R1(config)# **interface g0/1**

R1(config-if)# **ip ips iosips out**

Part 2: Modify the Signature

R1(config)# **ip ips signature-definition**

R1(config-sigdef)# **signature 2004 0**

R1(config-sigdef-sig)# status

R1(config-sigdef-sig-status)# **retired false**

R1(config-sigdef-sig-status)# **enabled true**

R1(config-sigdef-sig-status)# exit

R1(config-sigdef-sig)# engine

R1(config-sigdef-sig-engine)# **event-action produce-alert** R1(config-sigdef-sig-engine)# **event-action deny-packet-inline**

R1(config-sigdef-sig-engine)# exit

R1(config-sigdef-sig)# exit

R1(config-sigdef)# exit

Do you want to accept these changes? [confirm] **<Enter>**

**Step 2: Use show commands to verify IPS.**

R1(config )#show ip ips all

**Step 3: Verify that IPS is working properly.**

From PC-C, attempt to ping PC-A. (Fail)

From PC-A, attempt to ping PC-C. (successful)

**Step 4: View the syslog messages.**

1. a. Click the **Syslog** server.
2. b. Select the Services tab.
3. c. In the left navigation menu, select **SYSLOG** to view the log file.