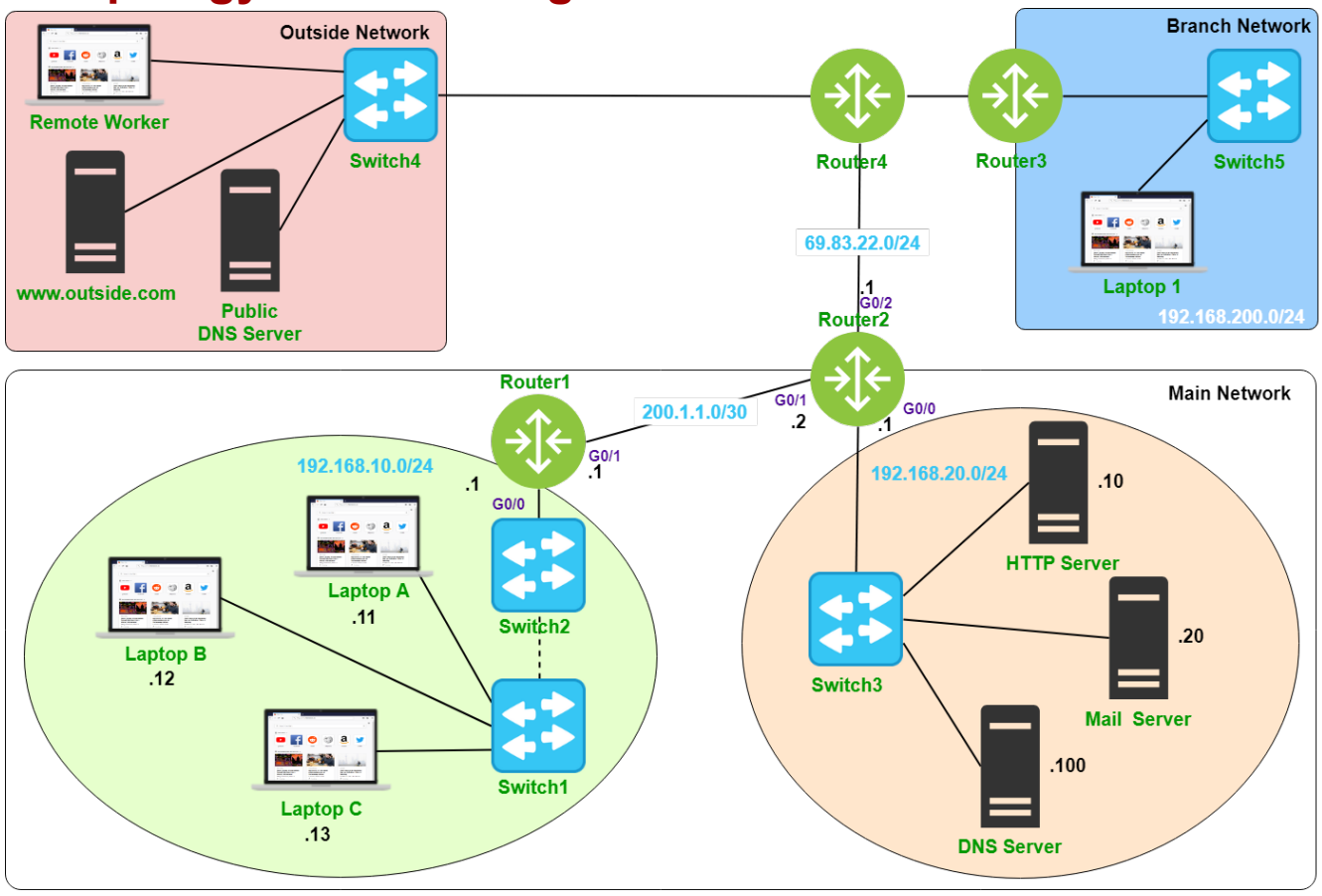
Lab 8 – Intrusion Detection & Prevention

Lab Topology and Learning Goals



Intrusion Detection and Prevention Systems (IDPS) protect the network from advanced threats such as viruses, worms and other malware. Deployed inline on network boundaries, IDPS protects the network from emerging threats by means of signature definition updates. In this lab, we deploy IPS on the network edge to protect against external network threats.

Lab Instructions and Required Resources

- Complete this lab in the Packer Tracer file: **INFO-6078 – Lab 8 – IDPS.pkz**
- Take Lab Quiz: **Lab 8 - Requires Respondus LockDown Browser**

Lab 8 – Intrusion Detection & Prevention

Configure and Enable Cisco IPS

Cisco IPS will be used to scan incoming network traffic for malicious content.
When deploying IPS on network hardware, you would need to install Cisco's public crypto key and update the devices definitions via a signature file.
As Packet Tracer is a simulator, we do not need to complete these steps.

Modify the License on Router2

Activate the security technology package license to enable Cisco IPS support
Router2(config)# license boot module c2900 technology-package securityk9
Accept the EULA by typing yes

Reboot the router to load the features
Router2# copy run start
Router2# reload

Verify Network Operation

On the **Remote Worker** laptop, send a ping to the **Web Server** (**192.168.20.10)**
If the ping fails, troubleshoot as necessary

From the **Web Server**, send a ping to the **Remote Worker** laptop (**100.40.66.11**)
If the ping fails, troubleshoot as necessary

Ensure the Time is Configured Correctly

Ensure the time is set correctly on Router2 to ensure the IPS timestamp information captures the actual time the event occurred
Router2# show clock

If the time is not correct, set the correct time
Router2# clock set ?
Router2# clock set hh:mm:ss 1-31 month year

Enable the timestamp service
Router2(config)# service timestamps log datetime msec

Lab 8 – Intrusion Detection & Prevention

Enable Logging on Router2

Cisco IPS supports logging to the console, or to a syslog server
Enable logging to the console
Router2(config)# logging on
Router2(config)# logging buffered 4096

Verify logging settings
Router2# show logging

Create an IPS Folder on Router2

Create a folder to store IPS signature files on the router's flash
Router2# mkdir flash:ips

Verify the directory has been created
Router2# show flash

Configure an IPS Rule on Router2

Router2(config)# ip ips name FanshaweIPS

View the State of IPS Before Configuration

Router2# show ip ips all

Configure the Signature Storage Location

Router2(config)# ip ips config location flash:ips

Configure IPS to Send Logging Messages to Syslog

Router2(config)# ip ips notify log

Change IPS Signature Category from All to Basic

```
Router2(config)# ip ips signature-category
Router2(config-ips-category)# category all
Router2(config-ips-category-action)# retired true
Router2(config-ips-category-action)# exit
Router2(config-ips-category)# category ios_ips basic
Router2(config-ips-category-action)# retired false
Router2(config-ips-category-action)# exit
Router2(config-ips-category)# exit
Do you want to accept these changes? [confirm] <Enter>
```

Apply IPS to the Interface

```
Router2(config)# interface gigabitEthernet 0/2
Router2(config-if)# ip ips FanshaweIPS in
```

Review the IPS Configuration

```
Router2# show ip ips all
```

Notice that we now have one active signature. Normally there are many more active signatures when configuring IPS on a real device.

Modify a Signature to drop ICMP Traffic

Modify the signature (signature 2004, ID 0), and unretire the echo request signature

```
Router2(config)# ip ips signature-definition
Router2(config-sigdef)# signature 2004 0
Router2(config-sigdef-sig)# status
Router2(config-sigdef-sig-status)# retired false
Router2(config-sigdef-sig-status)# enabled true
Router2(config-sigdef-sig-status)# exit
Router2(config-sigdef-sig)# engine
Router2(config-sigdef-sig-engine)# event-action produce-alert
Router2(config-sigdef-sig-engine)# event-action deny-packet-inline
Router2(config-sigdef-sig-engine)# exit
Router2(config-sigdef-sig)# exit
Router2(config-sigdef)# exit
Do you want to accept these changes? [confirm] <Enter>
```

Lab 8 – Intrusion Detection & Prevention

Verify IPS Operation

From the **Web Server**, send a ping to the **Remote Worker** laptop (**100.40.66.11**)
Is the ping successful?

From the **Remote Worker** laptop, send a ping to the **Web Server** (**192.168.20.10)**
Is the ping successful?

From Laptop A, send a ping to the **Web Server** (**192.168.20.10)**
Is the ping successful?

View the log messages generated on **Router2**

On **Router2** verify the IPS configuration
Router2# show ip ips all

View Detailed Information About the Signature you Modified

Router2# show ip ips signatures sigid 2004 subid 0