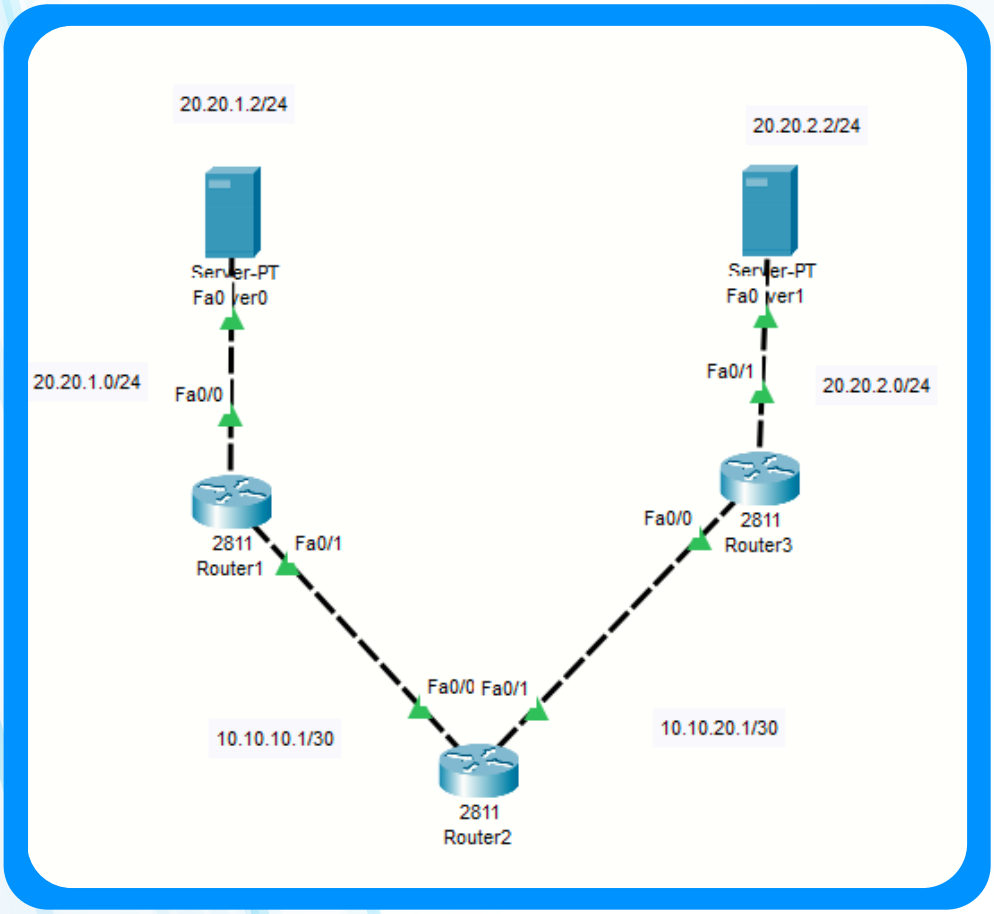
Esta es la topología presentada para la configuración de IPS.

Para este laboratorio se utilizaron routers 2811 debido a que en este modelo de router se puede configurar IPS en packet tracer.

En este laboratorio se configurará el cisco IOS IPS, el cual es parte de una característica del IOS Firewall de cisco. Esta nos permite examinar algunos patrones de ataques y alertar o mitigar cuando estos ocurren. El IPS por si solo, no es suficiente para convertir un router en un Firewall para internet, pero cuando le añadimos otras características de seguridad, podemos tener una poderosa defensa.



David Antonio Zobarzo Fernández

```
Router1#
Router1#mkdir ips
Create directory filename [ips]?
Created dir flash:ips

Router1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router1(config)#interface fastethernet 0/1
Router1(config-if)#ip address 10.10.10.1 255.255.255.252
Router1(config-if)#no shutdown

Router1(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to
up
exit
Router1(config)#ip route 0.0.0.0 0.0.0.0 10.10.10.2
Router1(config)#
```

En el Router1 creamos la carpeta "ips" para almacenar firmas y configuraciones de IPS. También se realizaron configuraciones de conectividad básica.

Con el comando "ip ips name" se crea la regla con el nombre infografía la cual se activará en la interfaz. Luego se debe indicar la memoria flash como el lugar de almacenamiento de las configuraciones. Finalmente se deben definir las categorías de las firmas que se usarán (estas están predefinidas en las categorías, lo que facilita su clasificación y agrupación).

Hay que tener en consideración que la categoría "ALL" contiene todas las firmas disponibles en el dispositivo, si no desactivamos esta categoría el router podría quedar sin memoria. Una buena práctica es desactivar antes de utilizar otra categoría.

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip ips name infografia
Router(config)#ip ips config location flash
Router(config)#ip ips config location flash:
Router(config)#ip ips signature-category
Router(config-ips-category)#category all
Router(config-ips-category-action)#retired true
Router(config-ips-category-action)#exit
Router(config-ips-category)#category ios_ips basic
Router(config-ips-category-action)#retired false
Router(config-ips-category-action)#exit
Router(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

Router(config)#
```

```
Router1(config)#interface fastethernet 0/1
Router1(config-if)#ip ips infografia in
Router1(config-if)#
 %IPS-6-ENGINE_BUILDS_STARTED:  00:16:04 UTC mar. 01 1993

 %IPS-6-ENGINE_BUILDING: atomic-ip - 3 signatures - 1 of 13
engines

 %IPS-6-ENGINE_READY: atomic-ip - build time 8 ms - packets
for this engine will be scanned

 %IPS-6-ALL_ENGINE_BUILDS_COMPLETE: elapsed time 8 ms

Router1(config-if)#ip ips infografia out
Router1(config-if)#
```

Finalmente se aplica la regla "infografía" creada anteriormente a la interfaz

Se puede escoger el tráfico a inspeccionar.

In: es para el trafico de entrada.
Out: es para el tráfico de salida.

En Router2 y Router3 se realiza la configuración básica de conectividad.

```
Router2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router2(config)#interface fastethernet 0/0
Router2(config-if)#ip address 10.10.10.2 255.255.255.252
Router2(config-if)#no shutdown
Router2(config-if)#exit
Router2(config)#ip route 0.0.0.0 0.0.0.0 10.10.10.1
Router2(config)#interface fastethernet 0/1
Router2(config-if)#ip address 10.10.20.1 255.255.255.252
Router2(config-if)#no shutdown
Router2(config-if)#exit
Router2(config)#ip route 0.0.0.0 0.0.0.0 10.10.20.2
Router2(config)#ip route 20.20.1.0 255.255.255.0 10.10.10.1
Router2(config)#ip route 20.20.2.0 255.255.255.0 10.10.20.2
Router2(config)#
```

```
Router3(config)#interface fastethernet 0/0
Router3(config-if)#ip address 10.10.20.2 255.255.255.252
Router3(config-if)#no shutdown
Router3(config-if)#interface fastethernet 0/1
Router3(config-if)#ip address 20.20.2.1 255.255.255.0
Router3(config-if)#no shutdown
Router3(config-if)#exit
Router3(config)#ip route 0.0.0.0 0.0.0.0 10.10.20.1
Router3(config)#
```

En el dispositivo final se debe realizar un ping desde servidor a servidor y luego aplicamos la configuración en el Router1 del estado de firmas y definir una acción a una firma o un grupo de firmas basadas en categorías. En el siguiente ejemplo se mostrará como desactivar la firma echo request, habilitándolo y cambiando su acción a alerta y denegando los paquetes entrantes.

```
C:\>ping 20.20.2.2

Pinging 20.20.2.2 with 32 bytes of data:

Reply from 20.20.2.2: bytes=32 time<1ms TTL=125
Reply from 20.20.2.2: bytes=32 time<1ms TTL=125
Reply from 20.20.2.2: bytes=32 time<1ms TTL=125
Reply from 20.20.2.2: bytes=32 time<1ms TTL=125

Ping statistics for 20.20.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

```
Router1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router1(config)#ip ips signature-definition
Router1(config-sigdef)#signature 2004 0
Router1(config-sigdef-sig)#status
Router1(config-sigdef-sig-status)#retired false
Router1(config-sigdef-sig-status)#enabled true
Router1(config-sigdef-sig-status)#exit
Router1(config-sigdef-sig)#engine
Router1(config-sigdef-sig-engine)#event-action produce-alert
Router1(config-sigdef-sig-engine)#event-action deny-packet-inline
Router1(config-sigdef-sig-engine)#exit
Router1(config-sigdef-sig)#exit
Router1(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

Router1(config)#
```

```
C:\>ping 20.20.2.2

Pinging 20.20.2.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 20.20.2.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Ping realizado nuevamente

Nuevamente en el dispositivo final se debe probar el ping que ya se realizó con anterioridad y el IPS interactuará según lo configurado, a continuación la prueba.

Esta es la respuesta que muestra el Router1 después de la configuración de IPS.

```
%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

Router1(config)#
 %IPS-4-SIGNATURE: Sig:2004 Subsig:0 Sev:25  [20.20.1.2 ->
20.20.2.2:0] RiskRating:25

 %IPS-4-SIGNATURE: Sig:2004 Subsig:0 Sev:25  [20.20.1.2 ->
20.20.2.2:0] RiskRating:25

 %IPS-4-SIGNATURE: Sig:2004 Subsig:0 Sev:25  [20.20.1.2 ->
20.20.2.2:0] RiskRating:25

 %IPS-4-SIGNATURE: Sig:2004 Subsig:0 Sev:25  [20.20.1.2 ->
20.20.2.2:0] RiskRating:25
```