Práctica 9 Redes Seguras: Configuración IPS

Se recomienda configurar la hora en los dispositivos de red con:

```
FW# clock set 15:00:00 05 december 2024
```

Necesitamos licencia securityK9, si no estuviera habilitado se usa el comando:

```
license boot module c1900 technology package securityk9
```

Se debe revisar que hay alcance del FireWall a la máquina de servicios. Antes de realizar la práctica se debe eliminar el contenido de un directorio:

```
delete flahs:ipsdir/*
```

Tras eso comprobamos que se haya eliminado correctamente con:

```
dir flash:ipsdir
```

Tras eso configuramos el IPS. Le podemos pasar como parámetro una ACL para asignar que tipos de paquetes se van a revisar y cuales no.

```
FW(config)# ip ips name iosips_munics1
FW(config)# ip ips name ips list ?
```

Tras eso habilitamos un servicio de notificación de eventos con:

```
FW(config)# ip http server
FW(config)# ip ips notify sdee
```

Tras eso habilitamos la salida de syslog:

```
FW(config)# ip ips notify log
FW(config)# service timestamps log datetime msec
FW(config)# logging <IP máquina de gestión>
```

Para activar los mensajes de syslog se debe activar terminal monitor si estamos por SSH

From:
http://knoppia.net/ - **Knoppia**

Permanent link:
http://knoppia.net/doku.php?id=redes:lab9

Last update: **2024/12/11 18:06**