**IDS-IPS**

**IDS--入侵检测系统**

**IPS--入侵防御系统**

**为什么需要IDS和IPS：**

**因为经过调查发现，绝大多数的攻击不是来自外部，而是来自内部。**

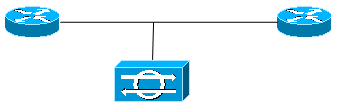
**4.0版本以前叫IDS**

**5.0版本以后叫IPS**

**IDS--入侵检测系统 只支持混杂模式**

**IPS--入侵防御系统 支持混杂模式和在线模式**

**混杂模式：**

****

**在线模式：**

****

**使用路由器可以实现IOS IDS和IOS IPS，用IOS软件来实现，并且都是在线模式。**

**从安装的设备不同，IPS又可分为HIPS（主机上的IPS）和NIPS（网络上的IPS）**

**logging trap ? //定义logging消息**

**logging host 12.1.1.1 //定义logging信息发送到哪个服务器上去**

**IOS12.3以上才支持做IOS IDS或IOS IPS**

**IDS和IPS是如何工作的：（通过使用signature来工作）**

**signature--对非法流量的定义，包含它的特征信息。可以理解为流量特征条目**

**IPS的IOS中内置了大约100个左右的signature,另外的要通过加载SDF文件来增加signature，SDF可以不断升级。**

**注意：进行检测不能影响正常通信**

**1、首先是一些基本配置**

**ip ips sdf**

**ip ips fail closed 如果SDF文件调用不成功，默认会把所有流量丢弃，这个问题很严重。如果你确认你的文件就在本地，用这个命令。**

**ip ips name IPS 还可以带一个访问列表**

**ip ips name IPS list**

**int s0/0**

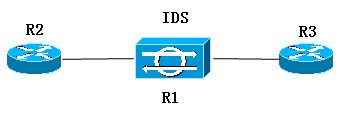
**ip ips IPS [in|out] 应用到接口：可以两个方向都应用**

**2、可以对signature进行一些调整，可单独禁用其中一些**

**ip ips signature 2000 [disable|delete|list] delete会删除这个sinature,list的意思是匹配的话就用这个sinature进行对照**

**IPS中有四种动作：**

**实验配置：**

****

**IDS(config)#ip audit name AUDIT info action alarm**

**IDS(config)#ip audit name AUDIT attack action alarm drop reset**

**IDS(config)#int e0**

**IDS(config-if)#ip audit AUDIT in**

**info 告警级别 Ping的包就是这个级别**

**attack 攻击级别**

**可以用Ping命令来做这个测试**

**SYN攻击**

**TCP.利用三次握手.客户端对于在第三次握手时的ACK不给予回应.使服务器处于"半激活状态"从而利用服务器的资源,**

ip access-list ex SYN

per tcp any 150.100.1.0 0.0.0.255

ip tcp intercept list SYN

ip tcp inter watch-timeout 15

ip tcp inter mode watch

**mode有watch和intercept两种**

**interspect--外部访问内部服务器时。先和中间路由器建立连接，成功后，中间路由器再和内部服务器建立连接，这样，所有的访问都是由中间路由器来中转。这种模式对路由器资源占用很大，现在基本不用。**

**watch--外部访问内部服务器，直接建TCP连接，中间路由器不参与，但会监视，如果在规定时间内，TCP连接还没建立好的话，就关闭这个连接。**

**ip tcp intercept watch-timeout 15 设定超时时间。**

**-------------------------------------------------------------------------------**