**IOS防火墙**

**什么是防火墙：**

**防火墙用来在网络区域之间进行访问控制的技术**

**IOS防火墙通过ACL和inspect监控策略的配合来实现对网络的访问控制。**

**firewall常用技术：**

**1、packet filtering 包过滤**

**2、application layer gateway 应用层网关**

**3、stateful packet filtering 状态化的包过滤**

**cisco的IOS防火墙技术分为三大块：**

**1、cisco IOS Firewall--CBAC 在控制过程中会自动结合ACL**

**2、authentication proxy（基于用户的认证授权技术）,要结合三A服务器来做**

**3、IDS、IPS(4.0版以前叫IDS，5.0以后的叫IPS)**

**DMZ区域**

**非军事化区域：就是人为划分出来的一个网络区域，可以将一些要允许外部用户访问的服务器放入这个区域。**

**特点：外网和内网都可以向DMZ区域发起访问，但不允许DMZ区域主动向其它区域发起访问**

**多重DMZ区域**

**在网络中划分出多个DMZ区域，不同的DMZ区域只提供某一类特定的服务。**

**cisco IOS Firewall(CBAC)**

**CBAC能够实现状态化的包过滤**

**状态化的包过滤技术能够根据内部出去的流量自动的在边缘网关路由器上放行相对应的外部流量回来。**

**通常在使用时，CBAC是与ACL结合使用来实现流量的控制。**

**需要先对网络进行划分，确定外部区域、内部区域、DMZ区域。**

**相比较自反访问列表，CBAC功能更强，它能基于应用层信息及动态的端口号来监控流量。**

**步骤：**

**1、定义内部、外部接口**

**2、定义访问列表，在outside接口配置一个访问列表，deny不需要的流量，通常deny ip any any，但注意在老版本中要让icmp的包通过，不然P不通。(12.3版本以前)**

**3、定义一个inspect的rule**

**4、将定义的rule应用到接口下**

**写CBAC列表:**

**ip inspect name CBAC tcp 只能对单session的起作用，如telnet**

**ip inspect name CBAC ftp 这是一个多session的tcp流量，要用这条专用命令才行**

**ip inspect name CBAC http**

**ip inspect name CBAC ftp audit-trail 针对单一协议设置审计**

**ip inspect audit-trail 全局下开启审计**

**ip inspect audit-off 全局关闭报警**

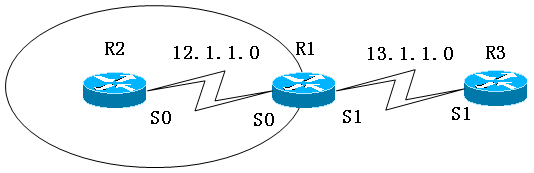
**ip inspect name CBAC icmp 这个命令在高版本才有,12.3以后才有**

**应用在接口下：**

**可用在内部接口的IN方向或外部接口的OUT方向**

**R2(config-if)#ip inspect CBAC [in|out]**

**例一：两端口的防火墙，路由器的s0口接内部，s1口接外部**

****

**第一步：在路由器上应用，阻止所有数据进入内部**

**R1(config)#access-list 100 deny ip any any**

**R1(config)#int s1**

**R1(config-if)#ip access-group 100 in**

**第二步：**

**R1(config)#ip inspect name CBAC tcp**

**第三步：**

**R1(config)#int s0**

**R1(config-if)#ip inspect CBAC in**

**注意：做本试验，如果三台路由器间起了路由协议，ACL要放行路由协议的流量，否则路由不通。**

**R1(config)#access-list 100 permit eigrp any any**

**R1(config)#access-list 100 deny ip any any**

**原理：**

**ip inspect CBAC in 应用之后，针对内网访问外网的tcp流量，会在路由器上生成相应的状态化表项（其实就是记录了出去的流信息)，当回来的数据包到达路由器的入接口时，要先去匹配这些状态化表项，如果匹配，就放进来，不匹配的话，再去做ACL检查。**

**show ip inspect sessions 在路由器上看状态化条目**

**show ip inspect interfaces**

**show ip inspect name CBAC**

**show ip inspect all**

**ip inspect audit-trail 开启审计信息，默认是关闭的,在全局模式下用是全局有效**

**ip inspect alert-off 关闭报警信息，默认是打开的。**

**利用CBAC，还可以抵御DOS攻击**

**R1(config)#ip inspect max-incomplite {high|low} 可设定最大和最小TCP半开连接数，用来抵御DOS攻击**

**R1(config)#ip inspect one-minute high 1000 设定一分钟内最多允许多少半开连接**

**R1(config)#ip inspect one-minute low 1000**

**R1(config)#ip inspect udp 1 设定UDP的timeout**

**no ip inspect 清除所有inspect配置**

**例二、三接口防火墙实验1：**

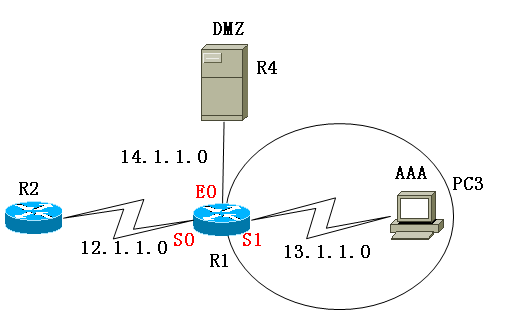
**需求：**

**DMZ是一台WWW服务器**

**inside可以访问outside和DMZ**

**outside可以访问DMZ**

**DMZ不能主动发起访问**

****

**1、R1的S0接口配置：**

**R1(config)#access-list 100 permit tcp any host 14.1.1.4 eq telnet**

**R1(config)#int s0**

**R1(config-if)#ip access-group 100 in**

**2、R1的S1接口配置：(也可在E0口的out方向做inspect，如第三步所示)**

**R1(config)#ip inspect name CBAC tcp**

**R1(config)#int s1**

**R1(config-if)#ip inspect CBAC in**

**3、R1的E0接口配置：**

**R1(config)#access-list 102 deny ip any any**

**R1(config)#int e0**

**R1(config-if)#ip access-group 102 in**

**R1(config)#ip inspect name DMZ tcp**

**R1(config)#int e0**

**R1(config-if)#ip inspect DMZ out**

**例三、三接口防火墙实验2：**

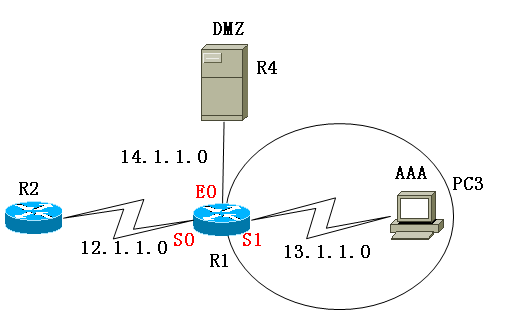
**需求：**

**inside可以PING通R2**

**inside可以telnet DMZ**

**R2可以telnet DMZ**

**DMZ不能主动发起访问**

****

**1、R1的S0接口配置：**

**R1(config)#access-list 100 permit tcp host 12.1.1.2 host 14.1.1.4 eq telnet**

**R1(config)#int s0**

**R1(config-if)#ip access-group 100 in**

**2、R1的S1接口配置：**

**R1(config)#access-list 101 permit tcp host 13.1.1.3 host 14.1.1.4 eq telnet**

**R1(config)#access-list 101 permit icmp host 13.1.1.3 host 12.1.1.2**

**R1(config)#int s1**

**R1(config-if)#access-list 101 in**

**R1(config)#ip inspect name CBAC tcp**

**R1(config)#ip inspect name CBAC icmp 旧版的不支持**

**R1(config)#int s1**

**R1(config-if)#ip inspect CBAC in**

**3、R1的E0接口配置：**

**R1(config)#access-list 102 deny ip any any**

**R1(config)#int e0**

**R1(config-if)#ip access-group 102 in**

**R1(config)#ip inspect name DMZ tcp**

**R1(config)#int e0**

**R1(config-if)#ip inspect DMZ out**

**Auth-Proxy基于用户的认证和授权技术**

**原理：**

**先让用户进行AAA认证，符合后推送相应的ACL策略给NAS，允许这个用户的相应流量进入。**

**分三块配置：**

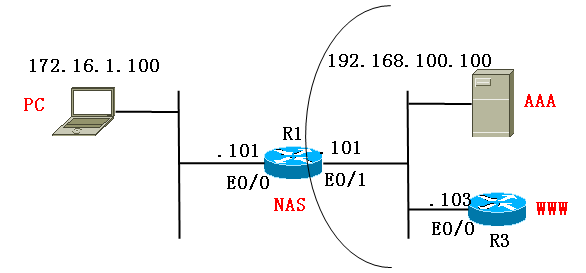
**1、配置AAA**

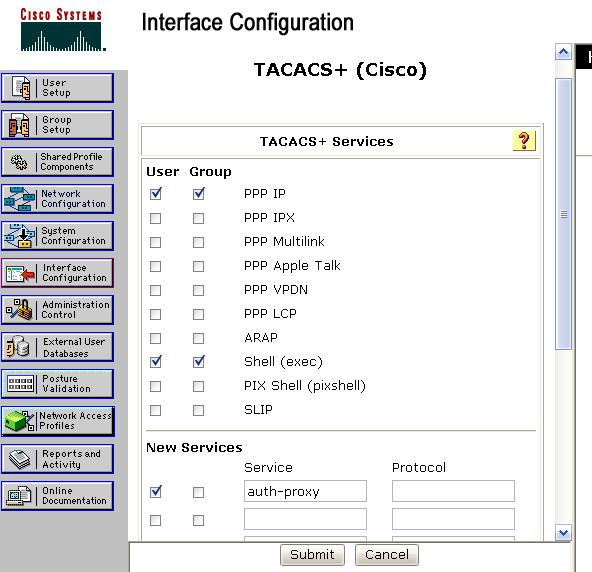
**2、配置ACL**

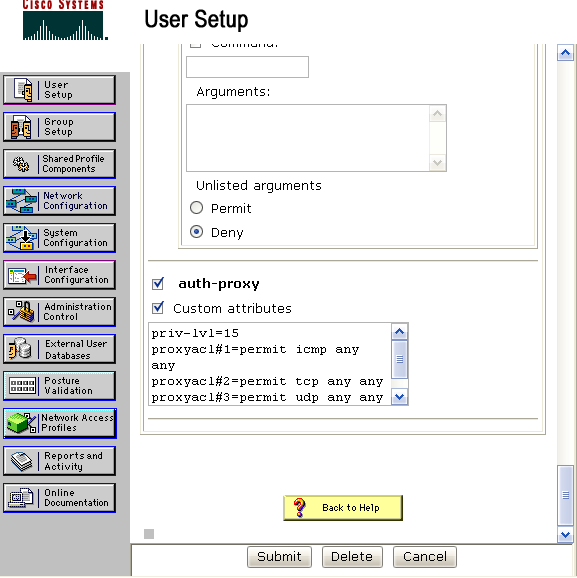
**3、配置auth-proxy**

**show ip auth-proxy chche 看缓存记录**

**实验：**

****

****

****