思科认证:配置CBAC 提升Cisco路由器安全Cisco认证考试 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/571/2021_2022__E6_80_9D_E7_A7_91_E8_AE_A4_E8_c101_571804.htm 在Cisco路由器上创建ACL(访问控制列表)是管理员常用的数据过滤和网络安全防护措施，但是ACL的局限性是非常明显的，因为它只能检测到网络层和传输层的数据信息，而对于封装在IP包中的恶意信息它是无能为力的。因此，ACL并不可靠，需要CBAC(基于上下文的访问控制)的配合，这样网络安全性将会极大提升。本文将和大家一起探讨Cisco路由器上CBAC的部署的技术细节及其相关技巧。 一、CBAC简述 CBAC(context-based access control)即基于上下文的访问控制，它不用于ACL(访问控制列表)并不能用来过滤每一种TCP/IP协议，但它对于运行TCP、UDP应用或某些多媒体应用(如Microsoft的NetShow或Real Audio)的网络来说是一个较好的安全解决方案。除此之外，CBAC在流量过滤、流量检查、警告和审计蛛丝马迹、入侵检测等方面表现卓越。在大多数情况下，我们只需在单个接口的一个方向上配置CBAC，即可实现只允许属于现有会话的数据流进入内部网络。可以说，ACL与CBAC是互补的，它们的组合可实现网络安全的最大化。 二、CBAC的合理配置 1.CBAC配置前的评估 在进行CBAC配置之前需要对网络的安全标准、应用需求等方面进行评估然后根据需要进行相应的配置。通常情况下，用户可以在一个或多个接口的2个方向上配置CBAC。如果防火墙两端的网络都需要受保护的话，如在Extranet或Intranet的配置中，就可以在2个方向上配置CBAC。若防火墙被放置在2个合作伙伴公司网络的中间，则可能想

要为某些应用在一个方向上限制数据流，并为其它应用在反方向上限制数据流。 特别要注意的是，CBAC只能用于IP数据流。只有TCP和UDP数据包能被检查，其他IP数据流 (如ICMP)不能被CBAC检查，只能采用基本的访问控制列表对其进行过滤。在不作应用层协议审查时，像自反访问控制列表一样，CBAc可以过滤所有的TCP和UDP会话。但CBAC也可以被配置来有效地处理多信道(多端口)应用层协议：cu-SeeMe(仅对whitePine版本)、FTP、H.323(如NetMeeting和ProShare)、HTTP(Java拦阻)、Java、MicrosftNetshow、UNIX的r系列命令(如rlogin、rexec和rsh).RealAudio、RPC(SunRPc，非DCERPC)MircosoftRPC、SMTP、SQL.Net、StreamWorks、TFTP、VDOLive。 2.选择配置接口 为了恰当地配置CBAc，首先必须确定在哪个接口上配置CBAC。下面描述了内部口和外部接口间的不同之处。 配置数据流过滤的第一步是决定是否在防火墙的一个内部接口或外部接口上配置CBAC。在该环境下，所谓“ 内部 ”是指会话必须主动发起以让其数据流被允许通过防火墙的一侧.“ 外部 ”是指会话不能主动发起的一侧(从外部发起的会话被禁止)。如果要在2个方向上配置CBAc，应该先在一个方向上使用适当的“ Intemal ”和“ Extemal ”接口指示配置CBAC。在另一个方向上配置CBAC时，则将该接口指示换成另一个。 CBAC常被用于2种基本的网络拓扑结构之一。确定哪种拓扑结构与用户自己的最吻合，可以帮助用户决定是否应在一个内部接口或是在一个外部接口上配置CBAC。 图l给出了第1种网络拓扑结构。在该简单的拓扑结构中，CBAC被配置在外部接口S0上。这可以防止指定的协议数据流进入该防火墙路由器和内部网络，

除非这些数据是由内部网络所发起会话的一部分。 图2给出了第2种网络拓扑结构。在该拓扑结构中，CBAC被配置在内部接口E0上，允许外部数据流访问DMZ(连接在接口E1上的停火区)中的服务(如 DNS服务)，同时防止指定的协议数据流如内部网络，除非这些数据流是由内部网络所发起的会话的一部分。这两种拓扑结构之间的关键不同点是：第1种拓扑结构不允许外部数据流不经过CBAC过滤器就进入了路由器.第2中拓扑结构允许外部数据流入路由器，让他们能不经过CBAC过滤器就到达位于DMZ区中的公共服务器。图2 