Cisco路由器的安全配置方案思科认证 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/644/2021_2022_Cisco_E8_B7_AF_E7_94_c101_644551.htm 一,路由器访问控制的安全配置 1,严格控制可以访问路由器的管理员。任何一次维护都需要记录备案。 2,建议不要远程访问路由器。即使需要远程访问路由器，建议使用访问控制列表和高强度的密码控制。 3,严格控制CON端口的访问。具体的措施有： A,如果可以开机箱的，则可以切断与CON口互联的物理线路。 B,可以改变默认的连接属性，例如修改波特率(默认是96000，可以改为其他的)。 C,配合使用访问控制列表控制对CON口的访问。 如：Router(Config)#Access-list 1 permit 192.168.0.1 Router(Config)#line con 0 Router(Config-line)#Transport input none Router(Config-line)#Login local Router(Config-line)#Exec-timeoute 5 0 Router(Config-line)#access-class 1 in Router(Config-line)#end D,给CON口设置高强度的密码。 4,如果不使用AUX端口，则禁止这个端口。默认是未被启用。禁止如： Router(Config)#line aux 0 Router(Config-line)#transport input none Router(Config-line)#no exec 5,建议采用权限分级策略。如： Router(Config)#username BluShin privilege 10 G00dPa55w0rd Router(Config)#privilege EXEC level 10 telnet Router(Config)#privilege EXEC level 10 show ip access-list 6,为特权模式的进入设置强壮的密码。不要采用enable password设置密码。而要采用enable secret命令设置。并且要启用Service password-encryption。 7,控制对VTY的访问。如果不需要远程

访问则禁止它。如果需要则一定要设置强壮的密码。由于VTY在网络的传输过程中为加密，所以需要对其进行严格的控制。如：设置强壮的密码；控制连接的并发数目；采用访问列表严格控制访问的地址；可以采用AAA设置用户的访问控制等。 8,IOS的升级和备份，以及配置文件的备份建议使用FTP代替TFTP。如： Router(Config)#ip ftp username BluShin Router(Config)#ip ftp password 4tppa55w0rd Router#copy startup-config ftp: 9,及时的升级和修补IOS软件。 