Cisco路由器安全配置方案 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/284/2021_2022_Cisco_E8_B7_AF_E7_94_c101_284836.htm 一、 路由器网络服务安全配置 1 禁止CDP（Cisco Discovery Protocol）。如：Router（Config）#no cdp run Router（Config-if）# no cdp enable 2 禁止其他的TCP、UDP Small服务。 Router（Config）# no service tcp-small-servers Router（Config）# no service udp-samll-servers 3 禁止Finger服务。 Router（Config）# no ip finger Router（Config）# no service finger 4 建议禁止HTTP服务。 Router（Config）# no ip http server如果启用了HTTP服务则需要对其进行安全配置：设置用户名和密码；采用访问列表进行控制。 5 禁止BOOTp服务。 Router（Config）# no ip bootp server 6 禁止IP Source Routing. Router（Config）# no ip source-route 7 建议如果不需要ARP-Proxy服务则禁止它，路由器默认识开启的。 Router（Config）# no ip proxy-arp Router（Config-if）# no ip proxy-arp 8 禁止IP Directed Broadcast. Router（Config）# no ip directed-broadcast 9 禁止IP Classless. Router（Config）# no ip classless 10 禁止ICMP协议的IP Unreachables， Redirects， Mask Replies. Router（Config-if）# no ip unreacheables Router（Config-if）# no ip redirects Router（Config-if）# no ip mask-reply 11 建议禁止SNMP协议服务。在禁止时必须删除一些SNMP服务的默认配置。如：Router（Config）# no snmp-server community public Ro Router（Config）# no snmp-server community admin RW 12 如果没必要则禁止WINS和DNS服务。 Router（Config）# no ip domain-lookup如果需

要则需要配置：Router（Config）# hostname Router Router（Config）# ip name-server 219.150.32.xxx 13 明确禁止不使用的端口。如：Router（Config）# interface eth0/3 Router（Config）# shutdown二、路由器访问控制的安全配置（可选） 路由器的访问控制是比较重要的安全措施，但是目前由于需求不明确，可以考虑暂时不实施。作为建议提供。 1 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。 2 严格控制CON端口的访问。配合使用访问控制列表控制对CON口的访问。 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同时给CON口设置高强度的密码。 3 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 4 建议采用权限分级策略。如：Router（Config）#username test privilege 10 xxxx Router（Config）#privilege EXEC level 10 telnet Router（Config）#privilege EXEC level 10 show ip access-list 5 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. Router（config）#service password-encryption Router（config）#enable secret 6 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。三、路由器路由协议安全配置1 建议启用IP Unicast Reverse-Path Verification.它能够检查源IP地址的准确性，从而可以防止一定的IP Spooling.但是它只能在启用CEF（Cisco Express Forwarding）的路由器上使用。 uRPF有三种方式，strict方式、ACL方式和loose方式。在接入路由器上实施时，对于通过单链路接入网络的用户，建议采用strict方式；对于通过多条链路接入到网络的用户，可以采用ACL方式和loose方式。在出口路由器上实施时，采用loose方式。Strict方式：Router# config t ！启用CEF Router（Config）# ip cef ！启用Unicast Reverse-Path Verification Router（Config）# interface eth0/1 Router（Config-if）# ip verify unicast reverse-path ACL方式：interface pos1/0 ip verify unicast reverse-path 190 access-list 190 permit ip {customer network} {customer network mask} any access-list 190 deny ip any any [log]这个功能检查每一个经过路由器的数据包的源地址，若是不符合ACL的，路由器将丢弃该数据包。 Loose方式：interface pos 1/0 ip ver unicast source reachable-via any这个功能检查每一个经过路由器的数据包，在路由器的路由表中若没有该数据包源IP地址的路由，路由器将丢弃该数据包。2 启用OSPF路由协议的认证。默认的OSPF认证密码是明文传输的，建议启用MD5认证。并设置一定强度密钥（key，相对的路由器必须有相同的Key）。