|  |
| --- |
| **老男孩信息系统安全配置基线**  **CISCO网络设备分册（初稿）** |
| **版本 V1.0** |

**二○一九年一月**

|  |  |  |  |
| --- | --- | --- | --- |
| ■版本变更记录 | | | |
| 时间 | 版本 | 说明 | 修改人 |
|  |  |  |  |
|  |  |  |  |

|  |
| --- |
| 目录 |
| [一. 概述 4](#_Toc408348093)  [1.1适用范围 4](#_Toc408348094)  [1.2规范依据 4](#_Toc408348095)  [1.3实施策略 4](#_Toc408348096)  [二. 安全配置基线标准 6](#_Toc408348097)  [2.1身份鉴别 6](#_Toc408348098)  [2.1.1分配用户账号 6](#_Toc408348099)  [2.1.2配置密码复杂度 7](#_Toc408348100)  [2.1.3加密账号静态口令 8](#_Toc408348101)  [2.1.4删除无关帐号 9](#_Toc408348102)  [2.1.5启用远程认证授权 10](#_Toc408348103)  [2.2访问控制 11](#_Toc408348104)  [2.2.1防止地址欺骗 11](#_Toc408348105)  [2.3安全审计 13](#_Toc408348106)  [2.3.1记录账号登录 13](#_Toc408348107)  [2.3.2记录用户操作 14](#_Toc408348108)  [2.3.3启用远程日志 16](#_Toc408348109)  [2.3.4启用NTP服务 18](#_Toc408348110)  [2.4入侵防范 19](#_Toc408348111)  [2.4.1过滤已知攻击 19](#_Toc408348112)  [2.5网络设备防护 21](#_Toc408348113)  [2.5.1启用SSH登录维护 21](#_Toc408348114)  [2.5.2启用登录失败处置 23](#_Toc408348115)  [2.5.3启用登录超时退出 23](#_Toc408348116)  [2.5.4更改设备缺省Banner 25](#_Toc408348117)  [2.5.5禁用非必要网络服务 25](#_Toc408348118)  [2.5.6限制管理员远程登录 27](#_Toc408348119)  [2.5.7更改SNMP默认Community串 28](#_Toc408348120)  [2.5.8限制SNMP服务主机 28](#_Toc408348121)  [2.5.9禁用SNMP写功能 29](#_Toc408348122)  [2.5.10启用协议的认证加密功能 30](#_Toc408348123)  [2.6其他安全项 31](#_Toc408348124)  [2.6.1关闭未使用接口 31](#_Toc408348125)  [三. 评审与修订 32](#_Toc408348126) |

1. 概述
   1. 适用范围

本配置基线适用于老男孩的CISCO网络设备，主要涉及CISCO网络设备安全配置方面的基本要求，用于指导安全例行工作、新系统入网安全检查等场合。

在未特别说明的情况下，均适用于所有运行的CISCO网络设备。

* 1. 规范依据

根据老男孩目前CISCO网络设备的安全现状，综合参考各信息系统运维部门的意见，结合金融行业等级保护实施指引，制定适合于老男孩的基线配置规范。

主要参考依据如下：

* JR/T0071-2012《金融行业信息系统信息安全等级保护实施指引》（2012年7月发布）
  1. 实施策略

结合网络和信息系统建设情况，考虑安全配置项影响的范围，结合以往工作经验，提出如下安全项目实施策略：

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **配置类别** | **安全基线项目名称** | **实施策略** |
| 1 | 身份鉴别 | 分配用户账号 | 必须实施 |
| 2 | 身份鉴别 | 配置密码复杂度 | 必须实施 |
| 3 | 身份鉴别 | 加密账号静态口令 | 必须实施 |
| 4 | 身份鉴别 | 删除无关帐号 | 按需实施 |
| 5 | 身份鉴别 | 启用远程认证授权 | 按需实施 |
| 6 | 访问控制 | 防止地址欺骗 | 按需实施 |
| 7 | 安全审计 | 记录账号登录 | 必须实施 |
| 8 | 安全审计 | 记录用户操作 | 按需实施 |
| 9 | 安全审计 | 启用远程日志 | 按需实施 |
| 10 | 安全审计 | 启用NTP服务 | 按需实施 |
| 11 | 入侵防范 | 过滤已知攻击 | 建议实施 |
| 12 | 网络设备防护 | 启用SSH登录维护 | 必须实施 |
| 13 | 网络设备防护 | 启用登录失败处置 | 必须实施 |
| 14 | 网络设备防护 | 启用登录超时退出 | 必须实施 |
| 15 | 网络设备防护 | 更改设备缺省Banner | 必须实施 |
| 16 | 网络设备防护 | 禁用非必要网络服务 | 建议实施 |
| 17 | 网络设备防护 | 限制管理员远程登录 | 按需实施 |
| 18 | 网络设备防护 | 更改SNMP默认Community串 | 按需实施 |
| 19 | 网络设备防护 | 限制SNMP服务主机 | 按需实施 |
| 20 | 网络设备防护 | 禁用SNMP写功能 | 按需实施 |
| 21 | 网络设备防护 | 启用协议的认证加密功能 | 按需实施 |
| 22 | 其他安全项 | 关闭未使用接口 | 按需实施 |

1. 安全配置基线标准
   1. 身份鉴别
      1. 分配用户账号

|  |  |
| --- | --- |
| **安全基线项目名称** | 分配用户账号（必须实施） |
| **安全基线编号** | 网络设备-CISCO-配置-1 |
| **安全基线项说明** | 按照用户分配帐号，避免不同用户间共享帐号，避免用户帐号和设备间通信使用的帐号共享。 |
| **配置方法** | **版本：IOS 12.x**  **1.参考配置操作**  Router# config t  Enter configuration commands, one per line. End with CNTL/Z.  Router(config)# service password-encryption  Router(config)# username ruser1 password 3d-zirc0nia  Router(config)# username ruser1 privilege 1  Router(config)# username ruser2 password 2B-or-3B  Router(config)# username ruser2 privilege 1  Router(config)# end  Router#  **2.补充操作说明**  无 |
| **检查方法** | **1.判定条件**   1. 配置文件中，存在不同的帐号分配 2. 网络管理员确认用户与帐号分配关系明确   **2.检测操作**  使用show running-config命令，如下例：  router#show running-config  Building configuration...  Current configuration:  !  service password-encryption  username ruser1 password 3d-zirc0nia  username ruser1 privilege 1  username ruser2 password 2B-or-3B  username ruser2 privilege 1  **3.补充说明**  使用共享帐号容易造成职责不清 |
| **依据** | 7.1.2.7网络：网络设备防护（G3）：a）应对登录网络设备的用户进行身份鉴别；  7.1.2.7网络：网络设备防护（G3）：c）网络设备用户的标识应唯一。 |
| **备注** | 需要手工检查，由管理员确认帐号分配关系。 |

* + 1. 配置密码复杂度

|  |  |
| --- | --- |
| **安全基线项目名称** | 配置密码复杂度（必须实施） |
| **安全基线编号** | 网络设备-CISCO-配置-2 |
| **安全基线项说明** | 对于采用静态口令认证技术的设备，口令长度至少8位，并包括数字、小写字母、大写字母和特殊符号四类中至少两类；且5次以内不得设置相同的口令；密码应至少每90天进行更换。 |
| **配置方法** | **版本：IOS 12.x**  **1.参考配置操作**  Router#configure terminal  Enter configuration commands, one per line. End with CNTL/Z.  Router(config)#aaa new-model  Router(config)#aaa authentication login default group tacacs+  Router(config)#aaa authentication enable default group tacacs+  Router(config)#tacacs-server host 192.168.6.18  Router(config)#tacacs-server key Ir3@1yh8n#w9@swD  Router(config)#end  Router#  **2.补充操作说明**  与外部TACACS+ server 192.168.6.18 联动，远程登录使用TACACS+ server验证；口令强度由TACACS+ server控制 |
| **检查方法** | 人工查询是否符合复杂度要求 |
| **依据** | 7.1.2.7网络：网络设备防护（G3）：e）身份鉴别信息应具有不易被冒用的特点，口令应有复杂度要求并定期更换。 |
| **备注** | 需客户自行设置密码 |

* + 1. 加密账号静态口令

|  |  |
| --- | --- |
| **安全基线项目名称** | 加密账号静态口令（必须实施） |
| **安全基线编号** | 网络设备-CISCO-配置-3 |
| **安全基线项说明** | 账号静态口令必须使用不可逆加密算法加密，以密文形式存放，如使用enable secret配置enable密码，不使用enable password配置enable密码。 |
| **配置方法** | **版本：IOS 12.x**  **1.参考配置操作**  Router# config t  Enter configuration commands, one per line. End with CNTL/Z.  Router(config)#service password-encryption  Router(config)# enable secret 2-mAny-rOUtEs  Router(config)# no enable password  Router(config)# end  **2.补充操作说明**  无 |
| **检查方法** | **1.判定条件**  配置文件无明文密码字段  **2.检测操作**  使用show running-config命令，如下例：  router#show running-config  Building configuration...  Current configuration:  !  service password-encryption  enable secret 5 $1oxphetTb$rTsF$EdvjtWbi0qA2g  username ciscoadmin password 7 Wbi0qA1$rTsF$Edvjt2gpvyhetTb  **3.补充说明**  如果不加密,使用show running-config命令,可以看到未加密的密码 |
| **依据** | 7.1.2.7网络：网络设备防护（G3）：g）当对网络设备进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听；  7.1.2.7网络：网络设备防护（G3）：e）身份鉴别信息应具有不易被冒用的特点，口令应有复杂度要求并定期更换。 |
| **备注** |  |

* + 1. 删除无关帐号

|  |  |
| --- | --- |
| **安全基线项目名称** | 删除无关账号（按需实施） |
| **安全基线编号** | 网络设备-CISCO-配置-4 |
| **安全基线项说明** | 删除与设备运行、维护等工作无关的帐号。 |
| **配置方法** | **版本：IOS 12.x**  **1.参考配置操作**  Router# config t  Enter configuration commands, one per line. End with CNTL/Z.  Router(config)# no username ruser3  **2.补充操作说明**  无 |
| **检查方法** | **1.判定条件**   1. 配置文件存在多帐号 2. 网络管理员确认所有帐号与设备运行、维护等工作有关   **2.检测操作**  使用show running-config命令，如下例：  router#show running-config  Building configuration...  Current configuration:  !  username user1 privilege 1 password password1  username nobodyuse privilege 1 password password1  **3.补充说明**  删除不用的帐号，避免被利用 |
| **依据** | 7.1.2.7网络：网络设备防护（G3）：a）应对登录网络设备的用户进行身份鉴别；  7.1.2.7网络：网络设备防护（G3）：c）网络设备用户的标识应唯一；  7.1.2.7网络：网络设备防护（G3）：n) 应定期检查并锁定或撤销网络设备中不必要的用户账号。 |
| **备注** | 需要手工检查，由管理员判断是否存在无关帐号 |

* + 1. 启用远程认证授权

|  |  |
| --- | --- |
| **安全基线项目名称** | 启用远程认证授权（按需实施） |
| **安全基线编号** | 网络设备-CISCO-配置-5 |
| **安全基线项说明** | 设备通过相关参数配置，与认证系统联动，满足帐号、口令和授权的强制要求。 |
| **配置方法** | **版本：IOS 12.x**  **1.参考配置操作**  Router#configure terminal  Enter configuration commands, one per line. End with CNTL/Z.  Router(config)#aaa new-model  Router(config)#aaa authentication login default group tacacs+  Router(config)#aaa authentication enable default group tacacs+  Router(config)#tacacs-server host 192.168.6.18  Router(config)#tacacs-server key Ir3@1yh8n#w9@swD  Router(config)#end  Router#  **2.补充操作说明**  与外部TACACS+ server 192.168.6.18联动，远程登录使用TACACS+ server验证 |
| **检查方法** | **1.判定条件**  帐号、口令配置，指定了认证系统  **2.检测操作**  使用show running-config命令，如下例：  router#show running-config  Building configuration...  Current configuration:  !  aaa new-model  aaa authentication login default group tacacs+  aaa authentication enable default group tacacs+  tacacs-server host 192.168.6.18  tacacs-server key Ir3@1yh8n#w9@swD  **3.补充说明**  无 |
| **依据** | 7.1.2.7网络：网络设备防护（G3）：a）应对登录网络设备的用户进行身份鉴别；  7.1.2.7网络：网络设备防护（G3）：c）网络设备用户的标识应唯一。 |
| **备注** |  |

* 1. 访问控制
     1. 防止地址欺骗

|  |  |
| --- | --- |
| **安全基线项目名称** | 防止地址欺骗（按需实施） |
| **安全基线编号** | 网络设备-CISCO-配置-6 |
| **安全基线项说明** | 配置网络设备，防止地址欺骗。 |
| **配置方法** | **版本：IOS 12.x**  **1.参考配置操作**  对向内流量配置：  Router(config)# no access-list 100  Router(config)# access-list 100 deny ip 192.168.10.0 0.0.0.255 any log  Router(config)# access-list 100 deny ip 127.0.0.0 0.255.255.255 any log  Router(config)# access-list 100 deny ip 10.0.0.0 0.255.255.255 any log  Router(config)# access-list 100 deny ip 0.0.0.0 0.255.255.255 any log  Router(config)# access-list 100 deny ip 172.16.0.0 0.15.255.255 any log  Router(config)# access-list 100 deny ip 192.168.0.0 0.0.255.255 any log  Router(config)# access-list 100 deny ip 192.0.2.0 0.0.0.255 any log  Router(config)# access-list 100 deny ip 169.254.0.0 0.0.255.255 any log  Router(config)# access-list 100 deny ip 224.0.0.0 15.255.255.255 any log  Router(config)# access-list 100 deny ip host 255.255.255.255 any log  Router(config)# access-list 100 permit ip any 192.168.10.0 0.0.0.255  Router(config)# access-list 100 deny ip any any log  Router(config)# interface eth0  Router(config-if)# description External interface to 192.168.0./16 net  Router(config-if)# ip address 192.168.10.20 255.255.0.0  Router(config-if)# ip access-group 100 in  Router(config-if)# exit  Router(config)# interface eth1  Router(config-if)# description Internal interface to 192.168.10.0/24 net  Router(config-if)# ip address 192.168.10.250 255.255.255.0  Router(config-if)# end  对向外流量配置：  Router(config)# no access-list 102  Router(config)# access-list 102 permit ip 192.168.10.0 0.0.0.255 any  Router(config)# access-list 102 deny ip any any log  Router(config)# interface eth 0/1  Router(config-if)# description "internal interface"  Router(config-if)# ip address 192.168.10.250 255.255.255.0  Router(config-if)# ip access-group 102 in  **2.补充操作说明**  假设内部网络是192.168.10.0 |
| **检查方法** | **1.判定条件**  各接口只转发属于自己ip范围内的源地址数据包流出  **2.检测操作**  使用show running-config命令，如下例：  router#show running-config  …  access-list 10 deny ip 192.168.0.0 0.0.0.255 any log  access-list 10deny ip 127.0.0.0 0.255.255.255 any log  …  int f1/1  description the outside interface of permeter router  ip access-group 10 in  …  access-list 11 permit ip 192.168.0.0 0.0.0.255 any  access-list 11 deny ip any any log  interface s1/1  description inside interface of perimeter router  ip address 192.168.0.254 255.255.255.0  ip access-group 11 in  **3.补充说明**  地址欺骗可以造成内部网络的混乱，让某些被欺骗的计算机无法正常访问内外网，让网关无法和客户端正常通信。 |
| **依据** | 7.1.2.2网络：访问控制（G3）：f）重要网段应采取技术手段防止地址欺骗。 |
| **备注** | 需客户根据业务情况配置 |

* 1. 安全审计
     1. 记录账号登录

|  |  |
| --- | --- |
| **安全基线项目名称** | 记录账号登录（必须实施） |
| **安全基线编号** | 网络设备-CISCO-配置-7 |
| **安全基线项说明** | 与记账服务器（如RADIUS服务器或TACACS服务器）配合，设备应配置日志功能，对用户登录进行记录，记录内容包括用户登录使用的帐号，登录是否成功，登录时间，以及远程登录时，用户使用的IP地址。 |
| **配置方法** | **版本：IOS 12.x**  **1.参考配置操作**  Router#configure terminal  Enter configuration commands, one per line. End with CNTL/Z.  Router(config)#aaa new-model  Router(config)#aaa accounting connection default start-stop group tacacs+  Router(config)#aaa accounting exec default start-stop group tacacs+ Router(config)#end  Router1#  **2.补充操作说明**  使用TACACS+ server |
| **检查方法** | **1.判定条件**  配置了AAA模板的上述具体条目  **2.检测操作**  使用show running-config命令，如下例：  router1#show runn | include aaa  Building configuration...  Current configuration:  !  aaa new-model  aaa authentication login default group tacacs+  aaa authorization exec default group tacacs+  aaa session-id common  **3.补充说明**  无 |
| **依据** | 7.1.2.3网络：安全审计（G3）：b）审计记录应包括：事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；  7.1.2.3网络：安全审计（G3）：c）应能够根据记录数据进行分析，并生成审计报表；  7.1.2.3网络：安全审计（G3）：d）应对审计记录进行保护，避免受到未预期的删除、修改或覆盖等。 |
| **备注** |  |

* + 1. 记录用户操作

|  |  |
| --- | --- |
| **安全基线项目名称** | 记录用户操作（按需实施） |
| **安全基线编号** | 网络设备-CISCO-配置-8 |
| **安全基线项说明** | 与记账服务器（如TACACS服务器）配合，设备应配置日志功能，记录用户对设备的操作，如帐号创建、删除和权限修改，口令修改，读取和修改设备配置，读取和修改业务用户的话费数据、身份数据、涉及通信隐私数据。记录需要包含用户帐号，操作时间，操作内容以及操作结果。 |
| **配置方法** | **版本：IOS 12.x**  **1.参考配置操作**  Router#configure terminal  Enter configuration commands, one per line. End with CNTL/Z.  Router(config)#aaa new-model  Router(config)#aaa accounting commands 1 default start-stop group tacacs+  Router(config)#aaa accounting commands 15 default start-stop group tacacs+  Router(config)#end  Router1#  **2.补充操作说明**  使用TACACS+ server |
| **检查方法** | **1.判定条件**  配置了AAA模板的上述具体条目  **2.检测操作**  使用show running-config命令，如下例：  router1#show runn | include aaa  Building configuration...  Current configuration:  !  aaa new-model  aaa accounting commands 1 default start-stop group tacacs+  aaa accounting commands 15 default start-stop group tacacs+  **3.补充说明**  无 |
| **依据** | 7.1.2.3网络：安全审计（G3）：b）审计记录应包括：事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；  7.1.2.3网络：安全审计（G3）：c）应能够根据记录数据进行分析，并生成审计报表；  7.1.2.3网络：安全审计（G3）：d）应对审计记录进行保护，避免受到未预期的删除、修改或覆盖等。 |
| **备注** |  |

* + 1. 启用远程日志

|  |  |
| --- | --- |
| **安全基线项目名称** | 启用远程日志（按需实施） |
| **安全基线编号** | 网络设备-CISCO-配置-9 |
| **安全基线项说明** | 设备应支持远程日志功能。所有设备日志均能通过远程日志功能传输到日志服务器。设备应支持至少一种通用的远程标准日志接口，如SYSLOG、FTP等。 |
| **配置方法** | **版本：IOS 12.x**  **1.参考配置操作**  路由器侧配置：  Router# config t  Enter configuration commands, one per line. End with CNTL/Z  Router(config)# logging on  Router(config)# logging trap information  Router(config)# logging 192.168.0.100  Router(config)# logging facility local6  Router(config)# logging source-interface loopback0  Router(config)# exit  Router# show logging  Syslog logging: enabled (0 messages dropped, 11 flushes, 0overruns)  Console logging: level notifications, 35 messages logged  Monitor logging: level debugging, 35 messages logged  Buffer logging: level informational, 31 messages logged  Logging to 192.168.0.100, 28 message lines logged  ..  Router#  **2补充操作说明**   1. 假设把router日志存储在192.168.0.100的syslog服务器上   路由器侧配置描述如下：  启用日志  记录日志级别设定“information”  记录日志类型设定“local6”  日志发送到192.168.0.100  日志发送源是loopback0  配置完成可以使用“show logging”验证  服务器侧配置参考如下：  Syslog服务器配置参考：  在Syslog.conf上增加一行  # Save router messages to routers.log  local6.debug /var/log/routers.log  创建日志文件  #touch /var/log/routers.log   1. 如果使用snmp存储日志参考配置如下：   Router# config t  Enter configuration commands, one per line. End with CNTL/Z.  Router(config)# logging trap information  Router(config)# snmp-server host 192.168.0.100 traps public  Router(config)# snmp-server trap-source loopback0  Router(config)# snmp-server enable traps syslog  Router(config)# exit |
| **检查方法** | 1.**判定条件**   1. Syslog logging和SNMP logging至少有一个为“enabled” 2. Logging to后面的主机名或IP指向日志服务器 3. 通常记录日志数不为0   **2.检测操作**  使用show logging命令，如下例：  Router# show logging  Syslog logging: enabled  Console logging: disabled  Monitor logging: level debugging, 266 messages logged.  Trap logging: level informational, 266 messages logged.  Logging to 192.180.2.238  SNMP logging: disabled, retransmission after 30 seconds  0 messages logged  Router#  **3.补充说明**  无 |
| **依据** | 7.1.2.3网络：安全审计（G3）：a）审计记录应包括：应对网络系统中的网络设备运行状况、网络流量、用户行为等进行日志记录；  7.1.2.3网络：安全审计（G3）：c）应能够根据记录数据进行分析，并生成审计报表；  7.1.2.3网络：安全审计（G3）：d）应对审计记录进行保护，避免受到未预期的删除、修改或覆盖等。 |
| **备注** | 根据应用场景的不同，如部署场景需开启此功能，则强制要求此项。建议核心设备必选，其它根据实际情况启用。 |

* + 1. 启用NTP服务

|  |  |
| --- | --- |
| **安全基线项目名称** | 启用NTP服务（按需实施） |
| **安全基线编号** | 网络设备-CISCO-配置-10 |
| **安全基线项说明** | 开启NTP服务，保证日志功能记录的时间的准确性。 |
| **配置方法** | **版本：IOS 12.x**  **1.参考配置操作**  配置命令如下：  Router# config t  Enter configuration commands, one per line. End with CNTL/Z.  Router(config)# interface eth0/0  Router(config-if)# no ntp disable  Router(config-if)# exit  Router(config)# ntp server 14.2.9.2 source loopback0  Router(config)# exit  **2.补充操作说明**  需要到每个端口开启NTP |
| **检查方法** | **1.判定条件**   1. 存在 ntp server 配置条目 2. 日志记录时间准确   **2.检测操作**   1. 使用show running-config命令，如下例：   router#show running-config  Building configuration...  Current configuration:  !  …  no ntp disable  ntp update-calendar  ntp server 128.237.32.2  ntp server 142.182.31.6   1. show logging | include NTP   000019: Jan 29 10:57:52.633 EST: %NTP-5-PEERSYNC: NTP synced to peer 172.25.1.5  000020: Jan 29 10:57:52.637 EST: %NTP-6-PEERREACH: Peer 172.25.1.5 is reachable  **3.补充说明**  日志时间不准确导致安全事件定位的不准确 |
| **依据** | 7.1.2.3网络：安全审计（G3）：b）审计记录应包括：事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；  7.1.2.7网络：网络设备防护（G3）：m) 应建立网络设备的时钟同步机制。 |
| **备注** |  |

* 1. 入侵防范
     1. 过滤已知攻击

|  |  |
| --- | --- |
| **安全基线项目名称** | 过滤已知攻击（建议实施） |
| **安全基线编号** | 网络设备-CISCO-配置-11 |
| **安全基线项说明** | 在网络边界，设置安全访问控制，过滤掉已知安全攻击数据包，例如udp 1434端口（防止SQL slammer蠕虫）、tcp445,5800,5900（防止Della蠕虫）。 |
| **配置方法** | **版本：IOS 12.x**   1. **参考配置操作**   屏蔽常见的漏洞端口1433、4444,tftp UDP69,135,137,138,139,445,593, 1434， 5000，5554 ，5800,5900,6667,9996等：  Router(config)# no access-list 102  Router(config)# access-list 102 deny tcp any any eq 445 log  Router(config)# access-list 102 deny tcp any any eq 5800 log  Router(config)# access-list 102 deny tcp any any eq 5900 log  Router(config)# access-list 102 deny udp any any eq 1434 log  Router(config)#access-list 102 deny udp destination-port eq tftp log  Router(config)#access-list 102 deny tcp destination-port eq 135 log  Router(config)#access-list 102 deny udp destination-port eq 137 log  Router(config)#access-list 102 deny udp destination-port eq 138 log  Router(config)#access-list 102 deny tcp destination-port eq 139 log  Router(config)#access-list 102 deny udp destination-port eq netbios-ssn log  Router(config)#access-list 102 deny tcp destination-port eq 539 log  Router(config)#access-list 102 deny udp destination-port eq 539 log  Router(config)#access-list 102 deny tcp destination-port eq 593 log   1. **补充操作说明**   无 |
| **检查方法** | **1.判定条件**   1. 存在类似acl，拒绝上述端口   **2.检测操作**  使用show running-config命令，如下例：  router#show running-config  …  access-list 102  access-list 102 deny tcp any any eq 445 log  access-list 102 deny tcp any any eq 5800 log  access-list 102 deny tcp any any eq 5900 log  access-list 102 deny udp any any eq 1434 log  …  **3.补充说明**  如果不进行上述设置将导致远程攻击者对部分常见应用发功攻击或病毒感染 |
| **依据** | 7.1.2.5网络：入侵防范（G3）：a）应在网络边界处监视以下攻击行为：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP碎片攻击和网络蠕虫攻击等；  7.1.2.5网络：入侵防范（G3）：b）当检测到攻击行为时，记录攻击源IP、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时应提供报警。 |
| **备注** |  |

* 1. 网络设备防护
     1. 启用SSH登录维护

|  |  |
| --- | --- |
| **安全基线项目名称** | 启用SSH登录维护（必须实施） |
| **安全基线编号** | 网络设备-CISCO-配置-12 |
| **安全基线项说明** | 使用telnet进行远程设备维护的时候，由于密码和通讯都是明文的，易受sniffer侦听，所以应采用SSH替代telnet。  SSH (Secure Shell)服务使用tcp 22 端口，客户端软件发起连接请求后从服务器接受公钥，协商加密方法，成功后所有的通讯都是加密的。 |
| **配置方法** | **1.参考配置操作**   * 配置主机名和域名   router# config t  Enter configuration commands, one per line. End with CNTL/Z.  router(config)# hostname Router  Router(config)# ip domain-name Router.domain-name   * 配置访问控制列表   Router(config)# no access-list 12  Router(config)# access-list 12 permit host 192.168.0.200  Router(config)# line vty 0 4  Router(config-line)# access-class 12 in  Router(config-line)# exit   * 配置账号和连接超时   Router(config)# service password-encryption  Router(config)# username normaluser password 3d-zirc0nia  Router(config)# username normaluser privilege 1  Router(config)# line vty 0 4  Router(config-line)# login local  Router(config-line)# exec-timeout 5 0   * 生成rsa密钥对   Router(config)# crypto key generate rsa  The name for the keys will be: Router.domain-name  Choose the size of the key modulus in the range of 360 to  2048 for your General Purpose Keys. Choosing a key modulus  greater than 512 may take a few minutes.  How many bits in the modulus [512]: 2048  Generating RSA Keys …  [OK]   * 配置仅允许ssh远程登录   Router(config)# line vty 0 4  Router(config-line)# transport input ssh  Router(config-line)# exit  Router(config)#  **2.补充操作说明**  配置描述：   * 配置ssh要求路由器已经存在主机名和域名 * 配置访问控制列表，仅授权192.168.0.200访问192.168.0.100 ssh * 配置远程访问里连接超时 * 生成rsa密钥对，如果已经存在可以使用以前的。默认存在rsa密钥对sshd就启用，不存在rsa密钥对sshd就停用。   配置远程访问协议为ssh |
| **检查方法** | * 存在rsa密钥对，命令Router(config)# show crypto key mypubkey rsa； * 远程登录指定ssh协议，show running-config命令，输出中查看是否有transport input ssh字样。 |
| **依据** | 7.1.2.7网络：网络设备防护（G3）：g）当对网络设备进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。 |
| **备注** | 该项配置需要确认对应的CISCO设备的IOS版本是否支持SSH功能，如不支持，建议通过ACL控制TELNET服务登录源地址。  结合运行维护工作的实际情况，目前网络管理平台的配置管理模块需要开启路由交换上TELNET功能。因此可保留针对网管平台的TELNET登录支持，同时针对其他人工登录方式使用SSH方式登录。 |

* + 1. 启用登录失败处置

|  |  |
| --- | --- |
| **安全基线项目名称** | 启用登录失败处置（必须实施） |
| **安全基线编号** | 网络设备-CISCO-配置-13 |
| **安全基线项说明** | 设置登录失败策略，在30秒钟内对网络设备连续错误登录5次，账号锁定10分钟。 |
| **配置方法** | **1.参考配置操作**  Router(config)#login block-for 600 attempts 5 within 30  Router(config)#login delay 2  **2.补充说明**  该项配置要求设备OS的版本最低为12.4(15)T1，否则不支持。 |
| **检查方法** | **1.检测操作**  Router#show running-config | in login  查看是否包含如下关键命令语句：  login block-for 60 attempts 5 within 10  login delay 2  **2.补充说明**  无 |
| **依据** | 7.1.2.7网络：网络设备防护（G3）：f）应具有登录失败处理功能，可采取结束会话、限制非法登录次数和当网络登录连接超时自动退出等措施。 |
| **备注** |  |

* + 1. 启用登录超时退出

|  |  |
| --- | --- |
| **安全基线项目名称** | 启用登录超时退出（必须实施） |
| **安全基线编号** | 网络设备-CISCO-配置-14 |
| **安全基线项说明** | 配置登录账户超时自动退出，适用于TELNET、SSH、HTTP等管理连接和CONSOLE口登录连接等。 |
| **配置方法** | **1.参考配置操作**   * Console登录连接超时：   Router# config t  Enter configuration commands, one per line. End with CNTL/Z.  Router(config)# line con 0  Router(config-line)# exec-timeout 5 0  远程登录连接超时：  Router# config t  Enter configuration commands, one per line. End with CNTL/Z.  Router(config)# line vty 0 4  Router(config-line)# exec-timeout 5 0  **2.补充操作说明**  本例配置连接超时时间为5分钟 |
| **检查方法** | * 每种登录方式均设置了timeout值。用show running-config命令，如下例：   router#show running-config  Building configuration...  Current configuration:  ！  //下为console登录限制超时时间为10分钟  line con 0  login local  exec-timeout 10 0  exit  //下为telent登录限制超时时间为10分钟  line vty 0 4  login local  access-class 2 in  exec-timeout 10 0  exit  //限制ssh登录超时时间为90秒  ip ssh timeout 90  … |
| **依据** | 7.1.2.7网络：网络设备防护（G3）：f）应具有登录失败处理功能，可采取结束会话、限制非法登录次数和当网络登录连接超时自动退出等措施。 |
| **备注** |  |

* + 1. 更改设备缺省Banner

|  |  |
| --- | --- |
| **安全基线项目名称** | 更改设备缺省Banner（必须实施） |
| **安全基线编号** | 网络设备-CISCO-配置-15 |
| **安全基线项说明** | 修改路由交换设备的缺省Banner信息，Banner最好不要有系统平台或地址等有碍安全的信息。 |
| **配置方法** | 1. **参考配置操作**   修改banner命令如下：  Router# config t  Enter configuration commands, one per line. End with CNTL/Z.  Router(config)# banner motd ^T  Legal Notice: Access to this device is restricted.   1. **补充操作说明**   无 |
| **检查方法** | 登录查看Banner输出是否有平台、地址等敏感信息。 |
| **依据** | 7.1.2.7网络：网络设备防护（G3）：g）当对网络设备进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。 |
| **备注** |  |

* + 1. 禁用非必要网络服务

|  |  |
| --- | --- |
| **安全基线项目名称** | 禁止非必要网络服务（建议实施） |
| **安全基线编号** | 网络设备-CISCO-配置-16 |
| **安全基线项说明** | 关闭不必要的网络服务或功能：  禁用TCP SMALL SERVERS；  禁用UDP SMALL SERVERS；  禁用Finger ；  禁用HTTP SERVER；  禁用BOOTP SERVER；  关闭DNS查询功能，如要使用该功能，则显式配置DNS SERVER。  不必要的服务会加大设备的危险，例如：启动BOOTP协议将导致攻击者有更多的机会攻击此网络设备； |
| **配置方法** | 1. **参考配置操作**  * 禁用tcp/udp小服务   Router# config t  Enter configuration commands, one per line. End with CNTL/Z.  Router(config)# no service tcp-small-servers  Router(config)# no service udp-small-servers  Router(config)# exit   * 禁用Finger   Router(config)# no ip finger  Router(config)# no service finger   * 禁用HTTP SERVER   Router(config)# no ip http server   * 禁用BOOTP SERVER   Router(config)# no ip bootp server   * 关闭DNS查询功能   Router(config)# no ip domain-lookup   * 显式配置DNS SERVER   Router(config)# ip name-server 192.168.0.1  Router(config)# ip domain-lookup   1. **补充操作说明**   本例显式配置DNS SERVER指向192.168.0.1 |
| **检查方法** | 使用show running-config命令，参考操作指南中确定哪些功能处于禁止状态；查看输出中哪些处于no状态； |
| **依据** | 7.1.2.7网络：网络设备防护（G3）：k）对网络设备系统自带的的服务端口进行梳理，关掉不必要的系统服务端口，并建立相应的端口开放审批制度。 |
| **备注** | 根据业务需要关闭 |

* + 1. 限制管理员远程登录

|  |  |
| --- | --- |
| **安全基线项目名称** | 限制管理员远程登录（按需实施） |
| **安全基线编号** | 网络设备-CISCO-配置-17 |
| **安全基线项说明** | 远程执行管理员权限操作，应先以普通权限用户远程登录后，再通过enable命令进入相应级别再后执行相应操作。 |
| **配置方法** | **版本：IOS 12.x**  **1.参考配置操作**  Router# config t  Enter configuration commands, one per line. End with CNTL/Z.  Router(config)# service password-encryption  Router(config)# username normaluser password 3d-zirc0nia  Router(config)# username normaluser privilege 1  Router(config)# line vty 0 4  Router(config-line)# login local  Router(config-line)# exec-timeout 5 0  Router(config-line)# end  **2.补充操作说明**  设定帐号密码加密保存  创建normaluser帐号并指定权限级别为1；  设定远程登录启用路由器帐号验证；  设定超时时间为5分钟； |
| **检查方法** | **1.判定条件**   1. VTY使用用户名和密码的方式进行连接验证   **2.检测操作**  使用show running-config命令，如下例：  router#show running-config  Building configuration...  Current configuration:  !  service password-encryption  username normaluser password 3d-zirc0nia  username normaluser privilege 1  line vty 0 4  login local  **3.补充说明**  会导致远程攻击者通过黑客工具猜解帐号口令 |
| **依据** | 7.1.2.7网络：网络设备防护（G3）：b）应对网络设备的管理员登录地址进行限制；  7.1.2.7网络：网络设备防护（G3）：h）应实现设备特权用户的权限分离。 |
| **备注** |  |

* + 1. 更改SNMP默认Community串

|  |  |
| --- | --- |
| **安全基线项目名称** | 更改SNMP默认Community串（按需实施） |
| **安全基线编号** | 网络设备-CISCO-配置-18 |
| **安全基线项说明** | 修改SNMP的Community默认字符串，防止信息泄漏。 |
| **配置方法** | 1. **参考配置操作**   修改SNMP的Community默认通行字命令如下：  Router# config t  Enter configuration commands, one per line. End with CNTL/Z.  Router(config)# snmp-server community my\_readonly RO  Router(config)# snmp-server community my\_readwrite RW   1. **补充操作说明**   无 |
| **检查方法** | 命令：Router#show ru | include snmp-server community，输出为snmp-server communityPassword；查看Password字段是否为非默认。 |
| **依据** | 7.1.2.7网络：网络设备防护（G3）：g）当对网络设备进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听； |
| **备注** |  |

* + 1. 限制SNMP服务主机

|  |  |
| --- | --- |
| **安全基线项目名称** | 限制SNMP服务主机（按需实施） |
| **安全基线编号** | 网络设备-CISCO-配置-19 |
| **安全基线项说明** | 只与特定主机进行SNMP协议交互，有效设置对snmp服务的访问控制,可以减少信息泄露的机会。 |
| **配置方法** | 1. **参考配置操作**   使用ACL限制只与特定主机进行SNMP协议交互  Router# config t  Enter configuration commands, one per line. End with CNTL/Z.  Router(config)# access-list 75 permit host 14.2.6.60  Router(config)# access-list 75 deny any log 2．   1. **补充操作说明**   仅允许14.2.6.60收集路由器SNMP信息 |
| **检查方法** | * 命令show running-config，查看输出中SNMP服务绑定ACL进行控制。示例如下：   Router#show running  ….  access-list 3 permit host 10.1.1.1  access-list 3 deny any log  snmp-server community testc 3 |
| **依据** | 7.1.2.2网络：网络设备防护（G3）：b）应能根据会话状态信息为数据流提供明确的允许/拒绝访问的能力，控制粒度为端口级； |
| **备注** |  |

* + 1. 禁用SNMP写功能

|  |  |
| --- | --- |
| **安全基线项目名称** | 禁用SNMP写功能（按需实施） |
| **安全基线编号** | 网络设备-CISCO-配置-20 |
| **安全基线项说明** | 禁用SNMP的写（WRITE）功能。 |
| **配置方法** | 1. **参考配置操作**   Router # config t  Enter configuration commands, one per line. End with CNTL/Z.  Router (config)# no snmp-server community admin RW   1. **补充操作说明**   无 |
| **检查方法** | * 命令show running-config，查看输出中SNMP权限是否为Read-Only（简写为RO）。示例输出：   Router#show running | include snmp-server  snmp-server community testro |
| **依据** |  |
| **备注** |  |

* + 1. 启用协议的认证加密功能

|  |  |
| --- | --- |
| **安全基线项目名称** | 启用协议的认证加密功能（按需实施） |
| **安全基线编号** | 网络设备-CISCO-配置-21 |
| **安全基线项说明** | 设备与RADIUS服务器、TACACS服务器、NTP服务器、SNMP主机等支持认证加密功能的主机进行通信时，尽可能启用协议的认证加密功能，保证通信安全。 |
| **配置方法** | **版本：IOS 12.x**   1. **参考配置操作**   TACACS服务器：  Router#configure terminal  Enter configuration commands, one per line. End with CNTL/Z.  Router(config)#tacacs-server host 192.168.6.18  Router(config)#tacacs-server key Ir3@1yh8n#w9@swD  Router(config)#end  Router#  RADIUS服务器：  Router#configure terminal  Enter configuration commands, one per line. End with CNTL/Z.  Router(config)# radius-server host 192.168.6.18  Router(config)# radius-server key i\*Ma5in@u9p#s5wD   1. **补充操作说明**   启用TACACS服务器、RADIUS服务器认证 |
| **检查方法** | **1.判定条件**   1. 指定了服务器 2. 设定了认证key   **2.检测操作**  使用show running-config命令，如下例：  router#show running-config  …  ！TACACS服务器：  tacacs-server host 192.168.6.18  acacs-server key Ir3@1yh8n#w9@swD  …  ！RADIUS服务器：  radius-server host 192.168.6.18  radius-server key i\*Ma5in@u9p#s5wD  **3.补充说明**  无 |
| **依据** | 7.1.2.7网络：网络设备防护（G3）：g）当对网络设备进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听； |
| **备注** |  |

* 1. 其他安全项
     1. 关闭未使用接口

|  |  |
| --- | --- |
| **安全基线项目名称** | 关闭未使用接口（按需实施） |
| **安全基线编号** | 网络设备-CISCO-配置-22 |
| **安全基线项说明** | 设备维护中关闭未使用的接口，如路由器的AUX口；或通过SHUTDOWN命令关闭交换机上未使用接口 |
| **配置方法** | 1. **参考配置操作**   关闭AUX命令如下：  Router# config t  Enter configuration commands, one per line. End with CNTL/Z.  Router(config)# line aux 0  Router(config-line)# transport input none  Router(config-line)# login local  Router(config-line)# exec-timeout 0 1  Router(config-line)# no exec  Router(config-line)# exit   1. **补充操作说明**   无 |
| **检查方法** | 命令使用show running-config命令，查看交换机的interface是否存在shutdown情况或路由器的AUX口是否关闭。 |
| **依据** |  |
| **备注** |  |

1. 评审与修订

本标准由老男孩定期进行审查，根据审视结果修订标准，并颁发执行。