安全计算环境-网络设备-cisco（S3A3G3）作业指导书

控制点	安全要求	要求解读	测评方法	预期结果或主要证据	符合情况
身份鉴别	a)应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换	一般来说，用户登录路由器的方式包括:利用控制台端口(Console)通过串口进行本地登录连接。利用辅助端口(AUX)通过Modem进行远程拨号连接登录或者利用虚拟终端（VTY）通过TCP/IP网络进行TelnetT登录等。无论是哪一种登录方式，都需要对用户身份进行鉴别，口令是路由器用来防止非受权访问的常用手段，是路由器本身安全的一部分，因此需要加强对路由器口令的管理,包括口令的设置和存储，最好的口令存储方法是保存在TACACS+或RADIUS认证服务器上。管理员应当依据需要为路由器相应的端口加上身份签别最基本的安全控制。 路由器不允许配置用户名相同的用户，同时要防止多人共用一个账户，实行分账户管理，每名管理员设置一个单独的账户，避免出现问题后不能及时进行追查。 为避免身份鉴别信息被冒用，可以通过采用令牌、认证服务器等措施，加强身份鉴别信息的保护。如果仅仅基于口令的身份鉴别，应当保证口令复杂度和定期更改的要求。	1、Cisco:输入show run命令，存在如下类似用户列表配置: username admin privilege 15 password 0 xxxxxxxxx username audit privilege 10 password 0 xxxxxxxxx 或启用AAA服务器进行身份认证 aaa new-model aaa authentication login default group tacacs+ local enable aaa authentication enable default group tacacs+ enable 核查是否使用口令鉴别机制对登录用户进行身份标识和鉴别，用户标识是否唯一，是否存在密码为空的用户。 2、访谈管理员口令复杂度，并查看管理员登录过程验证；访谈管理员口令更换周期，并查看口令更改记录。 口今组成:应由数字、字母、特殊字符组成 口今长度:应大于8位 口令更换周期:口今一般三个月换一次	1）采取用户名口令进行身份鉴别； 2）身份标识具有唯一性； 3）用户口令8位以上由数字字母符号组成； 4）定期（90天以内）更换用户口令。	符合情况：采用了一种及以上的身份鉴别方式，身份标识具备唯一性，用户口令8位及以上，口令组成由大小写字母、数字和字符组成，口令每90天进行一次更换。 部分符合情况：预期结果1,2,3,4满足一部分为部分符合。 不符合情况：未采取身份鉴别方式，用户口令8位以下，且口令组成未采用大小写字母、数字和特殊字符，未定期进行口令更换。
	b)应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施	可以通过配置结束会话、限制管理员的最大登录失败次数、网络连接超时自动退出等多种措施实现登录失败处理功能。例如，可以利用"exec-timeout"命令.配置VTY的超时。避免一个空闲的任务一直占用VTY，从而避免恶意的攻击或远端系统的意外崩溃导致的资源独占。设置管理员最大登录失败次数，一旦该管理员的登录失败次数超过设定数值，系统将对其进行登录锁定，从而防止非法用户通过暴力破解的方式登录到路由器	1.默认登陆3次失败断开连接，不会锁定。检查登录失败锁定情况，分两种情况: a、telnet管理: 存在如下配置：login block-for 20 attempts 3 within 60 b、SSH管理: show ip ssh 查看如下配置 %Please create RSA keys (of atleast 768 bits size) to enable SSH v2. Authentication timeout: 120 secs; Authentication retries: 3 2、查看空闲超时时间：show running-config，查看VTY口下如下配置：exec-timeout X（分） X（秒）。 3、尽量争取测试验证。	1）启用了登录失败处理功能； 2）非法登录达到一定次数后将账户锁定； 3）配置了连接超时自动退出功能，超时时间不大于30分钟。	符合情况：启用了登录失败处理功能，且非法登录达到一定次数后进行限制，配置了连接自动退出功能。 部分符合情况：预期结果1,2,3满足一部分为部分符合。 不符合情况：未配置登录失败处理功能，未配置非法登录限制措施，未配置登录连接自动超时退出功能。
	c)当进行远程管理时，应采取必要措施、防止鉴别信息在网络传输过程中被窃听	当对网络设备进行远程管理时，为避免口令传输过程中别窃取，不应当使用明文传送的Telnet服务，而应当采用SSH、ITTPS等加密协议等方式进行交互式管理	核查远程管理采用何种协议， 输入show run命令，查看如下类似配置: line vty 0 4 exec-timeout 5 0 privilege level 15 password 7 05080F1C2243 transport input ssh	1）采用SSH、HTTPS等加密或其他的安全方式进行远程管理。	符合情况：采用SSH或HTTPS的加密方式进行远程管理。 部分符合情况：无部分符合情况。 不符合情况：采用telnet、http的方式进行远程管理。
	d)应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现	采用双因子鉴别是防止欺骗的有效方法，双因子鉴别不仅要求访问者知道一些鉴别信息，还需要访问者拥有鉴别特征，例如采用令牌、智能卡等	1、访谈身份鉴别过程采用哪几种鉴别技术，并查看管理员登录过程验证; 2、检查鉴别机制中是否采用了密码技术，如调用了密码机或采取SM1- SM4等算法	1）同时采用两种或两种以上组合的鉴别方式对用户身份进行鉴别; 2）其中一种方式采用密码技术。	符合情况：同时采用两种或两种以上的身份鉴别方式，且其中一种鉴别方式采用了密码技术。 部分符合情况：采用了两种及两种以上的身份鉴别方式，但未包含密码技术。 不符合情况：未同时采用两种或两种以上的身份鉴别方式。
	a)应对登录的用户分配账户和权限	为了确保交换机的安全，需要对登录的用户分配账户，并合理配置账户权限。例如，相关管理人员具有与职位相对应的账户和权限	1、核查用户账户和权限设置情况，输入show run命令，查看如下配置: username XXXXXXXX privilege xx password XXXXXXXX 2、访谈各帐户权限是否与相关管理人员职位相对应。	1）各帐户权限设置与实际业务需求一致。	符合情况：对登录的用户分配了不同的账户，且分配了不同的权限。 部分符合情况：无部分符合情况。 不符合情况：未对登录的用户分配不同的账户，且未分配相关的权限。

访问控制	b)应重命名或删除默认账户，修改默认账户的默认口令	对于路由器的默认账户，由于他们的某些权限与实际要求可能存在差异，从而造成安全隐患，因此这些默认账户应被禁用，并且应不存在默认账户admin.huawei及默认口令	1、输入show run命令，查看如下配置: username XXXXXXXX privilege xx password XXXXXXXX 核查是否存在默认帐户，如username为cisco、Cisco的帐户; 2、访谈管理是否修改默认口令，查看登录过程验证。	1）重命名默认账户、禁用或删除默认账户; 2）修改了默认帐户的默认口令。	符合情况：已重命名或删除默认账户，且已修改默认账户的默认口令。 部分符合情况：预期结果1,2为一部分符合为部分符合。 不符合情况：未重命名或删除默认账户，且使用默认口令登录。
	c)应及时删除或停用多余的、过期的账户，避免共享账户的存在	路由器中如果存在多余的、过期的账户，可能会被攻击者利用其进行非法操作的风险，因此应及时清理路由器中的账户，删除或停用多余的账户	1、 输入show run命令，查看如下配置: username XXXXXXXX privilege xx password XXXXXXXX 确认各个账户是否必要。 2、是否存在不同管理员使用同一账户。	1）不存在多余或过期账户; 2）不存在共用账户。	符合情况：通过show running未发现多余、过期账户存在，且管理员用户与账户之间一一对应，无共享账户存在。 部分符合情况：预期结果1,2为一部分符合为部分符合。 不符合情况：设备存在多余、过期账户，且存在共享账户。
	d)应授予管理用户所需的最小权限，实现管理用户的权限分离	根据管理用户的角色对权限进行细致的划分，有利于各岗位细致协调工作，同时仅授予管理用户所需的最小权限，避免出现权限的漏洞使得一些高级用户拥有过大的权限。例如，进行角色划分，分为网络管理员、安全管理员、系统管理员三个角色，并设置对应的权限	1、访谈管理员，进行角色划分，分为网络管理员，安全管理员、系统管理员三个角色，并设置对应的权限 2、Cisco路由器:输show run命令，存在如下类似配置: username admin privilege 15 password 0 xxxxxxxx usermame audit privilege 10 password 0 xxxxxxxx username operator privilege 7 password 0xxxxxxxx 3.网络管理员、安全管理员、系统管理员对应的账户为其工作任务所需的最小权限。	1）合理角色划分，管理用户的权限是否已进行分离（如管理员、审计员、操作员）; 2）各用户权限为其工作任务所需的最小权限。	符合情况：创建有系统管理员、审计管理员、安全管理员等账户通过LEVEL进行等级划分，并赋予去角色权限，各账户仅分配最小的权限。 部分符合情况：预期结果1,2为一部分符合为部分符合。 不符合情况：未创建系统管理员、审计管理员、安全管理员等账户角色，各账户均具备相同的管理员权限。
	e)应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则	访问控制策略由授权主体进行配置，它规定了主体可以对客体进行的操作，访问控制粒度要求主体为用户级或进程级，客体为文件、数据库表级	此项不适合，条款主要针对主机和数据库的测评，网络设备主要用户为运维管理人员，无其他用户	×	×
	f)访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级	访问控制策略由授权主体进行配置，它规定了主体可以对客体进行的操作、访问控制粒度要求主体为用户级或进程级，客体为文件、数据库表统。	此项不适合，条款主要针对主机和数据库的测评，网络设备主要用户为运维管理人员，无其他用户	×	×
	g)应对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问	敏感标记是强制访问控制的依据，主客体都有,它存在的形式无所谓，可能是整形的数字，也可能是字母，总之它表示主客体的安全级别。敏感标记由安全管理员进行设置，通过对重要信息资源设置敏感标记，决定主体以何种权限对客体进行操作，实现强制访问控	此项不适合	×	×
安全审计	a)应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计	为了对网络设备的运行状况、网络流量、管理记录等进行检测和记录，需要启用系统日志功能。系统日志中的每个信息都被分配了一个严重级别，并伴随一些指示性问题或事件的描述信息。 交换机的系统日志信息通常输出至各种管理端口、内部缓存或者日志服务器,在缺省情况下，控制台端口上的日志功能处于启用状态	查看日志开启情况：show logging查看如下配置: Console logging（控制台日志）: level debugging, 0 messages logged, xml disabled,filtering disabled Monitor logging（监控日志）: level debugging, 0 messages logged, xml disabled, filtering disabled Buffer logging（缓冲区日志）: enabled, xml disabled, filtering disabled	1）开启了日志审计功能; 2）对重要的用户行为和重要安全事件进行了审计。	符合情况：设备已开启log日志功能，审计范围能覆盖到每个用户，并对每个重要安全事件进行审计。 部分符合情况：预期结果1,2,3为一部分符合为部分符合。 不符合情况：设备未开启日志功能，未能审计到每个用户行为以及重要安全事件。
	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	对于交换机设备，日志审计内容需要记录时间、类型、用户、事件类型、事件是否成功等相关信息	1)查看具体日志：show loggin buffer，查看如下配置 %Oct 30 08:15:06:588 2015 HZ7503E-S OPTMOD/4/MODULE_IN:GigabitEthernet0/0/1: The transceiver is 1000_BASE_SX_SFP. 查看记录是否包含了事件的日期和时间、用户、事件类型、事件是否成功等信息。 2)查看设备时间是否与当前日期相符，确认日志的有效性：show clock	1）审计记录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; 2）系统时间正确。	符合情况：审计记录能覆盖到具体的日期和时间、用户、事件类型、事件是否成功及审计相关信息，系统时间正确。 部分符合情况：预期结果1,2为一部分符合为部分符合。 不符合情况：未开启审计功能，审计记录未包含日期和时间、用户、事件类型、事件是否成功及其他审计信息。

	c)应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等	审计记录能修帮助管理人员及时发现系统运行状况和网络攻击行为，因此需要对审计记录实施技术上和管理上的保护，历正未授权修改、删除和破坏	1）输入命令“show run”,查看如下配置：logging host 192.168.100.252；核查是否将日志发送至日志服务器或第三方日志管理平台； 2）访谈采用哪些日志备份方式，查看备份的日志记录。	1）采取技术措施对审计记录进行保护； 2）将日志发送到日志服务器或综合安全审计系统保存； 3）定期备份设备审计记录。	符合情况：部署有第三方日志审计系统，设备日志上传至第三方审计平台进行保护，日志保存时间长达6个月。 部分符合情况：预期结果1,2,3为一部分符合为部分符合。 不符合情况：未部署第三方日志审计系统，未对审计记录进行保护，日志保存时间不满足6个月。
	d)应对审计进程进行保护，防止未经授权的中断	保护好审计进程，当安全事件发生时能够及时记录事件发生的详细内容,非审计员的其他账户不能中断审计进程	1）核查非审计员的其他账户是否能中断审计进程； 2）核查是否通过堡垒机进行管理，远程管理地址是否限制为堡垒机。	1）非审计员的其他账户不能中断审计进程； 2）通过堡垒机对设备进行管理，且远程管理地址限制为堡垒机。	符合情况：非审计管理员的其他账户不能中断审计进程。 部分符合情况：无部分符合情况。 不符合情况：非审计管理员的其他账户能中断审计进程。
入侵防范	a)应遵循最小安装的原则仅安装需要的组件和应用程序	遵循最小安装原则，仅安装需要的组件和应用程序，能够极大的降低遭受攻击的可能性。及时更新系统补丁，避免遭受由于系统漏洞带来的风险	此项不适合，该项要求一般在服务器上实现	×	×
	b)应关闭不需要的系统服务、默认共享和高危端口	关闭不需要的系统服务、默认共享和高危端口，可以有效降低系统遭受攻击的可能性	输入show run命令。根据实际网络环境参考是否关闭不必要服务: no service tcp-small-servers no service udp-smal-servers. no cdp run no cdp enable no ip finger no service finger no ip bootp server no ip source-route no ip proxy-arp no ip directed-broadcast no ip domain-lookup	1）已关闭非必要的系统服务。	符合情况：已关闭不需要的系统服务、默认共享和高危端口等。 部分符合情况：无部分符合情况。 不符合情况：存在多余系统服务ftp，telnet等，存在高危端口和共享端口等。
	c)应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制	为了保证安全，需要对通过VTY访问网络设备的登录地址进行限制，避免未授权的访问，可以利用ip access-class 限制访问VTY的IP地址范围。同时，由于VTYs的数目有一定的限制，当所有的VTYs用完，就不能再建立远程的网络连接了。这就有可能被利用进行Dos (拒绝服务攻击)	输入show run命令，查看如下类似配置: access-list 10 access-list 10 permit 192.168.0.1 access-list 10 deny any line vty 0 4 access-class 10 in 核查是否对设备远程管理地址进行了限制，限制范围是否仅管理终端或堡垒机。	1）仅允许管理终端或堡垒机远程登录设备。	符合情况：通过策略限制设备仅通过某地址或地址段可进行远程管理。 部分符合情况：无部分符合情况。 不符合情况：未采取措施对远程管理设备的地址进行限制。
	d)应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求	本条款要求应用系统应对数据的有效性进行验证，主要验证那些通过人机接口(如程序的界面)输入或通过通信接口输入的数据格式或长度是否符合系统设定要求，防止个别用户输入畸形数据而导致系统出错(如SQL 注入攻击等) ,人而影响系统的正常使用甚至危害系统的安全	此项不适合，该项要求一般在应用层面上核查	×	×
	e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞	核查漏扫修补报告，管理员定期进行漏洞扫描。发现漏洞在经过充分测试评估后及时修补漏洞	1）访谈是否定期进行漏洞扫描，查看漏洞扫描报告； 2）是否对已发现的漏洞在经过充分测试评估后及时修补。	1）定期（至少每年一次，测评扫的不算）进行漏洞扫描，并生成漏洞扫描报告； 2）及时修补漏洞或经过测试评估后充分说明漏洞不进行修补。	符合情况：定期对设备进行漏洞扫描，且针对发现的漏洞经过测试评估后及时进行修补。 部分符合情况：无部分符合情况。 不符合情况：未定期对设备进行漏洞扫描，且未进对发现的漏洞进行测评评估后及时进行修补。
	f)应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警	要维护系统安全，必须进行主动监视，一般是在网络边界、核心等重要节点处部署IDS. IPS等系统，或在防火墙、UTM房用入侵检测功能，以检查息是否发生了入侵和攻击	此项不适合，该项要求一般在入侵防护系统上实现	×	×

恶意代码防范	应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断	无论是Windows主机还是Linux主机，都面临木马、蠕虫等病毒的破坏。因此一般的主机为防范病毒，均会安装反病毒软件，或者采用可信验证机制对系统程序、应用程序等进行可信执行验证	此项不适合，该项要求一般在服务器上实现	×	×
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心	设备应作为通信设备或边界设备对待	1)应核查是否基于可信根对设备的系统引导程序、系统程序、重要配置参数和关键应用程序等进行可信验证 2)应核查是否在应用程序的关键执行环节进行动态可信验证 3)应测试验证当检测到设备的可信性受到破坏后是否进行报警 4)应测试验证结果是否以审计记录的形式送至安全管理中心 (2.3)	1)计算设备具有可信根芯片或硬件 2)启动过程基于可信根对系统引导程序、系统程序，重要配置参数和关键应用程序等进行可信验证度量 3)在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心 4)安全管理中心可以接收设备的验证结果记录 (2.3)	符合情况：计算设备均部署了可信芯片或硬件进行可信验证，均基于可信根对引导程序、系统程序，重要配置参数和关键应用程序进行可信验证度量，在检测到可信性破坏后进行报警，并将验证结果送至安全管理中心，并验证。 部分符合情况：预期结果1，2，3，4点满足一部分为部分符合。 不符合情况：未采取措施计算设备部署了可信芯片或硬件进行可信验证，均基于可信根对引导程序、系统程序，重要配置参数和关键应用程序进行可信验证度量，在检测到可信性破坏后进行报警，并将验证结果送至安全管理中心，