ICS 35.040
L 80

中华人民共和国国家标准

GB/T 21050—2007

信息安全技术 网络交换机安全技术要求（评估保证级3）

Information security techniques—Security requirements for network switch (EAL3)

2007-08-24 发布　　2008-01-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

本标准依据GB/T 18336—2001《信息技术　安全技术　信息技术安全性评估准则》的要求，规定了网络交换机的安全技术要求。附录A和附录B是资料性附录，附录A对本标准的内在合理性进行了阐述，附录B是安全功能要求的应用注释。

本标准由全国信息安全标准化技术委员会提出并归口。

本标准起草单位：中国信息安全产品测评认证中心。

本标准主要起草人：李守鹏、徐长醒、付敏、王书毅、郭颖、刘楠、毕强、王迪、裘晓峰、闫石、王眉林、刘威鹏、李云雪、张展、苏智睿、王伟雄、王怡、万晓兰。

引　言

本标准定义了网络交换机应在生产商安全目标文档中包括的安全要求的最小集合。系统集成商和信息系统安全工程师可以利用本标准确认现有交换机的应用领域，以提供更为全面的安全方案。本标准规定了交换机应满足的用于信息保护的安全要求。

满足本标准的交换机，可以为组织提供自行处理的额外安全机制，以加强其对自身信息的保障。额外的安全机制包括但不限于以下几种：防火墙、网关、加密。另外，本标准适用于以下三种可能出现的管理情形，概括总结如下：

a) 购买者本人管理自己的设备。

b) 设备不是由购买者而是由网络供应商或商业组织管理。设备被安放在网络供应商或商业组织的场所。

c) 仅仅从提供商那里购买服务。

为正确执行交换机的管理功能，需要网络管理系统的支持。网络管理系统的连接参数是预先设置的，它是执行操作功能应有的一部分，但在本标准中不作为交换机的一部分。

本标准定义的要求适用于保护日常的私有敏感信息，此信息是与管理和控制相关的信息，不包括对通过交换机的用户数据的保护。本标准列出了交换机所需处理的假设、威胁和组织安全策略，并定义了交换机及其环境的独立的安全目的。最后，本标准提供了安全环境、安全目的和安全要求的对应关系。附录 A 描述了这些对应关系。

信息安全技术
网络交换机安全技术要求
（评估保证级3）

1 范围

本标准规定了网络交换机EAL3级的安全技术要求，主要包括网络交换机的安全假设、威胁和组织策略等安全环境，以及网络交换机EAL3级的安全目的、安全功能要求和安全保证要求。

本标准适用于网络交换机的研制、开发、测试、评估和采购。

本标准主要适用于信息系统安全工程师、产品生产商、安全产品评估者。

2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本标准，然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

GB/T 18336.1—2001 信息技术 安全技术 信息技术安全性评估准则 第1部分：简介和一般模型（idt ISO/IEC 15408-1:1999）

GB/T 18336.2—2001 信息技术 安全技术 信息技术安全性评估准则 第2部分：安全功能要求（idt ISO/IEC 15408-2:1999）

GB/T 18336.3—2001 信息技术 安全技术 信息技术安全性评估准则 第3部分：安全保证要求（idt ISO/IEC 15408-3:1999）

3 术语、定义、缩略语和约定

3.1 术语和定义

GB/T 18336—2001确立的以及下列术语和定义适用于本标准。

3.1.1

客户端 client

发起或接受数据传送的源。通过网络交换机的数据的源发者。

3.1.2

网络审计管理员 network audit management operator

仅具有查看权限，负责收集、分析和查看网络行为数据的网络管理角色。如：查看网络交换机配置和信息流策略等。

3.1.3

网络配置管理员 network management administrator

受到严格限制的具有部分网络管理能力的管理角色，可以执行网络交换机管理功能的子集，如：配置管理网络系统，利用权限解决网络故障等。该管理员同时具备网络审计管理员的能力。

3.1.4

网络安全管理员 network security administrator

具有所有管理级别的访问权限，可以访问网络交换机的各个区域，同时具备网络配置管理员和网络审计管理员的能力，如：创建、修改和存取访问控制列表、加载密钥、限制应用程序执行以及维护网络管

理审计日志等能力的网络管理角色。

3.1.5

网络交换机　network switch

网络中连接各个节点或其他网络设备的设备，提供了开放式系统互联模型二层的逻辑路径，基于数据链路层信息转发数据包，能够基于目的地址过滤。

3.1.6

节点　node

计算机网络系统中可以对信息进行存储或转发的设备。

3.1.7

可信信道　trusted channel

一种在网络交换机之间执行特定功能的连接，用来传输信息的控制信令、标识和鉴别数据等。

3.1.8

可信路径　trusted path

一条网络管理连接，允许通过该路径传输控制信息。可信路径的一端是网络管理端，另一端是被管理的网络交换机。

3.1.9

可信源　trusted source

能够被标识和鉴别的源或节点，从该源或节点发出的信息的完整性能够被核实和验证。

3.2　**缩略语**

ATM	异步传输模式	(Asynchronous Transfer Mode)
BGP	边界网关协议	(Border Gateway Protocol)
CMIP	通用管理接口协议	(Common Management Interface Protocol)
EAL	评估保证级	(Evaluation Assurance Level)
HTTP	超文本传输协议	(Hyper Text Transfer Protocol)
IP	互联网协议	(Internet Protocol)
IT	信息技术	(Information Technology)
LDP	标签分发协议	(Label Distribution Protocol)
MD5	报文摘要算法	(Message Digest 5)
NNI	网络到网络的接口	(Network to Network Interface)
OSPF	开放式最短路径优先	(Open Shortest Path First)
PNNI	专用网络到网络的接口	(Private Network to Network Interface)
PSTN	公共电话交换网	(Public Switched Telephone Network)
QoS	服务质量	(Quality of Service)
Rlogin	远程登录	(Remote login)
Rsh	远程 shell 协议	(Remote shell protocol)
RSVP	资源预留协议	(Resource Reservation Protocol)
RMON	远距离监控	(Remote Monitoring)
SNMP	简单网络管理协议	(Simple Network Management Protocol)
UNI	用户与网络接口	(User to Network Interface)

3.3　**约定**

本标准第 7 章“安全要求”中使用的操作约定如下：

3.3.1

反复

反复操作以多个带有空行的段落表示。

3.3.2

选择

选择操作以*下划线斜体字*表示。

3.3.3

赋值

赋值操作以“【*下划线斜体字*】”表示。

3.3.4

细化

细化操作在安全要求中有相应的声明。

4 网络交换机概述

网络交换机是一种连接网络的设备。从技术角度看，网络交换机运行在 OSI 模型的数据链路层或网络层。虽然 ATM、IP、光交换有各自不同的特性，但是它们的处理和控制方式是相似的。可信路径建立在网络交换机和管理系统之间，可信信道建立在网络交换机之间，通过可信路径可进行管理信息的交换，通过可信信道可进行网络控制信息（如，许可动态连接建立和包路由选择信息）的交换，网络控制信息由特定的请求和指令组成，如目的地址、路由选择控制和信令信息等。在 ATM 环境下，控制信息可以包括 ATM UNI、NNI 信令和 PNNI 路由选择。在 IP 环境下，控制信息可以包括 OSPF 、BGP、RSVP 和 LDP。

异步传输模式是一种面向连接的传输方法，它将传送的信息分成固定的 53 个字节长度的信元。建立连接的信元传输允许有受控延迟，流量控制可以使用固定优先级或尽力传输方式。IP 路由选择是以无连接方式传输包含在变长包内的信息。在主机之间，数据传输通常使用尽力传输方式，但不保证一定传输到目的主机。由于在传输之前没有建立逻辑路径，因此每个 IP 包可能动态地通过多个不同的路径。网络交换机基于指定的路由选择协议和网络状态动态的决定最佳路径。光网络交换机可作为多种服务的聚集器，如提供多服务平台、多波段平台。

对于光流量，至少有两种分类传输方法。一种是将流量送入完全不同的通信信道，通过建立互不影响的信道，来提供光核心的高速管道带宽，如：一个信道分配给了高优先级流量，一个信道分配给了延迟敏感数据，另一个信道分配给了尽力传输数据，等等。另一种分类传输的方法是所有类型的流量共享一个通用的通信信道，这意味着，沿着流量路径，每一个在实现队列中的网络元素都必须快速地执行分类方法。比较典型的是设备接入层执行的流量分类过程，它使用一种标记指示服务传输层该如何处理该流量，使得处在网络边界位置的光交换机知道在碰撞发生时该如何排列和区分流量的优先级。使用这种方法，不需要定义每种类型分配多少带宽，带宽是共享的并且被动态地分配。

网络交换机一般包括接口卡、端口、软件，以及驻留在其上的数据等。与网络交换机相关的所有电路都属于网络交换机的一部分，其中包括管理链路。虽然网络管理系统是必需的部件，但是它不属于本标准的规范范围，而且连接到网络交换机的其他网络部件也不属于本标准的规范范围。例如，交叉连接的数字传送系统、光传送系统、加密装置等。然而，网络交换机可以支持加密或具有连接加密装置的接口，用于加密用户数据、管理和控制信息。网络交换机具有保护网络管理和进行网络控制的功能，允许通过网络可靠传递用户信息，并具有可靠的质量和及时性。因此，本标准规范的网络交换机涉及了网络控制和管理信息。

网络控制信息包括在网络交换机之间的路由选择和信令信息。控制信息沿着路由、路径和信道控制流量传输，流量控制依赖于服务质量和丢弃信元或包的优先次序。通常控制信息可能包含在 ATM 信元或 IP 包头内，也可能在 IP 包的尾部。

ATM 网络交换机使用的 UNI(3.0、3.1、4.0)、NNI 或 Q.2931 等信令标准在网络交换机之间传递建立连接的呼叫控制信息。配置信息包含业务量描述和下游节点的定址信息，例如 PNNI、OSPF、

BGP、RSVP 和 LDP 等协议可用于在节点之间交换建立服务或保留资源的信息。对于可靠操作，网络鉴别和控制信息的完整性是必需的，路由选择和信令信息可能造成网络拓扑和交通流量信息的泄漏，因此它们是敏感的，保持路由选择和信令信息的保密性是必要的。

网络控制信息的重点主要集中在配置方面，而网络管理信息的重点主要集中在性能、故障、失效和审计方面。网络交换机通过用于管理的链路连接到负责管理的设备上，且该管理链路应该是一个可信路径。节点的保护可以通过对节点的访问保护实现，由于有多种节点访问方式，因此需要保护包括网络管理数据和网络控制信息在内的信息和资产。

有多种不同的方法来管理节点，最常用的管理方法之一叫作“带内”管理，该管理方法使用与客户相同的通信链路，管理流量使用如同客户流量一样的端口。“带内”管理可以使用如下协议：SNMP、RMON、CMIP、HTTP、Telnet 和 Rlogin 等。管理节点的另一种方法称为“带外”管理，该方法使用客户端端口之外的端口。“带外”管理还可以细分为如下几种：一是通过局部端口管理节点，例如使用一台物理上毗连于节点的笔记本电脑或哑终端连接到节点的串行接口上，对其进行管理；其次，节点也可以通过连接公用电话交换网 PSTN 的远程笔记本电脑或终端进行远程访问管理；第三，通过连接网络交换机的独立以太网接口的管理站进行远程管理(可以使用 Telnet、rsh、HTTP 协议等)。

通常存在许多不同的管理角色，所有的管理角色都被赋予一定的信任度，甚至他们的管理操作并未受到监控。管理场所是授权的访问区域，只有网络管理职员才有访问权限。通常可以通过基于网络地址的方式限制对管理连接的访问，多数管理角色只被授予执行自己职权的操作权限。不同的角色权限可能重叠或仅具有部分特权，仅有极少数的角色具有管理节点的全局特权。如“网络审计管理员”只具有查看、收集和分析网络性能数据的权限；“网络配置管理员”除拥有网络审计管理员权限外，还被赋予了访问执行配置管理、预防措施、故障查找和监测功能的权限；“网络安全管理员”具有执行加载密钥、创建和修改访问控制列表、以及限制应用程序执行的功能程序，因此，“网络安全管理员”拥有“网络配置管理员”的权限。

另外，对于组织通过购买网络服务的形式组网的情形，他们可以自己监测通过供应商网络的流量性能，以确定供应商的服务是否符合协议要求。网络供应商能够控制网络管理活动，并向客户提供网络管理报表，通过网络浏览方式以只读的权限访问管理报表，也可以直接提交给授权的个体或被认可的个体主动去获取报表。流量性能统计数据通常包括捕获量、捕获数据、日期、时间、网络使用统计与服务质量的水平、发送流量、接收流量等。

5 安全环境

5.1 假设

5.1.1 审计信息的审查(A. Audit_Review)

应周期性地审查和分析审计信息，以符合网络安全策略。

5.1.2 健壮的密码算法(A. Cryptanalytic)

网络交换机环境使用的加密算法应能抵抗密码分析攻击，并具有足够的健壮性来保护敏感数据。

5.1.3 环境的保护(A. Environment)

所有设备应该遵从环境标准，例如：对抗自然灾害的标准和电力安全的标准。网络交换机应有备份电源，以确保服务的可用性或防止数据的丢失。

5.1.4 威胁代理(A. ExpAgent)

网络交换机应能对抗由了解网络交换机实现中使用的安全性原理的专业人员发起的攻击。

5.1.5 物理保护(A. Physical)

网络交换机应置于访问受控的设施内，以避免未授权者的物理访问。还应防止网络交换机被偶然接触(例如，偶然撞击缆线可能造成无意识的破坏)。

5.1.6 **可靠的时间源(A. Time_Source)**

网络资源应连接到可靠的时间源。该时间源用于同步传输、流量审计的可靠时间戳、性能审计、管理员活动审计等。另外,还要有备份的时间源。

5.1.7 **人员培训(A. Train)**

应该培训所有人员,使其能够正确地运用、安装、配置和维护网络交换机及其安全功能和网络组件,并且所有人员应该严格遵循文档化的程序和规程。

5.2 **威胁**

5.2.1 **通信分析(T. Analysis)**

攻击者可能收集源和目标地址、大量数据,以及发送数据的日期和时间。

5.2.2 **未授权网络访问并获取数据(T. Capture)**

攻击者可能偷听、接入传输线,或用其他方式获取通信信道上传输的数据。

5.2.3 **节点泄漏(T. Compromised_Node)**

修改网络交换机配置文件或路由表,导致网络交换机运行异常、安全功能失效,或流量可能被重路由到未授权的节点。

5.2.4 **隐通道(T. Covert)**

隐通道通常在隐蔽区域隐藏信息,其目的是传送信息而不受监控。

5.2.5 **密码分析(T. Cryptanalytic)**

攻击者为了复原信息的内容,尝试对已加密的数据进行密码分析。

5.2.6 **拒绝服务(T. Denial)**

攻击者通过执行指令、发送超限额的高优先级流量数据,或执行其他操作,在网络上造成不合理的负载,造成授权客户端得不到应有的系统资源,即导致拒绝服务。

5.2.7 **部件或电源失效(T. Fail)**

系统部件或电源的失效,可能造成重要系统功能的破坏和重要系统数据的丢失。

5.2.8 **硬件、软件或固件的缺陷(T. Flaw)**

硬件、软件或固件的缺陷导致网络交换机及其安全功能的脆弱性。

5.2.9 **管理员网络授权的滥用(T. Hostile_Admin)**

管理员有意滥用其权限,不适当地访问或修改数据信息,例如:配置数据、审计数据、口令文件或误处理其他的敏感数据文件。

5.2.10 **管理错误(T. Mgmt_Error)**

网络配置管理员可能无意地不恰当地访问、修改了数据信息,或误用资源。

5.2.11 **修改协议(T. Modify)**

攻击者未经授权而修改或操纵协议(例如:路由选择、信号等协议)。

5.2.12 **网络探测(T. NtwkMap)**

攻击者可能进行网络探测来获得节点地址、路由表信息和物理位置。

5.2.13 **重放攻击(T. Replay_Attack)**

攻击者通过记录和重放通信会话,伪装成已验证的客户来非法获得网络交换机的访问权。管理信息也可能被记录和重放,从而用于伪装成已验证的管理员来得到对网络管理资源的访问权。

5.2.14 **配置数据泄漏(T. Sel_Pro)**

攻击者可能读取、修改或破坏网络交换机的安全配置数据。

5.2.15 **欺骗攻击(T. Spoof)**

客户端通过获得的网络地址来伪装成已授权的用户,未授权节点可能使用有效的网络地址来尝试访问网络。

5.2.16 **对管理端口的非授权访问(T. Unauth_Mgmt_Access)**

攻击者或滥用特权的网络配置管理员可能通过 Telnet、RMON 或其他方式访问管理端口,从而重新配置网络、引起拒绝服务、监视流量、执行流量分析等。

5.3 **组织安全策略**

5.3.1 **可核查性(P. Accountability)**

使用网络交换机传送信息的组织、拥有网络配置管理员角色的人员和开发者应该对其行为负责。

5.3.2 **审计管理人员的数据(P. Audit_Admin)**

网络管理系统应该能产生和传送审计记录,审计记录应提供充足的信息,用来判断产生会话的管理人员、管理日期、管理时间和管理行为,应周期性的审阅审计记录。

5.3.3 **操作员和节点的鉴别(P. Authentication)**

网络交换机应能支持对网络审计管理员、网络配置管理员和网络安全管理员的鉴别,并且网络交换机也应支持对等节点的鉴别。

5.3.4 **网络可用性(P. Availability)**

对于授权客户端的任务需求和传送信息需求,应能保证网络资源的有效性。

5.3.5 **信息的保密性(P. Confidentiality)**

在实时和存储状态下,应保持统计数据、配置信息和连接信息的保密性。为了保持其保密性,网络交换机要能够支持健壮的加密基础设施。对于加密装置,网络交换机要具备加解密能力或接口支持能力。

5.3.6 **默认配置(P. Default_Config)**

网络交换机的默认设置应能防止其安全功能的削弱或失效。所有有助于网络交换机安全性的功能应是默认生效的。

5.3.7 **安装和使用指南(P. Guidance)**

指南文件应能提供网络交换机的安装、配置和维护的指导。

5.3.8 **网络交换机信息更新(P. Information_Update)**

验证接收到的网络交换机信息文件、异常通知、补丁程序、升级文件等信息的完整性,上述文件或信息必须有实时的分发机制。

5.3.9 **内容的完整性(P. Integrity)**

管理和控制信息在传输期间应保持其内容的完整性。同时,所有信息在存储状态下要保持其完整性。

5.3.10 **互操作性(P. Interoperability)**

网络交换机应能与其他厂商的网络交换机互连互通。在网络交换机中要实现标准化的、非专有的协议(如路由选择、信令协议等)。厂商可以选择实现一些专有协议,但为了达到互通的目的,厂商也应在网络交换机中实现标准协议。

5.3.11 **故障通告(P. Notify)**

网络交换机及其安全环境应具备(或在其他设备的配合下)提醒和报警能力,例如:通过 SNMP 第 3 版的陷门机制发送固件、硬件或软件的失效通知。

5.3.12 **对等节点(P. Peer)**

安全的节点应有接受来自信任节点和不信任节点的流量的能力。为了保护信息,将在信任和不信任的节点之间过滤流量。

5.3.13 **信息管理规程(P. Procedures)**

网络交换机安全环境的规程应限制无意地泄露、修改敏感信息以及不恰当地使用资源。例如:敏感信息可能包括但不局限于:文档化的操作规程材料、设备安装规程、审计文件、配置文件、网络图表、物理连接和网络测试结果的信息。

5.3.14 **可靠传输(P. Reliable_Transport)**

应实现可靠的传送和检错机制协议,以用于网络管理和控制。

5.3.15 **网络可生存性与恢复(P. Survive)**

网络资源应能够从故意的破坏尝试中恢复,同时应具有从传输错误中恢复的能力。网络必须能抵御硬件或软件失效,或具有在合理时间内复原的能力。应记录用于恢复的任何环境。

5.3.16 **硬件、软件和固件的完整性(P. SysAssur)**

应提供使完整性生效、初始化、软硬固件升级的功能和规程。应在初始安装和软件升级和固件交换时确保其完整性。

6 安全目的

6.1 网络交换机安全目的

6.1.1 **网络访问控制(O. Access_Control)**

网络交换机应实现访问控制策略,访问控制策略基于但不限于网络交换机的任务、网络交换机标识、源和目标地址、端口层次的过滤(如 Telnet、SNMP)等。

6.1.2 **安全风险报警通知(O. Alarm)**

网络交换机应有发现硬件、软件、固件的失败或错误的能力。网络交换机应提供安全相关事件、失败或错误提示的告警能力。

6.1.3 **网络配置保密性(O. Cfg_Confidentiality)**

网络交换机应保证配置和连接信息不会泄露。

6.1.4 **配置完整性(O. Cfg_Integrity)**

网络交换机应保证审计文件、配置、连接信息和其他信息的完整性。网络交换机不需负责存储这些信息。

6.1.5 **管理配置数据(O. Cfg_Manage)**

应有获取和保存网络交换机的配置和连接信息的能力,必须保证存储的完整性,能进行系统部件的鉴别与系统连接的鉴别。

6.1.6 **控制数据的可信通道(O. Ctrl_Channel)**

提供对等网络交换机之间传输控制数据的完整性和保密性;提供独立的可信信道。为了支持保密性,网络交换机必须支持加密基础设施。该加密基础设施要支持包括客户端注册、密钥管理和信道隔离在内的服务。

6.1.7 **受控标识和鉴别(O. Ctrl_I&A)**

只有在请求连接的目标地址、标识、鉴别和权限与控制策略一致时,才能连接到网络交换机。

6.1.8 **检测非授权连接(O. Detect_Connection)**

网络交换机应能检测并告警未经授权的连接。

6.1.9 **故障发生时安全状态的保存(O. Fail_Secure)**

网络交换机应能保存部件失效或停电事件时的系统安全状态。

6.1.10 **生命周期安全(O. Lifecycle)**

对网络交换机实行管理和维护,保证在其生命周期内,正确地实现和保护其安全功能。对硬件、软件或固件的升级,应保证不会影响其他的安全功能。

6.1.11 **管理数据的可信路径(O. Mgmt_Path)**

对于网络交换机和网络管理站之间传输的信息,应保证其完整性和保密性,应提供独立的可信信道。为了支持保密性,网络交换机必须支持加密基础设施。该加密基础设施要支持包括客户端注册、密钥管理和信道隔离在内的服务。

6.1.12 **安全修复和补丁(O. Patches)**

网络交换机应安装最新的补丁和安全修复。

6.1.13 **业务优先级(O. Priority_of_Service)**

即使使用尽力传输方式,网络交换机也应对所有的流量分配优先级。控制资源访问方式,防止低级别服务干扰或延迟高级别的服务。

6.1.14 **地址保护(O. Protect_Addresses)**

网络交换机应保护已授权组织的内部地址的保密性和完整性。在网络交换机收到数据后,应能正确地解析出经过授权的源地址和目的地址。

6.1.15 **协议(O. Protocols)**

在网络交换机中应实现能与其他厂商的网络交换机互操作的标准协议,并在网络交换机中实现可靠交付和错误检测的协议。

6.1.16 **避免重放攻击(O. Replay_Prevent)**

网络交换机应具有防止非授权用户伪装成已授权用户的能力,保护其自身免受重放攻击。

6.1.17 **网络交换机的自身防护(O. Sel_Pro)**

网络交换机必须做好自身防护,以对抗非授权用户对其安全功能的旁路、抑制或篡改。

6.1.18 **网络交换机及其安全功能的测试(O. Test)**

网络交换机及其安全功能的测试应严格遵照文档化的测试计划和规程。脆弱性测试应致力于寻找可能违反网络交换机安全策略的方法。所有的测试方法和结果都应有文档记录。

6.1.19 **带标识的审计流量记录(O. Traf_Audit)**

审计记录应包括日期、时间、发送速度、接受速度、节点标识符和负责传输数据的组织。网络交换机应验证审计记录的完整性,但网络交换机无需负责存储审计记录。

6.1.20 **系统数据备份的完整性和保密性(O. Trust_Backup)**

应确保网络交换机的系统文件和配置参数有冗余备份。备份文件的存储方式应符合网络安全策略,保证文件的完整性和保密性。另外,应能使用备份文件再生网络交换机的配置,在出现失效或泄密的情况下恢复网络交换机的功能;网络文件可自动的复制到其他的管理站。

6.1.21 **可信的恢复(O. Trusted_Recovery)**

应确保网络交换机在出现失效或错误后能够恢复到安全状态,应确保在更换失效的部件后,能够恢复系统状态,并且保证不会引发错误或造成其他的安全隐患。

6.1.22 **未用区域(O. Unused_Fields)**

网络交换机应保证恰当的设定了协议头内所有未使用域的数值。

6.1.23 **软硬固件验证(O. Validation)**

应通过合适的功能和规程,确保所有硬件、软件和固件的完整性,并保证所有硬件、软件和固件都可正确地安装和操作。

6.2 **环境安全目的**

6.2.1 **带标识的审计记录(OE. Admin_Audit)**

网络配置管理员和网络安全管理员的活动应被审计,审计记录的存储和维护应符合安全策略。

6.2.2 **管理属性(OE. Attr_Mgt)**

网络安全管理员应管理控制策略,只赋予授权的网络管理人员必需的权利。管理人员应在通过标识与鉴别后承担其特权角色。

6.2.3 **审计记录查阅(OE. Audit_Review)**

应定期的查阅所有审计记录,网络审计管理员应定期的查阅网络流量审计记录。

6.2.4 **加密机制支持(OE. Cryptography)**

为了支持保密性,网络交换机必须支持加密基础设施。该加密基础设施要支持包括客户端注册、密

钥管理和信道隔离在内的服务。

6.2.5 **环境保护(OE. Environment)**

应提供对物理环境的保护,例如对抗火灾、地震、掉电等。

6.2.6 **指导性文档(OE. Guide_Docs)**

应提供安装、配置、操作和程序性指导文档,防止安装、配置和操作上的错误。指导文件也要用于网络交换机及其安全功能的维护。

6.2.7 **管理标识和鉴别(OE. Mgmt_I&A)**

管理人员应在通过标识与鉴别后才能承担其特权角色。

6.2.8 **可信人员(OE. Personnel)**

应使用可信赖的和有能力的员工。人员应经过基本培训,并进行经常性培训。

6.2.9 **物理保护(OE. Physical)**

应有物理保护措施,以避免恶意攻击、未经授权的修改、破坏和盗窃事件的发生。

6.2.10 **网络同步(OE. Synchronization)**

网络交换机应连接到可靠的时间源,以保证正确的网络资源同步。

7 安全要求

7.1 安全功能要求

表1列出了网络交换机信息技术安全功能要求组件,并对各组件给出了详细的说明。

表1 安全功能要求组件

安全功能要求类	安全功能要求组件	组件名称
安全审计(FAU类)	FAU_GEN. 1	审计数据产生
	FAU_GEN. 2	用户身份关联
	FAU_SAR. 1	审计查阅
	FAU_SEL. 1	选择性审计
用户数据保护(FDP类)	FDP_ACC. 1	子集访问控制
	FDP_ACF. 1	基于安全属性的访问控制
	FDP_ETC. 2	有安全属性的用户数据输出
	FDP_IFC. 1	子集信息流控制
	FDP_IFF. 1	简单安全属性
	FDP_ITC. 2	有安全属性的用户数据输入
	FDP_UIT. 1	数据交换完整性
	FDP_UIT. 2	原发端数据交换恢复
标识和鉴别(FIA类)	FIA_UAU. 2	任何行动前的用户鉴别
	FIA_UID. 2	任何行动前的用户标识
	FIA. AFL. 1	鉴别失败处理
安全管理(FMT类)	FMT_MOF. 1	安全功能行为的管理
	FMT_MSA. 1	安全属性的管理
	FMT_MSA. 3	静态属性初始化
	FMT_MTD. 1	安全功能数据的管理
	FMT_SMR. 2	安全角色限制

表 1(续)

安全功能要求类	安全功能要求组件	组件名称
安全功能保护(FPT 类)	FPT_AMT.1	抽象机测试
	FPT_FLS.1	带保存安全状态的失败
	FPT_ITC.1	传送过程中安全功能间的保密性
	FPT_ITI.1	安全功能间修改的检测
	FPT_PHP.1	物理攻击的被动检测
	FPT_RCV.3	无过度损失的自动恢复
	FPT_RCV.4	功能恢复
	FPT_RPL.1	重放检测
	FPT_STM.1	可靠的时间戳
	FPT_TDC.1	安全功能间基本安全功能数据的一致性
	FPT_TST.1	安全功能检测
资源利用(FRU 类)	FRU_FLT.1	低容错
	FRU_PRS.2	全部服务优先级
网络交换机访问(FTA 类)	FTA_TSE.1	网络交换机会话建立
可信路径/信道(FTP 类)	FTP_ITC.1	安全功能间可信信道
	FTP_TRP.1	可信路径

7.1.1 安全审计(FAU 类)

7.1.1.1 审计数据产生(FAU_GEN.1)

FAU_GEN.1.1 网络交换机的安全功能应能为下列可审计事件产生审计记录:

a) 审计功能的启动和关闭。

b) *基本级*审计的所有可审计事件。

c) 【*对网络审计管理员、网络配置管理员和网络安全管理员的审计:访问权限和能力的分配或撤销、任何由网络管理人员所做出的更改、进程运行期间的时间和日期、网络管理人员执行活动的时间和日期。*

对于网络流量的审计:能够记录主干网内的源和目的节点、传输和接收流量的大小、日期和时间。】

FAU_GEN.1.2 网络交换机的安全功能应在每个审计记录中至少记录如下信息:

a) 事件的日期和时间、事件类型、主体身份、事件的结果(成功或失败);

b) 对每种审计事件类型是基于保护轮廓或安全目标文档中安全功能要求组件的可审计事件进行定义的,其他相关审计事件包括:【*收到不可信源的流量、接受来自不可信源的流量、恢复安全性相关事件的响应行动、恢复一个与安全性相关事件花费的时间、被安全性相关事件影响的所有组件。*】。

依赖关系:FPT_STM 可靠的时间戳。

7.1.1.2 用户身份关联(FAU_GEN.2)

FAU_GEN.2.1 网络交换机的安全功能应能将每个可审计事件与引起该事件的用户身份相关联。用户的网络管理审计数据将关注网络管理角色涉及到的人员,而用户的流量统计数据将关注网络交换机的标识。

依赖关系:FAU_GEN.1 审计数据产生;

FIA_UID.1 适时标识。

7.1.1.3 审计查阅(FAU_SAR.1)

FAU_SAR.1.1 网络交换机的安全功能应为【*指定的网络安全管理员*】提供从审计记录中读取【*所有审计数据*】的能力。

FAU_SAR.1.2 网络交换机的安全功能应以便于用户理解的方式提供审计记录。

依赖关系:FAU_GEN.1 审计数据产生。

7.1.1.4 选择性审计(FAU_SEL.1)

FAU_SEL.1.1 网络交换机的安全功能根据以下属性包括或排除审计事件集中的可审计事件:*客体标识、用户标识、主体标识、主机标识、事件类型*。

依赖关系:FAU_GEN.1 审计数据产生;

FMT_MTD.1 安全功能数据的管理。

7.1.2 用户数据保护(FDP 类)

7.1.2.1 子集访问控制(FDP_ACC.1)

FDP_ACC.1.1 网络交换机的安全功能应对【*通信请求*】执行【*访问控制策略*】。

依赖关系:FDP_ACF.1 基于安全属性的访问控制。

7.1.2.2 基于安全性属性的访问控制(FDP_ACF.1)

FDP_ACF.1.1 网络交换机的安全功能应基于【*标识、鉴别和连接通信会话中另一个成员的节点的授权*】对客体强制执行【*访问控制策略*】。

FDP_ACF.1.2 网络交换机的安全功能应执行以下规则,以决定受控主体与受控客体间的操作是否被允许:【*源网络交换机的地址必须在目的网络交换机的访问控制列表中标识出来,授权必须发生在接收消息之前*】。

FDP_ACF.1.3 网络交换机的安全功能应基于以下附加规则决定主体对客体的访问授权:【*合法键值的拥有者、网络交换机的角色(处理仅从可信源来的流量,或配置成也可从不可信源接收流量)、时间和流量特征(如控制信息)*】。

FDP_ACF.1.4 网络交换机的安全功能应基于【*发送者的地址*】明确拒绝主体对客体的访问。

依赖关系:FDP_ACC.1 子集访问控制;

FMT_MSA.3 静态属性初始化。

7.1.2.3 有安全属性的用户数据输出(FDP_ETC.2)

FDP_ETC.2.1 网络交换机的安全功能在安全功能策略的控制下输出用户数据到安全功能的控制范围之外时,应执行【*安全属性的应用程序*】。

FDP_ETC.2.2 网络交换机的安全功能应输出带有相关安全属性的用户数据。

FDP_ETC.2.3 网络交换机的安全功能在安全属性输出到安全功能的控制范围之外时,应确保其与输出的数据确切关联。

FDP_ETC.2.4 网络交换机的安全功能在用户数据从安全功能的控制范围输出时,【*传输数据的网络交换机必须保证具有完整性保护*】。

依赖关系:FDP_ACC.1 子集访问控制或 FDP_IFC.1 子集信息流控制。

7.1.2.4 子集信息流控制(FDP_IFC.1)

FDP_IFC.1.1 网络交换机的安全功能应对【*从不可信源接收到的控制信息(信令和路由信息)*】执行【*信息流控制策略*】。

依赖关系:FDP_IFF.1 简单安全属性。

7.1.2.5 简单安全属性(FDP_IFF.1)

FDP_IFF.1.1 网络交换机的安全功能应基于下列类型的主体和信息安全属性:

【*最小化的信息流控制策略,功能与访问控制策略相关联,可以识别控制信息的*

源，无论它是可信的或不可信的（可信源是可标识和可鉴别的，而且控制信息的完整性是可校验的），生成消息源的鉴别】，执行【*信息流控制策略*】。

FDP_IFF.1.2 如果有【*消息的源头可以被接收方标识和鉴别，并且消息的完整性是可校验的*】的规则，网络交换机的安全功能应允许受控主体和受控信息之间存在经由受控操作的信息流，即网络交换机的安全功能应允许在受控主体之间存在一个信息流。

FDP_IFF.1.3 网络交换机的安全功能应执行【*信息流控制策略：当做出路由和重新路由的决定时，来自可信源的控制信息的优先级要高于从不可信源接收的控制信息，正如在网络失败的事件中*】。

FDP_IFF.1.4 网络交换机的安全功能应提供下列功能：【*配置网络交换机的安全功能实现对来自不可信源数据接收的策略决定；审计接收到的来自不可信源的数据；从不可信源接收数据*】。

FDP_IFF.1.5 网络交换机的安全功能应根据【*可信的预先建立的（静态）路由，通过可信路径到网络管理站的管理信息*】的规则，明确授权信息流。

FDP_IFF.1.6 网络交换机的安全功能应基于【*配置安全策略以拒绝接收来自不可信源的数据*】的规则，明确拒绝信息流。

依赖关系：FDP_ACC.1 子集访问控制或 FDP_IFC.1 子集信息流控制；
FMT_MSA.3 静态属性初始化。

7.1.2.6 有安全属性的用户数据输入（FDP_ITC.2）

FDP_ITC.2.1 网络交换机的安全功能在安全功能策略的控制下从安全功能的控制范围之外输入用户数据时，应执行【*基于访问控制列表的标识的使用、拥有合法密钥证据的校验、完整性检查的校验或源地址的识别*】。

FDP_ITC.2.2 网络交换机的安全功能应使用与输入的数据相关的安全属性。

FDP_ITC.2.3 网络交换机的安全功能应确保使用的协议在安全属性和接收的用户数据之间提供了明确的联系。

FDP_ITC.2.4 网络交换机的安全功能应确保对输入的用户数据安全属性的解释与用户数据源的解释是一致的。

FDP_ITC.2.5 网络交换机的安全功能在安全功能策略的控制下从安全功能的控制范围之外输入用户数据时，应执行【*赋值*】。

依赖关系：FDP_ACC.1 子集访问控制或 FDP_IFC.1 子集信息流控制；
FTP_ITC.1 安全功能间可信信道或 FTP_TRP.1 可信路径；
FPT_TDC.1 安全功能间基本安全功能数据的一致性。

7.1.2.7 数据交换完整性（FDP_UIT.1）

FDP_UIT.1.1 网络交换机的安全功能应执行【*信息控制策略*】，使得能以某种方式*传送、接收*用户数据，保护数据避免出现*篡改、删除、插入、重用*错误。

FDP_UIT.1.2 网络交换机的安全功能应能根据收到的用户数据，判断是否出现了*篡改、删除、插入、重用*。

依赖关系：FDP_ACC.1 子集访问控制或 FDP_IFC.1 子集信息流控制；
FTP_ITC.1 安全功能间可信信道或 FTP_TRP.1 可信路径；
FTP_TRP.1 可信路径。

7.1.2.8 原发端数据交换恢复（FDP_UIT.2）

FDP_UIT.2.1 网络交换机的安全功能应执行【*帧序列检查、循环冗余码校验、流量整形、抗重放、和完整复制所有网络管理数据文件给某一分离的备份源*】，以便能在原发端

可信 IT 产品的帮助下，从【*包的序列变化、重放包、不完整的数据传输、丢掉的包、网络拥塞和主要网络管理系统中的失败*】中恢复。

依赖关系：FDP_ACC.1 子集访问控制或 FDP_IFC.1 子集信息流控制；
FTP_ITC.1 安全功能间可信信道或 FTP_TRP.1 可信路径。

7.1.3 标识和鉴别(FIA 类)

7.1.3.1 任何行动前的用户鉴别(FIA_UAU.2)

FIA_UAU.2.1 在允许执行任何代表用户的其他安全功能促成的行动执行前，网络交换机的安全功能应要求该用户已被成功鉴别。

依赖关系：FIA_UID.1 适时标识。

7.1.3.2 任何行动前的用户标识(FIA_UID.2)

FIA_UID.2.1 在允许执行任何代表用户的其他安全功能促成的行动之前，网络交换机的安全功能应要求用户标识自己。

依赖关系：无依赖关系。

7.1.3.3 鉴别失败处理(FIA_AFL.1)

FIA_AFL.1.1 当与【*鉴别事件列表*】相关的【*数目*】次不成功鉴别尝试出现时，网络交换机的安全功能应加以检测。

FIA_AFL.1.2 当达到或超过所定义的不成功鉴别尝试的次数时，网络交换机的安全功能应【*行为列表*】。

依赖关系：FIA_UAU.1 适时鉴别。

7.1.4 安全管理(FMT 类)

7.1.4.1 安全功能行为的管理(FMT_MOF.1)

FMT_MOF.1.1 网络交换机的安全功能应仅限于【*网络安全管理员角色*】对【*网络交换机在安装时和贯穿整个生命周期的安全修复/补丁、选择可审计事件、管理用户账户、管理审计日志、管理访问控制策略、管理信息流控制策略、到可信时间源的网络交换机连接、包括网络交换机数据文件的备份和恢复的网络交换机资源的维护*】功能具有*确定其行为、禁止、允许、修改其行为*的能力。

网络交换机的安全功能应仅限于【*网络配置管理员负责建立和配置连接*】对【*网络交换机的配置和网络交换机资源的维护*】功能具有*确定其行为、禁止、允许、修改其行为*的能力。

依赖关系：FMT_SMR.1 安全角色。

7.1.4.2 安全属性的管理(FMT_MSA.1)

FMT_MSA.1.1 网络交换机的安全功能应执行【*访问控制列表*】，以仅限于【*网络安全管理员角色*】能够对【*选择可审计事件，管理审计日志，网络管理系统访问控制列表和账户，网络用户访问控制列表和账户*】安全属性*改变默认值、查询、修改、删除*。

网络交换机的安全功能应执行【*访问控制列表*】，以仅限于【*网络配置管理员角色*】能够对安全属性【*网络用户访问控制列表和账户*】进行*改变默认值、查询、修改、删除*。

网络交换机应执行【*访问控制列表*】，以仅限于【*网络审计管理员、网络配置管理员、网络安全管理员角色*】，能够执行【*监控和收集网络行为属性*】以及【*监控和分析流量行为*】安全属性的能力。

依赖关系：FDP_ACC.1 子集访问控制或 FDP_IFC.1 子集信息流控制；
FMT_MSR.1 安全角色。

7.1.4.3 静态属性初始化(FMT_MSA.3)

FMT_MSA.3.1 网络交换机的安全功能应执行【*访问控制策略*】,以便为用于执行安全功能策略的安全属性提供*受限的*默认值。

FMT_MSA.3.2 网络交换机的安全功能应允许【*负责建立和配置连接的网络配置管理员或网络安全管理员角色*】为生成的客体或信息指定替换性的初始值以代替原来的默认值。

依赖关系:FMT_MSA.1 安全属性的管理;
FMT_SMR.1 安全角色。

7.1.4.4 安全功能数据的管理(FMT_MTD.1)

FMT_MTD.1.1 网络交换机的安全功能应仅限于【*网络安全管理员*】能够对【*当前网络管理审计数据的指定区域和网络流量数据*】进行*改变默认值、查询*的操作。
网络交换机的安全功能应仅限于【*网络配置管理员*】能够对【*当前网络流量审计数据的指定区域*】进行*改变默认值、查询*的操作。
网络交换机的安全功能应仅限于【*网络审计管理员*】能够对【*当前网络流量审计数据的指定区域*】进行*查询*的操作。

依赖关系:FMT_SMR.1 安全角色。

7.1.4.5 安全角色限制(FMT_SMR.2)

FMT_SMR.2.1 网络交换机的安全功能应维护【*网络安全管理员*】角色。

FMT_SMR.2.2 网络交换机的安全功能应能够把管理员用户和角色关联起来。

FMT_SMR.2.3 网络交换机的安全功能应确保条件【*网络审计管理员或网络配置管理员不能假定为网络安全管理员角色*】得到满足。

依赖关系:FIA_UID.1 适时标识。

7.1.5 安全功能保护(FPT 类)

7.1.5.1 抽象机测试(FPT_AMT.1)

FPT _AMT.1.1 网络交换机的安全功能应在*初始化启动期间和*【*网络安全管理员或网络配置管理员*】*提出请求时*运行一组测试,以证明作为网络交换机安全功能基础的由抽象机提供的安全假定的正确执行。

依赖关系:无依赖关系。

7.1.5.2 带保存安全状态的失败(FPT_FLS.1)

FPT_FLS.1.1 网络交换机的安全功能在【*硬件组件失败、短期电源中断*】失败发生时应保存一个安全状态。

依赖关系:无依赖关系。

7.1.5.3 传送过程中安全功能间的保密性(FPT_ITC.1)

FPT_ITC.1.1 在网络交换机的安全功能数据从安全功能到远程可信 IT 产品的传送过程中,网络交换机的安全功能应保护所有的安全功能数据不被非授权泄漏。

依赖关系:无依赖关系。

7.1.5.4 安全功能间修改的检测(FPT_ITI.1)

FPT_ITI.1.1 网络交换机的安全功能应具备:检测网络交换机与远程可信 IT 产品间传送的所有安全功能数据是否被修改的能力,其强度必须【*等于或超出由 MD5 提供的完整性保护算法的强度*】。

FPT_ITI.1.2 网络交换机的安全功能应提供验证在安全功能与远程可信 IT 产品间传送的所有安全功能数据的完整性及执行如果检测到修改所采取的【*数据的再次传输和产生审计记录*】的能力。

依赖关系：无依赖关系。

7.1.5.5 物理攻击的被动检测(FPT_PHP.1)

FPT_PHP.1.1 网络交换机安全功能应对可能危及自身安全的物理篡改提供明确的检测。

FPT_PHP.1.2 网络交换机的安全功能应提供判断安全功能设备或安全功能元件是否已被物理篡改的能力。

依赖关系：FMT_MOF.1 安全功能行为的管理。

7.1.5.6 无过度损失的自动恢复(FPT_RCV.3)

FPT_RCV.3.1 当不能从失败或服务中断自动恢复时，网络交换机的安全功能应进入维护方式，该方式提供将网络交换机返回到一个安全状态的能力。

FPT_RCV.3.2 对【*备份电源供应、冗余处理器、网络管理系统错误或失败、组件(卡，端口)失败*】，网络交换机的安全功能应确保通过自动化过程使网络交换机返回到一个安全状态。

FPT_RCV.3.3 网络交换机的安全功能提供的从失败或服务中断状态恢复的功能，应确保安全功能控制范围内的安全功能数据或客体的损失在不超过【*赋值*】的情况下恢复到初始状态。

FPT_RCV.3.4 网络交换机的安全功能应提供决定客体能否被恢复的能力。

依赖关系：FPT_TST.1 安全功能检测；

AGD_ADM.1 管理员指南。

7.1.5.7 功能恢复(FPT_RCV.4)

FPT_RCV.4.1 网络交换机的安全功能应确保【*包括但不限于如下安全功能和故障情况：自动保护切换、冗余处理器的切换、备份电源供应的切换、信息传输连接的的保存、循环冗余校验、帧序列检查、抗重放等安全功能，和如硬件组件故障、停电、软件错误/故障、系统处理器故障、网络管理系统故障、电路失效或组件故障等故障情况*】有如下特性，即安全功能或者已成功完成，或者对指明的故障情况恢复到一致的安全状态。

依赖关系：无依赖关系。

7.1.5.8 重放检测(FPT_RPL.1)

FPT_RPL.1.1 网络交换机的安全功能应检测【*消息(如管理和控制)、安全协商消息、被封装为信元或包传输的特定的特征(时间戳、哈希值、密钥等)*】的重放。

FPT_RPL.1.2 检测到重放时，网络交换机的安全功能应执行【*审计、验证对于重放中来自合法的源的请求、阻挡来自源头的通信、发送陷阱以测试线路和扫描非授权的连接*】。

依赖关系：无依赖关系。

7.1.5.9 可靠的时间戳(FPT_STM.1)

FPT_STM.1.1 网络交换机的安全功能应能为自身的应用提供可靠的时间戳。

依赖关系：无依赖关系。

7.1.5.10 安全功能间基本安全功能数据的一致性(FPT_TDC.1)

FPT_TDC.1.1 当网络交换机的安全功能与其他可信 IT 产品共享其安全功能的数据时，网络交换机的安全功能应提供对*网络审计信息、控制信息和安全参数*一致性解释的能力。

FPT_TDC.1.2 当解释来自其他可信 IT 产品的安全功能数据时，网络交换机的安全功能应使用*开发者(在安全目标文档中)指定的已鉴别的协议*。

依赖关系：无依赖关系。

7.1.5.11 安全功能检测(FPT_TST.1)

FPT_TST.1.1 网络交换机的安全功能应在*初始化启动期间和【网络安全管理员或网络配置管理员】提出请求时*运行一组自检,以表明网络交换机安全功能操作的正确性。

FPT_TST.1.2 网络交换机的安全功能为授权用户提供对网络交换机安全功能的数据完整性的验证能力。

FPT_TST.1.3 网络交换机的安全功能为授权用户提供对存储的网络交换机的安全功能可执行代码完整性的验证能力。

依赖关系:FPT_AMT.1 抽象机测试。

7.1.6 资源利用(FRU 类)

7.1.6.1 低容错(FRU_FLT.1)

FRU_FLT.1.1 网络交换机的安全功能应确保【*硬件故障、软件错误、线路故障、路由控制和管理信息的恶意修改、缓冲区溢出、极端的网络拥塞、自然灾害(地震,洪水等),短暂的电源中断*】发生时,能够执行【*自动切换到备份组件或电源供应、安全信息传送、信息传送连接的保存、流量的正确路由、正确的信元/包的内部处理、流量整形、签署的服务质量/优先级的保存、当持续发生带有预攻击控制信息的特定网络操作时丢掉已被破坏的数据并对事件进行审计*】操作。

依赖关系:FPT_FLS.1 带保存安全状态的失败。

7.1.6.2 全部服务优先级(FRU_PRS.2)

FRU_PRS.2.1 网络交换机的安全功能应给在安全功能中的每个主体分配一种优先级。

FRU_PRS.2.2 网络交换机的安全功能应确保对所有可共享资源的每次访问都应基于分配给主体的优先级进行协调分配。

依赖关系:无依赖关系。

7.1.7 网络交换机访问(FTA 类)

7.1.7.1 网络交换机会话建立(FTA_TSE.1)

FTA_TSE.1.1 网络交换机的安全功能应能拒绝基于【*节点标识、接收到的鉴别数据、标识为不可信的数据源、角色、地址、时间(维护窗口,或当适当的监控程序没有就位时)、或基于安全状态*】的会话建立。

依赖关系:无依赖关系。

7.1.8 可信路径/信道(FTP 类)

7.1.8.1 安全功能间可信信道(FTP_ITC.1)

FTP_ITC.1.1 网络交换机的安全功能应在其自身和远程可信 IT 产品之间提供一条通信信道,此信道在逻辑上与其他通信信道截然不同,并且能够对其端节点提供确定的标识,以及保护信道中数据免遭修改和泄露。

FTP_ITC.1.2 网络交换机的安全功能应允许*安全功能,远程的可信 IT 产品*经可信信道发起通信。

FTP_ITC.1.3 对于【*控制信息的传输和安全属性的改变*】,网络交换机的安全功能应经可信信道发起通信。

依赖关系:无依赖关系。

7.1.8.2 可信路径(FTP_TRP.1)

FTP_TRP.1.1 网络交换机的安全功能应在它自身和*远程、本地*用户之间提供一条通信路径,此路径在逻辑上与其他通信路径截然不同,并且能够对其端节点提供确定的标识,以及保护通信数据免遭修改或泄露。

FTP_TRP.1.2 网络交换机的安全功能应允许*远程、本地*用户经可信路径发起通信。

FTP_TRP.1.3　对于*初始鉴别和【网络管理信息的传输】*，网络交换机的安全功能应要求使用可信路径。

依赖关系：无依赖关系。

7.2　安全保证要求

表2列出了网络交换机信息技术安全保证要求组件，并对各组件给出了详细的说明。

表2　安全保证要求组件

安全保证要求类	安全保证要求组件	组件名称
配置管理(ACM类)	ACM_CAP.3	授权控制
	ACM_SCP.1	网络交换机配置管理范围
交付及运行(ADO类)	ADO_DEL.1	交付过程
	ADO_IGS.1	安装、生成和启动过程
开发(ADV类)	ADV_FSP.1	非形式化功能规范
	ADV_HLD.2	安全加强的高层设计
	ADV_RCR.1	非形式化对应性论证
指导性文档(AGD类)	AGD_ADM.1	管理员指南
	AGD_USR.1	用户指南
生命周期支持(ALC类)	ALC_DVS.1	安全措施标识
测试(ATE类)	ATE_COV.2	范围分析
	ATE_DPT.1	测试：高层设计
	ATE_FUN.1	功能测试
	ATE_IND.2	独立性测试—抽样
脆弱性评定(AVA类)	AVA_MSU.1	指南审查
	AVA_SOF.1	网络交换机安全功能强度评估
	AVA_VLA.1	开发者脆弱性分析

7.2.1　配置管理(ACM类)

7.2.1.1　授权控制（ACM_CAP.3）

开发者行为元素：

ACM_CAP.3.1D 开发者应为网络交换机提供一个参照号。

ACM_CAP.3.2D 开发者应使用配置管理系统。

ACM_CAP.3.3D 开发者应提供配置管理文档。

证据的内容和形式元素：

ACM_CAP.3.1C 网络交换机的参照号对其每一个版本应是唯一的。

ACM_CAP.3.2C 应该给网络交换机标记上其参照号。

ACM_CAP.3.3C 配置管理文档应包括一个配置清单和一个配置管理计划。

ACM_CAP.3.4C 配置清单应描述组成网络交换机的配置项。

ACM_CAP.3.5C 配置管理文档应描述用以唯一标识配置项的方法。

ACM_CAP.3.6C 配置管理系统应唯一标识所有配置项。

ACM_CAP.3.7C 配置管理计划应描述配置管理系统是如何使用的。

ACM_CAP.3.8C 证据应该论证配置管理系统的运作与配置管理计划相一致。

ACM_CAP.3.9C 配置管理文档应提供证据以证明在配置管理系统下有效地维护了所有的配

置项。

ACM_CAP.3.10C 配置管理系统应提供措施使得对配置项只能进行授权修改。

评估者行为元素：

ACM_CAP.3.1E 评估者应确认所提供的信息满足证据的内容和形式的所有要求。

依赖关系：ACM_SCP.1 网络交换机 配置管理范围；

ALC_DVS.1 安全措施标识。

应用注释：术语“参考号”可能涉及到一个版本号、命名计划等。

7.2.1.2 网络交换机配置管理范围（ACM_SCP.1）

开发者行为元素：

ACM_SCP.1.1D 开发者应提供配置管理文档。

证据的内容和形式元素：

ACM_SCP.1.1C 配置管理文档应说明配置管理系统至少能跟踪以下几项：网络交换机实现表示，设计文档，测试文档，用户文档，管理员文档和配置管理文档。

ACM_SCP.1.2C 配置管理文档应描述配置管理系统是如何跟踪配置项的。

评估者行为元素：

ACM_SCP.1.1E 评估者应确认所提供的信息满足证据的内容和形式的所有要求。

依赖关系：ACM_CAP.3 授权控制。

7.2.2 交付及运行（ADO 类）

7.2.2.1 交付过程（ADO_DEL.1）

开发者行为元素：

ADO_DEL.1.1D 开发者应将把网络交换机及其部分交付给用户的程序文档化。

ADO_DEL.1.2D 开发者应使用交付程序。

证据的内容和形式元素：

ADO_DEL.1.1C 交付文档应描述给用户方分配网络交换机的版本时为维护安全所必需的所有程序。

评估者行为元素：

ADO_DEL.1.1E 评估者应确认所提供的信息都满足证据的内容和形式的所有要求。

依赖关系：无依赖关系。

7.2.2.2 安装、生成和启动过程（ADO_IGS.1）

开发者行为元素：

ADO_IGS.1.1D 开发者应将网络交换机安全地安装、生成和启动所必要的程序文档化。

证据的内容和形式元素：

ADO_IGS.1.1C 文档应描述网络交换机安全地安装、生成和启动所必要的步骤。

评估者行为元素：

ADO_IGS.1.1E 评估者应确认所提供的信息都满足证据的内容和形式的所有要求。

ADO_IGS.1.2E 评估者应决定安装、生成和启动程序最终产生了安全的配置。

依赖关系：AGD_ADM.1 管理员指南。

7.2.3 开发（ADV 类）

7.2.3.1 非形式化功能规范（ADV_FSP.1）

开发者行为元素：

ADV_FSP.1.1D 开发者应当提供功能规范。

证据的内容和形式元素：

ADV_FSP.1.1C 功能规范应当使用非形式化风格来描述网络交换机安全功能及其外部接口。

ADV_FSP.1.2C 功能规范应是内在统一的。

ADV_FSP.1.3C 功能规范应当描述所有外部网络交换机安全功能接口的用途与使用方法，适当的时候，要提供影响、例外情况和错误信息的细节。

ADV_FSP.1.4C 功能规范应当完备地表示网络交换机安全功能。

评估者行为元素：

ADV_FSP.1.1E 评估者应确认所提供的信息满足证据的内容和形式的所有要求。

ADV_FSP.1.2E 评估者应决定功能规范是网络交换机安全功能要求的一个精确且完备的实例化。

依赖关系：ADV_RCR.1 非形式化对应性论证。

7.2.3.2 安全加强的高层设计(ADV_HLD.2)

开发者行为元素：

ADV_HLD.2.1D 开发者应当提供安全功能的高层设计。

证据的内容和形式元素：

ADV_HLD.2.1C 高层设计的表示应当是非形式化的。

ADV_HLD.2.2C 高层设计应当是内在一致的。

ADV_HLD.2.3C 高层设计应当按子系统来描述安全功能的结构。

ADV_HLD.2.4C 高层设计应当描述安全功能的每一个子系统所提供的安全功能。

ADV_HLD.2.5C 高层设计应当标识安全功能所要求的任何基础性的硬件、固件或软件，和在这些硬件、固件或软件中实现的支持性保护机制提供的功能表示。

ADV_HLD.2.6C 高层设计应当标识安全功能子系统的所有接口。

ADV_HLD.2.7C 高层设计应当标识安全功能子系统的哪些接口是外部可见的。

ADV_HLD.2.8C 高层设计应当描述安全功能子系统所有接口的用途与使用方法，并适当提供影响、例外情况和错误消息的细节。

ADV_HLD.2.9C 高层设计应当描述把网络交换机分成网络交换机安全策略实施子系统和其他子系统的这种分离。

评估者行为元素：

ADV_HLD.2.1E 评估者应当确认所提供的信息满足证据的内容和形式的所有要求。

ADV_HLD.2.2E 评估者应当决定功能规范是网络交换机安全功能要求的一个精确且完备的实例化。

依赖关系：ADV_FSP.1 非形式化功能规范；

ADV_RCR.1 非形式化对应性论证。

7.2.3.3 非形式化对应性论证(ADV_RCR.1)

开发者行为元素：

ADV_RCR.1.1D 开发者应当在所提供的安全功能表示的所有相邻对之间提供其对应性分析。

证据的内容和形式元素：

ADV_RCR.1.1C 对于所提供的安全功能表示的每个相邻对，应论证：较为抽象的安全功能表示的所有相关安全功能都在较不抽象的安全功能表示中得到正确且完备的细化。

评估者行为元素：

ADV_RCR.1.1E 评估者应当确认所提供的信息满足证据的内容和形式的所有要求。

依赖关系：无依赖关系。

7.2.4 指导性文件(AGD 类)

7.2.4.1 管理员指南(AGD_ADM.1)

开发者行为元素：

AGD_ADM.1.1D 开发者应当提供针对系统管理员的管理员指南。

证据的内容和形式元素：

AGD_ADM.1.1C 管理员指南应当描述网络交换机管理员可使用的管理功能和接口。

AGD_ADM.1.2C 管理员指南应当描述如何以安全的方式管理网络交换机。

AGD_ADM.1.3C 管理员指南应当包含在安全处理环境中必须进行控制的功能和权限的警告。

AGD_ADM.1.4C 管理员指南应当描述所有与网络交换机的安全运行有关的用户行为的假设。

AGD_ADM.1.5C 管理员指南应当描述所有受管理员控制的安全参数，合适时，应指明安全值。

AGD_ADM.1.6C 管理员指南应当描述每一种与需要执行的管理功能有关的安全相关事件，包括改变安全功能所控制的实体的安全特性。

AGD_ADM.1.7C 管理员指南应当与为评估而提供的其他所有文档保持一致。

AGD_ADM.1.8C 管理员指南应当描述与管理员有关的 IT 环境的所有安全要求。

评估行为元素：

AGD_ADM.1.1E 评估者应确认所提供的信息满足证据的内容和形式的所有要求。

依赖关系：ADV_FSP.1 非形式化功能规范。

7.2.4.2 用户指南(AGD_USR.1)

开发者行为元素：

AGD_USR.1.1D 开发者应当提供用户指南。

证据的内容和形式元素：

AGD_USR.1.1C 用户指南应该描述网络交换机的非管理员用户可用的功能和接口。

AGD_USR.1.2C 用户指南应该描述网络交换机提供的用户可访问的安全功能的用法。

AGD_USR.1.3C 用户指南应该包含受安全处理环境中所控制的用户可访问的功能和权限的警告。

AGD_USR.1.4C 用户指南应该清晰地阐述网络交换机安全运行中用户所必须负的职责，包括有关在网络交换机安全环境阐述中找得到的用户行为的假设。

AGD_USR.1.5C 用户指南应该与为评估而提供的其他所有文档保持一致。

AGD_USR.1.6C 用户指南应该描述与用户有关的 IT 环境的所有安全要求。

评估者行为元素：

AGD_USR.1.1E 评估者应确认所提供的信息满足证据的内容和形式的所有要求。

依赖关系：ADV_FSP.1 非形式化功能规范。

应用注释：在本要求中，“用户”不是指产生原发流量的实体，而是指具备设备操作权限子集的网络配置管理员角色。

7.2.5 生命周期支持(ALC 类)

7.2.5.1 安全措施标识(ALC_DVS.1)

开发者行为元素：

ALC_DVS.1.1D 开发者应提供开发安全文档。

证据的内容和形式元素：

ALC_DVS.1.1C 开发安全文档应描述在网络交换机的开发环境中，用以保护网络交换机设计和实现的保密性和完整性在物理、程序、人员以及其他方面必要的安全措施。

ALC_DVS.1.2C 开发安全文档应提供在网络交换机的开发和维护过程中执行安全措施的证据。

评估者行为元素：

ALC_DVS.1.1E 评估者应确认所提供的信息满足证据的内容和形式的所有要求。

ALC_DVS.1.2E 评估者应确认应用了安全措施。

依赖关系：无依赖关系。

7.2.6 **测试(ATE 类)**

7.2.6.1 **范围分析(ATE_COV.2)**

开发者行为元素:

ATE_COV.2.1D 开发者将提供测试覆盖范围的分析。

证据的内容和形式元素:

ATE_COV.2.1C 测试范围的分析应当论证在测试文档中标识的测试和功能规范中描述的网络交换机安全功能间的对应。

ATE_COV.2.2C 测试覆盖范围的分析应当论证功能规范中所描述安全功能和测试文档所标识的测试之间的对应性是完备的。

评估者行为元素:

ATE_COV.2.1E 评估者应当确认提供的信息满足证据的内容和形式的要求。

依赖关系:ADV_FSP.1 非形式化功能规范;

ATE_FUN.1 功能测试。

7.2.6.2 **测试:高层设计(ATE_DPT.1)**

开发者行为元素:

ATE_DPT.1.1D 开发者应当提供测试深度的分析。

证据的内容和形式元素:

ATE_DPT.1.1C 深度分析应当论证测试文档中所标识的测试足以论证该安全功能运行是和高层设计一致的。

评估者行为元素:

ATE_DPT.1.1E 评估者应当确认提供的信息满足证据的内容和形式的要求。

依赖关系:ADV_HLD.2 安全加强的高层设计;

ATE_FUN.1 功能测试。

应用注释:本要求依赖 ADV_HLD.1,本标准选择 ADV_HLD.2 作为 EAL3 级的保证级别要求。

7.2.6.3 **功能测试(ATE_FUN.1)**

开发者行为元素:

ATE_FUN.1.1D 开发者应当测试网络交换机安全功能,并文档化结果。

ATE_FUN.1.2D 开发者应提供测试文档。

证据的内容和形式元素:

ATE_FUN.1.1C 测试文档应当包括测试计划、测试程序描述,预期的测试结果和实际的测试结果。

ATE_FUN.1.2C 测试计划应当标识要测试的安全功能,描述要执行的测试目标。

ATE_FUN.1.3C 测试过程描述应当标识要执行的测试,并描述每个安全功能的测试概况,这些概况包括对于其他测试结果的顺序依赖性。

ATE_FUN.1.4C 预期的测试结果应当表明成功测试运行后的预期输出。

ATE_FUN.1.5C 开发者执行测试的结果应当论证每个被测试的安全性功能已按照规定运行了。

评估者行为元素:

ATE_FUN.1.1E 评估者应当确认所提供的信息满足证据的内容和形式的所有要求。

依赖关系:无依赖关系。

7.2.6.4 **独立性测试—抽样(ATE_IND.2)**

开发者行为元素:

ATE_IND.2.1D 开发者应当提供用于测试的网络交换机。

证据的内容和形式元素:

ATE_IND.2.1C 网络交换机应与测试相适应。

ATE_IND.2.2C 开发者应提供一个与开发者的安全功能测试中使用的资源相当的集合。

评估者行为元素：

ATE_IND.2.1E 评估者应当确认所提供的信息满足证据的内容和形式的所有要求。

ATE_IND.2.2E 评估者应当适当测试一个安全功能子集，以确认网络交换机按照相应的规范运行了。

ATE_IND.2.3E 评估者应抽样执行测试文档里的测试样本，以验证开发者测试的结果。

依赖关系：ADV_FSP.1 非形式化功能规范；

AGD_ADM.1 管理员指南；

AGD_USR.1 用户指南；

ATE_FUN.1 功能测试。

7.2.7 脆弱性评定(AVA 类)

7.2.7.1 指南审查(AVA_MSU.1)

开发者行为元素：

AVA_MSU.1.1D 开发者应当提供指导性文档。

证据的内容和形式元素：

AVA_MSU.1.1C 指导性文档应当确定对网络交换机的所有可能的运行方式(包括失败和操作失误后的运行)，这些运行方式的后果以及对于保持安全运行的意义。

AVA_MSU.1.2C 指导性文档应当是完备的、清晰的、一致的、合理的。

AVA_MSU.1.3C 指导性文档应当列出所有预期环境的假设。

AVA_MSU.1.4C 指导性文档应当列出所有外部安全措施(包括外部程序的、物理的或人员的控制)的要求。

评估者行为元素：

AVA_MSU.1.1E 评估者应当确认所提供的信息满足证据的内容和形式的所有要求。

AVA_MSU.1.2E 评估者应当重复所有配置与安装程序，以确认只使用所提供的指导性文档就可以让网络交换机安全配置和使用。

AVA_MSU.1.3E 评估者应当决定指导性文档的使用能检测到所有不安全状态。

依赖关系：ADO_IGS.1 安装、生成和启动过程；

ADV_FSP.1 非形式化功能规范；

AGD_ADM.1 管理员指南；

AGD_USR.1 用户指南。

7.2.7.2 网络交换机安全功能强度评估(AVA_SOF.1)

开发者行为元素：

AVA_SOF.1.1D 开发者应对安全目标文档中标识的每个具有网络交换机安全功能强度声明的安全机制进行安全功能强度分析。

证据的内容和形式元素：

AVA_SOF.1.1C 对于具有网络交换机安全功能强度声明的每个安全机制，安全功能强度分析应说明该机制达到或超过本标准或安全目标文档定义的最低强度。

AVA_SOF.1.2C 对于具有特定网络交换机安全功能强度声明的每个安全机制，安全功能强度分析应说明该机制达到或超过本标准或安全目标文档定义的特定功能强度。

评估者行为元素：

AVA_SOF.1.1E 评估者应确认所提供的信息满足证据的内容和形式的所有要求。

AVA_SOF.1.2E 评估者应确认强度声明是正确的。

依赖关系：ADV_FSP.1 非形式化功能规范；
ADV_HLD.2 安全加强的高层设计。

7.2.7.3 开发者脆弱性分析(AVA_VLA.1)

开发者行为元素：

AVA_VLA.1.1D 开发者应当分析网络交换机可交付材料，以寻找用户违反网络交换机安全策略的明显途径，并将分析结果文档化。

AVA_VLA.1.2D 开发者应当文档化明显的脆弱性分布。

证据的内容和形式元素：

AVA_VLA.1.1C 对所有已标识的脆弱性，文档应当能说明在所期望的网络交换机环境中无法利用这些脆弱性。

评估者行为元素：

AVA_VLA.1.1E 评估者应当确认提供的信息满足证据的内容和形式的所有要求。

AVA_VLA.1.2E 评估者应当在开发者脆弱性分析的基础上实施穿透性测试，确保已经表述了明显的脆弱性。

依赖关系：ADV_FSP.1 非形式化功能规范；
ADV_HLD.2 安全加强的高层设计；
AGD_ADM.1 管理员指南；
AGD_USR.1 用户指南。

附 录 A
（资料性附录）
安全环境、安全目的及安全要求间的关系合理性说明

A.1 概述

本附录介绍了本标准中安全环境、安全目的和安全要求之间的对应关系。目的是证明本标准是一个完整的内在一致的安全要求，并且为网络交换机在安全环境中提供有效的策略集合。

本附录主要给出了安全目的和安全要求的合理性，汇总了假设、安全目的覆盖的策略和威胁，以及安全目的覆盖的安全要求；并概述了本标准选择的安全保证要求(EAL3)。

A.2 安全目的合理性

下面的表 A.1、表 A.2 说明了网络交换机的安全目的能应对所有可能的威胁、假设和组织安全策略，即每一种威胁、假设和组织安全策略都至少有一个或一个以上安全目的与其对应，因此是完备的。没有一个安全目的没有相应的威胁、假设和组织安全策略与之对应，这证明每个安全目的都是必要的；没有多余的安全目的不对应威胁、假设和组织安全策略，因此说明了安全目的是充分的。

表 A.1 安全环境与安全目的对应关系

安全环境	安全目的
A. ExpAgent	O. Access_Control, O. Ctrl_Channel, O. Ctrl_I&A, O. Detect_Connection, O. Mgmt_Path, O. Protect_Addresses, O. Replay_Prevent, O. Traf_Audit
A. ExpAgent	O. Unused_Fields, O. Trust_Backup
A. Time_Source	O. Traf_Audit
P. Accountability	O. Ctrl_I&A, O. Lifecycle, O. Traf_Audit
P. Authentication	O. Access_Control, O. Ctrl_I&A
P. Availability	O. Access_Control, O. Alarm, O. Priority_Of_Service, O. Fail_Secure, O. Replay_Prevent
P. Confidentiality	O. Cfg_Confidentiality, O. Ctrl_Channel, O. Mgmt_Path, O. Trust_Backup
P. Default_Config	O. Trusted_Recovery
P. Information_Update	O. Patches, O. Validation
P. Integrity	O. Cfg_Integrity, O. Cfg_Manage, O. Mgmt_Path, O. Ctrl_Channel
P. Interoperability	O. Protocols

表 A.1(续)

安全环境	安全目的
P. Notify	O. Alarm
P. Peer	O. Access_Control,O. Ctrl_Channel, O. Ctrl_I&A,O. Protect_Addresses
P. Procedures	O. Cfg_Confidentiality,O. Cfg_Manage, O. Mgmt_Path,O. Patches,O. Traf_Audit, O. Trust_Backup
P. Reliable_Transport	O. Ctrl_Channe,O. Priority_of_Service, O. Protocols,O. Replay_Prevent O. Traf_Audit
P. Survive	O. Alarm,O. Cfg_Manage,O. Fail_Secure, O. Lifecycle,O. Test,O. Trust_Backup, O. Trusted_Recovery,O. Validation
P. SysAssur	O. Lifecycle, O. Test, O. Validation
T. Analysis	O. Ctrl_Channel,O. Detect_Connection, O. Mgmt_Path,O. Protect_Addresses
T. Capture	O. Ctrl_Channel, O. Detect_Connection, O. Mgmt_Path
T. Compromised_Node	O. Priority_Of_Service,O. Protect_Addresses, O. Traf_Audit,O. Trusted_Recovery
T. Covert	O. Unused_Fields
T. Cryptanalytic	O. Ctrl_Channel, O. Mgmt_Path
T. Denial	O. Ctrl_Channel,O. Priority_Of_Service, O. Replay_Prevent,O. Traf_Audit
T. Fail	O. Fail_Secure,O. Alarm, O. Trust_Backup,O. Trusted_Recovery, O. Validation
T. Flaw	O. Lifecycle,O. Patches, O. Test,O. Validation
T. Hostile_Admin	O. Trust_Backup, O. Trusted_Recovery
T. Mgmt_Error	O. Cfg_Manage,O. Trust_Backup, O. Trust_Backup,O. Trusted_Recovery
T. Modify	O. Ctrl_Channel, O. Trusted_Recovery, O. Validation

表 A.1(续)

安全环境	安全目的
T. Ntwk_Map	O. Ctrl_Channel,O. Detect_Connection, O. Protect_Addresses,O. Mgmt_Path
T. Replay_Attack	O. Access_Control,O. Ctrl_Channel, O. Ctrl_I&A,O. Detect_Connection, O. Mgmt_I&A,O. Replay_Prevent
T. Sel_Pro	O. Sel_Pro
T. Spoof	O. Ctrl_I&A, O. Detect_Connection, O. Protect_Addresses
T. Unauth_Mgmt_Access	O. Access_Control,O. Detect_Connection, O. Trust_Backup,O. Trusted_Recovery
A. Audit_Review	OE. Admin_Audit,OE. Audit_Review
A. Cryptanalytic	OE. Cryptography
A. Environmental	OE. Environment
A. ExpAgent	OE. Admin_Audit,OE. Attr_Mgt, OE. Audit_Review,OE. Cryptography, OE. Mgmt_I&A,OE. Personnel, OE. Physical
A. Physical	OE. Environment, OE. Physical
A. Time_Source	OE. Admin_Audit, OE. Synchronization
A. Train	OE. Guide_Docs, OE. Personnel
P. Accountability	OE. Admin_Audit

表 A.2 安全目的与安全环境的对应关系

安全目的	安全环境
O. Access_Control	A. ExpAgent, P. Authentication, P. Availability, P. Peer, T. Replay_Attack, T. Unauth_Mgmt_Access
O. Alarm	P. Availability, P. Notify, P. Survive, T. Fail
O. Cfg_Confidentiality	P. Confidentiality, P. Procedures

表 A.2(续)

安全目的	安全环境
O. Cfg_Integrity	P. Integrity
O. Cfg_Manage	P. Integrity, P. Procedures, P. Survive, T. Mgmt_Error
O. Ctrl_Channel	A. ExpAgent, P. Confidentiality, P. Integrity, P. Peer, P. Reliable_Transport, T. Analysis, T. Capture, T. Cryptanalytic, T. Denial, T. Modify, T. Ntwk_Map
O. Ctrl_Channel	T. Replay_Attack
O. Ctrl_I&A	A. ExpAgent, P. Accountability, P. Authentication, P. Peer, T. Replay_Attack, T. Spoof
O. Detect_Connection	A. ExpAgent, T. Analysis, T. Capture, T. Ntwk_Map, T. Replay_Attack, T. Spoof, T. Unauth_Mgmt_Access
O. Fail_Secure	P. Availability, P. Survive, T. Fail, T. Trans_Error
O. Lifecycle	P. Accountability, P. Survive, P. SysAssur, T. Flaw
O. Mgmt_Path	A. ExpAgent, P. Confidentiality, P. Integrity, P. Procedures, T. Analysis, T. Capture, T. Cryptanalytic, T. Ntwk_Map
O. Patches	P. Informaiton_Update, P. Procedures, T. Flaw
O. Priority_Of_Service	P. Reliable_Transport, T. Compromised_Node, T. Denial
O. Protect_Addresses	A. ExpAgent, P. Peer, T. Analysis, T. Compromised_Node, T. Ntwk_Map
O. Protect_Addresses	T. Spoof
O. Protocols	P. Interoperability, P. Reliable_Transport
O. Replay_Prevent	A. ExpAgent, P. Availabiltiy, P. Reliable_Transport, T. Denial, T. Replay_Attack
O. Protocols, P. Interoperability	P. Reliable_Transport
O. Replay_Prevent	A. ExpAgent, P. Availabiltiy, P. Reliable_Transport, T. Denial, T. Replay_Attack

表 A.2(续)

安全目的	安全环境
O. Sel_Pro	T. Sel_Pro
O. Test	P. Survive, P. SysAssur, T. Flaw
O. Traf_Audit	A. ExpAgent,A. Time_Source, P. Accountability,P. Procedures, P. Reliable_Transport,T. Compromised_Node, T. Denial
O. Trust_Backup	A. ExpAgent,P. Confidentiality
O. Trust_Backup	T. Unauth_Mgmt_Access,P. Procedures, P. Survive,T. Fail,T. Hostile_Admin, T. Mgmt_Error
O. Trusted_Recovery	P. Default_Config,P. Survive, T. Compromised_Node,T. Fail, T. Hostile_Admin,T. Mgmt_Error, T. Unauth_Mgmt_Access
O. Unused_Fields	A. ExpAgent,T. Covert
O. Validation	P. Information_Update,P. Survive
O. Validation	P. Information_Update,P. Survive, P. SysAssur,T. Fail,T. Flaw,T. Modify
O. Validation	P. Information_Update,P. Survive, P. SysAssur,T. Fail, T. Flaw,T. Modify
OE. Admin_Audit	Audit_Review,A. ExpAgent, A. Time_Source,P. Accountability, P. Audit_Admin,P. Authentication, P. Procedures,T. Hostile_Admin, T. Mgmt_Error,T. Unauth_Mgmt_Access
OE. Attr_Mgt	A. ExpAgent, T. Modify
OE. Audit_Review	A. Audit_Review, A. ExpAgent, P. Audit_Admin
OE. Cryptography	A. Cryptanalytic, A. ExpAgent
OE. Environment	A. Environmental, A. Physical, T. Fail

表 A.2(续)

安全目的	安全环境
OE. Guide_Docs	A. Train, P. Accountability, P. Guidance, P. Information_Update, P. Procedures, P. SysAssur
OE. Personnel	A. ExpAgent, A. Train, T. Hostile_Admin, T. Mgmt_Error, T. Modify, T. Unauth_Mgmt_Access
OE. Physical	A. ExpAgent, A. Physical, T. Fail, T. Ntwk_Map, T. Unauth_Mgmt_Access
OE. Synchronization	A. Time_Source

A.2.1 组织安全策略

A.2.1.1 可核查性(P. Accountability)

使用网络交换机传送信息的组织、拥有网络配置管理员角色的人员和开发者应该对其行为活动负责。

基本原理:

OE. Admin_Audit:带标识的审计记录

OE. Admin_Audit 对 P. Accountability 的支持,是通过确保具有网络管理角色的人能够对他们在网络管理系统中的行为负责。审计记录至少要报告网络管理人员的身份、网络管理人员在系统中执行的行为、行为产生的时间和日期。

O. Ctrl_I&A:受控标识和鉴别

O. Ctrl_I&A 对 P. Accountability 的支持,是通过与访问控制策略相一致的标识和鉴别来确保组织对他们的行为负责。

OE. Guide_Docs:指导性文档

OE. Guide_Docs 对 P. Accountability 的支持,是要求开发者对其所提供的指导性文档负责。

O. Lifecycle:生命周期安全

O. Lifecycle 对 P. Accountability 的支持,是要求开发者在硬件、软件或固件升级时应保持或增加安全特性。

OE. Mgmt_I&A:管理标识和鉴别

OE. Mgmt_I&A 对 P. Accountability 的支持,是通过对管理人员的标识和鉴别,来保证他们能够对其行为活动负责。

O. Traf_Audit:带标识的审计流量记录

O. Traf_Audit 对 P. Accountability 的支持,是依据流量记录的产生和分析,保证客户能够对其行为活动负责。流量记录至少应该标识与数据传输、流量大小、传输的时间和日期有关的节点。例如,当发送大于允许值的流量而超过带宽,并导致网络拒绝为其他客户服务的时候,流量审计能定位这种组织责任。

A.2.1.2 审计管理人员的数据(P. Audit_Admin)

网络管理系统应该能产生和传送审计记录,审计记录应提供充足的信息,用来断定在会话发生时管理员、管理日期、管理时间和管理行为,应该周期性的审阅审计记录。

基本原理:

OE. Admin_Audit:带标识的审计记录

OE. Admin_Audit 对 P. Audit_Admin 的支持,是通过确保具有网络管理角色的人能够对他们在网络管理系统中的行为负责。审计记录至少要报告网络管理人员的标识、网络管理人员在系统中的行为

活动、行为产生的时间和日期。

OE. Audit_Review：审计记录查阅

OE. Audit_Review 对 P. Audit_Admin 的支持，是通过保证审计记录的周期性审阅。

OE. Mgmt_I&A：管理标识和鉴别

OE. Mgmt_I&A 对 P. Audit_Admin 的支持，是通过在会话建立前先标识和鉴别网络管理人员的角色。

A. 2. 1. 3　操作员和节点的鉴别(P. Authentication)

网络交换机应能支持对网络审计管理员、网络配置管理员和网络安全管理员的鉴别，并且网络交换机也应支持对等节点的鉴别。

基本原理：

O. Access_Control：网络访问控制

O. Access_Control 对 P. Authentication 的支持，在于必须在访问控制策略有效的情况下实施鉴别。

OE. Admin_Audit：带标识的审计记录

OE. Admin_Audit 对 P. Authentication 的支持，为网络配置管理员或者网络安全管理员在获得其设定的角色前必须进行鉴别以产生审计记录。

O. Ctrl_I&A：受控标识和鉴别

O. Ctrl_I&A 对 P. Authentication 的支持，是通过只有在标识和鉴别之后才允许连接。

OE. Mgmt_I&A：管理标识和鉴别

OE. Mgmt_I&A 对 P. Authentication 的支持，在于设定角色之前必须进行鉴别。

A. 2. 1. 4　网络可用性(P. Availability)

为保证满足客户端的任务需求以及信息传输应保证网络资源的可用性。

基本原理：

O. Access_Control：网络访问控制

O. Access_Control 对 P. Availability 的支持，是通过只允许对网络的授权使用。阻止所有未授权的访问，预防网络交换机和网络的过度负担。

O. Alarm：安全风险报警通知

O. Alarm 对 P. Availability 的支持，是通过检测和报警与失败、错误或与安全相关的事件，来保证网络对客户的有效性。警告对于纠正问题具有迅速的响应，并且让网络正确的运行而持续对客户有效。

O. Fail_Secure：故障发生时安全状态的保存

O. Fail_Secure 对 P. Availability 的支持，是通过保存系统在停止期间的安全状态，来保证网络的有效性。

O. Priority_of_Service：提供服务优先级

O. Priority_of_Service 对 P. Availability 的支持，是通过保证客户不能消耗多于分配给他们的处理时间和宽带，避免网络资源对其他客户无效。

O. Replay_Prevent：避免重放攻击

O. Replay_Prevent 对 P. Availability 的支持，是通过拒绝旧的或复制的信息包，避免过度地利用网络资源。

A. 2. 1. 5　信息的保密性(P. Confidentiality)

在实时和存储状态下，应保持统计数据、配置信息和连接信息的保密性。为了保持其保密性，网络交换机必须能够支持一个健壮的加密基础设施。对于加密装置，网络交换机要具备加解密能力或接口支持能力。

基本原理：

O. Cfg_Confidentiality：网络配置保密性

O. Cfg_Confidentiality 对 P. Confidentiality 的支持，是通过保证配置和连接信息的保密性。

O. Ctrl_Channel：控制数据的可信通道

O. Ctrl_Channel 对 P. Confidentiality 的直接支持，是通过保证传输控制信息的保密性。

O. Mgmt_Path：管理数据的可信路径

O. Mgmt_Path 对 P. Confidentiality 的直接支持，是通过保证网络管理数据的保密性。

O. Trust_Backup：系统数据备份的完整性和保密性

O. Trust_Backup 对 P. Confidentiality 的直接支持，是通过保证存储网络文件和配置参数的保密性。

A. 2. 1. 6　默认配置（P. Default_Config）

网络交换机的默认设置应能防止其安全功能的削弱或失效。所有有助于网络交换机安全性的功能应是默认生效的。

基本原理：

O. Trusted_Recovery：可信的恢复

O. Trusted_Recovery 对 P. Default_Config 的支持，是通过保证失败时对安全状态的恢复。如果恢复为默认的设置，那么要保持网络的安全性。

A. 2. 1. 7　安装和使用指南（P. Guidance）

指南文件应能提供网络交换机安全安装、配置和维护的指导。

基本原理：

OE. Guide_Docs：指导性文档

OE. Guide_Docs 保证文档将提供网络交换机的安装、配置和维护的指导。

A. 2. 1. 8　网络交换机信息更新（P. Information_Update）

验证已接收的网络交换机信息文件、异常通知、补丁程序、升级文件等信息的完整性，上述文件或信息必须有实时的分发机制。

基本原理：

OE. Guide_Docs：指导性文档

OE. Guide_Docs 对 P. Information_Update 的支持，是通过保证指导性文档提供实时的分发机制。

O. Patches：安全修复和补丁

O. Patches 对 P. Information_Update 的直接支持，是通过在网络上分发或安装最新的补丁程序。

O. Validation：软硬固件验证

O. Validation 对 P. Information_Update 的直接支持，是通过保证所有软硬固件补丁和升级程序的完整性。

A. 2. 1. 9　内容的完整性（P. Integrity）

管理和控制信息在传输期间应保持其内容的完整性，同时要保持所有信息在存储状态下的完整性。

基本原理：

O. Cfg_Integrity：配置完整性

O. Cfg_Integrity 对 P. Integrity 的支持，是通过保证信息在存储状态下的完整性。

O. Cfg_Manage：管理配置数据

O. Cfg_Manage 对 P. Integrity 的支持，是通过保证网络管理信息在存储状态下的完整性。

O. Ctrl_Channel：控制数据的可信通道

O. Ctrl_Channel 对 P. Integrity 的支持，是通过保证控制信息在对等网络交换机之间传输的完整性。

O. Mgmt_Path：管理数据的可信路径

O. Mgmt_Path 对 P. Integrity 的支持，是通过保证网络管理信息在网络交换机和网络管理站之间

传输的完整性。

A.2.1.10 互操作性(P. Interoperability)

网络交换机应能与其他厂商的网络交换机互连互通。在网络交换机中要实现标准化的、非专有的协议(如路由选择、信令协议等)。厂商可以选择性的实现一些专有协议,但为了达到互通的目的,厂商也应在网络交换机中实现标准协议。

基本原理:

O. Protocols:协议

O. Protocols 对 P. Interoperability 的支持,是通过保证在网络交换机中执行协议,以达到互操作的目的。

A.2.1.11 故障通告(P. Notify)

网络交换机及其安全环境应具备(或在其他设备配合下)提醒和报警能力,例如:通过 SNMP 第 3 版的陷门机制发送部件、固件、硬件或软件的失效通知。

基本原理:

O. Alarm:安全风险报警通知

O. Alarm 对 P. Notify 的支持,是通过保证对于任何组件的失败或错误,都具备检测和报警的能力。

A.2.1.12 对等节点(P. Peer)

安全的节点应有接受来自信任的和不信任节点的流量的能力。为了保护信息,将会在信任的和不信任的节点之间过滤流量。

基本原理:

O. Access_Control:网络访问控制

O. Access_Control 对 P. Peer 的支持,是通过保证只有授权人员才能够访问安全节点。

O. Ctrl_Channel:控制数据的可信通道

O. Ctrl_Channel 对 P. Peer 的支持,是通过保证所有在对等网络交换机之间传输的控制数据的完整性和保密性。

O. Ctrl_I&A:受控标识和鉴别

O. Ctrl_I&A 与 O. Access_Control 联合支持 P. Peer。O. Ctrl_I&A 保证只对授权实体提供连通性,并且与访问控制策略保持一致,要求正确的标识和鉴别实体。

O. Protect_Addresses:地址保护

O. Protect_Addresses 通过提供发送和接收授权实体地址的保密性和完整性,以保证在信任的和不信任的网络交换机之间传递流量。

A.2.1.13 信息管理规程(P. Procedures)

网络交换机安全环境中的规程应限制无意的泄露、敏感信息的修改以及资源的不恰当使用。例如:敏感信息可能包括但不限于文档化的操作规程材料、设备安装规程、审计文件、配置文件、网络图表、物理连接和网络测试结果的信息。

基本原理:

OE. Admin_Audit:带标识的审计记录

OE. Admin_Audit 对 P. Procedures 的支持,是通过保证使用适当的程序来存储和保护网络管理人员的审计记录。

OE. Audit_Review:审计记录查阅

OE. Audit_Review 对 P. Procedures 的支持,是通过保证周期性的查阅审计记录。查阅审计记录能够发现对资源的不正确利用。

O. Cfg_Confidentiality:网络配置保密性

O. Cfg_Confidentiality 对 P. Procedures 的支持，是通过保证使用适当的程序来保持配置和连接信息的保密性。

O. Cfg_Manage：管理配置数据

O. Cfg_Manage 对 P. Procedures 的支持，是通过保证使用适当的程序来记录和保持配置和连接信息，并且确保存储的完整性。

OE. Guide_Docs：指导性文档

OE. Guide_Docs 对 P. Procedures 的支持，是通过保证具有详细的程序，以提供正确的安装、维护、配置和利用网络交换机及其安全功能。

O. Mgmt_Path：管理数据的可信路径

O. Mgmt_Path 对 P. Procedures 的支持，是通过保证所有在网络交换机和网络管理站之间传输的管理数据的完整性和保密性。

O. Patches：安全修复和补丁

O. Patches 对 P. Procedures 的支持，是通过保证使用适当的程序，以通知、分发和安装最新的补丁，保持对网络资源的正确操作和利用。正确的使用无缺陷的软件，将减少信息泄露的风险。

O. Traf_Audit：带标识的审计流量记录

O. Traf_Audit 对 P. Procedures 的支持，是通过保证使用适当的程序，来产生和维持流量审计记录的完整性。

O. Trust_Backup：系统数据备份的完整性和保密性

O. Trust_Backup 对 P. Procedures 的支持，是通过保证使用适当的程序，来维持网络信息的一致和正确存储，避免信息的泄露或修改。

A. 2. 1. 14　可靠传输(P. Reliable_Transport)

应实现特定的可靠传输和检错机制协议以用于网络管理和控制。

基本原理：

O. Ctrl_Channel：控制数据的可信通道

O. Ctrl_Channel 对 P. Reliable_Transport 的支持，是通过验证收到的控制数据的完整性。

O. Priority_of_Service：提供服务优先级

O. Priority_of_Service 对 P. Reliable_Transport 的支持，是通过保证依据设备提供的服务优先级来传输信息。

O. Protocols：协议

O. Protocols 对 P. Reliable_Transport 的支持，是通过保证在网络交换机中执行标准协议，从而保证可信的传输流量。

O. Replay_Prevent：避免重放攻击

O. Replay_Prevent 对 P. Reliable_Transport 的支持，是通过保证能够检测和拒绝旧的和复制的数据包，避免这些数据包干涉其他的通信。

O. Traf_Audit：带标识的审计流量记录

O. Traf_Audit 对 P. Reliable_Transport 的支持，是通过记录和分析网络流量，来保证流量通信的可靠性。

A. 2. 1. 15　网络可生存性与恢复(P. Survive)

网络资源应能够从敌意的破坏尝试中恢复，同时必须具有从传输期间的错误中恢复的能力。网络必须能抵御硬件或软件失效，或具有在合理时间内复原的能力。用于恢复的任何环境都应被记录下来。

基本原理：

O. Alarm：安全风险报警通知

O. Alarm 对 P. Survive 的支持，是通过网络交换机对安全相关事件和失败或错误提供的报警能力，

并且要求对纠正问题、恢复网络交换机以及将网络交换机的安全功能恢复到操作的正常状态，从而保证网络交换机和网络交换机安全功能的可生存性。

O. Cfg_Manage：管理配置数据

O. Cfg_Manage 对 P. Survive 的支持，是通过保证配置和连接信息的持续性和信息的存储完整性。在这种方式下，能够迅速的重建必需的网络配置。

O. Fail_Secure：故障发生时安全状态的保存

O. Fail_Secure 对 P. Survive 的支持，是通过在组件或电力失败的事件中保持系统的安全状态，来提供弹性和可生存性。

O. Lifecycle：生命周期安全

O. Lifecycle 对 P. Survive 的支持，是通过保证贯穿网络交换机整个生命周期的安全功能被保护，以便资源能够保持从抵抗错误或逆着安全的尝试进行恢复的能力。

O. Test：网络交换机及其安全功能的测试

O. Test 对 P. Survive 的支持，是通过保证网络将有能力生存或从失败中恢复。

O. Trust_Backup：系统数据备份的完整性和保密性

O. Trust_Backup 对 P. Survive 的支持，是通过所有网络交换机和网络文件的复制，包括配置参数的复制，将确保从破坏尝试的事件中或者与网络交换机、主要管理系统相关的失败操作得到迅速恢复。

O. Trusted_Recovery：可信的恢复

O. Trusted_Recovery 对 P. Survive 的支持，是通过保证网络交换机有能力从失败状态中恢复。

O. Validation：软硬固件验证

O. Validation 对 P. Survive 的支持，是通过保证所有的硬件、软件和固件被正确的安装和使用，从而确保网络将有能力抵抗、恢复或幸免于失败、错误或危及安全的尝试。

A. 2. 1. 16　硬件、软件和固件的完整性(P. SysAssur)

应提供使完整性生效、初始化、软硬固件升级的功能和规程。应在初始安装和软件升级和固件交换时确保其完整性。

基本原理：

OE. Guide_Docs：指导性文档

OE. Guide_Docs 对 P. SysAssur 的支持，是通过解释网络交换机及其安全功能的特征、程序和预期的行为。

O. Lifecycle：生命周期安全

O. Lifecycle 对 P. SysAssur 的支持，是通过保证特征和程序的完整性，以正确执行网络交换机及其安全功能。

O. Test：网络交换机及其安全功能的测试

O. Test 对 P. SysAssur 的支持，是通过保证正确的执行网络交换机及其安全功能。

O. Validation：软硬固件验证

O. Validation 对 P. SysAssur 的支持，是通过保证所有硬件、软件和固件的完整性，从而使其正确的执行。

A. 2. 2　威胁

A. 2. 2. 1　通信分析(T. Analysis)

攻击者可能收集源和目标地址、大量数据和发送数据的日期、时间。

基本原理：

O. Ctrl_Channel：控制数据的可信通道

O. Ctrl_Channel 减轻 T. Analysis 的威胁，是通过保持控制信息的保密性以及支持加密机制。

O. Detect_Connection：检测非授权连接

O. Detect_Connection 抵抗 T. Analysis 的威胁，是通过网络交换机所具备的检测和警报未授权连接的能力。

O. Mgmt_Path：管理数据的可信路径

O. Mgmt_Path 抵抗 T. Analysis 的威胁，是通过保证所有管理数据的完整性和保密性。

O. Protect_Addresses：地址保护

O. Protect_Addresse 抵抗 T. Analysis 的威胁，是通过保护资源和接受的授权地址的保密性和完整性，从而防止攻击者发现真实地址。

A.2.2.2 未授权网络访问并获取数据(T. Capture)

攻击者可能偷听、接入传输线或用其他方式获取通信信道上传输的数据。

基本原理：

O. Ctrl_Channel：控制数据的可信通道

O. Ctrl_Channel 抵抗 T. Capture 的威胁，是通过保证控制平面信息的保密性和完整的持续力。

O. Detect_Connection：检测非授权连接

O. Detect_Connection 抵抗 T. Capture 的威胁，是通过具备对任何未授权连接的检测能力。

O. Mgmt_Path：管理数据的可信路径

O. Mgmt_Path 抵抗 T. Analysis 的威胁，是通过为管理数据通讯提供一个可信路径，以防止攻击者试图捕获网络管理数据。

A.2.2.3 节点泄漏(T. Compromised_Node)

节点成为不安全的，可以使得网络交换机配置文件或路由表被修改，导致网络交换机异常运行，网络交换机安全功能失效，或流量可能被重路由经过未授权的节点。

基本原理：

OE. Audit_Review：审计记录查阅

OE. Audit_Review 抵抗 T. Compromised_Node 的威胁，是通过审阅和分析流量的审计记录，从而发现异常的网络流量模式。

O. Priority_of_Service：提供服务优先级

O. Priority_of_Service 抵抗 T. Compromised_Node 的威胁，是通过对提供服务优先级的控制和执行，从而防止仅对一个指定的优先级的传输流量的节点进行操作的尝试。

O. Protect_Addresses：地址保护

O. Protect_Addresse 抵抗 T. Compromised_Node 的威胁，是通过保证地址的保密性和完整性。

O. Traf_Audit：带标识的审计流量记录

O. Traf_Audit 与 OE. Audit_Review 联合抵抗 T. Compromised_Node 的威胁，是通过流量记录的产生而体现的获取持续的异常行为的能力。

O. Trusted_Recovery：可信的恢复

O. Trusted_Recovery 减轻 T. Compromised_Node 的威胁，是通过保证在除了危及网络交换机安全的情况下，并且在破坏或中断操作之后，网络交换机能够恢复到一个安全状态。

A.2.2.4 隐通道(T. Covert)

隐通道通常在隐蔽区域中隐藏信息，其目的是用于不被监控地传送信息。

基本原理：

O. Unused_Fields ：未用区域

O. Unused_Fields 对 T. Covert 威胁的直接抵抗，在于阻塞或适当使用任何未用区域，不会使其用于隐藏和传输信息。

A.2.2.5 密码分析(T. Cryptanalytic)

攻击者为了复原信息内容而去尝试进行已加密数据的密码分析。

基本原理：

O. Ctrl_Channel：控制数据的可信通道

O. Ctrl_Channel 抵抗 T. Cryptanalytic 的威胁，是通过加密机制的支持和可控信息完整性的持续力，从而保证控制信息的保密性。

O. Mgmt_Path：管理数据的可信路径

O. Mgmt_Path 抵抗 T. Cryptanalytic 的威胁，是通过加密机制的支持和管理数据完整性的持续力，从而保证管理数据的保密性。

A. 2. 2. 6　拒绝服务(T. Denial)

攻击者通过执行指令、发送超限额的高优先级流量数据或执行其他操作，在网络上造成不合理的负载，造成授权客户端得不到应有的系统资源，即导致拒绝服务。

基本原理：

O. Ctrl_Channel：控制数据的可信通道

O. Ctrl_Channel 抵抗 T. Denial 的威胁，是通过保证控制信息的完整性，从而能够正确运行，避免资源对于其他客户的失效。

O. Priority_of_Service：提供服务优先级

O. Priority_of_Service 抵抗 T. Denial 的威胁，是通过控制和加强服务预定的优先级，从而确保一个流量的优先级将不会过度干涉或延迟服务提供的不同优先级的流量。

O. Replay_Prevent：避免重放攻击

O. Replay_Prevent 抵抗 T. Denial 的威胁，是通过阻止消耗网络资源的重放信息。因此，网络交换机阻止重放信息的能力将有助于保证网络资源对于授权客户的有效性。

O. Traf_Audit 减少 T. Denial 的威胁，是通过获取流量统计，来鉴别独占网络资源的网络交换机。

A. 2. 2. 7　部件或电源失效(T. Fail)

一个或多个系统部件或电源失效可能造成重要系统功能破坏和重要系统数据的丢失。

基本原理：

O. Alarm：安全风险报警通知

O. Alarm 减少 T. Fail 的威胁，是通过允许对纠正错误或失败具有迅速的响应。

OE. Environment：环境保护

OE. Environment 减少 T. Fail 的威胁，是通过使网络交换机发展，以便能够保护它自己并且抵抗环境的威胁，例如失火、动力、储运损耗等等。

O. Fail_Secure：故障发生时安全状态的保存

O. Fail_Secure 有助于抵抗 T. Fail 的威胁，是通过保证网络交换机及其安全功能能够恢复到安全状态。

OE. Physical：物理保护

OE. Physical 减少 T. Fail 的威胁，是通过对资源的物理保护，来帮助防止恶意的或无意的然而又是有害的物理攻击。

O. Trust_Backup：系统数据备份的完整性和保密性

O. Trust_Backup 减少 T. Fail 的威胁，是通过产生网络数据的复制版本，从而快速地使网络交换机及其安全功能恢复到正确的操作。

O. Trusted_Recovery：可信的恢复

O. Trusted_Recovery 减少 T. Fail 的威胁，是通过保证除了在危及网络交换机安全的情况下，并且在操作中断之后，网络交换机能够恢复到一个安全状态。O. Trusted_Recovery 也保证在使系统重新一体化的时候，取代失败的组件，这样将恢复为不会引起错误或造成对网络的其他部分的安全破坏。

O. Validation：软硬固件验证

O. Validation 抵抗 T. Fail 的威胁，是通过保证所有组件被正确的安装和使用。

A.2.2.8 硬件、软件或固件的缺陷(T. Flaw)

硬件、软件或固件的缺陷导致网络交换机及其安全功能的脆弱性。

基本原理：

O. Lifecycle：生命周期安全

O. Lifecycle 减少 T. Flaw 的威胁，是通过保存贯穿网络交换机整个可操作的生命周期中的网络交换机安全功能的正确操作。

O. Patches：安全修复和补丁

O. Patches 减少 T. Flaw 的威胁，是通过保证大多数最新的修复和补丁被安装，从而确保能够抵抗存在于网络交换机及其安全功能的缺陷。

O. Test：网络交换机及其安全功能的测试

O. Test 减少 T. Flaw 的威胁，是通过发现隐藏操作或危及网络交换机及其安全功能的缺陷。

O. Validation：软硬固件验证

O. Validation 减少 T. Flaw 的威胁，是通过验证完整性、正确的安装和所有软硬固件的使用，从而有助于鉴别那些可以引起网络交换及其安全功能的缺陷。

A.2.2.9 管理员网络授权的滥用(T. Hostile_Admin)

网络配置管理员或网络安全管理员有意滥用权限，不适当地访问或修改了数据信息，例如：配置数据、审计数据、口令文件或误处理其他的敏感数据文件。

基本原理：

OE. Admin_Audit：带标识的审计记录

OE. Admin_Audit 抵抗 T. Hostile_Admin 的威胁，监控和记录各个行为和身份，那么滥用特权的威胁就会减少。

OE. Audit_Review：审计记录查阅

OE. Audit_Review 减少 T. Hostile_Admin 的威胁，是通过周期性的监控和审阅行为。

OE. Mgmt_I&A：管理标识和鉴别

OE. Mgmt_I&A 减少 T. Hostile_Admin 的威胁，是通过在审计记录中获取网络管理人员的标识。

OE. Personnel：可信人员

OE. Personnel 抵抗 T. Hostile_Admin 的威胁，是通过雇用可信赖的和有能力的人员。

O. Trust_Backup：系统数据备份的完整性和保密性

O. Trust_Backup 减少 T. Hostile_Admin 的威胁，是通过确保产生网络数据的复制版本。如果主系统失效，那么从系统能够快速进入运行状态，从而保证操作的连续性。另外，如果网络文件没有存储在从管理站，而是在另一个存储设备上，那么网络参数依然能够得到保护。

O. Trusted_Recovery：可信的恢复

O. Trusted_Recovery 减少 T. Hostile_Admin 的威胁，是在运行中断时，在不危及安全的情况下，网络能够恢复到一个安全状态。

A.2.2.10 管理错误(T. Mgmt_Error)

拥有网络配置管理员角色的人员可能无意的不恰当访问或修改了数据信息，或误用资源。

基本原理：

OE. Admin_Audit：带标识的审计记录

OE. Admin_Audit 通过对错误的验证使得各种行为及其影响能够得到纠正，从而降低了 T. Mgmt_Error 的威胁。

O. Cfg_Manage：管理配置数据

O. Cfg_Manage 通过对与网络交换机及网络信息的恢复有关的配置和连接信息的捕捉和保持，降

低了 T. Mgmt_Error 的威胁。

OE. Personnel:可信人员

OE. Personnel 通过雇佣和培养一批可信的有能力的人员降低了 T. Mgmt_Error 的威胁。

O. Trust_Backup:系统数据备份的完整性和保密性

当有严重错误发生时,O. Trust_Backup 能够在首选系统恢复过程时通过第二系统继续操作,从而降低 T. Mgmt_Error 的威胁。

O. Trusted_Recovery:可信的恢复

O. Trusted_Recovery 通过确保在一系列中断操作发生时,在没有安全泄漏的情况下恢复到安全状态,从而降低了 T. Mgmt_Error 的威胁。

A. 2. 2. 11 修改协议(T. Modify)

攻击者未经授权的修改或操纵协议(例如:路由选择、信号等协议)。

基本原理:

OE. Attr_Mgt:管理属性

OE. Attr_Mgt 减轻了 T. Modify 的威胁。网络操作管理者和网络安全管理者有特权以至于恶意的网络操作人员可以相对容易进行修改操作。然而,当网络操作人员的标识被捕捉并审计后此种威胁可以有效地降低。

O. Ctrl_Channel:控制数据的可信通道

O. Ctrl_Channel 通过确保控制信息以及信号化的信息的保密性和完整性来减弱 T. Modify 的威胁。

OE. Personnel:可信人员

通过雇佣可信赖的员工,这些人不会滥用他们的权利做未授权的修改或者对使用中的配置和协议做特殊处理来减弱 T. Modify 的威胁。

O. Trusted_Recovery:可信的恢复

当 T. Modify 威胁引起了操作中的不连续,O. Trusted_Recovery 能确保网络交换机和网络能够返回到安全状态,从而减轻 T. Modify 的威胁。

O. Validation:软硬固件验证

O. Validation 通过确保在网络交换机和网络中使用各种软件、硬件、固件的完整性和操作的正确性,来减弱 T. Modify 的威胁。

A. 2. 2. 12 网络探测(T. NtwkMap)

攻击者可能进行网络探测来获得节点地址、路由表信息和物理位置。

基本原理:

O. Ctrl_Channel:控制数据的可信通道

通过确保控制信息的保密性及完整性 O. Ctrl_Channel 来减弱 T. Ntwk_Map 的威胁。

O. Detect_Connection:检测非授权连接

通过对未授权连接的检测,O. Detect_Connection 来减弱 T. Ntwk_Map 的威胁。

OE. Physical:物理保护

OE. Physical 通过对网络交换机资源的物理保护可降低攻击者企图通过未授权的连接捕捉网络信息的威胁,从而减弱 T. Ntwk_Map 的威胁。

O. Protect_Addresses:地址保护

O. Protect_Addresses 通过确保传送和接收地址的保密性和完整性来减弱 T. Ntwk_Map 的威胁。

O. Mgmt_Path:管理数据的可信路径

通过为所有管理数据确保可信路径,O. Mgmt_Path 减弱了 T. Ntwk_Map 的威胁。可信路径保护了数据,同时给攻击者为分析和发现网络信息,获得管理数据增加了困难。

A.2.2.13 重放攻击(T.Replay_Attack)

攻击者通过记录通信会话,并重放它们伪装成已验证的客户端非法获取网络交换机的访问权。管理信息也可能被记录和重放,从而用于伪装成已验证的网络配置管理员或网络安全管理员来得到对网络管理资源的访问权。

基本原理:

O.Access_Control:访问控制机制

通过强制执行访问控制机制,为攻击者获得网络交换机和网络的访问权增加了难度,从而降低了T.Replay_Attack的威胁。

O.Ctrl_Channel:控制数据的可信通道

由于网络交换机支持加密基础设施,因此它能确保控制信息的完整性和保密性,从而降低了T.Replay_Attack的威胁。

O.Ctrl_I&A:受控标识和鉴别

O.Ctrl_I&A通过要求标识和鉴别,增加了攻击者获得网络交换机访问权的难度,从而降低了T.Replay_Attack的威胁。

O.Detect_Connection:检测非授权连接

O.Detect_Connection确保了对非授权连接的检测,消除了通过记录和重放信息以获得网络交换机和网络资源访问权的可能,从而降低了T.Replay_Attack的威胁。

OE.Mgmt_I&A:管理标识和鉴别

OE.Mgmt_I&A通过要求标识和鉴别,增加了攻击者获得网络管理资源的难度,从而降低了T.Replay_Attack的威胁。

O.Replay_Prevent:避免重放攻击

O.Replay_Prevent直接对抗了T.Replay_Attack的威胁。

O.Replay_Prevent确保了网络交换机能够拒绝旧的和复制的信息包,以保证其自身免受重放攻击的威胁。

A.2.2.14 配置数据泄漏(T.Sel_Pro)

攻击者可能读、修改或破坏重要的网络交换机的安全配置数据。

基本原理:

O.Sel_Pro:自身安全配置泄露直接对抗了T.Sel_Pro。

A.2.2.15 欺骗攻击(T.Spoof)

客户端企图得到网络交换机资源,通过获得的网络地址来伪装成已授权的用户。未授权节点可能使用有效的网络地址来尝试访问网络。

基本原理:

O.Ctrl_I&A:受控标识和鉴别

O.Ctrl_I&A通过强制执行标识和鉴别增加了攻击者获取网络交换机访问权的困难,从而增加了设法执行欺骗的困难,因此对抗了欺骗攻击的威胁。

O.Detect_Connection:检测非授权连接

O.Detect_Connection通过对未授权连接的检测阻止了攻击者企图获取网络地址的可能,从而对抗了欺骗攻击的威胁。

OE.Mgmt_I&A:管理标识和鉴别

OE.Mgmt_I&A通过强制执行标识和鉴别增加了攻击者获取网络交换机访问权的困难,从而增加了执行欺骗操作的困难,因此对抗了欺骗攻击的威胁。

O.Protect_Addresses:地址保护

O.Protect_Addresses通过确保传输和接收地址的保密性和完整性,阻止了攻击者企图获得合法的

网络地址的可能，从而对抗了欺骗攻击的威胁。

A.2.2.16 对管理端口的非授权访问(T. Unauth_Mgmt_Access)

攻击者或滥用特权的网络配置管理员可能通过 Telnet、RMON 或其他方式访问管理端口，从而重新配置网络、引起拒绝服务、监视流量、执行流量分析等。

基本原理：

O. Access_Control：网络访问控制

O. Access_Control 通过执行网络访问控制机制对特权进行了限制，从而对抗了 T. Unauth_Mgmt_Access 的威胁。

OE. Admin_Audit：带标识的审计记录

OE. Admin_Audit 通过对负有责任的网络管理人员的行为的审计减弱了 T. Unauth_Mgmt_Access 的威胁。

OE. Audit_Review：审计记录查阅

OE. Audit_Review 通过定期的审计和查阅所有的行为，从而减弱了 T. Unauth_Mgmt_Access 的威胁。

O. Detect_Connection：检测非授权连接

O. Detect_Connection 确保对非授权连接的检测，有助于发现对管理数据的非授权的访问，从而减弱了 T. Unauth_Mgmt_Access 的威胁。

OE. Mgmt_I&A：管理标识和鉴别

OE. Mgmt_I&A 通过要求对网络管理人员进行标识和鉴别，审计这些人员并且与他们的行为相联系，减弱了 T. Unauth_Mgmt_Access 的威胁。

OE. Personnel：可信人员

OE. Personnel 通过雇佣和培养可信赖的网络管理人员降低了滥用特权的威胁。

OE. Physical：物理保护

OE. Physical 通过对资源的物理保护避免了恶意攻击和未授权修改，从而降低了 T. Unauth_Mgmt_Access 的威胁。

O. Trust_Backup：系统数据备份的完整性和保密性

O. Trust_Backup 通过确保网络交换机数据文件存储的保密性和完整性，降低了 T. Unauth_Mgmt_Access 的威胁。当未授权访问管理数据或者伪造网络参数时，O. Trust_Backup 要求能较快的恢复。

O. Trusted_Recovery：可信的恢复

O. Trusted_Recovery 确保当出现中断操作时网络交换机能够返回安全状态，从而减弱了 T. Unauth_Mgmt_Access 的威胁。

A.3 安全要求合理性

表 A.3 和表 A.4 说明了安全目的覆盖范围的全面性，即安全目的应涉及已确定安全环境的所有方面。首先，表 A.3 列出了每一个安全目的所覆盖的安全要求，之后对每一个安全目的覆盖的个体做了论述。

表 A.3 安全要求与安全目的对应关系

安全目的	安全要求
O. Access_Control	FDP_ACC. 1，FDP_ACF. 1，FDP_IFC. 1， FDP_IFF. 1，FIA_UAU. 2，FIA_UID. 2， FTA_TSE. 1

表 A.3(续)

安全目的	安全要求
OE. Admin_Audit	FAU_GEN. 1,FAU_GEN. 2,FAU_SEL. 1, FMT_MSA. 1,FMT_MSA. 3,FMT_MTD. 1 FPT_STM. 1,FPT_TDC. 1
O. Alarm	FPT_AMT. 1,FPT_TST. 1
OE. Attr_Mgt	FAU_SAR. 1,FMT_MSA. 1, FMT_MTD. 1,FMT_SMR. 2
OE. Audit_Review	FAU_SAR. 1,FPT_TDC. 1
O. Cfg_Confidentiality	FTP_ITC. 1,FTP_TRP. 1
O. Cfg_Integrity	FPT_ITI. 1,FPT_TST. 1, FTP_ITC. 1,FTP_TRP. 1
O. Cfg_Manage	FTP_TRP. 1
OE. Cryptography	FTP_ITC. 1,FTP_TRP. 1
O. Ctrl_Channel	FDP_UIT. 1,FTP_ITC. 1, FPT_ITI. 1,FDP_IFF. 1
O. Ctrl_I&A	FDP_ACC. 1,FDP_ACF. 1, FDP_IFC. 1,FDP_IFF. 1, FIA_UAU. 2,FIA_UID. 2, FTA_TSE. 1
O. Detect_Connection	FPT_ITI. 1,FPT_RPL. 1
OE. Environment	FPT_FLS. 1,FPT_RCV. 3, FPT-RCV. 4,FRU_FLT. 1
O. Fail_Secure	FPT_FLS. 1,FPT_RCV. 3, FPT_RCV. 4,FRU_FLT. 1
OE. Guide_Docs	ADV_FSP. 1,ALC_DVS. 1, AGD_ADM. 1,AGD_USR. 1, AVA_MSU. 1,AVA_VLA. 1
O. Lifecycle	FPT_AMT. 1,FPT_TDC. 1, FPT_TST. 1
O. Mgmt_Path	FDP_IFF. 1,FDP_ITC. 2, FDP_ETC. 2,FDP_UIT. 1, FPT_ITI. 1,FTP_TRP. 1
O. Patches	FMT_MOF. 1
OE. Personnel	AGD_ADM. 1,AGD_USR. 1, FMT_MOF. 1,FMT_MSA. 1, FMT_MSA. 3
OE. Physical	FPT_PHP. 1
O. Priority_Of_Service	FDP_IFF. 1,FRU_PRS. 2, FRU_FLT. 1

表 A.3(续)

安全目的	安全要求
O. Protect_Addresses	FDP_ITC. 2,FDP_ETC. 2,FPT_ITC. 1, FTP_ITC. 1,FTP_TRP. 1
O. Protocols	FDP_ETC. 2,FDP_ITC. 2,FDP_UIT. 1, FPT_FLS. 1,FPT_ITI. 1
O. Replay_Prevent	FDP_ETC. 2,FDP_ITC. 2, FDP_UIT. 2,FPT_ITI. 1, FPT_RPL. 1
O. Sel_Pro	FIA_AFL. 1
OE. Synchronization	FMT_MOF. 1,FPT_STM. 1
O. Test	ATE_COV. 2,ATE_FUN. 1, ATE_IND. 2,AVA_SOF. 1, AVA_VLA. 1,FPT_AMT. 1, FPT_TST. 1
O. Traf_Audit	FAU_GEN. 1,FAU_GEN. 2, FAU_SAR. 1,FAU_SEL. 1, FDP_IFF. 1,FPT_STM. 1、FPT_TDC. 1
O. Trust_Backup	FDP_UIT. 2
O. Trusted_Recovery	FPT_RCV. 3,FPT_RCV. 4, FPT_FLS. 1
O. Unused_Fields	FPT_ITI. 1
O. Validation	FPT_AMT. 1,FPT_TST. 1
OE. Mgmt_I&A	FIA_UAU. 2,FIA_UID. 2

表 A.4 安全目的与安全要求的对应关系

安全要求	安全目的
ACM_CAP. 3	EAL3 的要求
ACM_SCP. 1	EAL3 的要求
ADO_DEL. 1	EAL3 的要求
ADO_IGS. 1	EAL3 的要求
ADV_HLD. 2	EAL3 的要求
ADV_RCR. 1	EAL3 的要求
AGD_ADM. 1	EAL3 的要求,OE. Guide_Docs,OE. Personnel
AGD_USR. 1	EAL3 的要求,OE. Guide_Docs,OE. Personnel
ALC_DVS. 1	EAL3 的要求,OE_Guide_Docs
ATE_COV. 2	EAL3 的要求,O. Test
ATE_DPT. 1	EAL3 的要求
ATE_FUN. 1	EAL3 的要求,O. Test

表 A.4(续)

安全要求	安全目的
ATE_IND.2	EAL3 的要求,O.Test
AVA_MSU.1	EAL3 的要求,OE.Guide_Docs
AVA_SOF.1	EAL3 的要求
AVA_VLA.1	EAL3 的要求,OE.Guide_Docs,O.Test
FAU_GEN.1	OE.Admin_Audit,O.Traf_Audit
FAU_GEN.2	OE.Admin_Audit,O.Traf_Audit
FAU_SAR.1	OE.Admin_Audit,OE.Attr_Mgt, OE.Audit_Review,O.Traf_Audit
FAU_SEL.1	OE.Admin_Audit,
FAU_SEL.1	O.Traf_Audit,
FDP_ACC.1	O.Access_Control,O.Ctrl_I&A
FDP_ACF.1	O.Access_Control,O.Ctrl_I&A,
FDP_ETC.2	O.Mgmt_Path,O.Protect_Addresses, O.Protocols,O.Replay_Prevent
FDP_IFC.1	O.Access_Control,O.Ctrl_I&A
FDP_IFF.1	O.Access_Control,O.Ctrl_I&A, O.Ctrl_Channel,O.Mgmt_Path, O.Priority_Of_Service,O.Traf_Audit
FDP_ITC.2	O.Mgmt_Path,O.Protect_Addresses, O.Protocols,O.Replay_Prevent
FDP_UIT.1	O.Ctrl_Channel,O.Mgmt_Path,O.Protocols
FDP_UIT.2	O.Replay_Prevent,O.Trust_Backup
FIA_UAU.2	O.Access_Control,OE.Mgmt_I&A,.Ctrl_I&A
FIA_UID.2	O.Access_Control,OE.Mgmt_I&A, O.Ctrl_I&A
FIA_AFL.1	O.Sel_Pro
FMT_MOF.1	O.Patches,OE.Personnel,OE.Synchronization
FMT_MSA.1	OE.Admin_Audit,OE.Attr_Mgt, OE.Personnel
FMT_MSA.3	OE.Admin_Audit,OE.Personnel
FMT_MTD.1	OE.Admin_Audit,OE.Attr_Mgt
FMT_SMR.2	OE.Attr_Mgt
FPT_AMT.1	O.Alarm,O.Lifecycle,O.Test,O.Validation
FPT_FLS.1	OE.Environment,O.Fail_Secure, O.Protocols,O.Trusted_Recovery
FPT_ITC.1	O.Ctrl_Channel,

表 A.4(续)

安全要求	安全目的
FPT_ITI.1	O.Protect_Addresses,O.Cfg_Integrity, O.Ctrl_Channel,O.Detect_Connection,
FPT_ITI.1	O.Mgmt_Path,.Protocols,.Replay_Prevent, O.Unused_Fields
FPT_PHP.1	OE.Physical
FPT_RCV.3	OE.Environment,O.Fail_Secure, O.Trusted_Recovery
FPT_RCV.4	OE.Environment,O.Fail_Secure, O.Trusted_Recovery,
FPT_RPL.1	O.Detect_Connection,O.Replay_Prevent
FPT_STM.1	OE.Admin_Audit,OE.Synchronization, O.Traf_Audit
FPT_TDC.1	OE.Admin_Audit,OE.Audit_Review,.Lifecycle, O.Traf_Audit
FPT_TST.1	O.Alarm,O.Cfg_Integrity,
FPT_TST.1	O.Lifecycle,O.Test,O.Validation
FRU_FLT.1	OE.Environment,O.Fail_Secure, O.Priority_Of_Service
FRU_PRS.2	O.Priority_Of_Service
FTA_TSE.1	O.Access_Control,O.Ctrl_I&A
FTP_ITC.1	O.Cfg_Confidentiality,O.Cfg_Integrity, O.Ctrl_Channel,
FTP_TRP.1	OE.Cryptography,O.Protect_Addresses O.Cfg_Confidentiality,O.Cfg_Integrity, O.Cfg_Manage,OE.Cryptography,
FTP_TRP.1	O.Mgmt_Path,O.Protect_Addresses

A.3.1 网络访问控制(O.Access_Control)

网络交换机应实现访问控制策略,访问控制策略基于但不限于网络交换机的任务(只处理可信的或不可信的,或者处理混合流量)、网络交换机的标识(由一个机构、网络提供者所有,同时也支持许多机构或客户端所有)、源和目标地址、端口层次的过滤(如 Telnet、SNMP)等。

O.Access_Control 在网络交换机中的实现是依靠 FDP_ACC.1:子集访问控制;FDP_ACF.1:基于安全属性的访问控制——对期望通讯的网络交换机强制执行访问控制机制;FIA_UAU.2:任何行动前的用户鉴别;FIA_UID.2:任何行动前的用户标识,要求与访问控制机制相关联的标识和鉴别。此外,O.Access_Control 也是以下三个安全功能要求组件所实现:FTA_TSE.1:网络交换机会话建立,此功能可拒绝与网络交换机的会话建立;FDP_IFF.1:简单安全属性和 FDP_IFC.1:子集信息流控制,该功能要求针对接收到的信息执行与访问控制机制相关的信息流控制机制。

A.3.2 带标识的审计记录(OE.Admin_Audit)

网络配置管理员和网络安全管理员的活动应被审计,审计记录的存储和维护应符合安全策略。

OE. Admin_Audit 的实现通过以下几个安全功能要求组件：在网络交换机的环境方面是 FPT_TDC. 1：安全功能间基本安全功能数据的一致性，它确保审计记录能够被解释；FMT_MTD. 1：安全功能数据的管理；FAU_SEL. 1 选择性审计；FMT_MSA. 1：安全属性的管理；FMT_MSA. 3：静态属性初始化，该功能赋予网络安全管理员配置审计日志的特权；FAU_GEN. 1 和 FAU_GEN. 2 通过生成审计日志和与引起该事件的网络管理角色相关联的审计数据可直接实现此安全目标。生成审计日志的一个重要的方面是获取行为的时间，因此 FPT_STM. 1：可靠的时间戳是用来支持 OE. Admin_Audit 的一个适当的要求。

A. 3. 3　安全风险报警通知(O. Alarm)

网络交换机应有发现元件、硬件、软件或固件失败或错误的能力。网络交换机应提供安全相关事件和失败或错误提示的告警能力。

O. Alarm 在网络交换机中的实现通过 FPT_AMT. 1：抽象机测试和 FPT_TST. 1：安全功能检测，它要求对安全功能侦错的测试。

A. 3. 4　管理属性(OE. Attr_Mgt)

网络安全管理员应管理控制策略，只赋予经授权的网络管理人员以必需的权利。管理人员应在通过标识与鉴别后承担其特权角色。

OE. Attr_Mgt 的实现通过 FAU_SAR. 1：审计查阅，它使得网络安全管理员有权查阅所有的审计记录；FMT_MSA. 1：安全属性的管理；FMT_MTD. 1：安全功能数据的管理；和 FMT_SMR. 2：安全角色限制，它通过不同的角色限制网络管理系统的某些特权来实现 OE. Attr_Mgt。

A. 3. 5　审计记录查阅(OE. Audit_Review)

所有的审计记录都应定期的被查阅，网络审计管理员应定期的查阅网络流量审计记录。

OE. Audit_Review 的实现通过 FPT_TDC. 1：安全功能间基本安全功能数据的一致性，它确保了审计记录能够被解释；FAU_SAR. 1：审计查阅，它通过要求对审计记录的查阅实现了 OE. Audit_Review。

A. 3. 6　网络配置保密性(O. Cfg_Confidentiality)

网络交换机应保证配置和连接信息不会泄露。

O. Cfg_Confidentiality 的实现通过 FPT_ITC. 1：传送过程中安全功能间的保密性；FTP_TRP. 1：可信路径，它要求一条可以保护控制信息免遭泄漏的可信信道和针对管理信息的可信路径。

A. 3. 7　配置完整性(O. Cfg_Integrity)

网络交换机应保证审计文件、配置、连接信息和属于网络交换机的其他信息的完整性。网络交换机不需负责存储这些信息。

O. Cfg_Integrity 在网络交换机中的实现是通过 FPT_ITI. 1：安全功能间修改的检测；FPT_TST. 1：安全功能检测；FTP_TRP. 1：可信路径；FTP_ITC. 1：安全功能间可信信道，它要求安全功能数据在传输中受到保护免遭修改，对修改行为进行检测和对安全功能数据完整性的验证。

A. 3. 8　管理配置数据(O. Cfg_Manage)

应有获取和保存每个网络交换机的配置和连接信息的计划，该计划必须保证存储的完整性，能进行系统部件的鉴别与系统连接的鉴别。

O. Cfg_Manage 的实现依靠 FTP_TRP. 1：可信路径，为网络交换机的配置和连接信息提供可靠的传输路径。

A. 3. 9　加密机制支持(OE. Cryptography)

为了支持保密性，网络交换机必须支持加密基础设施。该加密基础设施要支持包括客户端注册、密钥管理和信道隔离在内的服务。

OE. Cryptography 的实现依靠 FTP_ITC. 1：安全功能间可信信道和 FTP_TRP. 1：可信路径，它考虑了保护数据免遭泄漏的选项。

A.3.10 控制数据的可信通道(O.Ctrl_Channel)

提供对等网络交换机之间传输控制数据的完整性和保密性;提供独立的可信信道。为了支持保密性,网络交换机必须支持加密基础设施。该加密基础设施要支持包括客户端注册、密钥管理和信道隔离在内的服务。

O.Ctrl_Channel 是通过可信信道的实现来实现的,FTP_ITC.1:安全功能间可信信道;FDP_UIT.1:数据交换完整性,FPT_ITC.1:传送过程中安全功能间的保密性,FPT_ITI.1:安全功能间修改的检测,以保护信息免受泄漏和修改。O.Ctrl_Channel 的实现也依靠 FDP_IFF.1:简单安全属性,它要求为信息流提供一个可信信道。

A.3.11 受控标识和鉴别(O.Ctrl_I&A)

只有在请求连接的目标地址、标识、鉴别和权限与控制策略一致时,才能连接到网络交换机。

O.Ctrl_I&A 在网络交换机中的实现依靠 FDP_ACC.1:子集访问控制,FDP_IFF.1:简单安全属性,FDP_ACF.1:基于安全性属性的访问控制,用于强制执行访问控制机制、认证和鉴权。O.Ctrl_I&A 的实现也依靠于 FTA_TSE.1:网络交换机会话建立,FDP_IFC.1:子集信息流控制,FIA_UAU.2:任何行动前的用户鉴别,FIA_UID.2:任何行动前的用户标识,该安全功能要求组件用于通信会话的确立和验证信息是否来自可信源。

A.3.12 检测非授权连接(O.Detect_Connection)

网络交换机应能检测并告警未经授权的连接。

O.Detect_Connection 在网络交换机中的实现依靠 FPT_ITI.1:安全功能间修改的检测,FPT_RPL.1:重放检测,这些要求扫描端口,旨在发现未经授权的连接。

A.3.13 环境保护(OE.Environment)

应提供对物理环境的保护,例如对抗火灾、地震、掉电等。

OE.Environment 的实现依靠 FPT_FLS.1:带保存安全状态的失败,FPT_RCV.3:无过度损失的自动恢复,FPT_RCV.4:功能恢复,FRU_FLT.1:低容错,通过在自然灾害或电源中断时保障网络交换机的正常操作实现了 OE.Environment。

A.3.14 故障发生时安全状态的保存(O.Fail_Secure)

网络交换机应能保存部件失效或停电事件时的系统安全状态。

O.Fail_Secure 在网络交换机中的实现依靠 FPT_FLS.1:带保存安全状态的失败,FPT_RCV.3:无过度损失的自动恢复,FPT_RCV.4:功能恢复,FRU_FLT.1:低容错,这些保证了网络交换机能够返回安全状态。

A.3.15 指导性文档(OE.Guide_Docs)

应提供安装、配置、操作和程序性指导文档,从而防止安装、配置和操作上的错误。指导文件也要用于网络交换机及其安全功能的维护。

对网络交换机来说 OE.Guide_Docs 是由以下几项来确保的,AGD_ADM.1:管理员指南,AGD_USR.1:用户指南,ALC_DVS.1:安全措施标识。同时,OE.Guide_Docs 也是由以下几项来确保的,ADV_FSP.1:非形式化功能规范,AVA_MSU.1:指南审查,AVA_VLA.1:开发者脆弱性分析,这些要求指导性文档确定各种模式的操作和脆弱性。

A.3.16 生命周期安全(O.Lifecycle)

对网络交换机实行管理和维护,保证其安全功能在其生命周期中被正确的实现和受到保护。对硬件、软件或固件的升级应保证其不影响任何其他的安全功能。

O.Lifecycle 在网络交换机中的实现是依靠 FPT_AMT.1:抽象机测试,FPT_TST.1:安全功能检测,它要求自测以确保对安全功能的正确操作。O.Lifecycle 的实现也依靠 FPT_TDC.1:安全功能间基本安全功能数据的一致性,它要求解释安全功能数据一致性的能力。

A.3.17 管理数据的可信路径(O.Mgmt_Path)

应保证网络交换机和网络管理站之间传输信息的完整性和保密性,应提供独立的可信信道。网络交换机必须支持加密基础设施。该加密基础设施要支持包括客户端注册、密钥管理和信道隔离在内的服务。

O.Mgmt_Path 在网络交换机中的实现是依靠 FTP_TRP.1:可信路径,FPT_ITI.1:安全功能间修改的检测,FDP_ITC.2:有安全属性的用户数据输入,FDP_UIT.1:数据交换完整性,FDP_ETC.2:有安全属性的用户数据输出,它为管理数据在传输过程中提供了完整性和保密性。O.Mgmt_Path 的实现也依靠 FDP_IFF.1:简单安全属性,它为管理信息提供一条可信路径。

A.3.18 安全修复和补丁(O.Patches)

网络交换机应安装最新的补丁和安全修复。

O.Patches 在网络交换机中的实现是依靠 FMT_MOF.1:安全功能行为的管理,它要求网络安全管理员对网络交换机安装补丁和安全修复负责。

A.3.19 可信人员(OE.Personnel)

应雇佣和使用可信赖和有能力的员工。人员应经过基本培训和其后的经常性培训。

对网络交换机来说 OE.Personne 的确保是依靠 AGD_ADM.1:管理员指南,AGD_USR.1:用户指南,它要求对在作为网络管理角色时对网络交换机的安全操作的行为进行描述。OE.Personnel 的实现也依靠 FMT_MOF.1:安全功能行为的管理,FMT_MSA.1:安全属性的管理,FMT_MSA.3:静态属性初始化,所有这些都为网络安全管理者、网络管理者和网络属性管理行为者分配了可信的职责。

A.3.20 物理保护(OE.Physical)

应有物理保护措施以避免恶意攻击、未经授权的修改、破坏和盗窃事件的发生。

OE.Physical 的实现依靠 FPT_PHP.1:物理攻击的被动检测,它要求网络交换机能够识别物理攻击。

A.3.21 提供服务优先级(O.Priority_of_Service)

即使使用尽力传输方式,网络交换机也应对所有的流量分配优先级。控制资源访问方式,防止低级别服务干扰或延迟高级别的服务。

O.Priority_Of_Service 在网络交换机中的实现依靠 FRU_PRS.2:全部服务优先级,它要求对优先级进行分配,FRU_FLT.1:低容错,它确保在错误发生时保存服务的优先级。O.Priority_Of_Service 的实现也依靠 FDP_IFF.1:简单安全属性,它要求优先级只能分配给接收到的来自可信服务的信息。

A.3.22 地址保护(O.Protect_Addresses)

网络交换机应保护已授权组织内部地址的保密性和完整性。在网络交换机收到数据后,应能正确地解析出经过授权的源地址和目的地址。

O.Protect_Addresses 在网络交换机中的实现依靠 FTP_TRP.1:可信路径,FTP_ITC.1:安全功能间可信信道,FDP_ITC.2:有安全属性的用户数据输入,FDP_ETC.2:有安全属性的用户数据输出,FPT_ITC.1:传送过程中安全功能间的保密性,它强制执行网络交换机安全功能,通过防止数据的泄漏、修改、重新获得、丢失来保护地址。

A.3.23 协议(O.Protocols)

在网络交换机中应实现能与其他厂商的网络交换机互操作的标准协议,并在网络交换机中实现可靠交付和错误检测的协议。

O.Protocols 在网络交换机中的实现依靠 FDP_ETC.2:有安全属性的用户数据输出,它要求网络交换机确保完整性,FDP_ITC.2:有安全属性的用户数据输入,用于确保数据的完整性和协议能够清晰的把数据与安全属性联系在一起。O.Protocols 的实现也依靠 FDP_UIT.1:数据交换完整性,FPT_FLS.1:带保存安全状态的失败,FPT_ITI.1:安全功能间修改的检测,FPT_ITI.1:安全功能间修改的检测,用于检测在数据传输过程中的错误和修改。

A.3.24 避免重放攻击(O.Replay_Prevent)

网络交换机应具有防止未经授权的代理伪装成经过授权的代理能力,保护其自身免受重放攻击。

O.Replay_Prevent 在网络交换机中的实现依靠 FDP_ITC.2:有安全属性的用户数据输入,FDP_ETC.2:有安全属性的用户数据输出,FPT_ITI.1:安全功能间修改的检测,FDP_UIT.2:原发端数据交换恢复,FPT_RPL.1:重放检测,它要求对重放的信息进行检测同时强制执行反重放。

A.3.25 网络交换机的自身防护(O.Sel_Pro)

网络交换机必须做好自身防护,以对抗非授权用户对网络交换机安全功能的旁路、抑制或篡改的尝试。

O.Sel_Pro 的实现依靠 FMT_AFL.1 鉴别失败处理,它要求设置在一定次数失败尝试后锁定登录机制,以抵抗旁路或篡改的尝试。

A.3.26 网络同步(OE.Synchronization)

网络交换机应被连接到一个可靠的时间源,以保证正确的网络资源同步。

OE.Synchronization 的实现依靠 FMT_MOF.1:安全功能行为的管理,FPT_STM.1:可靠的时间戳,它要求与时间源建立一个可靠的连接。

A.3.27 网络交换机及其安全功能的测试(O.Test)

网络交换机及其安全功能的测试应严格遵照文档化的测试计划和规程。脆弱性测试应致力于寻找可能违反网络交换机安全性策略的方法。所有的测试方法和结果都应有文档记录。

O.Test 的实现依靠 FPT_TST.1:安全功能检测,FPT_AMT.1:抽象机测试,它通过测试要求确保对网络交换机和安全功能的正确操作。O.Test 也由以下几项确保:ATE_COV.2:范围分析,ATE_FUN.1:功能测试,ATE_IND.2:独立性测试,AVA_SOF.1:网络交换机安全功能强度评估,AVA_VLA.1:开发者脆弱性分析,所有这些都要求对网络交换机的属性、功能或者脆弱性进行分析和测试。

A.3.28 带标识的审计流量记录(O.Traf_Audit)

审计记录应包括日期、时间、发送速度、接受速度、节点标识符和负责传输数据的组织。网络交换机应验证所有的审计记录的完整性,但网络交换机无须负责存储审计记录。

O.Traf_Audit 的实现依靠 FAU_GEN.1:审计数据产生,FPT_TDC.1:安全功能间基本安全功能数据的一致性,FAU_SAR.1:审计查阅,FAU_SEL.1:选择性审计,它要求生成的数据有容易解析的格式和可自定义可审计事件的能力。O.Traf_Audit 的实现也依靠 FAU_GEN.2:用户身份关联,它要求把审计事件与引起该事件的人员相联系的能力和洞察力,FPT_STM.1:可靠的时间戳,它要求捕捉到与审计事件相关联的准确时间,FDP_IFF.1:简单安全属性,它要求对来自于不可信源的接收进行审计的能力。

A.3.29 系统数据备份的完整性和保密性(O.Trust_Backup)

应确保网络交换机的网络文件和配置参数有冗余备份。备份文件应以符合网络安全策略的方式存储,以便保证文件的完整性和保密性,另外,应能由备份文件充分地再生网络交换机的配置,以用于在出现失败事件或安全泄密的情况下恢复网络交换机的功能;网络文件可自动地复制备份到另外的管理站。

O.Trust_Backup 的实现依靠 FDP_UIT.2:原发端数据交换恢复,它要求备份管理数据以确保对网络交换机的连续操作。

A.3.30 可信的恢复(O.Trusted_Recovery)

应确保网络交换机在失效或错误后恢复到没有安全泄密的安全状态,应确保失效部件更替后,系统的状态恢复,并且保证不会引发错误或造成其他安全缺陷。

O.Trusted_Recovery 在网络交换机中的实现依靠 FPT_RCV.3:无过度损失的自动恢复,FPT_RCV.4:功能恢复,它要求在中断操作之后能够恢复到安全状态,FPT_FLS.1:带保存安全状态的失败,此外,该安全目标也可通过在错误发生时对安全状态的保存以达到恢复到安全状态的目的。

A.3.31 未用区域(O.Unused_Fields)

网络交换机应保证协议头内所有未被使用域的数值都被恰当地设定。

O.Unused_Fields 在网络交换机中的实现依靠 FPT_ITI.1:安全功能间修改的检测,要求安全功能可以检测到传输过程中安全功能数据的任何修改。在协议头中的数据应被作为安全功能数据的一部分。

A.3.32 软硬固件验证(O.Validation)

应通过合适的功能和规程,确保所有硬件、软件和固件的完整性,并保证所有硬件、软件和固件都可正确地安装和操作。

O.Validation 在网络交换机中的实现依靠 FPT_AMT.1:抽象机测试,FPT_TST.1:安全功能检测,通过测试有助于验证网络交换机及其各个部分的正确的操作和功能。

A.3.33 管理标识和鉴别(OE.Mgmt_I&A)

管理人员应在通过标识与鉴别后才能承担其特权角色。

OE.Mgmt_I&A 的实现依靠 FIA_UAU.2:任何行动前的用户鉴别和 FID_UID.2:任何行动前的用户标识,它要求任何网络交换机安全功能执行前用户必须首先标识自己的身份并提供正确的鉴别数据。

A.4 依赖关系的基本原理

在选取安全功能要求组件和安全保证要求组件时,必须满足所选组件之间的相互依赖关系,表 A.5 列出了所选安全功能要求组件的依赖关系,表 A.6 列出了所选安全保证要求组件的依赖关系。

表 A.5 安全功能要求组件依赖关系

安全功能要求	依赖关系
FAU_GEN.1	FPT_STM.1
FAU_GEN.2	FAU_GEN.1FIA_UID.1
FAU_SAR.1	FAU_GEN.1
FAU_SEL.1	FAU_GEN.1,FMT_MTD.1
FDP_ACC.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1,FMT_MSA.3
FDP_ETC.2	FDP_ACC.1
FDP_IFC.1	FDP_IFF.1
FDP_IFF.1	FDP_ACC.1 或者 FDP_IFC.1, FMT_MSA.3
FDP_ITC.2	FDP_ACC.1,FTP_ITC.1, FTP_TRP.1,FPT_TDC.1
FDP_UIT.1	FDP_ACC.1 或者 FDP_IFC.1, FTP_ITC.1 或者 FTP_TRP.1, FTP_TRP.1
FDP_UIT.2	FDP_ACC.1,FTP_ITC.1
FIA_UAU.2	FIA_UID.1
FIA_UID.2	—
FIA_AFL.1	FIA_UAU.1

表 A.5(续)

安全功能要求	依赖关系
FMT_MOF.1	FMT_SMR.1
FMT_MSA.1	FDP_ACC.1 或者 FDP_IFC.1， FMT_SMR.1
FMT_MSA.3	FMT_MSA.1， FMT_SMR.1
FMT_MTD.1	FMT_SMR.1
FMT_SMR.2	FIA_UID.1
FPT_AMT.1	—
FPT_FLS.1	—
FPT_ITC.1	—
FPT_ITI.1	—
FPT_PHP.1	FMT_MOF.1
FPT_RCV.3	FPT_TST.1,AGD_ADM.1
FPT_RCV.4	—
FPT_RPL.1	—
FPT_STM.1	—
FPT_TDC.1	—
FPT_TST.1	FPT_AMT.1
FRU_FLT.1	FPT_FLS.1
FRU_PRS.2	—
FTA_TSE.1	—
FTP_ITC.1	—
FTP_TRP.1	—

表 A.6 安全保证要求组件依赖关系

安全保证要求	依赖关系
ACM_CAP.3	ACM_SCP.1,ALC_DVS.2
ACM_SCP.1	ACM_CAP.3
ADO_DEL.1	—
ADO_IGS.1	AGD_ADM.1
ADV_FSP.1	ADV_RCR.1
ADV_HLD.2	ADV_FSP.1,ADV_RCR.1
ADV_RCR.1	—
AGD_ADM.1	ADV_FSP.1
AGD_USR.1	ADV_FSP.1
ALC_DVS.1	—

表 A.6(续)

安全保证要求	依赖关系
ATE_COV.2	ADV_FSP.1,ATE_FUN.1
ATE_DPT.1	ADV_HLD.1,ATE_FUN.1
ATE_FUN.1	—
ATE_IND.3	ADV_FSP.1, AGD_ADM.1, AGD_USR.1, ATE_FUN.1
AVA_MSU.1	ADO_IGS.1, ADV_FSP.1, AGD_ADM.1, AGD_USR.1
AVA_SOF.1	ADV_FSP.1, ADV_HLD.1
AVA_VLA.1	ADV_FSP.1, ADV_HLD.1, AGD_ADM.1, AGD_USR.1

A.5 功能强度基本原理

符合本标准要求的网络交换机具备基本安全功能强度。在对抗 5.2 描述的威胁时,具有基本安全功能强度的网络交换机能够保护潜在的高价值信息。基本安全功能强度能够抵抗的攻击潜力,等同于攻击者具有基本级别的专业技术、资源和动机。这个功能强度与第 6 章中描述的安全目的一致,并且被安全功能要求所支持。

附 录 B
（资料性附录）
安全功能要求的应用注释

B.1 审计数据产生(FAU_GEN.1)

FAU_GEN.1.2 有指派审计从不可信源接受流量事件的能力。拒绝或接受来自不可信源流量的能力应该是一个符合局部安全策略配置的可选择项。

B.2 数据交换完整性(FDP_UIT.1)

就本标准而言，FDP_UIT.1 中的术语——用户数据，可被定义为控制信息或管理信息。

B.3 原发端数据交换恢复(FDP_UIT.2)

本标准陈述了可信 IT 产品要对数据交换恢复有所帮助。这个要求是精炼的，以便适应其他类型的网络交换机。

B.4 任何行动前的用户鉴别(FIA_UAU.2)

对于这一需求，术语“用户”指传输信息的源。如果信息的源来自不可信源，那么网络交换机的配置选择项连同信息流控制策略和使用控制策略将允许或不允许接收信息。

B.5 任何行动前的用户标识(FIA_UID.2)

对于这一需求，术语“用户”指传输信息的源。如果信息的源来自不可信源，那么网络交换机的配置选择项连同信息流控制策略和使用控制策略将允许或不允许接收信息。

B.6 安全功能行为的管理(FMT_MOF.1)

FMT_MOF.1 依赖于 FMT_SMR.1，选择 FMT_SMR.2 是因其叙述了控制网络安全管理员、网络审计管理员和网络配置管理员角色之间关系的规则。

B.7 安全属性的管理(FMT_MSA.1)

FMT_MSA.1 依赖于 FMT_SMR.1，选择 FMT_SMR.2 是因其叙述了控制网络安全管理员、网络审计管理员和网络配置管理员角色之间关系的规则。

B.8 安全功能数据的管理(FMT_MTD.1)

FMT_MTD.1 依赖于 FMT_SMR.1，选择 FMT_SMR.2 是因其叙述控制网络安全管理员、网络审计管理员和网络配置管理员角色之间关系的规则。

B.9 安全角色限制(FMT_SMR.2)

FMT_SMR.2 依赖于 FIA_UID.1，选择 FIA_UID.2 的原因是要求在网络配置管理员或网络安全管理员被标识之前，任何网络交换机的安全功能都不能被执行。

B.10 抽象机测试(FPT_AMT.1)

抽象机指的是任何网络交换机执行的与网络管理功能相关的硬件、固件和/或软件。

B.11 全部服务优先级(FRU_PRS.2)

本标准中,“主体”指的是一个连接的性能特征的集合。性能特征能够按照传输速率、错误比率、延时和其他特征进行测量。

B.12 安全功能间可信信道(FTP_ITC.1)

1) 远程可信IT产品指交换机。
2) 对于客户端,可信信道提供了从交换机到交换机之间功能执行的安全连接。可信信道被用来传输消息的控制信息以及预期的客户端行为,例如:标识和鉴别。可信信道是路由选择信道、信令信道或者远程用户连接(例如:telnet、Rlogin等等),同时也指控制信道。

B.13 可信路径(FTP_TRP.1)

可信路径是一条通信路径,在其上的数据交换可由信道任意一端初始化,并且路径的两端都是可以标识的。可信路径包含了已标识过的网络交换机安全功能的数据和指令的子集。对本标准来说,可信路径就是一条网络管理连接。因此,路径的一端是网络管理站,另一端是被管理的网络交换机。

参 考 文 献

[1] GB/T 18336.1～18336.3—2001《信息技术 安全技术 信息技术安全性评估准则》
[2] GB/T 18018《信息安全技术 路由器安全技术要求》
[3] Protection Profile for Switches and Routers. Draft Version 2.1, February 22, 2001
[4] Telecommunications Switch Protection Profile. Draft Version, NIST
[5] A Goal VPN Protection Profile For Protecting Sensitive Information. July 10, 2000

中华人民共和国
国家标准
信息安全技术
网络交换机安全技术要求
（评估保证级3）
GB/T 21050—2007
*
中国标准出版社出版发行
北京复兴门外三里河北街16号
邮政编码：100045
网址 www.spc.net.cn
电话：68523946 68517548
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230 1/16 印张 3.75 字数 105千字
2008年1月第一版 2008年1月第一次印刷
*
书号：155066·1-30428 定价 38.00 元

GB/T 21050-2007