国 际 电 信 联 盟

ITU-T M.3016.3

国际电信联盟
电信标准化部门

(04/2005)

M系列：电信管理，包括TMN和网络维护

电信管理网

管理平面的安全：安全机制

ITU-T M.3016.3建议书

国际电信联盟

ITU-T M系列建议书

电信管理，包括 TMN 和网络维护

引言与维护和维护组织的一般原则	M.10-M.299
国际传输系统	M.300-M.559
国际电话电路	M.560-M.759
公共信道信令系统	M.760-M.799
国际电报系统和相片传真传输	M.800-M.899
国际租用一次群和超群链路	M.900-M.999
国际租用电路	M.1000-M.1099
移动电信系统和业务	M.1100-M.1199
国际公众电话网	M.1200-M.1299
国际数据传输系统	M.1300-M.1399
标志和信息交换	M.1400-M.1999
国际传送网	M.2000-M.2999
电信管理网	**M.3000-M.3599**
综合业务数字网	M.3600-M.3999
公共信道信令系统	M.4000-M.4999

欲了解更详细信息，请查阅ITU-T建议书目录。

ITU-T M.3016.3建议书

管理平面的安全：安全机制

摘　要

本建议书定义了电信管理网中管理平面的安全机制。本建议书主要关注于网元（NE）和管理系统（MS）的管理平面安全特性，NE 和 MS 属于电信基础设施中的一部分。

来　源

ITU-T 第 4 研究组（2005-2008）按照 ITU-T A.8 建议书规定的程序，于 2005 年 4 月 13 日批准了 ITU-T M.3016.3 建议书。

前　言

国际电信联盟（ITU）是从事电信领域工作的联合国专门机构。ITU-T（国际电信联盟电信标准化部门）是国际电信联盟的常设机构，负责研究技术、操作和资费问题，并且为在世界范围内实现电信标准化，发表有关上述研究项目的建议书。

每四年一届的世界电信标准化全会（WTSA）确定 ITU-T 各研究组的研究课题，再由各研究组制定有关这些课题的建议书。

WTSA 第 1 号决议规定了批准建议书须遵循的程序。

属 ITU-T 研究范围的某些信息技术领域的必要标准，是与国际标准化组织（ISO）和国际电工技术委员会（IEC）合作制定的。

注

本建议书为简要而使用的“主管部门”一词，既指电信主管部门，又指经认可的运营机构。

遵守本建议书的规定是以自愿为基础的，但建议书可能包含某些强制性条款（以确保例如互操作性或适用性等），只有满足所有强制性条款的规定，才能达到遵守建议书的目的。“应该”或“必须”等其他一些强制性用语及其否定形式被用于表达特定要求。使用此类用语不表示要求任何一方遵守本建议书。

知识产权

国际电联提请注意：本建议书的应用或实施可能涉及使用已申报的知识产权。国际电联对无论是其成员还是建议书制定程序之外的其他机构提出的有关已申报的知识产权的证据、有效性或适用性不表示意见。

至本建议书批准之日止，国际电联尚未收到实施本建议书可能需要的受专利保护的知识产权的通知。但需要提醒实施者注意的是，这可能不是最新信息，因此大力提倡他们查询电信标准化局（TSB）的专利数据库。

目 录

引言

电信网是全球通信和经济的重要基础设施。为控制此基础设施的管理功能提供适当的安全是必需的。电信网络管理安全有很多标准存在。然而遵循程度较低，而且在不同的电信设备和软件组件中是不一致的。本建议书确定了安全机制，允许设备提供商、代理及业务提供商能够实现一个安全的电信管理基础设施。尽管目前这些安全机制已经代表了当前对技术状态的理解，但技术在不断发展中，条件也会发生变化，为了更加成功，本建议书必须根据条件的变化而发展。本建议书应作为一个基础，业务提供商可能包括附加的安全机制来满足他们特定的超出本建议书所涉及的需求。

本建议书是 ITU-T M.3016.x 系列建议书的一部分，该系列建议书将为持续发展的网络的管理平面安全提供指南和建议：

TU-T M.3016.0 建议书 — 管理平面的安全：概述。

ITU-T M.3016.1 建议书 — 管理平面的安全：安全需求。

ITU-T M.3016.2 建议书 — 管理平面的安全：安全服务。

ITU-T M.3016.3 建议书 — 管理平面的安全：安全机制。

ITU-T M.3016.4 建议书 — 管理平面的安全：简表文稿。

ITU-T M.3016.3建议书

管理平面的安全：安全机制

1 范围

ITU-T M.3016.1- M.3016.3 建议书为提供适当的管理功能安全定义了一系列安全需求、业务和机制，这些管理功能是支持电信基础设施所必需的。由于不同的行政部门和组织机构对安全有不同级别的要求，ITU-T M.3016 1- M.3016.3 建议书不指定某项安全需求、业务或机制为必选项或可选项。

本建议书确定了电信管理中管理平面的安全机制。本建议书主要关注于网元（NE）和管理系统（MS）的管理平面安全特性，NE 和 MS 属于电信基础设施中的一部分。

本建议书为通用建议书，不是针对电信管理网（TMN）中的某一个特定接口的安全机制。

ITU-T M.3016.4 建议书中定义的文稿用来帮助各组织、行政部门及其他国家/国际机构等指定对需求支持的必选项和可选项，以及取值范围和取值等，以此来实现他们各自的安全策略。

2 参考文献

下列 ITU-T 建议书和其他参考文献的条款，通过在本建议书中的引用而构成本建议书的条款。在出版时，所指出的版本是有效的。所有的建议书和其他参考文献都面临修订，使用本建议书的各方应探讨使用下列建议书和其他参考文献最新版本的可能性。当前有效的 ITU-T 建议书清单定期出版。本建议书中引用某个独立文件，并非确定该文件具备建议书的地位。

— ITU-T Recommendation G.8080/Y.1304 (2001), *Architecture for the Automatically Switched Optical Network (ASON)*, plus Amendment 2 (2005).

— ITU-T Recommendation M.3010 (2000), *Principles for a telecommunications management network*.

— ITU-T Recommendation M.3016.0 (2005), *Security for the management plane: Overview*.

— ITU-T Recommendation M.3016.2 (2005), *Security for the management plane: Security services*.

— ITU-T Recommendation M.3016.3 (2005), *Security for the management plane: Security mechanism*.

— ITU-T Recommendation M.3016.4 (2005), *Security for the management plane: Profile proforma*.

— ITU-T Recommendation X.509 (2000), *Information technology – Open Systems Interconnection: The Directory: Public-key and attribute certificate frameworks,* plus Corrigendum 1 (2001), Corrigendum 2 (2002), and Corrigendum 3 (2004).

— ITU-T Recommendation X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT Applications*, plus Amendment 1 (1996).

— ITU-T Recommendation X.805 (2003), *Security architecture for systems providing end-to-end communications*.

3 定义

本建议书未规定新的术语。

4 缩写

本建议书采用下列缩写：

CORBA	公共对象请求代理体系
DoS	拒绝服务
EMS	网元管理系统
FTP	文件传输协议
HTTP	超文本传输协议
IETF	互联网工程工作小组
IP	互联网协议
IPSec	互联网协议安全
ISO/IEC	国际标准化组织/国际电子技术委员会
ITU-T	国际电信联盟电信标准化部门
MS	管理系统，含任何 EMS、NMS 和 OSS[1]
NE	网元
NE/MS	网元或管理系统
NMS	网络管理系统
NTP	网络时间协议
NTPv3	NTP 第三版
OAM&P	操作、管理、维护和指配
OS	运行系统
OSS	运营支撑系统
RFC	征求意见
SAML	安全声明标记语言
SNMP	简单网络管理协议
SNMPv3	SNMP 第三版
SOAP	简单对象访问协议
SSH	安全外壳
SSL	安全套接层

[1] OSS在电信管理网层次结构中，一般可用来与MS用在相同的上下文中。

TCP 传输控制协议

TLS 传输层安全

TMN 电信管理网

XML 扩展标记语言

5 约定

在 ITU-T M.3016.1，M.3016.2 和 M.3016.3 建议书中，用一个描述符来表示不同的需求、服务和机制。描述符的组成包括下述三个字母，后带一个数字：

— REQ：表示需求；

— SER：表示服务；

— MAC：表示机制。

6 安全机制

本节包含了为操作、管理、维护和指配（OAM&P）以及运营支撑系统（OSS）安全而定义的特定的安全机制，可将 OAM&P 和 OSS 应用于基础设施、服务和应用的管理平面安全。

如下的表 1 复制自 ITU-T M.3016.0 建议书（ITU-T M.3016.0 建议书中的表 4）。该表概述了安全需求和安全服务间的关系，并且作为本系列建议书中其他建议书组织的基础。例如，ITU-T M.3016.1 建议书讨论了安全功能需求，ITU-T M.3016.2 建议书讨论了安全服务，而本建议书（ITU-T M.3016.3 建议书）讨论了适用于安全服务的特定的安全机制。

本节仅定义了标准解决方案所涵盖的安全服务，其他可能的服务（如拒绝服务的检测）将不予考虑。

表1/M.3016.3－安全需求和安全服务间的映射

安全功能需求	安全服务
身份认证	用户鉴权 对等实体鉴权 数据源鉴权
受控访问和授权	访问控制
机密性保护 — 已存储数据	访问控制 机密性
机密性保护 — 传送中数据	机密性
数据完整性保护 — 已存储数据	访问控制
数据完整性保护 — 传送中数据	完整性
责任制	不可否认
活动日志	审计跟踪
安全告警上报	安全告警
安全审计	审计跟踪
DCN 的保护	分组检测

如下的表 2 简要描述了本节的组织：

表2/M.3016.3－本节的组织

节　号	内　　容
6.1	讨论了鉴权安全机制，包括用户鉴权和对等实体鉴权。
6.2	讨论了数据源鉴权。
6.3	讨论了访问控制安全机制。
6.4	讨论了数据机密性安全机制。
6.5	讨论了数据完整性安全机制。
6.6	讨论了审计跟踪安全机制。

6.1　用户鉴权

用户鉴权是验证一个人所声明的身份的行为。用户鉴权可能基于的安全机制包括：

— 用户 ID 和口令（使用适当的复杂口令）的组合，口令可以是一次性的口令（如安全号）。

— 多因素鉴权。

— 独立的签名鉴权。

本节将详细讨论用户鉴权的安全机制。

6.1.1　用户ID和口令鉴权

用户 ID 和静态口令可能会在用户鉴权中使用。用户鉴权证明了合法的系统用户的真实身份，也阻止了非法入侵者的伪装侵袭。通过适当的鉴权，使得跟踪活动，并应用访问控制来限制用户进行未授权操作或扮演未授权角色成为可能，如 6.2 节所述。

用户 ID 和口令鉴权包括为每个用户分配一个独立的用户 ID，然后再分配一个适当复杂的安全口令，该口令与用户 ID 联合使用来证明用户身份。

口令应当包括足够多的字符，并应随机化，确保不被其他人或机器的自动技术猜测出来。复杂口令的字符可能包括如下所述的要求：

机制 1:　可能要求口令包含最小数量的字符长度（如 8 个字符）。

机制 2:　可能要求口令不能包含一些特定的字符。

机制 2a:　可能要求口令不能是用户 ID 的重复，或是用户 ID 的倒序。

机制 2b:　可能要求口令中任何地方都不能包含已成形的字符序列（如字典中的单词或产品名称等）。

机制 3:　可能要求口令不能包含多于指定重复次数的连续的同一字符的重复。

机制 4:　可能要求口令至少包含指定数量的小写和/或大写希腊字符。

机制 5:　可能要求口令至少包含指定数量的数字字符。

机制 6: 可能要求口令至少包含指定数量的特殊字符。

口令的管理对于确保一个安全的鉴权系统来说也是非常重要的。希望得到如下所述的口令系统管理能力：

机制 7: 口令管理系统可能要求输入旧的口令，以阻止其他用户在已登录用户不知情的情况下修改一个已登录用户的口令。

机制 8: 系统可能会进行自动地检测来确保新的登录口令与之前旧的口令不同（因为一般来说，口令是通过一个单向的加密系统来存储的，会要求提供旧的口令来允许系统判断新旧口令的不同程度[2]）。

机制 9: 系统可能会支持一个口令的历史列表来防止口令的重复使用。

机制 10: 系统可能会在一定时间间隔后强制修改口令。

机制 11: 当使用非法口令企图进入系统达到一定次数后，系统可能会在一段时间内（如 60 分钟）限制其尝试其他口令，或者将该用户锁住。被加锁的用户需要与系统安全管理员联系来解除锁定。

6.1.2 多因素鉴权

多因素鉴权指的是这样一种鉴权流程，即在鉴权时需要两个或更多不同类型的信息或因素，来证实被鉴权用户的身份。多因素鉴权的要求提高了鉴权系统的安全性，可以不仅仅依赖于某种单一的因素，因为单一的因素可能更易于被欺骗。

在多因素鉴权中典型采用的鉴权因素包括：

一些用户所**知道**的信息：如，安全口令或通行短语。

一些用户所**具有**的信息：如，令牌、灵通卡、一次性口令发生器。

一些用户**本身**的信息： 如，指纹或其他生物测量值。

一个通用的多因素鉴权机制为双因素鉴权，即要求两个鉴权信任书。一个双因素鉴权的典型示例为银行卡系统，用户必须携带他们拥有的卡，并且还需要检验与卡相关的安全 PIN 码。

机制 12: 具有指定因素数目的多因素鉴权。

6.1.3 个人签名用户鉴权

用户鉴权可能会支持安全的个人签名方法，和 X.509 建议书中定义的认证书公共密钥基础设施。在安全的个人签名中，协议仍然会对信任书实体提出挑战，然而，一个用户可能不必输入信任书，因为信任书已经以某种方式（如 Kerberos）安全隐藏了。使用安全的个人签名技术可以减少用户不得不多次进行系统鉴权的必要性，多次鉴权对用户来说是很不方便的。

机制 13: 个人签名鉴权。

6.2 对等实体和数据源鉴权

使用对等实体鉴权安全机制来验证对等系统所声称的身份。使用数据源鉴权安全机制来确保所接收的数据来源于声称发送了这些消息的系统。对等实体鉴权和数据源鉴权是紧密相关的，并且可能基于如下的安全机制：

---

[2] 作为单向加密系统的例外，对称加密的口令也可能会用做口令，该口令需要解码以便在可靠的系统到系统间通信或独立签名时作内部使用或临时使用。

— 密码鉴权机制。

— 可信任的路径鉴权机制。

本节将详细讨论这些鉴权安全机制。

6.2.1 密码鉴权

密码鉴权机制在系统间（如系统到系统，应用到应用等）进行数据通信时提供鉴权，并且是建立具有完全的数据完整性私密通信的基础。在数据通信过程中，发送实体的密码鉴权允许消息的接收者来鉴别发送者的身份（对等实体鉴权），并且确定消息的源（数据源鉴权）。在一个安全的通信通道中，对等实体和数据源鉴权可能会基于与每个消息相关的密码信息来将发送实体的身份与消息绑定起来。接收者会检查与消息同时提供的密码信息来验证发送实体的真实身份。

可用于对等实体鉴权和数据源鉴权的密码技术包括：公共密钥加密，对称密钥加密，数字签名和数字散列（哈希）技术[3]。密码鉴权可能是单向的，即仅是会话的一端被鉴权；也可能是双向的，即会话的双方均被鉴权。双向鉴权更安全，可以用来帮助阻止积极的侵袭。

机制 14: 基于公共密钥加密的对等实体鉴权和数据源鉴权。

机制 15: 基于对称密钥加密的对等实体鉴权和数据源鉴权。

机制 16: 基于数字签名的对等实体鉴权和数据源鉴权。

机制 17: 基于数字散列技术的对等实体鉴权和数据源鉴权。

机制 18: 双向的加密鉴权。

6.2.2 可信任的路径用户鉴权

可信任的路径鉴权是一种安全机制，该机制可以保证系统到系统的鉴权交互是在一个安全的通信路径上得到保护的。该机制仅可由系统激活，且不能被假冒。一个可信任的路径可以或者是一个专用的物理通道（如：直接连接到系统的终端），或者是一个包括完整性和重放保护的加密路径（如：IPsec 虚拟专用网，安全套接层/传输层安全（SSL/TLS）隧道，或是安全外壳（SSH）等）[4]。关于 IPSec，SSL/TLS 和 SSH 安全协议的讨论见附录 I。

机制 19: 基于可信任的路径的对等实体鉴权和数据源鉴权。

6.3 访问控制

一个 TMN 应当提供能力确保参与者不对信息和资源进行未授权地访问。访问控制安全机制确保仅有授权的用户才被允许访问管理系统的安全资源。

---

[3] 美国国家标准协会T1.243-1995，《操作、管理、维护》。

[4] 摘自国家计算机安全中心，NCSC-TG-004-88，《计算机安全术语集》，1998年10月（网址在 http://csrc.nist.gov/SBC/ PDF/NCSC-TG-004_COMPUSEC_Glossary.pdf）。

访问控制安全机制可能由一个中央系统来提供，并且常常与鉴权系统相结合。例如，一个中央远端接入拨号用户系统（RADIUS）服务器可能会与一个轻权目录访问协议（LDAP）数据库相结合，共同提供一个中央系统进行鉴权和访问控制。

访问控制安全机制可能具有如下特性：

机制 20: 所有的管理活动都要与特定的个人相联系。

机制 21: 访问控制安全机制可能支持“最小权限”思想（即一个人扮演一种角色，将仅具有对该角色所允许的功能进行读取数据、修改数据或执行管理活动等操作的权限）

机制 22: 至少应该有几个管理员账号不因为与口令相关的活动而被锁住，如登录失败或超时等。

机制 23: 可以定义多个管理员角色，每个角色根据关键的安全管理活动的不同而具有不同的权限级别。例如，一个系统可能会定义五种管理员用户角色，另一个系统可能会定义三种管理员用户角色。在这两种情况下，都允许所定义的角色具有对如下安全活动的不同的权限：

机制 23a: 定义和分配用户权限。

机制 23b: 增加和删除用户 ID。

机制 23c: 初始化和重置登录口令。

机制 23d: 初始化和修改加密密钥。

机制 23e: 设置系统的登录口令超时门限。

机制 23f: 为每个用户设置系统的登录失败次数限制个数。

机制 23g: 解除锁定或修改系统的锁定超时值。

机制 23h: 设置系统的去活超时值。

机制 23i: 设置系统安全日志和告警配置。

机制 23j: 管理系统安全日志流程。

机制 23k: 升级安全软件。

机制 23l: 终止任何用户和系统会话。

机制 23m: 定义和分配新用户和用户组的应用层权限。

机制 23n: 维护一个访问应用程序的所有请求的记录。

机制 23o: 在应用级别增加和删除用户。

机制 23p: 监测所有的应用安全日志。

机制 23q: 配置应用安全日志和告警。

机制 23r: 管理应用安全日志流程。

机制 23s: 终止任何用户的应用会话。

6.4 数据机密性

使用数据机密性安全机制来防止对交互数据的非授权接收。本节将讨论提供数据机密性的密码安全机制。

数据机密性基于密码基础。密码系统使用基于标准的和公众可用的特定算法，因此可以允许大范围的审查，并易于实现。密码的“强度”基于所使用的加密算法，以及所使用的密钥长度（即，强度指的是解密工程师寻找或猜测某个特定算法中使用的密钥值所要求的时间长度）。

安全协议（如 IPsec，SSL/TLS，SSH）一般都提供数据源鉴权，数据完整性和数据机密性（见附件 A 对 IPsec，SSL/TLS 和 SSH 安全协议的讨论）。其他协议，如简单网络管理协议第 3 版（SNMPv3）[5]，公共对象请求代理体系（CORBA），边界网关协议和开放的最短路径优先协议等的安全扩展也都设计为可以提供数据源鉴权和数据完整性。

用于产生、存储、分配、销毁和废除数据机密性加密密钥的方法是非常重要的。另外，其他因素，如密钥长度、密钥选择、算法选择等也对一个专用密码系统的安全强度具有直接的影响和作用。

6.4.1 对称的数据机密性

对称的，或安全的密钥加密指的是这样一个加密系统，在此加密系统中加密和解密密钥是相同的。对称的密码系统要求在进行初始分配时对每个用户都共享一个唯一的安全密钥（如加密密钥）。密钥必须通过一个安全的途径提供给每个用户，或由用户内部产生（如根据某个共享的安全根密码），因为知道了加密密钥就意味着知道了解密密钥，反之亦然。

数据机密性安全机制可能会基于对称的加密算法，如数据加密标准（DES），高级加密标准（AES），三倍数据加密算法（3DES），和其他算法等。

DES 是一个已经应用了多年的 56-比特的对称加密算法。由于它具有短的密钥长度，因此在使用大量的并行计算时，DES 由于密钥的枯竭而广受争议，目前 DES 被认为是较弱的算法。美国国家标准和技术协会（NIST）对 DES 给出了较低的评价。

NIST 选择了 AES 来替代 DES 作为美国政府应用的标准对称加密算法。AES 的密钥长度可为 128 比特，192 比特和 256 比特。

3DES 从本质上来说还是 DES 算法，只是使用两个 56-比特密钥或三个 56-比特密钥运行三次。3DES 由联邦信息处理标准（FIPS）定义，见出版物 46-3，《数据加密标准》，1999 年 10 月，附录 2，第 22 页（见网址:http://csirc.nist.gov/publications/fips/fips46-3/fips46-3.pdf）。

3DES 执行时，可以或者使用两个独立的 56-比特密钥，或者使用三个独立的 56-比特密钥，相应的分别可以具有 112 比特和 168 比特的强度。然而 3DES 会受到所谓的“在中间相遇”的攻击，即能够将两个密钥长度的 3DES 强度缩减为 57 个比特，而不是期望的 112 比特。同样的攻击可以将三个密钥长度的 3DES 强度缩减为 112 个比特，而不是期望的 168 比特。这样，若需要较高的安全 3DES，则要使用三个独立的密钥，而最差的强度也需要使用 112 比特。

DES 算法由于使用较短的 56-比特密钥，因此执行起来可能会相对快一些，而 3DES 从本质上来说，必须执行三次 DES，因此会慢很多。AES，具有的最短的密钥长度为 128 比特，其加密强度要强于 3DES，然而在硬件和软件上执行速度都可能非常快。例如，AES 的一个软件实现，与 DES 在同一个平台上运行，其执行速度几乎接近于 DES，但是密码强度要远远强于 DES。

机制 24: 基于 DES 加密算法的对称数据机密性。

[5] SNMPv3也可能提供机密性。

机制 25: 基于 AES 加密算法的对称数据机密性。

机制 26: 基于 3DES 加密算法的对称数据机密性。

6.4.2 不对称数据机密性

不对称加密系统指的是这样一个加密系统，在此加密系统中加密和解密密钥是相关但不同的。其中一个密钥为公共密钥（公钥），而另一个密钥为私密密钥（私钥）。公钥不同于私钥，并且要从公钥中导出私钥在计算上是不可行的。公钥被广泛地发布，而私钥总是保持私密。

数据机密性安全机制可能会基于不对称加密算法，如 Rivest Shamir Adleman（RSA）， 椭圆曲线加密法（ECC）和其他等。

RSA 算法是一种广泛应用的不对称算法，可以应用于加密和数字签名。RSA 基于大素数因子分解的数学难点。RSA 算法的公钥长度为 1024 比特和 2048 比特。注意：具有 2048 比特长度密钥的 RSA 在加密强度上与 128 比特密钥长度的对称加密算法的强度基本相同。

椭圆曲线加密法（ECC）是一种用于公钥加密的新方法（相比较 RSA 算法而言）。使用 ECC 算法，在某个特定的域中定义一个椭圆曲线，然后，可以解决该域的椭圆曲线离散对数问题。与其他公钥算法相比，ECC 算法的主要优势在于它的密钥长度，一个 160-比特长度的 ECC 密钥在安全性上与一个 1024-比特长度的 RSA 密钥的安全性基本相同。一个 210-比特长度的 ECC 密钥在安全性上与一个 2048-比特长度的 RSA 密钥的安全性基本相同。更小的 ECC 密钥长度，意味着更低的计算开销和一个更有效的加密系统[6]。

机制 27: 基于指定密钥长度的 RSA 加密算法的不对称数据机密性。

机制 28: 基于指定密钥长度的 ECC 加密算法的不对称数据机密性。

6.4.3 数据机密性 — 小结

为提供数据机密性，可能会使用到的算法示例以表格方式列于表 3 中。一些议题必须被考虑到，如格式化、填充、错误处理条件、选择合适的素数、公用指数的大小等，以及在 ECC 算法中，基域和曲线也必须被考虑到，然而，这些议题都不在本建议书的范围之内。

表3/M.3016.3－数据机密性加密算法示例

类　　别	算　　法	说　　明
对称加密算法	AES	高级加密标准
	3-DES	三倍数据加密算法
	DES	数据加密标准
不对称加密算法	RSA	Rivest, Shamir, Adleman
	ECC	椭圆曲线加密法

[6] 关于RSA，Diffie-Hellman和ECC算法的更详细信息见《数字签名标准》，2002年11月（网址在http://csrc.nist.gov/cryptval/dss.htm）。

6.5 数据完整性

使用数据完整性安全机制来保证被传送的数据不被修改。

数据完整性基于密码基础。密码系统使用基于标准的和公众可用的特定算法，因此可以允许大范围的审查，并易于实现。安全协议（如 IPsec，SSL/TLS，SSH）除了提供其他安全服务，如数据机密性和数据源鉴权外，一般都提供基于底层加密算法的数据完整性（见附件 A 对 IPsec，SSL/TLS 和 SSH 安全协议的讨论）。

用于产生、存储、分配、销毁和废除数据完整性加密密钥的方法是极为重要的。另外，其他因素，如密钥长度、密钥选择、算法选择等也对一个专用密码系统的安全强度具有直接的影响和作用。

6.5.1 对称数据完整性

对称的，或安全的密钥加密指的是这样一个加密系统，在此加密系统中信息发送方和接收方所使用的用于数据完整性的密钥是相同的。对称的密码系统要求在进行初始分配时对每个用户都共享一个唯一的安全密钥（如验证密钥）。密钥必须通过一个安全的途径提供给每个用户，或由用户内部产生（如根据某个共享的安全根密码）。

对于任意长度消息的对称数据完整性安全机制都可能基于键控的消息摘要算法与哈希函数相结合。键控的消息摘要算法包括：具有消息摘要 5 的散列消息认证代码（HMAC-MD5-96）[7]算法和具有安全散列算法 1 的散列消息认证代码（HMAC-SHA-1-96）[8]。

机制 29: 基于 HMAC-MD5-96 加密算法的对称数据完整性。

机制 30: 基于 HMAC-SHA-1-96 加密算法的对称数据完整性。

6.5.2 不对称数据完整性

不对称数据完整性系统指的是这样一个系统，在此系统中签名和验证所使用的密钥是相关但不同的。其中验证密钥为公共密钥（公钥），而签名密钥为私密密钥（私钥）。签名密钥不同于验证密钥，且从验证密钥中导出签名密钥是不可行的。验证密钥被广泛地发布，而签名密钥总是保持私密。

数据完整性安全机制可能基于不对称的加密算法，如数字签名算法（DSA）和 Rivest Shamir Adleman（RSA）算法。

具备不对称数据完整性安全机制后，发送方可以使用一个签名密钥（私钥）来对一个消息摘要作出标记，同时接收方使用验证密钥（公钥）来验证消息摘要所作的标记是由声明的发送方所做出的。

机制 31: 基于指定密钥长度的 DSA 加密算法的不对称数据完整性。

机制 32: 基于指定密钥长度的 RSA 加密算法的不对称数据完整性。

---

[7] 互联网工程工作小组（IETF）RFC2403，《ESP和AH中HMAC-MD5-96的使用》，C. Madson, R. Glenn，1998年11月。

[8] 互联网工程工作小组（IETF） RFC2404，《ESP和AH中HMAC-SHA-1-96的使用》，C. Madson, R. Glenn，1998年11月。

6.5.3 数据完整性 — 小结

为提供数据完整性，可能会使用到的算法示例以表格方式列于表 4 中。一些议题必须被考虑到，如格式化、填充、错误处理条件、选择合适的素数等，然而，这些议题都不在本建议书的范围之内。

表 4/M.3016.3－数据完整性加密算法示例

类　　别	算　　法	说　　明
不对称消息验证算法	DSA	数字签名算法
对称消息验证算法	HMAC-MD5-96	具有消息摘要 5 的散列消息认证码
	HMAC-SHA-1-96	具有安全散列算法 1 的散列消息认证码

6.6 审计跟踪

网元和管理系统应当提供足够的能力允许进行调查、审计、实时检测、分析和保护等活动，这样才能够实施正确的补救措施。本节考虑了用于安全审计日志的安全机制。关于安全审计日志的内容和格式的更详细信息不在本建议书的定义范围之内。

安全审计日志存储在网元和管理系统中。这些安全日志可能存储于本地，也可能会传送到一个中央日志库和/或日志分析设备。

Syslog 是用于将安全审计日志从本地存储设备传送到中央日志库的一种通用机制。

一般而言，一个设备能够将任何活动存入日志，包括：修改安全属性和服务，修改访问控制，或修改设备的其他配置参数，每次登录企图及其结果，以及每次退出或会话终止等，不论是通过远端执行还是通过控制台执行。将与 OAM&P 消息相关的非安全事件，有时又称为“最新修改”的消息记入日志，对所有可审计的行为来说是必须的。

网元或管理系统将审计日志记录加上顺序标签，并进行密码鉴权（标记）后，可能将审计日志记录发送到一个不能变更的审计服务器中。安全审计日志可能通过一个可信任的路径发送到中央库。为确保对行为的正确分析，大量日志原始资料的日期和时间必须被正确地和安全地同步（如通过 NTPv3）。

机制 33:　基于 Syslog 的安全审计日志。

机制 34:　安全审计日志记录包含如下信息：

机制 34a: 关于活动或已记入日志的实际行为的描述。

机制 34b: 发起活动的用户或进程的身份及安全级别。

机制 34c: 活动发生的日期和时间。

机制 34d: 网络源和目的地信息，若需要时（如登录时）。

机制 34e: 活动执行的成功或失败指示。

机制 34f: 需要审计的任何行为。

机制 35:　发送到一个不能变更的审计服务器中的安全审计日志。

机制 36: 已进行密码签名的安全审计日志。

机制 37: 通过一个可信任的路径发送到中央库的安全审计日志。

6.7 密钥交换

对于对称数据机密性和对称数据完整性应用程序，加密密钥必须在终端系统间安全地交换。这些对称算法的密钥常规应当通过一种与鉴权紧密绑定的过程进行交换，以免入侵者在鉴权过程和密钥分发过程之间得逞。

用于产生、存储、分配、销毁和废除这些加密密钥的方法是极为重要的。另外，其他因素，如密钥长度、密钥选择、算法选择等也对密码系统所提供的安全性具有直接的影响和作用。

有不同的方法能够用于指配和/或交换加密密钥。一个概念上很简单的方法是预共享密钥交换，即密钥被带外发送，且指配给每一个必要的终端系统。例如，密钥能够由授权的网络管理者选择并配置给终端系统。在终端系统数量较少时，可以采用预共享密钥交换，但对于具有大量终端系统的情况而言，这种方法的扩展性不好，因为这种方法在产生和配置大量密钥时会变得很繁琐。

不对称算法，如 Rivest, Shamir, Adleman（RSA）能够用于支持密钥交换服务。使用 RSA，一个终端系统选择对称加密密钥，并且在 RSA 加密算法的保护下将密钥发送到其他终端系统。使用该方法时，不对称算法应当具有适当的密钥长度以保护被发送的对称密钥。例如，为了保护一个 128-比特的对称密钥，RSA 算法应当使用 2048-比特长度密钥或更长密钥，所使用的密钥加密强度应当与 128-比特对称密钥的加密强度大致相当。

Diffie-Hellman 密钥一致算法是用于密钥分发的一种通用方法。使用 Diffie-Hellman 算法，终端可以通过一个公众网络独立地获得安全对称加密密码。在 Diffie-Hellman 过程中，仅有中间结果在终端间发送，且安全密钥决不会被泄漏。如果选择了正确的 Diffie-Hellman 素数个数，对于入侵者而言，要从中间结果中导出安全密钥，在计算上是不可行的。

对于 RSA 算法和 Diffie-Hellman 算法，一些议题也必须被考虑到，如选择合适的素数，选择公共指数，错误处理条件等。

机制 38: 基于预共享密钥的加密密钥交换。

机制 39: 基于指定 RSA 密钥长度的不对称 RSA 算法的加密密钥交换。

机制 40: 基于 Diffie-Hellman 密钥一致算法，且拥有一个特定的 Diffie-Hellman 素数组的加密密钥交换。

6.8 告警上报

在检测到任何安全侵害，或不能够继续记录审计日志时，都应当向管理员发送安全告警。

机制 41: 安全告警上报机制，如 X.736 建议书中所定义。

6.9 分组过滤

为了保护 DCN 不受袭击，且不丢失 DCN 的信息，应当对基于分组连接的设备使用分组过滤功能。

机制 42: 基于如下一个或多个检测条件的分组过滤：

机制 42a: 源 IP 地址。

机制 42b: 目的地 IP 地址。

机制 42c: 协议。

机制 42d: 源端口。

机制 42e: 目的地端口。

并且提供如下一个或多个行为：

机制 42f: 通过。

机制 42g: 停止。

机制 42h: 修改。

机制 42i: 前向。

并且应具备潜在的能力来考虑到之前的决定（即状态相关的）。

附 录 I

IPsec，SSL/TLS和SSH安全机制

I.1 IPsec

IPsec 明确了 IP 层的安全，通过联合使用加密和协议安全机制来提供 IPSec。IPSec 协议在网络层（层 3）和传输层（层 4）间运行，能够用于保护任何类型的数据流（TCP 或 UDP），且独立于应用程序。设计 IPSec 是用来为 IPv4 和 IPv6 提供具有交互能力的、高质量的、基于加密系统的安全机制。IPSec 提供的安全服务集包括：

a) 数据完整性；

b) 基于 IP 地址的数据源鉴权；

c) 机器到机器的鉴权；

d) 抗重放保护；

e) 数据机密性；

f) 加密密钥交换。

为满足这些目标，需要用到两类业务流安全服务：认证头（AH）和封装的安全负载（ESP），同时，还需要用到加密密钥管理程序和协议。认证头（AH）服务为 IP 分组提供了数据源鉴权、机器到机器的鉴权和数据完整性。封装安全负载（ESP）服务除为 IP 分组提供数据源鉴权，机器到机器的鉴权和数据完整性外，还提供了数据机密性服务。IPsec 机制的设计独立于加密算法，这种设计可以允许选择不同的算法集，而不会影响到其他方面的实现。

密钥管理由互联网密钥交换（IKE）协议来提供。终端之间密钥的协商可以手工进行，也可以自动进行。自动的密钥协商可以基于预共享的密钥（如口令）或是 X.509 建议书中定义的信任书。

参见[RFC 2401], [RFC 2402], [RFC 2403], [RFC 2404], [RFC 2405], [RFC 2406], [RFC 2407], [RFC 2408], [RFC 2409], [RFC 2410], [RFC 2411], [RFC 2412], [RFC 3602], [RFC 2451], [FIPS-197]。

I.2 SSL/TLS

安全套接层（SSL）安全协议为传输层（层 4）的 TCP/IP 连接提供数据加密、服务器鉴权、消息完整性和可选的客户鉴权服务。SSL 当前版本为 3.0。传输层安全（TLS）是 SSL 的 IETF 标准版本，其超越 SSL 的安全增强点包括：

- 要求支持 Diffie-Hellman 和 DSA 数字签名算法（DSA），可选支持 RSA。
- 使用增强的散列消息鉴权算法（HMAC）来替代一个非标准的，SSL 定义的 MAC 算法。
- 修改了密钥生成算法，该算法使用 MD5（消息摘要 5）和带有 HMAC 的 SHA-1（安全哈希算法 1）。

SSL/TLS 协议运行在网络层之上（层 4），并且仅能与传输控制协议（TCP）共同工作，而不能与用户数据报协议（UDP）共同工作。一般运行在 SSL/TLS 之上的应用层协议包括，但不限于：超文本传输协议（HTTP），简便目录访问协议（LDAP），以及互联网消息访问协议。更高层的应用层协议也可以运行在 SSL/TLS 之上，但不需关心 SSL/TLS 的任何细节，然而，应用层必须通过使用 I/O 回调函数与 SSL/TLS 相连接起来。

SSL/TLS 协议为 TCP 业务流提供了三个安全功能：数据机密性、数据完整性和鉴权。

SSL/TLS 安全协议体系结构提供了两个可以运行在 TCP 之上的层：

- SSL/TLS 上层协议；
- SSL/TLS 记录协议。

SSL/TLS 上层协议包括：SSL/TLS 握手协议，SSL/TLS 密码交换协议和 SSL/TLS 警报协议。SSL/TLS 会话由 SSL/TLS 握手协议最初发起，提供如下功能：

a) 鉴权和安全机制的协商。

b) 客户端和服务器端的鉴权（使用服务器或客户的公钥/私钥）。

c) 建立安全密钥。

一旦 SSL/TLS 会话被建立，即可使用 SSL/TLS 记录协议来提供批量数据传输服务。SSL/TLS 记录协议提供如下功能：

a) 基于服务器密钥的数据源鉴权。

b) 数据完整性。

c) 机密性。

注意：目前 SSL 的版本为版本 3（SSLv3），TLS 的版本为版本 1。不建议使用更早的 SSL 和 TLS 版本。

SSL/TLS 允许使用单向鉴权或双向鉴权，在单向鉴权中，仅有服务器端对客户端进行鉴权；而双向鉴权中，客户端和服务器端相互进行鉴权。单向鉴权是在公众互联网中常用的方法。对于网络管理应用程序，建议使用双向鉴权，让通信双方都知道正在与他们通信的对方，正是想与之通信的终端。

参见 [RFC 2246]，[RFC 3546]，[SSL V3]。

I.3 SSH

SSH 是应用层（层 7）安全协议，一般用来直接替代不安全的协议如 Telnet 和文件传输协议（FTP）等。Telnet 和 FTP 是不安全的协议，因为它们显式地传送口令及其他所有的数据。SSH 也可通过使用端口前向方式来保护其他协议，因此 SSH 可作为通用的网络安全协议来使用。

SSH 有两个版本：SSHv1 和 SSHv2。SSHv1 发布于 1998 年，现在认为它是不安全的，并且已经被废除了。

安全外壳第 2 版（SSHv2）的特性有：

- 完整地替代 Telnet，Rlogin，Rsh，Rcp 和 FTP 协议，以提供安全的文件传输和文件拷贝。
- 对用户进行自动鉴权（口令不以明文传递）。
- 双向鉴权（服务器端和客户端均被鉴权）。
- 通过使用端口前向技术对随机的基于 TCP/IP 的应用程序进行隧道化。
- 对数据进行加密以提供数据机密性。
- 多种鉴权选择，包括口令、公钥和安全 ID 鉴权。
- 多个密码组可用。

SSHv2 体系结构包括三个主要的组件：

- 传输层协议[SSH-TRANS]提供服务器鉴权，数据机密性和数据完整性。该部分还可能可选地提供压缩功能。
- 用户鉴权协议[SSH-USERAUTH]为服务器对客户端的用户进行鉴权。
- 连接协议[SSH-CONNECT]将加密隧道复用到多个逻辑通道中。

连接协议提供的通道可以用于更广泛的目的。可为建立安全的交互式 Shell 会话提供标准的方法，也可为前向（隧道化）随机的 TCP/IP 端口和连接等提供标准的方法。

端口号 22 已经在 IANA 中注册为 SSHv2 应用程序使用的标准端口。

参见[SSH-ARCH]，[SSH-TRANS]，[SSH-USERAUTH]，[SSH-CONNECT]。

附 录 II

本附录描述了分组过滤的机制，分组过滤是用来加强数据通信网（DCN）的安全性。数据通信网（DCN）是连接管理应用程序（常位于网络操作中心）和网元之间的网络，可以提供集中的指配、告警监视、测试、计费、以及其他网络管理活动。RFC 3871 中的 2.8–2.10 小节提供了一个需求集，来对大型的互联网服务提供商的 IP 网络基础设施进行分组过滤。本文稿引用 RFC 3871 来定义对 DCN 的过滤。

分组过滤是一个过程，该过程基于某种确定的匹配条件[9]，来决定对每个通过网元的分组进行部署。可以有几种部署方式，如：通过、停止、前向（直接发向其他地方）等。分组过滤通过决定将什么样的业务流通过网元或管理系统来提供基本的保护机制。

主要考虑的是对从其他网络（如承载着客户业务流的网络，对等的管理网络系统等）进入到 DCN 的流量进行过滤。另外，DCN 的某些特定网元需要与其他网元隔离开来，因此，过滤也可应用于 DCN 的不同子网（或域）之间。

II.1 目标

分组过滤机制的主要目标在于：

1) 从客户业务流方面保护 DCN 基础设施。这种保护应当包括适当共享公共资源以避免服务质量的下降或服务拒绝。

2) 从对等网络方面保护 DCN 基础设施。

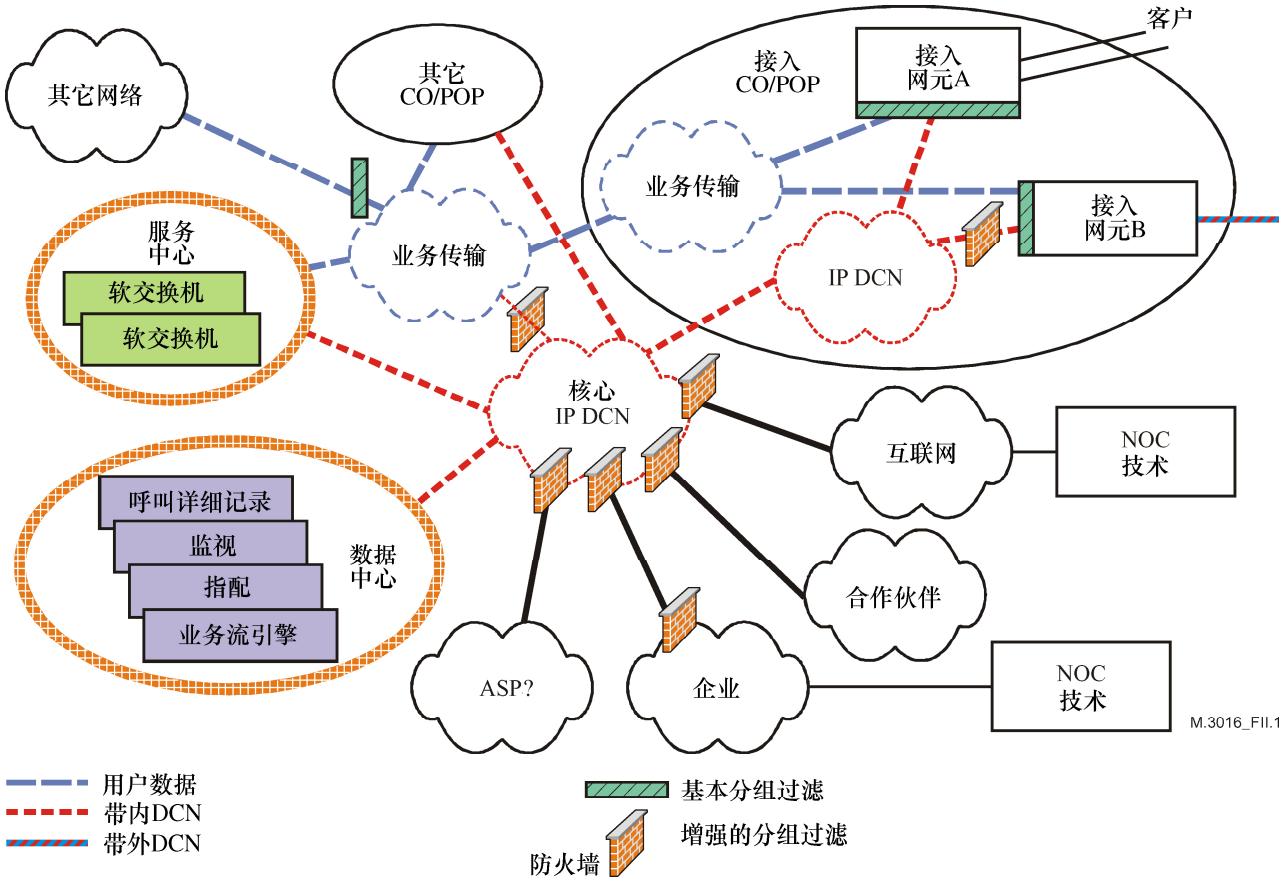
3) 预防 DCN 中与所应用的安全策略不一致的业务流量通过 DCN 基础设施传播到更多的地方。

II.2 影响分组过滤的网络设计考虑事宜

本附录并不暗示 DCN 设计的需求，然而，DCN 的设计和部署会影响到网络中分组过滤的部署和需求。图 II.1 显示了一个典型的 DCN 设计。

---

[9] 分组过滤的描述与分组路由很相似；然而，本附录关注的是分组过滤，而不是分组路由。



图II.1/M.3016.3－通用的DCN示例

有三种类型的 DCN 设计得到了普遍的认可：

- 带内管理：DCN 使用承载客户数据的业务网络所保留的带宽。例如，以太网链路上的一个 VLAN 可被用来承载管理业务流，或者一个 IPSec 或 SSH 连接可被用于互联网连接之上（如图 II.1 中，NOC 技术在互联网之上被连接）。
- 带外管理：DCN 是一个与承载客户业务流的业务网络完全不同的网络。该网络可覆盖在承载客户数据流的物理网络之上。
- 混合方式：结合带内管理和带外管理两种方式。

对这三种管理体系结构的比较和通用讨论已经超出了本建议书的范围（见 RFC 3871 的第 2.2 节）；然而，使用其中的哪一种将影响到对过滤的需求。

用于创建 DCN 的基本原理会根据所支持的网元种类、操作程序、以及参数选择、网络拓扑、经济等各方面的不同而有所变化，网络能力、恢复性，以及安全性等都是在设计每种类型的 DCN 时需要考虑的问题。

下一代被管理的业务供应将使用基于分组（如帧中继，ATM，IP，MPLS，以太网等）的传输设备来实现。这些业务的出现将使得对接入设备（CPE）的管理成为必须。

在必要时，可能会使用如下一种混合模型：在临界点（POP）使用带外管理，而在 POP 到 CPE 接入设备间使用带内管理，因为要在所有到 CPE 接入设备的通路上都使用带外管理在经济上可能是不可行的。图 II.1 中的“接入网元 B”显示了后一种情况。在这种情况下，增强的过滤（如防火墙）能够用来保护 DCN 不受 CPE 的侵袭。带内连接的另一个例子是对一个远端的，孤立的 POP 的管理，这种情况下，建立一个分离的网络是不可行的，应将业务网作为 DCN 的一个备份。

使用分组过滤也意味着 DCN 使用的地址空间与分配给客户的地址空间是分离的，且在这两个域间没有进行业务流交换的需求。地址空间的分离简化了分组过滤器的开发，分组过滤器可用来阻塞客户到管理资源的业务流。最简单的方法是将源于 DCN 之外的所有流向 DCN 的业务流量全部阻塞，这样来保护管理基础设施不受客户业务流的侵袭。然而，在某些情况下，业务流是必须在网外和 DCN 之间交换的，如两个服务提供商之间管理信息的交换（如两个 SP 之间位于中间点的 DCC）。

因此，必须实施指配以允许一些受限的业务流在不同的域间流动，且需要更多的控制（如增强的分组过滤）来提供足够的 DCN 安全。

图 II.1 显示了基于上述假设的 DCN 的设计。业务传输（图中蓝线）承载着客户的业务流。DCN（图中红线）承载着管理业务流。服务中心中包括向客户提供服务的服务器，以及客户所要访问的服务器（如软交换机）等。数据中心中包括用来对网络进行管理和监视的服务器和其他运行系统，客户不会直接访问这些服务器。从 DCN 到网元的连接可以使用 IP、X.25、异步或 ISO CLNS 等。

在 DCN 和业务网络的边界提供输入分组过滤是在‘接入网元’中提供 DCN 安全的基本需求。然而，这样的分组过滤可能还不够，因为侵袭可能来自 DCN 内部的一个网元或主机。因此，适当的分组过滤机制需要在 DCN 的多个点上进行战略实现，以确保与所应用的安全策略相一致。另外，当 DCN 连接到外部网络（如互联网，SP 的企业网，合作伙伴的网络等）时，可能需要实现增强的分组过滤。

由于分组过滤是整个网络安全策略的一个组成部分，因此它的使用必须在整个网络安全原则和策略的上下文中，网络安全原则和策略包括如区域划分和防御深度等。由于一个好的安全策略包括对主机自身（如软交换机）的安全需求，以及网络的区域划分等，这些都不在本建议书的范围之内。

为了保护管理基础设施，以及一般意义上的 DCN，对于网络操作员来说，将从 DCN 边界外（如从对等实体或从客户端）接收到的一些分组丢弃掉的措施是有用的。例如，具有无效源 IP 地址的分组，以及要发向 DCN 内部专用 IP 地址的分组等都不应当被允许进入 DCN 的边界。该功能被称之为输入过滤。该需求引自 [RFC 3871] 和[RFC 2827]。

有两种类型的分组过滤：

- 基于分组头信息的基本分组过滤，通过分组头信息，能够检测到伪装源地址的分组，并将其阻塞。
- 增强的分组过滤，包括：
  - — 分组状态检查，这种情况下，在作过滤决定时，会使用到上下文和状态信息。
  - — 对特定协议的动态过滤，在这种情况下，会根据协议负载所承载的信息而动态地打开过滤器。
  - — 深度分组检测，在这种情况下，具有任何异常的，不平常的、或可疑内容的应用层协议都会被检测。

II.3 基本分组过滤

连接到 DCN 的设备应当具备选项来停止从远端接口（如客户端或对等实体）接收来的包含非法源 IP 地址的分组。非法源 IP 地址可由以下部分组成：

- Bogon 地址（见 RFC 3871 的第 1.8 节）。
- Martians（见 RFC 3871 的第 1.8 节）。
- 未分配给客户的 IP 地址（或是对对等实体发送而言是非法的 IP 地址）。

分组过滤机制应当能够基于‘机制 42’所定义的属性，将从外部（如从客户端）发来的，且发向分配给 DCN 的地址组的业务流进行过滤。

分组过滤机制应当提供精确的基于每个接口的业务流统计。统计的粒度级别可以根据分组过滤机制的不同而变化。

设备应当能够过滤从 DCN 外部（如从客户端）发来的业务流，也就是说，能够基于‘机制 42’所定义的属性，通过任何一个接口，可能包括环回接口，将业务流直接发向网元。

分组过滤机制可能支持 TMN 模型中的多安全域观点，在这个模型中，一个安全域内的所有网元都必须受到一个公共安全策略的控制。

设备可能会具备能力根据业务流、异常、以及操作条件等产生适当的告警信息。

II.4 增强的分组过滤

当用户和管理业务流间存在着高度的交叉时，即用户和管理业务流在网络边界并没有很好地隔离，且 DCN 直接连接到其他网络时，应当考虑这些建议。另外，在被保护的子网边界（如 DCN 和数据中心之间）也应当使用这些过滤能力。

该机制应当检测 DCN 中所使用的应用协议，检测到任何异常的协议或反常的行为，都应当适当地阻塞这些业务流。

该机制应当检查 DCN 中业务流的内容，无论何时，都应当检测恶意的内容，如病毒、蠕虫、特洛伊等。

该机制应当提供保护以对抗拒绝服务（DoS）的攻击。

该机制应当能够进行状态相关的过滤，即在进行分组过滤时使用会话信息。一个会话的返回业务流应当总是被允许通过。

该机制应当对网络中所有承载端口信息的协议支持动态针孔能力，这些协议包括如 FTP，SIP 等。分组过滤机制应当检查负载中的端口信息，并且在会话的生命周期中打开该指定端口（动态针孔）的通信。一旦当会话突然终止时，应当存在一个适当的超时机制来关闭端口。

该机制应当支持协议的强制执行，包括停止错误的分组，或停止不正确的会话建立等。

其他所建议的过滤能力可参见 RFC 3871 中的 2.7-2.10 节。

参考资料

[RFC 2827] IETF RFC 2827 (2000), *Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing.*

[RFC 2401] IETF RFC 2401 (1998), *Security Architecture for the Internet Protocol*, http://www.ietf.org/rfc/rfc2401.txt?number=2401

[RFC 3704] IETF RFC 3704 (2004), *Ingress Filtering for Multihomed Networks.*

[RFC 3871] IETF RFC 3871 (2004), *Operational Security Requirements for Large Internet Service Provider (ISP) IP Network Infrastructure.*

[NDS/IP] 3GPP TS 33.210 (2001), *3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Network Domain Security; IP network layer security.*

[RFC 2402] IETF RFC 2402 (1998), *IP Authentication Header,* http://www.ietf.org/rfc/rfc2402.txt?number=2402

[RFC 2403] IETF RFC 2403 (1998), *The Use of HMAC-MD5-96 within ESP and AH,* http://www.ietf.org/rfc/rfc2403.txt?number=2403

[RFC 2404] IETF RFC 2404 (1998), *The Use of HMAC-SHA-1-96 within ESP and AH,* http://www.ietf.org/rfc/rfc2404.txt?number=2404

[RFC 2405] IETF RFC 2405 (1998), *The ESP DES-CBC Cipher Algorithm with Explicit IV,* http://www.ietf.org/rfc/rfc2405.txt?number=2405

[RFC 2406] IETF RFC 2406 (1998), *IP Encapsulating Security Payload (ESP),* http://www.ietf.org/rfc/rfc2406.txt?number=2406

[RFC 2407] IETF RFC 2407 (1998), *The Internet IP Security Domain of Interpretation for ISAKMP,* http://www.ietf.org/rfc/rfc2407.txt?number=2407

[RFC 2408] IETF RFC 2408 (1998), *Internet Security Association and Key Management Protocol (ISAKMP),* http://www.ietf.org/rfc/rfc2408.txt?number=2408

[RFC 2409] IETF RFC 2409 (1998), *The Internet Key Exchange (IKE),* http://www.ietf.org/rfc/rfc2409.txt?number=2409

[RFC 2410] IETF RFC 2410 (1998), *The NULL Encryption Algorithm and Its Use with IPsec,* http://www.ietf.org/rfc/rfc2410.txt?number=2410

[RFC 2411] IETF RFC 2411 (1998), *IP Security Document Roadmap,* http://www.ietf.org/rfc/rfc2411.txt?number=2411

[RFC 2412] IETF RFC 2412 (1998), *The OAKLEY Key Determination Protocol,* http://www.ietf.org/rfc/rfc2412.txt?number=2412

[RFC 3602] IETF RFC 3602 (2003), *The AES-CBC Cipher Algorithm and Its Use with IPsec*, http://www.ietf.org/internet-drafts/draft-ietf-ipsec-ciph-aes-cbc-04.txt

[RFC 2451] IETF RFC 2451 (1998), *The ESP CBC-Mode Cipher Algorithms,* http://www.ietf.org/rfc/rfc2451.txt

[RFC 2246] IETF RFC 2246 (1999), *The TLS Protocol, Version 1.0,* ftp://ftp.rfc-editor.org/in-notes/rfc2246.txt

[RFC 3546] IETF RFC 3546 (2003), *Transport Layer Security (TLS) Extensions,* ftp://ftp.rfc-editor.org/in-notes/rfc3546.txt

[SSL V3] *Secure Socket Layer Version 3.0 Specification, Netscape Communications.* http://wp.netscape.com/eng/ssl3/

[SSH-ARCH] YLONEN (T.): *SSH Protocol Architecture,* I-D draft-ietf-architecture-15.txt, October 2003. http://www.ietf.org/internet-drafts/draft-ietf-secsh-architecture-15.txt

[SSH-TRANS] YLONEN (T.): *SSH Transport Layer Protocol,* I-D draft-ietf-transport-17.txt, October 2003. http://www.ietf.org/internet-drafts/draft-ietf-secsh-transport-17.txt

[SSH-USERAUTH] YLONEN (T.): *SSH Authentication Protocol,* I-D draft-ietf-userauth-18.txt, September 2002. http://www.ietf.org/internet-drafts/draft-ietf-secsh-userauth-18.txt

[SSH-CONNECT] YLONEN (T.): *SSH Connection Protocol,* I-D draft-ietf-connect-18.txt, October 2003. http://www.ietf.org/internet-drafts/draft-ietf-secsh-connect-18.txt

[FIPS-46-3] Data Encryption Standard. (Describes both DES and 3DES). http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf

[FIPS-197] Advanced Encryption Standard (AES), FIPS Publication 197, National Institute of Standards and Technology, November 2001. http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[RFC 2437] IETF RFC 2437 (1998), *PKCS #1: RSA Cryptography Specifications Version 2.0,* http://www.ietf.org/rfc/rfc2437.txt?number=2437

ITU-T 系列建议书

A系列	ITU-T工作的组织
D系列	一般资费原则
E系列	综合网络运行、电话业务、业务运行和人为因素
F系列	非话电信业务
G系列	传输系统和媒质、数字系统和网络
H系列	视听和多媒体系统
I系列	综合业务数字网
J系列	有线网和电视、声音节目及其他多媒体信号的传输
K系列	干扰的防护
L系列	线缆的构成、安装和保护及外部设备的其他组件
M系列	**电信管理，包括TMN和网络维护**
N系列	维护：国际声音节目和电视传输电路
O系列	测量设备技术规程
P系列	电话传输质量、电话装置、本地线路网络
Q系列	交换和信令
R系列	电报传输
S系列	电报业务终端设备
T系列	远程信息处理业务的终端设备
U系列	电报交换
V系列	电话网上的数据通信
X系列	数据网和开放系统通信及安全
Y系列	全球信息基础设施、互联网的协议问题和下一代网络
Z系列	用于电信系统的语言和一般软件问题

瑞士印刷
2005年，日内瓦