国 际 电 信 联 盟

ITU-T X.1542

(09/2016)

国际电信联盟
电信标准化部门

X系列：数据网、开放系统通信和安全性

网络安全信息交换 – 事件/事故/探索法交换

会话信息消息的交换格式

ITU-T X.1542 建议书

国际电信联盟

ITU-T X 系列建议书

数据网、开放系统通信和安全性

公用数据网	X.1–X.199
开放系统互连	X.200–X.299
网间互通	X.300–X.399
报文处理系统	X.400–X.499
号码簿	X.500–X.599
OSI组网和系统概貌	X.600–X.699
OSI管理	X.700–X.799
安全	X.800–X.849
OSI应用	X.850–X.899
开放分布式处理	X.900–X.999
信息和网络安全	
一般安全问题	X.1000–X.1029
网络安全	X.1030–X.1049
安全管理	X.1050–X.1069
生物测定	X.1080–X.1099
安全应用和服务	
组播安全	X.1100–X.1109
家庭网络安全	X.1110–X.1119
移动安全	X.1120–X.1139
网页安全	X.1140–X.1149
安全协议	X.1150–X.1159
对等网络安全	X.1160–X.1169
网络身份安全	X.1170–X.1179
PITV安全	X.1180–X.1199
网络空间安全	
计算网络安全	X.1200–X.1229
反垃圾信息	X.1230–X.1249
身份管理	X.1250–X.1279
安全应用和服务	
应急通信	X.1300–X.1309
泛在传感器网络安全	X.1310–X.1339
PKI相关建议书	X.1340–X.1349
网络安全信息交换	
网络安全综述	X.1500–X.1519
脆弱性/状态信息交换	X.1520–X.1539
事件/事故/探索法信息交换	**X.1540–X.1549**
政策的交换	X.1550–X.1559
探索法和信息要求	X.1560–X.1569
标示和发现	X.1570–X.1579
确保交换	X.1580–X.1589
云计算安全	
云计算安全综述	X.1600–X.1601
云计算安全设计	X.1602–X.1639
云计算安全最佳实践和指导原则	X.1640–X.1659
云计算安全实现	X.1660–X.1679
其他云计算安全	X.1680–X.1699

欲了解更详细信息，请查阅ITU-T建议书目录。

ITU-T X.1542 建议书

会话信息的消息交换格式

摘要

在当今环境下，计算机网络可能同时会受到来自组织内部和组织外部的威胁。防火墙系统负责记录选定的入向和出向传输控制协议/网际协议（TCP/IP）连接的会话信息。

但是，目前提供的这些系统通常无法实现互操作，原因是，各个系统均有其自身独特的功能、控制机制和会话日志格式。

大多数安全管理员现今面临的需求是，需要在不同的防火墙系统甚至是不同的基础设施之间保持一致的会话信息交换格式。

ITU-T X.1542建议书阐述了会话信息的消息交换格式（SIMEF）的信息模型，并提供了使用可扩展标记语言（XML）方案描述的相关数据模型。SIMEF为分享有关集中式网络安全管理和安全信息交换系统的传输层会话日志信息，定义了一种数据模型表达方法。任何传输协议的规范均不属于本建议书的讨论范围。

历史沿革

版本	建议书	批准日期	研究组	唯一识别码*
1.0	ITU-T X.1542	2016-09-07	17	11.1002/1000/12852

关键词

数据模型、消息交换、网络安全、会话。

---

* 访问建议书，请在您的Web浏览器地址栏中输入网址http://handle.itu.int/，其次建议书的识别码，例如http://handle.itu.int/11.1002/1000/11830-en。

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）在电信，信息和通讯技术领域是国际电信联盟的常设机构。国际电信联盟电信标准化部门负责研究技术，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。

世界电信标准化大会（WTSA），每四年举行一次，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第一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

本建议书为简明扼要起见而使用的“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和适应性等），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”等其它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

国际电联提醒注意：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它机构提出的有关已申报的知识产权的证据、有效性或适应性不表示意见。

至本建议书截止之日起，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，这可能并非最新消息，因此特大力提倡他们通过下列网址查询电信标准化局（TSB）的专利数据库：http://www.itu.int/ITU-T/ipr/。

目录

ITU-T X.1542 建议书

会话信息的消息交换格式

1 范围

本建议书阐述会话信息的消息交换格式（SIMEF），是用于表达安全系统（如防火墙）输出之会话信息的一种数据模型，并对使用该模型的基本原理做了解释。提供了一个在可扩展标记语言（XML）中的数据模型的实施方案，提出了一个XML文档类型定义（DTD），并给出了例子。

2 参考文献

无。

3 定义

3.1 其它地方定义的术语

无。

3.2 本建议书定义的术语

本建议书定义以下术语：

3.2.1 分析仪：一个分析仪指的是一个网络安全系统，它通过分析入向和出向的会话信息来检测攻击。它还生成会话日志并将之发送给安全管理系统。

3.2.2 会话信息：会话信息包含传输控制协议/用户数据报告协议（TCP/UDP）会话、应用服务以及作为会话信息提供者的会话实体。会话被定义为作为翻译单元进行管理的流量集。TCP/UDP会话由唯一的（源IP地址、源TCP/UDP端口、目标IP地址、目标TCP/UDP端口）元组确定。

注 – 此定义是基于[b-IETF RFC 2663]。

4 缩略语和首字母缩略词

本建议书使用以下缩略语和首字母缩略词：

BSD 伯克利软件套件

CGI 公共网关接口

DTD 文档类型定义

FTP 文件传输协议

HTTP 超文本传输协议

IIP 互联网协议

LAN 局域网

NAT 网络地址转换

NTP 网络时间协议

POSIX	可移植的操作系统接口
SIMEF	会话信息消息的交换格式
SNA	共享的网络架构
SNMP	简单网络管理协议
TCP	传输控制协议
UDP	数据报协议
UML	统一建模语言
URL	统一资源定位符
UTF	通用字符集转换格式
VPN	虚拟专用网
XML	可扩展标记语言

5 惯例

UNIX ®是Open Group的一个注册商标。

POSIX ®是IEEE的一个注册商标。

6 概述

在当今的网络环境下，计算机网络可能同时会受到来自组织内部和组织外部的威胁。因此，绝大多数网络安全研究工作致力于开发综合网络安全管理系统和网络监控工具，以使某机构能够抓取通过网络设备的TCP/IP包，并将抓取的数据看作是客户端与服务器之间的会话序列。例如，防火墙系统负责记录选定的入向和出向TCP/IP连接的会话信息。

SIMEF的概念如图1所示。会话信息可收集自防火墙系统、网络地址转换（NAT）设备等。SIMEF规定了数据模型，它涵盖客户端/服务器的网络连接、最终用户的设备以及应用服务。SIMEF 定义了一个数据模型和相关的消息类，以与安全管理系统和信息共享系统共享感兴趣的传输层会话信息。它可以应用于入侵信息交换系统。

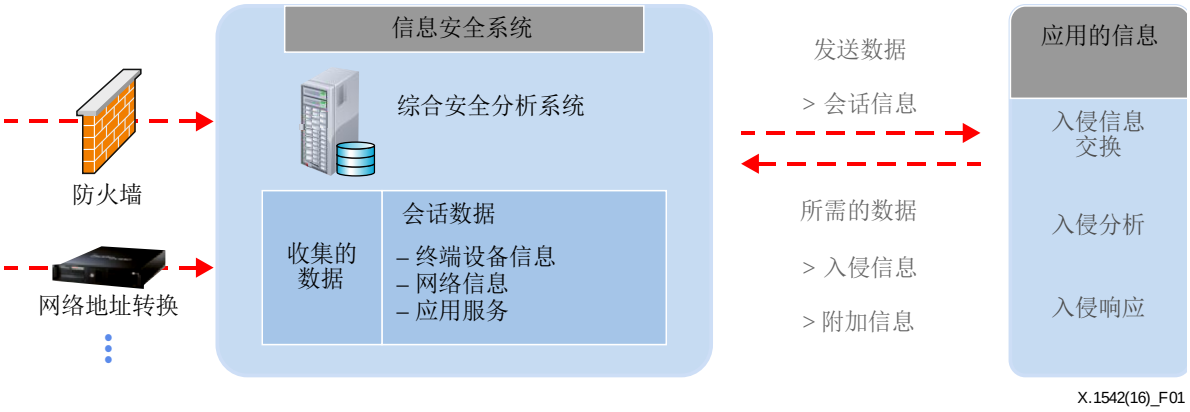


图1 – SIMEF概念

7 表达方法和定义

本建议书使用三种记法：用统一建模语言（UML）来描述数据模型；用XML来描述SIMEF文档中所用的标记；用SIMEF标记来描述文档本身。

7.1 SIMEF文件

本条款描述SIMEF XML文档格式化规则。绝大多数这些规则“继承”自用于格式化XML文档的规则。在7.1.1至7.1.2条款中对一个SIMEF XML文档序言的格式进行了描述。

7.1.1 XML声明

正在SIMEF兼容应用之间交换的SIMEF文档应以一个XML声明开始，并应指定所用的XML版本。建议对所用的编码做出说明。

一个SIMEF消息因此而应开始于：

```
<?xml version="1.0" encoding="UTF-8"?>
<simef: SIMEF-Message version="1.2" xmlns:simef="http://iana.org/simef"/>
```

SIMEF兼容的应用可选择在内部省略XML声明，以节省空间，只有当消息发送给另一个目的地时（例如，一个Web浏览器），才添加之。不建议采取这种做法，除非在不遗失每个消息之版本和编码信息的情况下能实现之。

因此，实施者可决定使分析仪和管理器在带外就其将用于交换消息的特定文档类型定义（DTD）达成共识（如此处定义的标准定义，或者带扩展的定义），然后省去SIMEF消息中的文档类型定义。用于磋商本协议的方法超出了本建议书的讨论范围。

7.1.2 SIMEF中的字符数据处理

出于可移植性的原因，SIMEF兼容的应用不应使用，并且不应将以UTF-8和UTF-16之外的字符编码来对SIMEF消息进行编码。符合XML标准，如果没有为SIMEF消息指定任何编码，那么假定为UTF-8。

7.1.2.1 字符实体引用

每当在数据中写这些字符时，建议SIMEF兼容的应用使用字符'&','<', '>', ""和'"（单引号）的实体引用表，以避免产生任何可能的误解。

7.1.2.2 空白处理

所有SIMEF元素都应支持"xml:space"属性。

7.1.2.3 SIMEF中的语言

SIMEF兼容的应用应指明以何语言来对其内容进行编码；一般地，这可以通过为顶级元素指定"xml:lang"（XML：语言）属性来实现，并使所有其他元素“继承”该定义。

7.2 SIMEF数据类型

在一个XML SIMEF消息内，所有的数据都应表示为文本，原因是，XML是一种文本格式化语言。它为数据模型中的类的属性提供类型信息。对模型中的每个数据类型，在XML SIMEF消息中都有特定的格式化要求；这些要求在本条款中予以陈述。

7.2.1 整数

整数属性通过INTEGER（整数）数据类型来表述。整数数据应以十进制或十六进制来编码。十进制整数编码使用数字'0'至'9'以及一个可选的符号（'+' 或'−'）。例如，"123"，"−456"。十六进制整数编码使用数字'0'至'9'以及'a'至'f'（或者其等同的大写字母），并以字符"0x"起始。例如，"0x1a2b"。

7.2.2 实数

实数（浮点数）属性通过REAL（实数）数据类型来表述。实数数据应以十进制来编码。实数编码指的是可移植的操作系统接口（POSIX）1003.1 [b-IEEE 1003.1]“strtod”库函数：一个可选的符号（'+' 或'−'），后跟一个非空的十进制数字字符串，可选地包含一个基点字符，然后是一个可选的指数部分。一个指数部分包含一个'e'或'E'，紧随其后的是一个可选的符号，之后是一个或多个十进制数字。例如，"123.45e02"、"-567,89e-03"。SIMEF兼容的应用应既支持基点字符'.'，也支持基数字符','。

7.2.3 字符和字符串

单个字符的属性通过CHARACTER（字符）数据类型来表述。已知长度的多字符属性通过STRING（字符串）数据类型来表述。字符和字符串数据没有任何特殊的格式要求，除了偶尔需要使用字符引用来表述特殊的字符。

7.2.3.1 字符实体引用

在XML文档内，在一些情形下，某些字符有特殊的含义。为在这些情形的某种情形中包括这些字符本身，应使用一种特殊的转义序列，称为实体引用。

有时需要转义的字符及其实体引用为：

字符	实体引用
&	&amp;
<	&lt;
>	&gt;
"	&quot;
'	&apos;

7.2.3.2 字符编码引用

由[b-ISO/IEC 10646]和Unicode（统一编码）标准定义的任何字符都可通过使用一个字符引用而包含在一个XML文档中。一个字符引用以字符'&'和'#'开始，以字符';'结束。在这些字符之间，插入字符的字符代码。

如果字符代码之前是一个'x'，那么以十六进制来解释；否则，以十进制来解释。例如，表示与的字符（&）编码为&或者&，表示小于符号的字符（<）编码为<或者<。ISO/IEC 10646和Unicode标准中规定的任何1字节、2字节或4字节字符都可包括在使用该技术的文档中。

7.2.4 字节

二进制数据通过BYTE（字节）数据类型来表述。二进制数据应通过整个使用base64来编码。

7.2.5 枚举类型

枚举类型通过ENUM（枚举）数据类型来表述，它由一个可接受之值的有序列表组成。

7.2.6 日期－时间字符串

日期－时间字符串通过DATETIME（日期时间）数据类型来表述。每个日期－时间字符串确定一个特定的时刻；不支持范围。根据[b-ISO 8601: 2004]的一个子集来对日期－时间字符串进行格式化，如下所示。括号中的章节引用指的是[b-ISO 8601:2004]的条款。

7.2.7 NTP时间戳

网络时间协议（NTP）时间戳通过NTPSTAMP（NTP时间戳）数据类型来表述，在[RFC 1305 b-IETF]和[b-IETF RFC 5905]中予以详细描述。一个NTP时间戳是一个64位无符号的定点数。整数部分在第一个32位中，分数部分在第二个32位中。在SIMEF消息内，对NTP时间戳，应被编码为两个32位的十六进制值，通过一个句号（' '）来隔开。例如，"0x12345678.0x87654321"。

7.2.8 端口列表

端口列表通过PORTLIST（端口列表）数据类型来表述，它由一个以逗号分隔的数字（单个整数）和范围（N－M意味着端口从N到M，含N和M）列表组成。在一个单个列表中可以使用数字和范围的任意组合。例如：

"5-25,37,42,43,53,69-119,123-514"。

7.2.9 唯一标识符

有两种类型的唯一标识符用于本建议书。这两种类型都通过STRING（字符串）数据类型来表述。在相关的XML元素中，这些标识符作为属性来实施，它们应具有唯一的值，如下所示：

1 设备类（条款8.2.3.2）"deviceid"（设备标识符）属性，如果指定，那么应有一个值，它在入侵检测环境中的所有分析仪上都是唯一的。

2 默认值为"0"，这指明分析仪不能生成唯一的标识符。若干类"ident"属性，如果指定，那么应有一个值，它在单个分析仪所发送的所有消息上都是唯一的。对用于确定一个目标的每种特定的数据组合而非对每个对象而言，"ident"属性值都应是唯一的。对象可有多个与之相关的"ident"值。例如，按名称，一个主机的标识符将有一个值，而按地址，该主机的标识符将有第二个值，按名称和地址，该主机的标识符则仍将会有另外一个值。

默认值为"0"，这指明分析仪不能生成唯一的标识符。

创建这些属性中所含之唯一值的方法说明超出了本建议书的讨论范围。

8 SIMEF数据模型

在本条款中，对SIMEF数据模型的单个组件进行了详细说明。提供了关于模型的UML图，以显示各组件之间是如何彼此相关的。

8.1 数据模型概述

数据模型主要组件之间的关系如图2所示。顶级类为SIMEF消息；每种类型的消息是该顶级类的一个子类。定义了两种类型的消息：连接和心跳。在每个消息内，消息类的子类用

于提供消息中承载的详细信息。连接消息类有若干个子类，如设备、策略、来源、目标和附加数据。

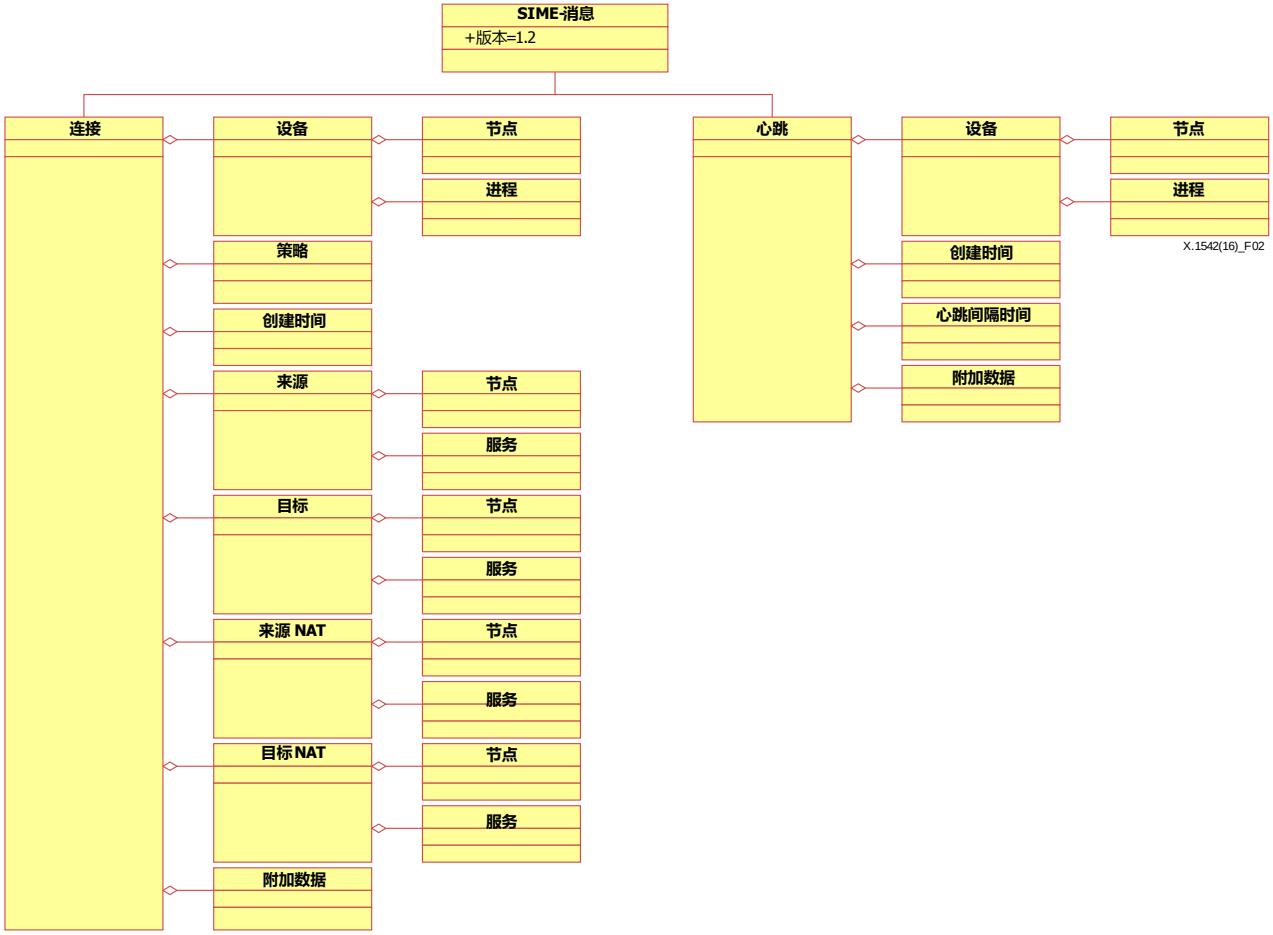


图2 – SIMEF数据模型

8.1.1 SIMEF类

所有SIMEF消息都为SIMEF消息类的实例；连接和心跳。在本条款中对各类进行了描述。见图3、表1和表2。

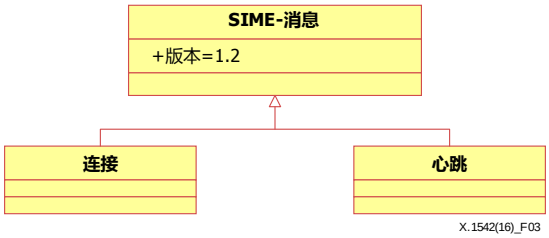


图3 – SIMEF数据模型的顶层类

表1 – SIMEF类的属性

属性	用法	数据类型	描述
版本	必需的	字符串	SIMEF版本信息， 缺省值：1.2。

表2 – SIMEF类的组件

类	聚合	数据类型	描述
连接	精确为1		会话信息类。
心跳	0或1		系统状态信息类， 可选提供。

8.2 消息类

对各个类，将在以下条款8.2.1至8.2.4中予以描述。

8.2.1 连接类

连接类用于容纳会话信息。它描述了由防火墙中连接所生成的日志的类型，它还显示了所有至内部和至外部的连接尝试的信息。见表3。连接类别关键属性可以使用的值见表4。一个连接类由若干个聚合类组成，如图4所示。对聚合类本身的描述，如表5所示。

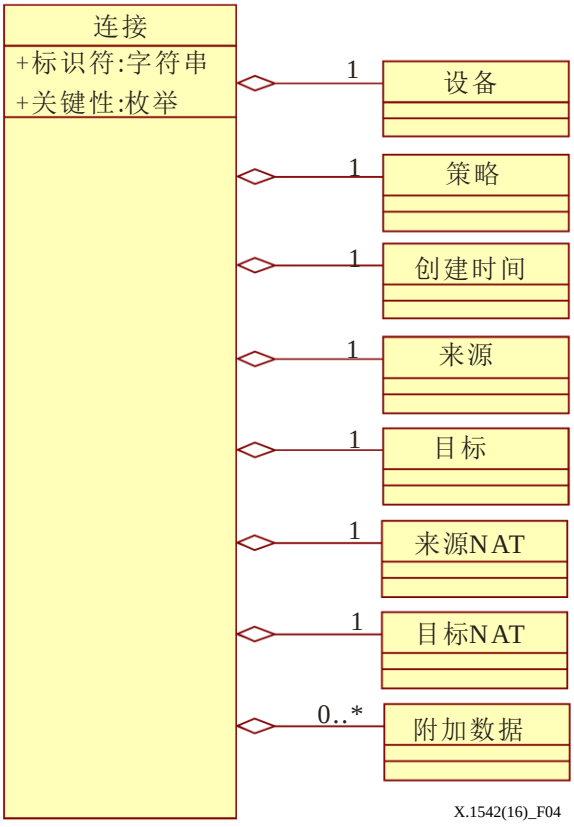


图4 – 连接类的聚合类

表3 – 连接类的属性

属性	用法	数据类型	描述
标识符	可选的	字符串	访问信息的唯一标识符。
关键性	可选的	枚举	依据对连接产生之事件的评估所做的分类，缺省值：未知。

表4 – 关键性属性的值

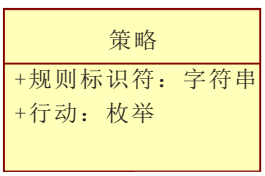
值	关键字	描述
0	未知	当事件的效果未知或者不能确定时。
1	正常	如果是正常连接。
2	可疑	如果是可疑连接。
3	警告	如果连接是一个警告。
4	关键	如果连接对行动敏感。

表5 – 连接类的组件

类	聚合	数据类型	描述
设备	精确为1		分析仪的信息产生一个日志。
策略	精确为1		用于连接的、分析仪中承载的信息。
创建时间	精确为1	日期－时间	日志创建时间。
来源	精确为1		产生连接之事件的来源。
目标	精确为1		产生连接之事件的目的地信息。
来源NAT	精确为1		产生连接之事件的NAT来源信息。
目标NAT	精确为1		产生连接之事件的NAT目的地信息。
附加数据	0或1		不在其他类中的、检测器产生的附加信息。

8.2.1.1 策略类

策略类提供行动信息，以指明在分析仪中如何处置会话。见图5。



X.1542(16)_F05

图5 – 策略类

策略类行动属性（见表6）允许的值如表7所示。

表6 – 策略类的属性

属性	用法	数据类型	描述
规则标识符	可选的	字符串	将由连接产生的、防火墙策略的唯一标识符。
行动	可选的	枚举	由连接导致的、依据操作防火墙进行的分类，缺省值：未知。

表7 – 行动属性的值

值	关键字	描述
0	未知	如果是未知行为。
1	通过	如果允许连接。
2	阻断	如果否认连接。
3	保护	如果加密所传送的数据包或者插入一个完整性检查代码[虚拟专用网（VPN）日志]。
4	拒绝	如果拒绝连接。不过，当否认访问时，则提供错误消息。

8.2.2 心跳类

分析仪使用心跳消息来向管理器指明其当前状况。心跳计划按常规周期来发送，也就是说，每隔10分钟或每隔一小时发送一次。从分析仪收到心跳消息，则向管理器表明分析仪在位并在运行着；缺少心跳消息（或者更有可能的是，缺少一些连续的心跳消息），则表明分析仪或其网络连接失败了。

所有的管理器都将支持对心跳消息的接收；不过，分析仪对这些消息的使用是可选的。管理器软件的开发人员应允许逐个分析仪地来配置软件，以便使用/不使用心跳消息。一个心跳消息由若干个聚合类构成，如图6所示。

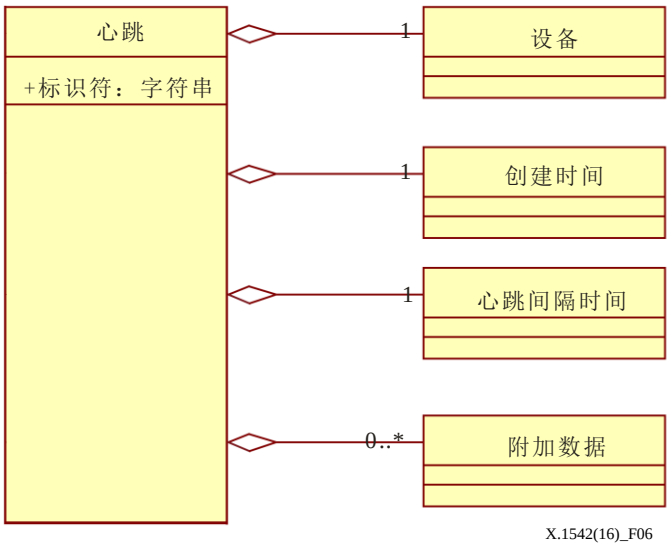


图6 – 心跳类的聚合类

心跳类的属性和组件信息分别如表8和表9所示。

表8 – 心跳类的属性

属性	用法	数据类型	描述
标识符	可选的	字符串	心跳的唯一标识符。

表9 – 心跳类的组件

类	聚合	数据类型	描述
设备	精确为1		发起心跳的分析仪标识信息。
创建时间	精确为1	日期—时间	创建心跳的时间。
心跳间隔时间	精确为1	整数	产生心跳的时间间隔（单位：秒）。
附加数据	0或1		不符合数据模型的、分析仪纳入的信息。

8.2.3 核心类

核心类（设备，创建时间，来源，目标，来源NAT，目标NAT，附加数据）是连接和心跳类的主要组成部分，如图7所示。在本条款中对各个类进行了描述。

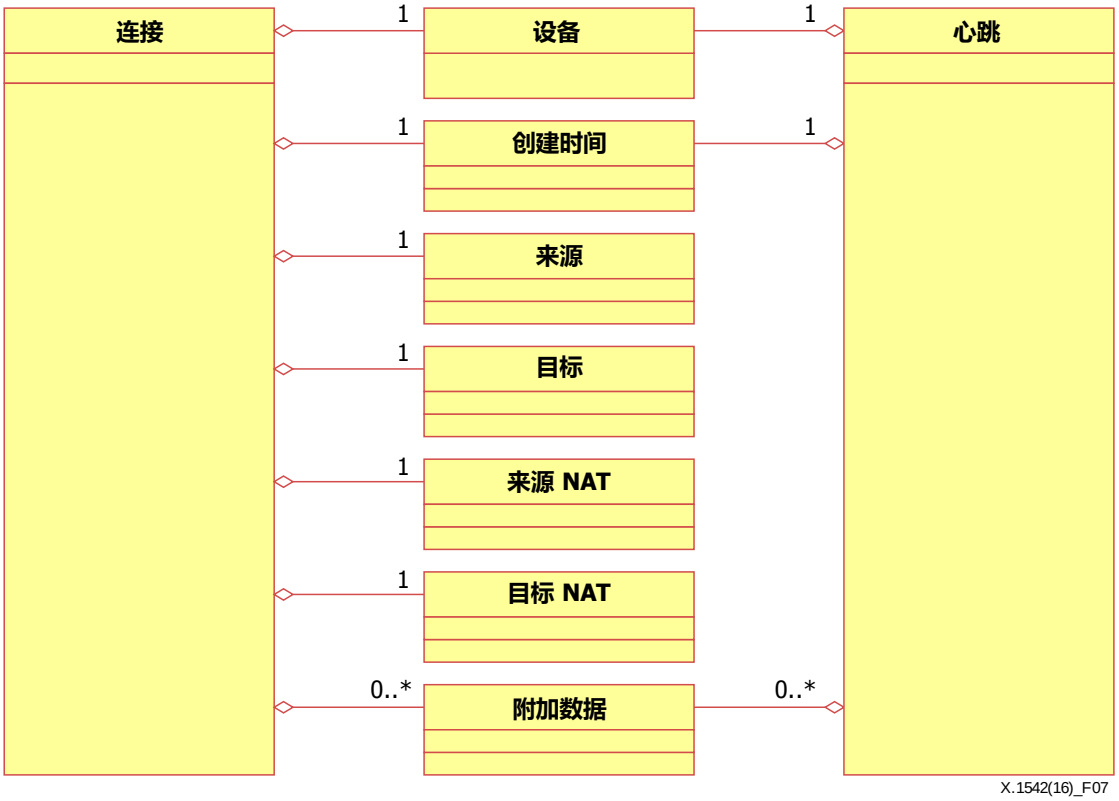


图7 – 核心类

8.2.3.1 设备类

设备类确定产生连接或心跳消息的的分析仪。对每个连接或心跳，只能编码一个设备，并且应是产生连接或心跳的那个设备。

设备类由三个聚合类构成，如图8所示。

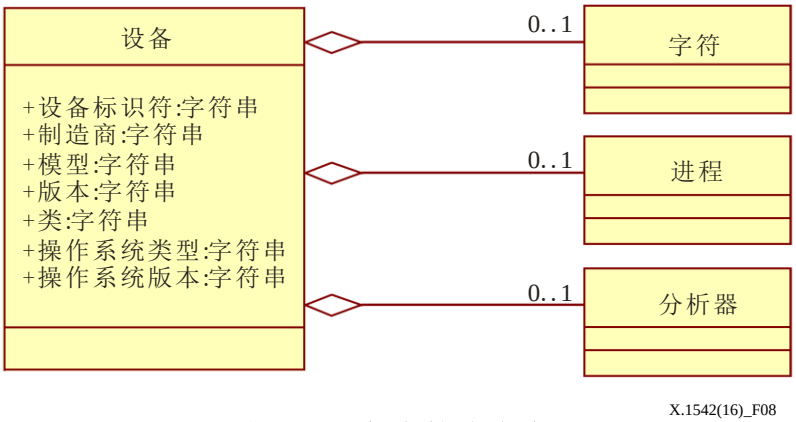


图8 – 设备类的聚合类

设备类有 7 个属性，如表 10 所示。

表10 – 设备类的属性

属性	用法	数据类型	描述
设备标识符	可选的	字符串	设备的唯一标识符。如果在其他类上使用"ident"属性来为那些对象提供唯一标识符，那么它也应提供一个有效的"deviceid"属性。
制造商	可选的	字符串	设备软件或硬件的制造商。
模型	可选的	字符串	设备软件或硬件的模型名称/号码。
版本	可选的	字符串	设备软件或硬件的版本号。
类	可选的	字符串	设备软件或硬件的类。
操作系统类型	可选的	字符串	操作系统名称。
操作系统版本	可选的	字符串	操作系统版本。

对 POSIX 1003.1 兼容系统的操作系统类型（ostype）属性，这是通过 uname()系统调用在 utsname.sysname 中返回的值，或者是"uname –s"命令的输出。

对 POSIX 1003.1 兼容系统的操作系统版本（osversion）属性，这是通过 uname()系统调用在 utsname.release 中返回的值，或者是"uname –r"命令的输出。

“制造商”、“模型”、“版本”和“类”属性内容是特定于供应商的，但可一起使用，以确定分析仪的不同类型。

构成某一设备类别的聚合类如表 11 所示。

表11 – 设备类的组件

类	聚合	数据类型	描述
节点	0或1		关于分析仪驻留在其上的主机或设备的信息（网络地址、网络名称等）。
进程	0或1		关于分析仪在其上执行的进程的信息。
分析仪	0或1		关于消息自其处通过的分析仪的信息。

8.2.3.2 创建时间类

创建时间类用于指明设备的当前日期和时间。如果而后应使用该差异来调整<创建时间>和<NTP 时间戳>元素中的时间，那么也应对 NTP 时间戳进行调整。

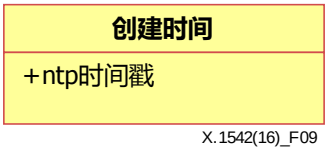


图9 – 创建时间类

创建时间类的属性如表12所示。

表12 – 创建时间类的属性

属性	用法	数据类型	描述
NTP时间戳	必需的	NTP时间戳	关于设备中当前时间的信息。

8.2.3.3 来源类

来源类包含关于产生一个会话之事件可能来源的信息。一个事件可有多个来源（例如，在一个分布式拒绝服务攻击中）。

来源类由三个聚合类构成，如图 10 所示。

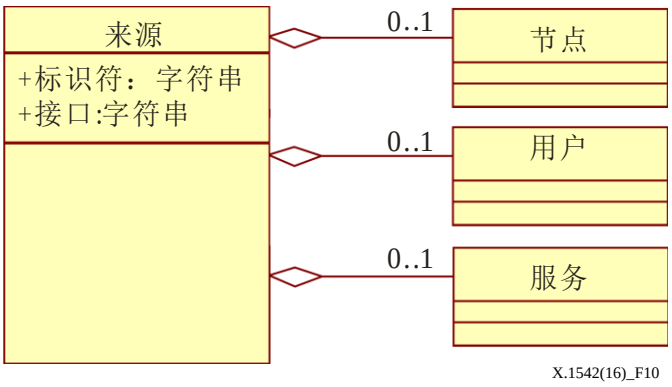


图10 – 来源类的聚合类

来源类有两个属性，如表13所示。

表13 – 来源类的属性

属性	用法	数据类型	描述
标识符	可选的	字符串	本来源的唯一标识符。
接口	可选的	字符串	可能由一个拥有多个接口的、基于网络的设备来使用，以指明在哪个接口上可见到本来源。

构成来源类的聚合类如表14所示。

表14 – 来源类的组件

类	聚合	数据类型	描述
节点	0或1		关于看起来正导致事件的主机或设备的信息（网络地址、网络名称等）。
用户	0或1		关于看起来正导致事件的用户的信息。
服务	0或1		关于事件中涉及的网络服务的信息。

8.2.3.4 目标类

目标类包含关于产生一个会话的事件其可能目标的信息。一个事件可有多个目标（例如，在端口扫描情况下）。

目标类有三个聚合类组成，如图 11 所示。

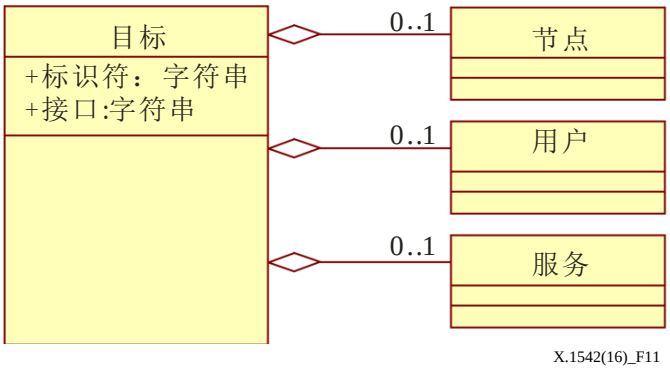


图11 – 目标类的聚合类

目标类有两个属性，如表15所示。

表15 – 目标类的属性

属性	用法	数据类型	描述
标识符	可选的	字符串	本目标的唯一标识符。
接口	可选的	字符串	可能由一个拥有多个接口的、基于网络的设备来使用，以指明在哪个接口上可见到本目标。

构成目标类的聚合类如表16所示。

表16 – 目标类的组件

类	聚合	数据类型	描述
节点	0或1		关于正在主导事件的主机或设备的信息（网络地址、网络名称等）。
用户	0或1		关于正在主导事件的用户的信息。
服务	0或1		关于事件中涉及的网络服务的信息。

8.2.3.5 来源NAT类

来源类包含关于产生一个会话的 NAT 事件其可能来源的信息。一个事件可有多个由 NAT 转换的来源。

来源 NAT 类由三个聚合类组成，如图 12 所示。

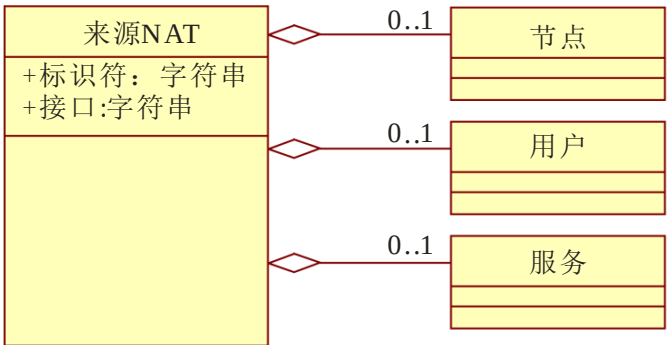


图12 – 来源NAT类的聚合类

来源类有两个属性，如表17所示。

表17 – 来源NAT类的属性

属性	用法	数据类型	描述
标识符	可选的	字符串	由NAT来转换的本来源的唯一标识符。
接口	可选的	字符串	可能由一个拥有多个接口的、基于网络的设备来使用，以指明在哪个接口上可见到由NAT来转换的本来源。

构成来源 NAT 类的聚合类如表 18 所示。

表18 – 来源NAT类的组件

类	聚合	数据类型	描述
节点	0或1		关于看起来正导致事件的主机或设备的信息（网络地址、网络名称等）。
用户	0或1		关于看起来正导致事件的用户的信息。
服务	0或1		关于事件中涉及的网络服务的信息。

8.2.3.6 目标NAT类

目标类包含关于产生一个会话的 NAT 事件其可能目标的信息。一个事件可有多个由 NAT 转换的目标。

目标 NAT 类由三个聚合类组成，如图 13 所示。

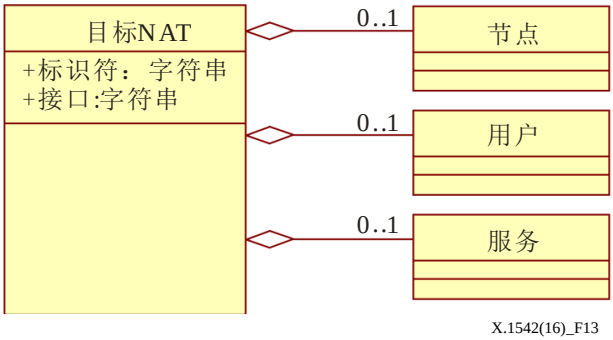


图13 – 目标NAT类的聚合类

目标 NAT 类有两个属性，如表 19 所示。

表19 – 目标NAT类的属性

属性	用法	数据类型	描述
标识符	可选的	字符串	由NAT来转换的本目标的唯一标识符。
接口	可选的	字符串	可能由一个拥有多个接口的、基于网络的设备来使用，以指明在哪个接口上可见到由NAT来转换的本目标。

构成目标类的聚合类如表 20 所述。

表20 – 目标NAT类的组件

类	聚合	数据类型	描述
节点	0或1		关于正在主导事件的主机或设备的信息（网络地址、网络名称等）。
用户	0或1		关于正在主导事件的用户的信息。
服务	0或1		关于事件中涉及的网络服务的信息。

8.2.3.7 附加数据类

附加数据类用于提供不能由 SIMEF 数据模型来表达的信息。附加数据可在以下情况中用于提供原子数据（整数、字符串等），即仅需发送少量的附加信息；它也可用于扩展数据模型和 DTD，以支持复杂数据的传输（例如，数据包头）。

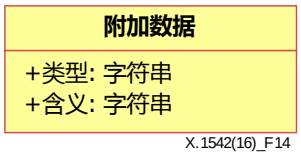


图14 – 附加数据类

附件数据类有两个属性，如表 21 所示。

表21 – 附加数据类的属性

属性	用法	数据类型	描述
类型	必需的	枚举	描述元素内容含义的数据类型。 缺省值：字符串。
含义	可选的	字符串	描述元素内容含义的一个字符串。

在下面的表22中对附加数据的类型进行了描述，显示了该属性允许的值。

表22 – 类型属性的值

值	关键字	描述
0	布尔	元素包含一个布尔值，即字符串“true”（真）或“false”（假）。
1	字节	元素内容是一个单个的8位字节。
2	字符	元素内容是一个单个的字符。
3	日期－时间	元素内容是一个日期－时间字符串。
4	整数	元素内容是一个整数。
5	NTP时间戳	元素内容是一个NTP时间戳。
6	端口列表	元素内容是一个端口列表。
7	实数	元素内容是一个实数。
8	字符串	元素内容是一个字符串。
9	字节串	元素内容是一个字节[]。
10	XML	元素内容是XML标记的数据。

附加数据类的这些值取决于供应商/实施方案；确保管理器理解由分析仪发送的字符串的方法超出了本建议书的讨论范围。

8.2.4 支持类

支持类构成核心类的主要部分，并在其间共享。

8.2.4.1 节点类

节点类用于识别主机和其他网络设备（路由器、交换机等）。

节点类由三个聚合类构成，如图 15 所示。属性、类型属性值和节点类别组件请分别参见表 23、24 和 25。

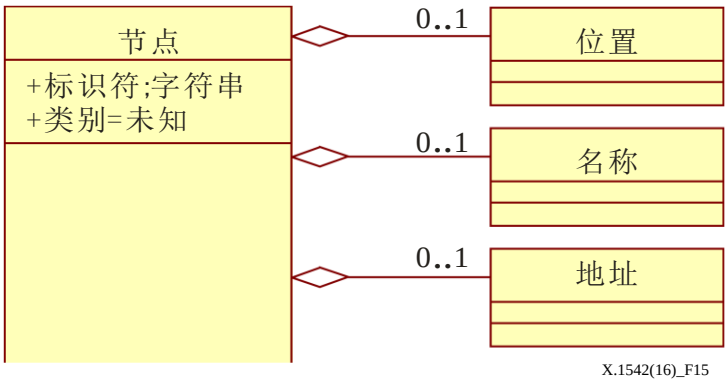


图15 – 节点类的聚合类

表23 – 节点类的属性

属性	用法	数据类型	描述
标识符	可选的	字符串	节点的唯一标识符；参见条款7.2.9。
类别	可选的	枚举	自其获得名称信息的“域名”。 缺省值：未知

表24 – 类型属性的值

值	关键字	描述
0	未知	域名未知或不相关。
1	ads	Windows 2000先进目录服务
2	afs	Andrew文件系统（Transarc）
3	coda	Coda分布式文件系统
4	dfs	分布式文件系统（IBM）
5	dns	域名系统
6	hosts	本地主机文件
7	kerberos	Kerberos领域
8	nds	Novell目录服务
9	nis	网络信息服务（Sun）
10	nisplus	网络信息服务+（Sun）
11	nt	Windows NT域名
12	wfw	Windows for Workgroups

表25 – 节点类的组件

类	聚合	数据类型	描述
位置	0或1	字符串	设备的位置。
名称	0或1	字符串	设备的名称。如果未给出任何地址信息，那么将提供该信息。
地址	0或1		设备的网络或硬件地址。 除非提供了一个名称（上述），否则至少应指定一个地址。

8.2.4.2 地址类

地址类用于描述网络、硬件和应用地址。

地址类由两个聚合类构成，如图 16 所示。

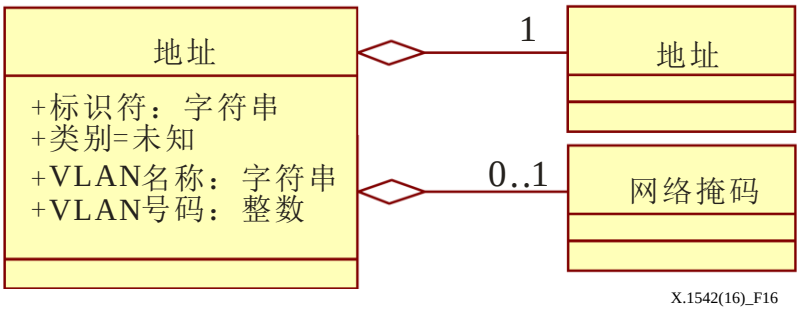


图16 – 地址类的聚合类

属性、类型属性值和地址类别组件请分别参见表 26、27 和 28。

表26 – 地址类的属性

属性	用法	数据类型	描述
标识符	可选的	字符串	地址的唯一标识符；参见条款7.2.9。
类别	可选的	枚举	所表达的地址类型。该属性允许的值如下所示。 缺省值：未知。
VLAN名称	可选的	字符串	地址所属之局域网（LAN）（虚拟LAN）的名称。
VLAN号码	可选的	整数	地址所属之局域网（LAN）（虚拟LAN）的号码。

表27 – 类型属性的值

值	关键字	描述
0	未知	地址类型位置。
1	异步传输模式	异步传输模式网络地址。
2	电子邮件	电子邮件地址（[b-IETF RFC 2822]）。
3	lotus-notes	Lotus Notes电子邮件地址。
4	介质访问控制	介质访问控制（MAC）地址。
5	SNA	IBM共享网络体系结构（SNA）地址
6	VM	IMB VM（"PROFS"）电子邮件地址
7	ipv4-地址	以点间隔的十进制记法的IPv4主机地址（a.b.c.d）
8	ipv4-地址-十六进制	十六进制记法的IPv4主机地址
9	ipv4-网络	以点间隔的十进制记法的IPv4网络地址、斜线、有效位（a.b.c.d/nn）
10	ipv4-网络-掩码	以点间隔的十进制记法的IPv4网络地址、斜线、以点间隔的十进制记法的网络掩码（a.b.c.d/w.x.y.z）
11	ipv6-地址	IPv6主机地址
12	ipv6-地址-十六进制	十六进制记法的IPv6主机地址
13	ipv6-网络	IPv6网络地址、斜线、有效位
14	ipv6-网络-掩码	IPv6网络地址、斜线、网络掩码

表28 – 地址类的组件

类	聚合	数据类型	描述
地址	精确为1	字符串	地址信息。该数据的格式由类别属性管理。
网络掩码	0或1	字符串	如果有的话，指的是地址的网络掩码。

8.2.4.3 用户类

用户类用于描述用户。它主要作为用户标识符聚合类的一种“容器”类，如图 17 所示。

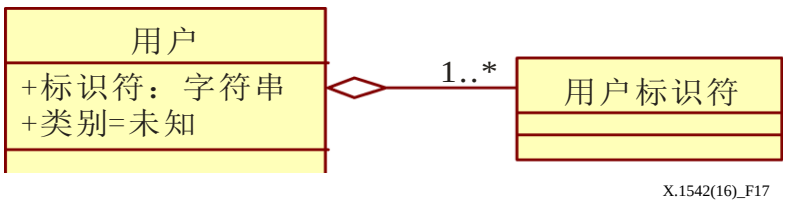


图17 – 用户类的聚合类

属性、类型属性值和用户类别组件请分别参见表29、30和31。

表29 – 用户类的属性

属性	用法	数据类型	描述
标识符	可选的	字符串	用户的唯一标识符；参见条款7.2.9。
类别	可选的	枚举	所表达的用户类型。 该属性允许的值如下所示。 缺省值：未知

表30 – 类型属性的值

值	关键字	描述
0	未知	用户类型未知。
1	应用	一个应用用户。
2	操作系统－设备	一个操作系统或设备用户。

表31 – 用户类的组件

类	聚合	数据类型	描述
用户标识符	1或更多		用户标识符，由其类型属性指明。

8.2.4.3.1 用户标识符类

用户标识符类提供关于用户的特定信息。在用户类中可使用多个用户标识符，以指明从一个用户转换到另一个用户的尝试，或者提供关于一个用户（或进程）特权的完整信息。

用户标识符类由两个聚合类构成，如图 18 所示。

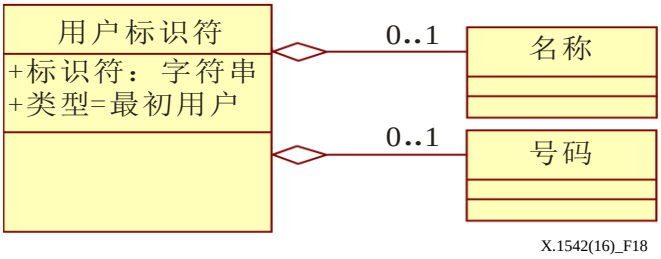


图18 – 用户标识符类的聚合类

属性、类型属性值和用户标识符类别组件请分别参见表32和33。

表32 – 用户标识符类的属性

属性	用法	数据类型	描述
标识符	可选的	字符串	用户标识符的唯一标识符；参见条款7.2.9。
类型	可选的	枚举	所表达的用户信息类型。 该属性允许的值如下所示。 缺省值=初始用户。

表33 – 类型属性的值

值	关键字	描述
0	当前用户	用户或进程正在使用的当前用户标识符。
1	初始用户	报告的用户或进程的实际标识符。在那些（a）进行某些类型审计以及（b）支持从"audit id"令牌中提取用户标识符的系统中，应使用该值。 在那些不支持此的系统中，以及在用户登入系统中时，应使用"login id"。
2	目标用户	用户或进程试图成为的用户标识符。这将应用于Unix系统，例如，当用户试图使用"su"、"rlogin"、"telnet"等时。
3	用户特权	用户或进程能使用的另一个用户标识符，或者与文件权限有关的一个用户标识符。 这种类型的多个用户标识符元素可用于指定权限列表。
4	当前组	正由用户或进程使用的当前组标识符（如果适用的话）。
5	组特权	组或进程能使用的另一个组标识符，或者与文件权限有关的一个组标识符。 例如，在伯克利软件套件（BSD）派生的Unix系统中，这种类型的多个用户标识符元素将用于纳入在"group list"中的所有组标识符。
6	其他特权	不用在用户、组或进程情形中，只用在文件情形中。分配给不匹配文件中用户或组权限的用户的文件。

构成用户标识符的聚合类在表34中列出。

表34 – 用户标识符类的组件

类	聚合	数据类型	描述
名称	0或1	字符串	一个用户或组的名称。
号码	0或1	整数	一个用户或组的号码。

8.2.4.4 进程类

进程类用于描述正在来源、目标和分析仪上被执行的进程。

进程类由五个聚合类构成，如图 19 所示。

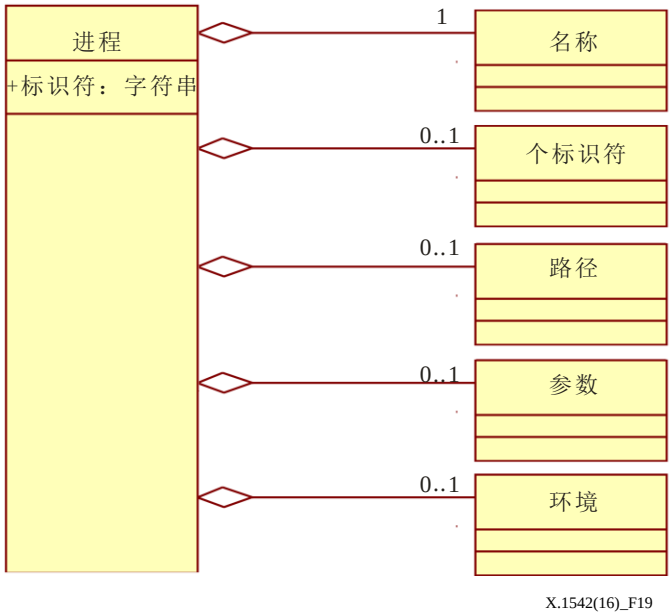


图19 – 进程类的聚合类

进程类有一个属性（见表35）。

表35 – 进程类的属性

属性	用法	数据类型	描述
标识符	可选的	字符串	进程的唯一标识符；参见条款7.2.9。

构成进程的聚合类列在表36中。

表36 – 进程类的组件

类	聚合	数据类型	描述
名称	精确为1	字符串	正在执行之程序的名称。
进程标识符	0或1	整数	进程的进程标识符。
路径	0或1	字符串	正在执行之程序的完整路径。
参数	0或1	字符串	程序的命令行参数。
环境	0或1	字符串	与进程相关的环境字符串；通常的格式为"VARIABLE=value"。

在进程类中，名称类是一个短的名称，通过多次使用arg，可以指定多个参数。通过多次使用env，可以指定多个环境字符串。

8.2.4.5 服务类

服务类用于描述来源和目标上的网络服务。它可通过名称、端口、端口列表和协议来确定服务。当服务作为来源的一个聚合类出现时，可理解为，服务是那个产生感兴趣的活动的服务；以及服务“附着于”也包含在来源中的节点、进程和用户信息。同样地，当服务作为目标的一个聚合类出现时，可理解为，服务是那个感兴趣的活动所导向的服务；以及服务“附着于”也包含在目标中的节点、进程和用户信息。如果服务既出现在来源中，也出现在

目标中，那么在这两个位置中的信息应是相同的。如果在这两个位置中的信息是相同的，那么实施者希望只在一个位置中承载之，它们应将之指定为目标类的一个聚合。

服务类由四个聚合类构成，如图 20 所示。

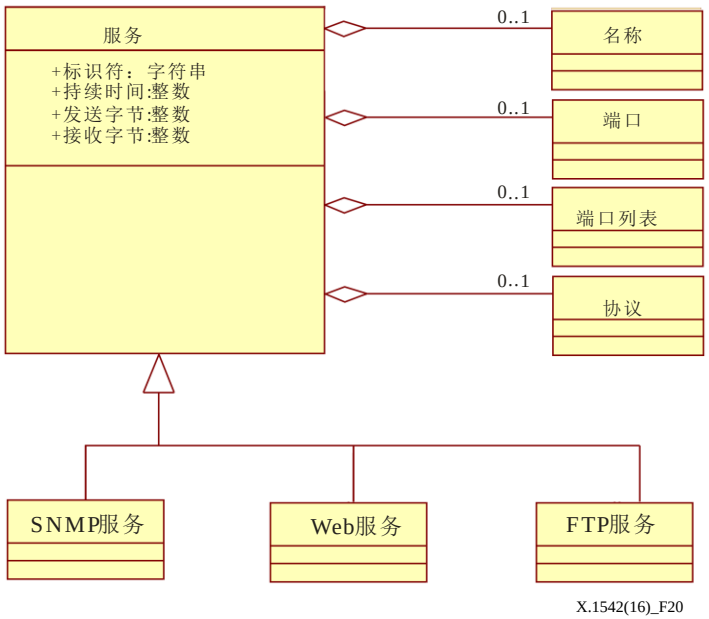


图20 – 服务类的聚合类

服务类有四个属性，列在表37中。

表37 – 服务类的属性

属性	用法	数据类型	描述
标识符	可选的	字符串	服务的唯一标识符；参见条款7.2.9。
持续时间	可选的	整数	连接时间。
发送字节	可选的	整数	连接后发送的字节长度。
接收字节	可选的	整数	连接后接收的字节长度。

构成服务的聚合类列在表38中。

表38 – 服务类的组件

类	聚合	数据类型	描述
名称	0或1	字符串	设备名称。只要可能，应使用来自互联网数字分配机构（IANA）众所周知之端口列表中的名称。
端口	0或1	整数	在用的端口号码。
端口列表	0或1	端口列表	在用的端口号码列表；关于格式化规则，参见条款7.2.8。
协议	0或1	字符串	关于在用协议的附加信息。

8.2.4.5.1 Web服务类

Web 服务类承载与 Web 通信流量有关的附加信息。

Web 服务类由四个聚合类构成，如图 21 所示。

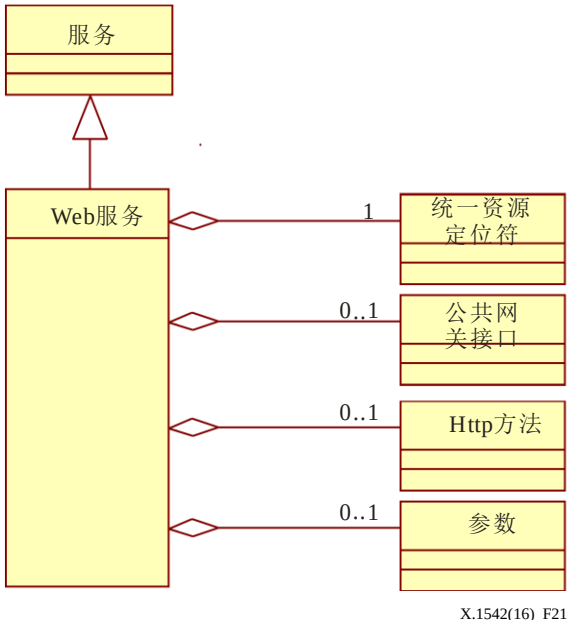


图21 – Web服务类的聚合类

构成Web服务的聚合类列在表39中。

表39 – Web服务类的组件

类	聚合	数据类型	描述
统一资源定位符	精确为1	字符串	请求中的统一资源定位符（URL）。
公共网关接口	0或1	字符串	请求中的公共网关接口（CGI）脚本，不带参数。
Http方法	0或1	字符串	请求中使用的超文本传输协议（HTTP）方法（PUT，GET）。
参数	0或1	字符串	公共网关接口（CGI）脚本的参数。

8.2.4.5.2 SNMP服务类

SNMP 服务类承载与简单网络管理协议（SNMP）通信流量有关的附加信息。

SNMP 服务类由八个聚合类构成，如图 22 所示。

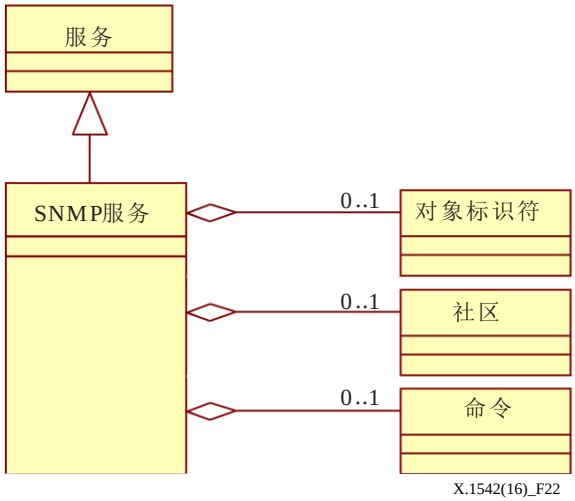


图22 – SNMP服务类的聚合类

构成SNMP服务的聚合类列在表40中。

表40 – SNMP服务类的组件

类	聚合	数据类型	描述
对象标识符	0或1	字符串	请求的对象标识符。
社区	0或1	字符串	对象的社群字符串。
命令	0或1	字符串	发送给SNMP服务器的命令（GET，SET等）。

8.2.4.5.3 FTP服务类

FTP 服务类承载与文件传输协议（FTP）通信流量有关的附加信息。

FTP 服务类由两个聚合类构成，如图 23 所示。

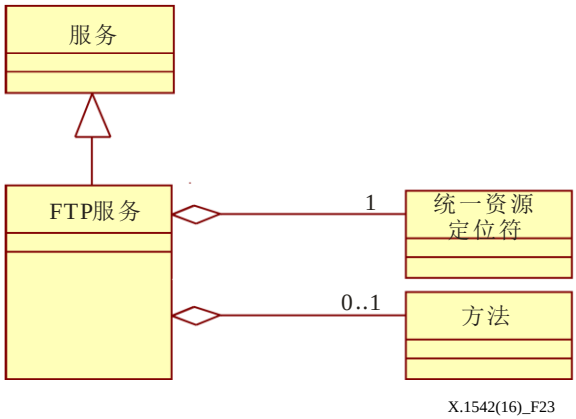


图23 – FTP服务类的聚合类

构成FTP服务类别的聚合类列在表41中。

表41 – FTP服务类的组件

类	聚合	数据类型	描述
统一资源标识符	精确为1	字符串	请求中的统一资源标识符。
方法	0或1	字符串	请求中所用的FTP方法（PUT, GET）。

9 安全方面的考虑

本条款讨论SIMEF实施者需考虑到的一些安全问题。

本建议书描述有关会话信息消息交换格式（SIMEF）的信息模型，并提供了一个通过XML模式来规范的相关数据模型。SIMEF定义了一种数据模型表达方法，以共享有关集中式网络安全管理和安全信息交换系统的传输层会话日志信息。

虽然没有任何安全问题直接适用于该数据的格式，但数据本身可包含安全敏感的信息，其机密性、完整性与/或可用性可能需要保护。

本建议书建议应对用于收集、传输、处理和存储该数据的系统予以保护，以防止未经授权的使用，并应对数据本身予以保护，以防止未经授权的访问。实现这种保护的方法和手段超出了本建议书的讨论范围。

附录 I

SIMEF例子和模式

（本附录并非本建议书的组成部分）

本附录描述SIMEF模型XML模式的例子。下面的例子描述的是XML模式、SYSLOG模式，以期将会话信息编码到SIMEF模型中去。

I.1 SIMEF模式

I.1.1 XML模式

```
<?xml version="1.0" encoding="UTF-8"?>

<simef:SIMEF-Message version="1.2" xmlns:simef="http://iana.org/simef/">
     <Connect ident="1008380" criticality="normal">
        <Device Deviceid="TTA-FW" model="FW1000">
           <Node>
              <Address category="ipv4-addr">
                <address>1.1.1.1</address>
              </Address>
           </Node>
        </Device>
        <CreateTime ntpstamp="0xaaaaaaaaaaaaaaaaaa">
                  2010-08-18T15:41:28+00:00
           </CreateTime>
        <Policy Ruleid="45" action="pass"></Policy>
           <Source>
           <Node>
              <Address category="ipv4-addr">
                <address>2.2.2.2</address>
              </Address>
           </Node>
           <Service duration="9" size="144">
              <port>38168</port>
              <protocol>17</protocol>
           </Service>
        </Source>
        <Target>
           <Node>
              <Address category="ipv4-addr">
                <address>3.3.3.3</address>
              </Address>
           </Node>
           <Service duration="9" size="0">
              <name>dns</name>
              <port>53</port>
              <protocol>17</protocol>
           </Service>
        </Target>
        <Classification origin="vendor-specific">
           <name>45</name>
        </Classification>
     </Connect>
</simef:SIMEF-Message>
```

I.1.2 SYSLOG 模式

```
  2014-03-18  15:41:28  Local0.Notice  1.1.1.1  TTA:  TTA-FW  device_id=  TTA
[Root]system-notification-00257(traffic):    start_time="2014-03-18    15:41:19"
duration=9 policy_id=45 service=dns proto=17 src zone=Untrust dst zone=Trust
action=Permit sent=144 rcvd=0 src=2.2.2.2 dst=3.3.3.3 src_port=38168 dst_port=53
src-xlated ip=2.2.2.2 port=38168 dst-xlated ip=3.3.3.3 port=53 session_id=1008380
reason=Close - AGE OUT<000>
```

I.2 SIMEF例子

I.2.1 防火墙许可

```
<?xml version="1.0" encoding="UTF-8"?>
<SIMEF-Message version=1.2>
       <Connect ident="1008380" criticality="1">
              <Device Deviceid="TTA-FW" manufacturer="TTA" model="FW1000">
                     <Node>
                            <Address category="ipv4-addr">
                                   <address>1.1.1.1</address>
                            </Address>
                     </Node>
              </Device>
              <Policy Ruleid="45" action="1"></Policy>
              <CreateTime ntpstamp="0xaaaaaaaaaaaaaaaaaa">
                     2014-03-18T15:41:28+00:00
              </CreateTime>
              <Source>
                     <Node>
                            <Address category="ipv4-addr">
                                   <address>2.2.2.2</address>
                            </Address>
                     </Node>
                        <Service duration="9" size="144">
                            <port>38168</port>
                            <protocol>17</protocol>
                     </Service>
              </Source>
              <Target>
                     <Node>
                            <Address category="ipv4-addr">
                                   <address>3.3.3.3</address>
                            </Address>
                     </Node>
                     <Service duration="9" size="0">
                            <name>dns</name>
                            <port>53</port>
                            <protocol>17</protocol>
                     </Service>
              </Target>
              <Classification origin="2">
                     <name>45</name>
              </Classification>
       </Connect>
</SIMEF-Message>
```

I.2.2 VPN日志

```
<?xml version="1.0" encoding="UTF-8"?>
<SIMEF-Message version=1.2>
       <Connect ident="1008057" criticality="1">
              <Device Deviceid="TTA-VPN" manufacturer="TTA" model="VPN1000">
                     <Node>
                            <Address category="ipv4-addr">
                                   <address>1.1.1.1</address>
                            </Address>
```

```
                </Node>
            </Device>
            <Policy ruleid="700" action="3"></Policy>
            <CreateTime ntpstamp="0xaaaaaaaaaaaaaaaaaaaa">
                2014-03-19T12:51:22+00:00
            </CreateTime>
            <Source>
                <Node>
                    <Address category="ipv4-addr">
                        <address>2.2.2.2</address>
                    </Address>
                </Node>
                <Service duration="41" size="16905">
                    <port>59078</port>
                    <protocol>TCP</protocol>
                </Service>
            </Source>
            <Target>
                <Node>
                    <Address category="ipv4-addr">
                        <address>3.3.3.3</address>
                    </Address>
                </Node>
                <Service duration="41" size="1448">
                    <name>junos-http</name>
                    <port>80</port>
                    <protocol>TCP</protocol>
                </Service>
            </Target>
            <Classification origin="2">
                <name>700</name>
            </Classification>
        </Connect>
</SIMEF-Message>
```

I.2.3 NAT日志

```
<?xml version="1.0" encoding="UTF-8"?>
<SIMEF-Message version=1.2>
        <Connect ident="1009632" criticality="1">
            <Device Deviceid="TTA-FW" manufacturer="TTA" model="FW1000">
            <Node>
                    <Address category="ipv4-addr">
                        <address>1.1.1.1</address>
                    </Address>
                </Node>
            </Device>
            <Policy ruleid="57" action="1"></Policy>
            <CreateTime ntpstamp="0xaaaaaaaaaaaaaaaaaaaa">
                2014-03-19T16:21:12+00:00
            </CreateTime>
            <Source>
                <Node>
                    <Address ident="" category="ipv4-addr">
                        <address>2.2.2.2</address>
                    </Address>
                </Node>
                <Service duration="41" size="16905">
                    <port>59078</port>
                    <protocol>TCP</protocol>
                </Service>
            </Source>
            <Target>
                <Node>
                    <Address ident="" category="ipv4-addr">
```

```
                        <address>3.3.3.3</address>
                    </Address>
                </Node>
                <Service duration="41" size="1448">
                    <name>junos-http</name>
                    <port>80</port>
                    <protocol>TCP</protocol>
                </Service>
            </Target>
            <SourceNat>
                <Node>
                    <name>trust</name>
                    <Address category="ipv4-addr">
                        <address>4.4.4.4</address>
                    </Address>
                </Node>
                <Service>
                    <port>59078</port>
                </Service>
            </SourceNat>
            <TargetNat>
                <Node>
                    <Address category="ipv4-addr">
                        <address>5.5.5.5</address>
                    </Address>
                </Node>
                <Service>
                    <port>80</port>
                </Service>
            </TargetNat>
        </Connect>
</SIMEF-Message>
```

参考书目

[b-ISO 8601:2004] ISO 8601:2004, *Data elements and interchange formats – Information interchange – Representation of dates and times.*

[b-ISO/IEC 10646] ISO/IEC 10646:2012, *Information technology – Universal Coded Character Set (UCS).*

[b-IEEE Std 1003.1] IEEE Std 1003.1-2008, *IEEE Standard for Information Technology – Portable Operating System Interface (POSIX(R)).*

[b-IETF RFC 1305] IETF RFC 1305 (1992), *Network time protocol (version 3): Specification, implementation.*

[b-IETF RFC 2663] IETF RFC 2663 (1999), *IP network address translator (NAT): Terminology and considerations.*

[b-IETF RFC 2822]) IETF RFC 2822 (2001), *Internet message format.*

[b-IETF RFC 5905] IETF RFC 5905 (2010), *Network time protocol version 4: Protocol and algorithms specification.*

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	视听及多媒体系统
I系列	综合业务数字网
J系列	有线网络和电视、声音节目及其它多媒体信号的传输
K系列	干扰的防护
L系列	环境与ICT、气候变化、电子废物、节能；线缆和外部设备其他组件的建设、安装和保护
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	测量设备的技术规范
P系列	电话传输质量、电话设施及本地线路网络
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、开放系统通信和安全性**
Y系列	全球信息基础设施、互联网协议问题、下一代网络、物联网和智慧城市
Z系列	用于电信系统的语言和一般软件问题

瑞士印刷
2017年，日内瓦