ICS 35.040
L 80
备案号:58557—2017

GM

中华人民共和国密码行业标准

GM/T 0052—2016

密码设备管理
VPN设备监察管理规范

**Cryptographic equipment management—
Monitoring management specification of VPN equipment**

2016-12-23 发布　　2016-12-23 实施

国家密码管理局　　发布

目　　次

前　言

本标准按照GB/T 1.1—2009给出的规则起草。

GM/T 0052《密码设备管理　VPN设备监察管理规范》是密码设备管理类规范之一。该类规范由一个基础规范和系列管理应用规范组成，目前包括：

——基础规范：GM/T 0050　密码设备管理　设备管理技术规范；

——管理应用规范：GM/T 0051　密码设备管理　对称密钥管理规范；

——管理应用规范：GM/T 0052　密码设备管理　VPN设备监察管理规范；

——管理应用规范：GM/T 0053　密码设备管理　远程监控与合规性检验接口数据规范。

本标准凡涉及密码算法相关内容，按国家有关法规实施。

本标准由密码行业标准化技术委员会提出并归口。

本标准起草单位：上海信息安全工程技术研究中心、上海交通大学信息安全学院、上海鹏越惊虹信息技术发展有限公司、上海华堂网络有限公司、卫士通信息产业股份有限公司、上海天融信网络安全技术有限公司、上海信昊信息科技有限公司。

本标准主要起草人：王隽、田立、周志洪、黄志荣、廖烨、邹铴、袁峰、潘淑媛、王贺刚、李俊山、张元臣、吕明忠、潘利民、李高健。

引　言

本标准依据GM/T 0050《密码设备管理　设备管理技术规范》中密码设备管理平台架构，提出针对重要信息系统与网络中VPN设备的监察管理规范，包括管理体系、管理流程、管理消息格式等。本标准采用的安全通道，依据GM/T 0050中的管理应用接口建立，相关内容请参考GM/T 0050。

密码设备管理
VPN 设备监察管理规范

1 范围

本标准规定了重要信息系统与网络中的 VPN 设备的监察管理，以发现和定位网络中的非法 VPN 设备，并检测合法设备在使用过程中的违规操作。

本标准适用于 VPN 设备监察管理系统及监察设备的研发与应用，也可用于指导检测该类监察设备。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GM/T 0022—2014 IPSec VPN 技术规范

GM/T 0024—2014 SSL VPN 技术规范

GM/T 0050—2016 密码设备管理 设备管理技术规范

GM/T 0053—2016 密码设备管理 远程监控与合规性检验接口数据规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

VPN 设备 VPN device

利用 VPN 技术实现网络中安全通信服务的设备。本标准中的 VPN 设备指 IPsec VPN 和 SSL VPN 设备，包括采用 IPsec、SSL 协议的符合国家标准的网络密码机。

3.2

VPN 设备的监察设备 VPN compliance monitoring agency

按照监察管理应用规则，实现对被监测网络中的目的数据包进行过滤分析，并上报关键信息的网络设备。

3.3

伯克利封包过滤器 berkeley packet filter

工作在操作系统内核的数据包捕获机制，先将链路层的数据包捕获再过滤，最后提供给应用层特定的过滤后的数据包。

3.4

白名单 white list

对已在国家密码管理主管部门备过案，并且“已知为良好”的 VPN 设备名单，管理应用层用来标识安全可信的合规设备列表。白名单中的信息包括：设备的注册 IP 地址、设备的密码算法标识等信息。

4 缩略语

下列缩略语适用于本文件。

BPF:伯克利封包过滤器(Berkeley Packet Filter)

IPSec:IP 安全协议(Internet Protocol Security)

ISAKMP:网络安全关联和密钥管理协议(Internet Security Association and Key Management Protocol)

PDU:分包数据单元(Package Data Unit)

SSL:安全套接层(Secure Socket Layer)

VPN:虚拟专用网(Virtual Private Network)

5 VPN 设备的监察管理体系

5.1 体系结构

VPN 设备监察管理体系遵循 GM/T 0050—2016 的 5.3,其体系结构如图 1 所示。

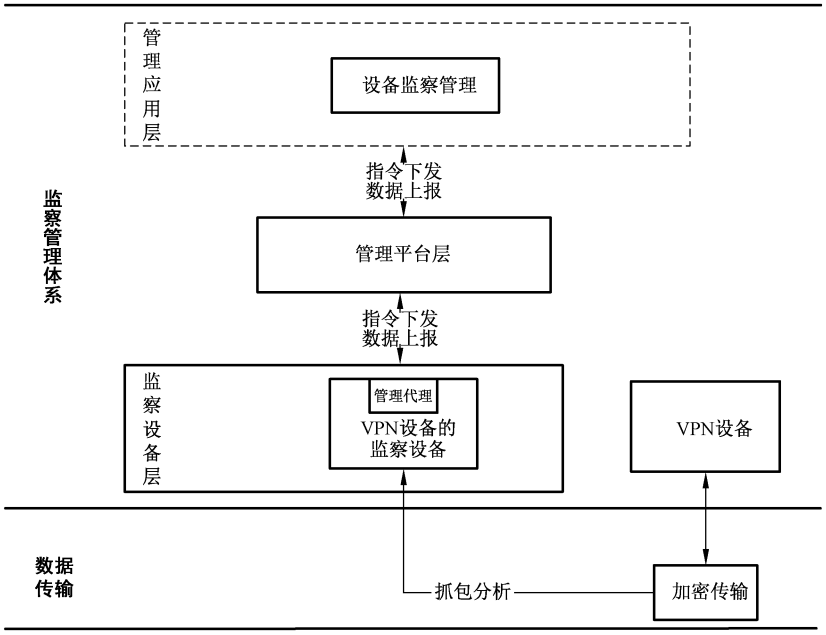

图 1 VPN 设备监察管理体系结构图

以下 5.3、5.4、5.5 详细描述图 1 中的各层内容。

5.2 功能要求

监察管理系统的功能要求为:

a) 在线获取 VPN 设备的监察数据;

b) 分析这些监察数据,判断 VPN 设备的应用是否合规;

c) 若发现不合规的 VPN 设备,则实时告警和取证分析;

d) 维护(新增、修改和删除)违规算法的列表;

e) 维护过滤 IP 列表,建立白名单机制;

f） 统计全网中 VPN 设备的通信次数；

g） 提供对历史数据的查询和统计分析。

5.3 管理应用层

本标准涉及的管理应用是 VPN 设备的监察管理。

对于 VPN 设备的监察管理，应通过抓取和检测 VPN 密钥协商阶段的数据包，分析网络中 VPN 设备应用情况，对违规 VPN 设备告警，确保 VPN 设备的合法合规。

5.4 管理平台层

对管理平台层的要求遵循 GM/T 0050—2016 的 5.5。

5.5 VPN 设备的监察设备层

VPN 设备的监察设备接受管理代理的管理，并遵循 GM/T 0050—2016 的 5.6 和 GM/T 0053—2016 的 5.3 和 5.4。

VPN 设备的监察设备部署在被监察网络的出入口，对网络内所有 VPN 设备通过旁路抓包的方式进行监察管理，负责接收管理应用层通过设备管理平台和安全通道下发的策略和指令，解析指令，并将执行结果返回。

VPN 设备监察设备的逻辑结构如图 2 所示。

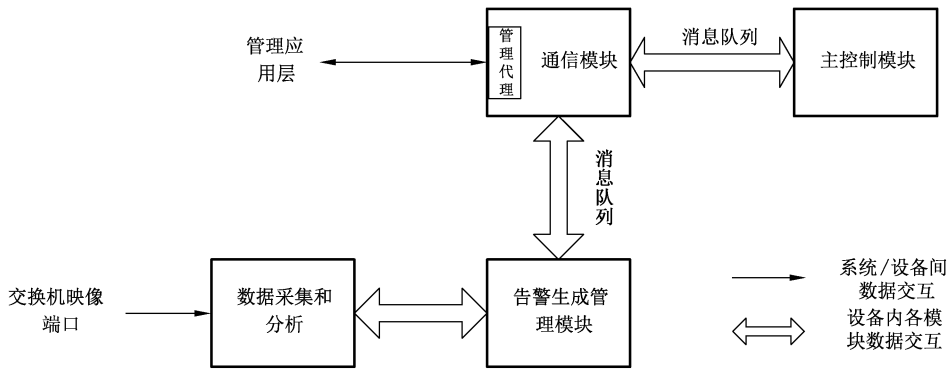

图 2 VPN 设备的监察设备示意图

VPN 设备的监察设备的主要功能有：

a） 高速数据包采集功能，实现对网络核心交换设备的实时数据采集分析。

b） VPN 通信发现功能，支持对 IPSec、SSL 的协议分析。

c） 加密算法判定功能，针对发现的 VPN 通信，提取相应加密算法标识等相关信息，对是否属合法密码算法进行判定。

d） VPN 设备定位功能，对发现的正在使用的 VPN 设备，定位设备所在网络地址或网段地址。将合法的 VPN 设备信息，记录到数据库中。对违规的 VPN 设备信息，记录到违规设备数据库中。

e） 信息采集及告警功能，将相关告警信息和管理应用层所需的其他采集信息，实时提交到管理应用层。

f） 管理及维护功能，支持管理应用层对 VPN 监察设备的实时状态检测，远程管理和维护等功能。

5.6 安全通信

密码设备管理体系中的管理应用是从管理应用层发起管理指令，通过设备管理平台层和安全通道到达设备管理代理，由管理代理负责解析，并按指令内容进行操作。

VPN 设备的监察设备接受管理代理的管理，其与设备管理平台间的所有消息，都通过安全通道发送，安全通道的消息 PDU 和使用说明遵循 GM/T 0050—2016 的第 6 章。

管理应用层与 VPN 设备的监察设备的交互信息包括两个方面：

a) VPN 设备的监察设备上报给管理应用层的信息，包括违规 VPN 报警信息等；

b) 管理应用层下发给 VPN 设备的监察设备的信息，包括 VPN 设备的监察设备的配置信息、过滤规则信息等。

5.7 VPN 设备的监察管理流程

监察管理系统工作流程如下：

a) 将 VPN 设备的监察设备部署到网络骨干节点，进行初始化，并配置上联 IP 地址；

b) VPN 设备的监察设备上电后自动和管理应用层发起连接，进行身份认证，包括与上联设备的 IP 双向绑定、设备 ID 认证；

c) 管理应用层通过 VPN 设备的监察设备的身份认证后，对该监察设备进行初始化配置；

d) VPN 监察设备根据配置规则，对抓到的数据包进行过滤，采集各类 VPN 数据包；

e) 检查抓到的 VPN 数据包，根据 IP 地址信息判断如果 VPN 设备在白名单中，则跳过后续检查步骤，无需进行进一步检查；

f) 如果 VPN 设备不在白名单中，则提取密码算法属性值（指密钥交换协议第一阶段的密钥算法属性值），若提取不到，则转到 i）；

g) 将提取的算法属性值，对照国家密码管理局发布的 GM/T 0022—2014 和 GM/T 0024—2014 规范中关于算法属性值的定义；

h) 若提取的算法属性值符合技术规范的定义，则 VPN 设备合规；否则，继续下一步；

i) VPN 监察设备将采集到的“违规”VPN 信息转换成统一格式，向管理应用层发送；

j) 遵循 GM/T 0053—2016 中 6.2 的要求，检验设备合规性，如果不合规，则实时报警；

k) 管理应用层将报警信息写入数据库。

其流程图如图 3 所示。

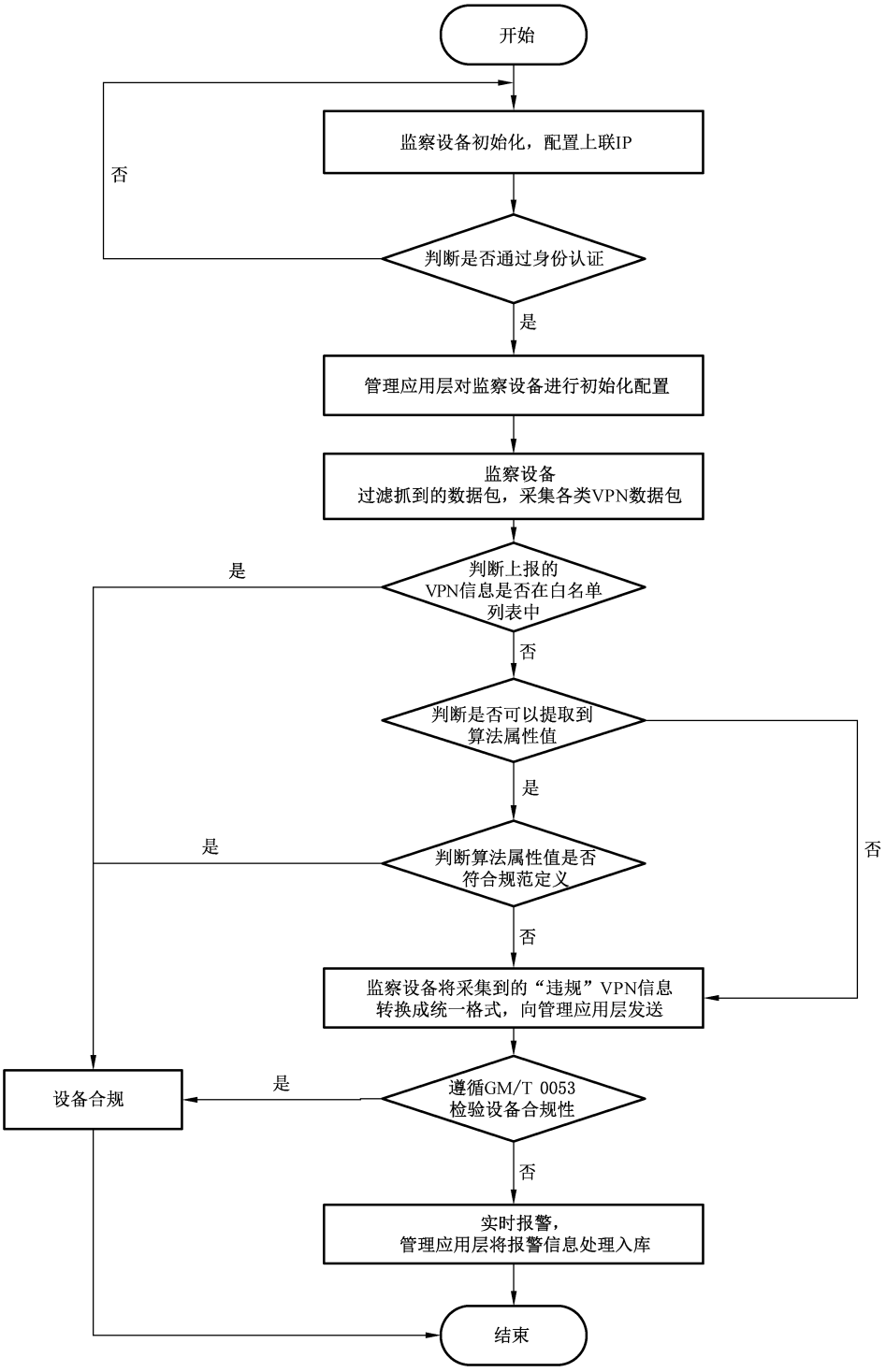

图 3　监察管理系统工作流程图

6　VPN 设备的监察数据采集规则

6.1　过滤规则

对采用私有协议加密的 VPN 设备，应在国家密码管理主管部门备案，备过案的 VPN 设备，只要通

过设备合规性检验，就认定是合规的，设备合规性检验遵循 GM/T 0053—2016 的 6.2。对于其他 VPN 设备，则根据本章的数据采集规则来监察其应用的合规性。

管理应用层向 VPN 设备的监察设备下发数据包的过滤规则，监察设备接收到包过滤规则消息后，根据过滤规则库在 VPN 网络通信的出入口节点进行数据包过滤和数据包内容分析，并将采集信息实时提交到管理应用层。

管理应用层下发的默认报文过滤规则，是 TCP 协议的 443 端口、UDP 协议的 500 和 4500 端口。其中：

TCP 协议的 443 端口对应于 SSL VPN 协议。

UDP 协议的 500 端口对应于 IPSec VPN 的 ISAKMP 协议。

UDP 协议的 4500 端口对应于与 IPSec VPN 存在 NAT 穿越并进行 UDP 封装的情况。

默认规则可写为：

tcp port 443 or udp port 500 or udp port 4500

针对厂家可能会对标准的网络端口进行修改的情况，报文过滤规则的端口范围可以放宽至 TCP 和 UDP 的所有端口。

报文过滤规则语言符合 BPF 语法，详细的 BPF 过滤器规则语言描述见参考文献[1]。

6.2 基于 IPSec VPN 协议的检测规则

对 IPSec VPN 的监察管理包括设备监察和设备所用算法的监察，具体监察步骤为：

a) 提取密码算法属性值，包括对称算法属性值、非对称算法属性值、杂凑算法属性值。若提取不到，则转到 d)；

b) 将提取的算法属性值，对照国家密码管理局发布的 GM/T 0022—2014 中关于算法属性值的定义；

c) 若提取的算法属性值符合规范中定义的，则 IPSec VPN 合规；否则，继续下一步；

d) VPN 监察设备将采集到的“违规”VPN 信息转换成统一格式，上报管理应用层。

其算法监察流程如图 4 所示。

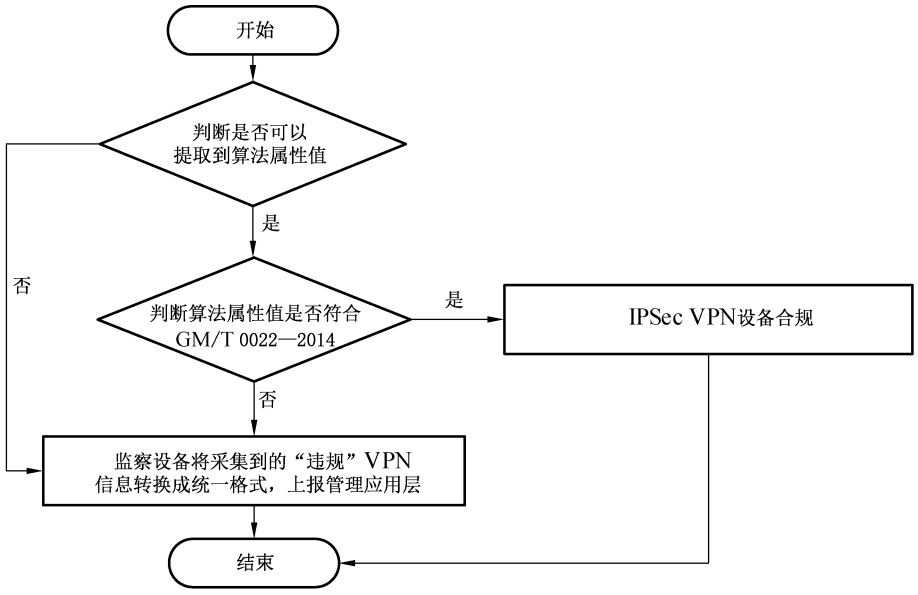

图 4 基于 IPSec VPN 协议的检测流程图

IPSec VPN 监察规则可支持野蛮模式。

6.3 基于 SSL VPN 协议的检测规则

对 SSL VPN 的监察管理包括对设备的监察和对设备所用算法的监察，具体步骤为：

a) 提取密码算法属性值，包括对称算法属性值、非对称算法属性值、杂凑算法属性值。若提取不到，则转到 d)；

b) 将提取的算法属性值，对照 GM/T 0024—2014 中规定的密码算法套件；

c) 若提取的算法属性值符合规范中定义的，则 SSL VPN 合规；否则，继续下一步；

d) VPN 监察设备将采集到的“违规”VPN 信息转换成统一格式，上报管理应用层。

其检测流程如图 5 所示。

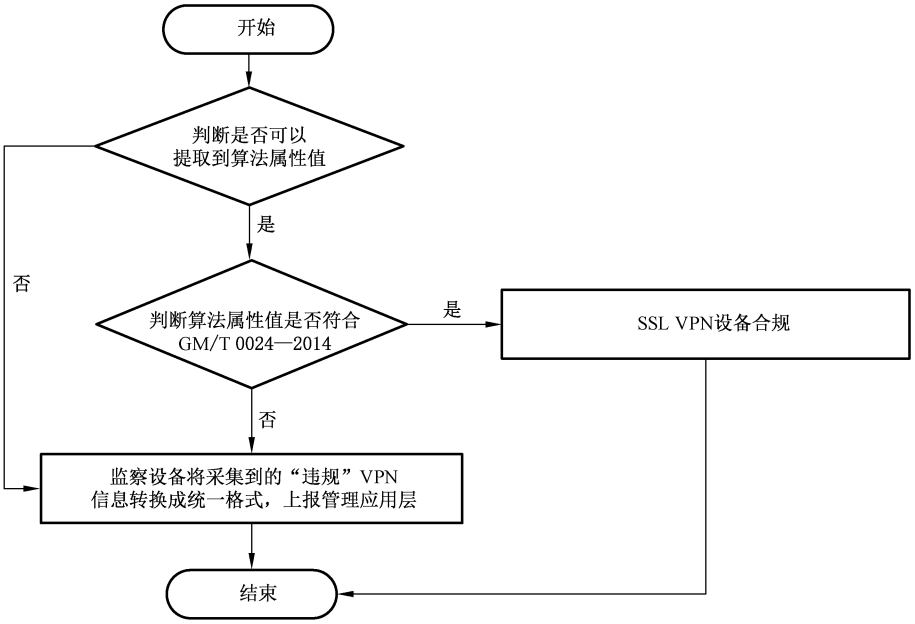

图 5 基于 SSL VPN 协议的检测流程图

7 VPN 设备的监察管理消息定义

7.1 概述

VPN 设备的监察管理的通信过程主要是管理应用层与监察设备之间的网络通信，所有消息都通过安全通道实行保密传输。

VPN 设备的监察管理消息调用 GM/T 0050—2016 中 9.4.1 SMF_Sec TunnelSendData 函数，将管理消息指令填充在设备管理平台指令的消息 PDU 中，管理消息赋值在 sendData 字段，如图 6 所示。

图 6 监察管理消息格式

其中：

操作类型 0xA3 标识安全通道发送数据消息。

管理应用标识 0xC5 指设备监察管理。

本章对管理应用标识 0xC5 后面的管理消息 PDU 做出规范。

消息格式采用 XML 定义，本标准定义了最基本的数据结构，可在此基础上按实际需要拓展，所有消息的最高层类是 agent，每一种类型的消息都是该类的子类，agent 中定义了 VPN 设备的监察设备的唯一 ID 标识、IP 地址及其他描述信息，由管理应用层给监察设备分配 ID，作为监察设备接入网络的授权标识之一，管理应用层收到 VPN 设备的监察设备消息，需要鉴别消息格式，根据监察设备 ID 等条件判别其合法性，若格式有误，则拒绝处理并指示监察设备重发。

VPN 设备监察管理的操作类型有 agent-config(VPN 设备的监察设备配置消息)、agent-rule(VPN 设备的监察设备规则消息)和 agent-alert(VPN 设备的监察设备告警)等。

7.2 VPN 设备的监察设备配置消息

VPN 设备的监察设备配置消息 agent-config 是管理应用层向监察设备下发的配置，直接作为 agent 的子类，主要涉及监察管理应用层对多个监察设备的管理、配置维护、策略规则下发等，定义了上联设备(servers 类)、心跳间隔、信息报告时间窗、时间戳等子类，servers 类中应包含多项 server 子类，通过 server 的元素值决定用于主用服务器还是其他用途，其消息格式定义如下：

Agent-config={更新时间(YYYY-MM-DD HH:MM:SS 格式)||上联设备配置(名称、ID、IP、端口)||VPN 设备的监察设备配置(VPN 设备的监察设备名称、ID、IP、端口)||心跳间隔||采样时间}。

```
〈? xml version="1.0" encoding="UTF-8"?〉
〈agent xmltype="agent-config" name="VPN 设备的监察设备名称" id="VPN 设备的监察设备 id" ip="VPN 设备的监察设备 IP"〉
〈agent-config〉
    〈update-time〉YYYY-MM-DD HH:MM:SS〈/update-time〉
    〈servers〉
        〈server name="上联设备名称" ip="上联设备 IP" status="1" default="yes" port="1070"/〉
    〈/servers〉
    〈client name="VPN 设备的监察设备名称" id="VPN 设备的监察设备 id" ip="VPN 设备的监察设备端 IP" port="1070"〉
        〈interface〉eth0〈/interface〉
    〈/client〉
    〈global-sets〉
        〈time-interval〉
            〈heartbeat〉30〈/heartbeat〉
            〈sample〉120〈/sample〉
        〈/time-interval〉
    〈/global-sets〉
〈/agent-config〉
〈/agent〉
```

详细消息定义参见 A.1。

7.3 过滤规则消息

VPN 设备的监察设备过滤规则消息 agent-rule 直接作为 agent 的子类，是针对 IPSec 和 SSL 的 VPN 协议配置的抓包规则，定义了 VPN 设备的监察设备采集信息的一系列过滤规则，监察设备根据过

滤规则决定采集哪些类型信息、无需采集哪些信息。目前规则为 TCP 443 端口，UDP 500 和 4 500 端口，而且，若抓到的算法属性值在过滤规则中已经定义，则认为属于合规的 VPN 连接，不需要上报到管理应用层。其消息格式定义如下：

Agent-rule={更新时间(YYYY-MM-DD HH:MM:SS 格式)||过滤规则表达式||IPSec/SSL 标识位||对称算法属性值||哈希算法属性值||认证算法属性值}

```
<? xml version="1.0" encoding="UTF-8"?>
<agent xmltype="agent-rule" description="agent config xml" name="*" id="*" ip="*">
<agent-rule>
    <update-time>YYYY-MM-DD HH:MM:SS</update-time>
    <localfilters>
        <localfilter>过滤表达式</localfilter>
    </localfilters>
    <filters>
        <filter>
            <filter-name>VPNPROTOCOL</filter-name>
            <init-param>
                <param-value>IPSEC</param-value>
                <param-value>SSL</param-value>
            </init-param>
        </filter>
    </filters>
    <auth-arithmetic-mappings type="IPSEC">
        <arithmetic type="ENC">
            <sn>128</sn>
    </arithmetic>
    <arithmetic type="HASH">
            <sn>2</sn>
            <sn>20</sn>
    </arithmetic>
    <arithmetic type="AUTH">
            <sn>10</sn>
    </arithmetic>
    <arithmetic type="GROUP"/>
    </auth-arithmetic-mappings>
    <auth-arithmetic-mappings type="SSL">
        <arithmetic type="ENC"/>
    </auth-arithmetic-mappings>
    </agent-rule>
</agent>
```

详细消息定义参见 A.2。

7.4 VPN 设备的监察设备告警消息

VPN 设备的监察设备告警消息 agent-alert 是 alert-reports 的子类，监察设备将违规 VPN 设备信

息以告警信息上传到管理应用层，告警信息的格式定义如下：

Agent-report ={VPN 设备的监察设备探测起始时间(YYYY-MM-DD HH:MM:SS 格式)||探测结束时间(YYYY-MM-DD HH:MM:SS 格式)||IPSec/SSL 标识位||对称算法属性值||哈希算法属性值||认证算法属性值||组算法属性值||VPN 设备的监察设备 IP||上联设备 IP||VPN 设备的监察设备端口||上联设备端口||是否合法||是否为密码设备

```
〈? xml version="1.0" encoding="UTF-8"?〉
〈agent ip="VPN 设备的监察设备 IP"  id="VPN 设备的监察设备 id"  name="VPN 设备的监察设备名称" description="agent.xml" xmltype=" alert-report "〉
〈agent-reports〉
    〈agent-report type="alert-report" description="report commu-alert"〉
    〈vpn〉
        〈detecting-time〉 YYYY-MM-DD HH:MM:SS 〈/detecting-time〉
        〈end-time〉 YYYY-MM-DD HH:MM:SS 〈/end-time〉
        〈protocol〉IPSEC〈/protocol〉
        〈arithmetic-enc〉加密算法属性值〈/arithmetic-enc〉
        〈arithmetic-hash〉杂凑算法属性值〈/arithmetic-hash〉
        〈arithmetic-auth〉公钥算法属性值〈/arithmetic-auth〉
        〈arithmetic-group〉组算法属性值〈/arithmetic-group〉
        〈sourceAddress〉VPN 设备的监察设备 IP〈/sourceAddress〉
        〈destAddress〉上联设备 IP〈/destAddress〉
        〈sourcePort〉VPN 设备的监察设备端口〈/sourcePort〉
        〈destPort〉上联设备端口〈/destPort〉
        〈islegal〉unknown〈/islegal〉
        〈isdevice〉unknown〈/isdevice〉
    〈/vpn〉
〈/agent-report〉
〈/agent〉
```

注：若 IPSec、SSL 协议标识位为 SSL，则算法属性值字段应为 SSL 算法套件 ID。

附 录 A
（资料性附录）
消息的 XML 定义举例

A.1 VPN 设备的监察设备配置消息的 XML 定义

```
〈? xml version="1.0" encoding="UTF-8"?〉
〈agent xmltype="agent-config" name="agent200801" id="agent200801" ip="192.168.47.221"〉
〈agent-config〉
〈update-time〉2007-12-21 02:29:17〈/update-time〉
〈servers〉
〈server name="www.bss.org" ip="127.0.0.1" status="1" default="yes" port="1070"/〉
〈server name="www.infosec" ip="127.0.0.1" status="0" default="no" port="1070"/〉
〈/servers〉
〈client name="agent200801" id="agent200801" ip="127.0.0.1" port="1070"〉
〈interface〉eth0〈/interface〉
〈/client〉
〈global-sets〉
〈time-interval〉
〈heartbeat〉30〈/heartbeat〉
〈sample〉120〈/sample〉
〈/time-interval〉
〈/global-sets〉
〈/agent-config〉
〈/agent〉
```

A.2 VPN 设备的监察设备过滤规则消息的 XML 定义

过滤规则为 TCP 443 端口，UDP 500 和 4500 端口。

```
〈? xml version="1.0" encoding="UTF-8"?〉
    〈agent xmltype="agent-rule" description="agent config xml" name="*" id="*" ip="*"〉
    〈agent-rule〉
〈update-time〉2007-12-20 16:37:05〈/update-time〉
〈localfilters〉
    〈localfilter〉(udp and port 500) or(tcp and port 443) or(udp and port 4 500)
〈/localfilter〉
〈/localfilters〉
〈filters〉
    〈filter〉
```

```
                <filter-name>VPNPROTOCOL</filter-name>
                <init-param>
                    <param-value>IPSEC</param-value>
                    <param-value>SSL</param-value>
        </init-param>
            </filter>
</filters>
<auth-arithmetic-mappings type="IPSEC">
            <arithmetic type="ENC">
                <sn>128</sn>
    </arithmetic>
    <arithmetic type="HASH">
                <sn>2</sn>
                <sn>20</sn>
    </arithmetic>
    <arithmetic type="AUTH">
                <sn>10</sn>
    </arithmetic>
    <arithmetic type="GROUP"/>
    </auth-arithmetic-mappings>
        <auth-arithmetic-mappings type="SSL">
            <arithmetic type="ENC"/>
        </auth-arithmetic-mappings>
            </agent-rule>
            </agent>
```

A.3 VPN 设备的监察设备告警消息的 XML 定义

```
    <? xml version="1.0" encoding="UTF-8"?>
    <agent ip="*"  id="*"  name="*"  description="agent xml"  xmltype="alert-report">
    <agent-reports>
    <agent-report  type="alert-report"  description="report commu-alert">
    <vpn>
        <detecting-time>2013-12-02 13:49:14</detecting-time>
        <end-time>2013-12-02 13:49:35</end-time>
        <protocol>IPSEC</protocol>
        <arithmetic-enc>5</arithmetic-enc>
        <arithmetic-hash>2</arithmetic-hash>
        <arithmetic-auth>3</arithmetic-auth>
        <arithmetic-group>2</arithmetic-group>
        <sourceAddress>*</sourceAddress>
        <destAddress>*</destAddress>
        <sourcePort>500</sourcePort>
```

```
        〈destPort〉500〈/destPort〉
        〈islegal〉unknown〈/islegal〉
        〈isdevice〉unknown〈/isdevice〉
〈/vpn〉
〈/agent-report〉
〈/agent-reports〉
〈/agent〉
```

参 考 文 献

[1] http://www.manpagez.com/man/7/pcap-filter/