ICS 35.040
L 80
备案号：

中华人民共和国密码行业标准

GM/T XXXX—XXXX

VPN设备应用合规性管理规范

Management Specification of VPN Equipment Compliance

（征求意见稿）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

××××-××-××发布　　××××-××-××实施

国家密码管理局 发布

目　　次

前　言

本标准依据 GB/T 1.1-2009《标准化工作导则 第 1 部分：标准的结构和编写》起草。

本标准在 GM/T AAAAA《密码设备管理技术规范》定义的密码设备管理应用体系的基础上制定。

请注意本标准的某些内容可能涉及专利。本标准的发布机构不承担识别这些专利的责任。

本标准的附录是资料性附录。

本标准由国家密码管理局提出并由国家密码行业标准化技术委员会归口。

本标准起草单位：上海(暨国家)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、袁峰、廖烨、潘淑媛、王贺刚、李俊山、吕明忠、潘利民、李高健。

本标准凡涉及密码算法相关内容，按国家有关法规实施。

引　言

本标准在 GM/T AAAAA《密码设备管理技术规范》定义的密码设备管理应用体系基础上制定，规范了重要信息系统与网络中的 VPN 设备合规性的管理应用，包括合规性管理流程、管理消息格式等。

本标准编制过程中得到了国家商用密码应用体系总体工作组的指导。

VPN 设备应用合规性管理规范

1　范围

本标准规范了重要信息系统与网络中的 VPN 设备合规性的管理应用，确保接入的 VPN 设备都是合规的，而且合法用户在使用过程中不会有非法操作。

本标准适用于 VPN 设备应用合规性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 AAAAA　密码设备管理技术规范

GM/T BBBBB　密码设备管理应用数据接口规范

GM/T 0022-2014　IPSec VPN 技术规范

GM/T 0024-2014　SSL VPN 技术规范

3　术语和定义

下列术语和定义适用于本标准。

3.1

VPN 设备　VPN device

VPN 设备是指利用 VPN 技术实现互联网上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 （TLS）协议的符合国家标准的网络密码机。

3.2

VPN 合规性监察设备　VPN compliance monitoring agency

VPN 合规性监察设备指按照合规性管理应用规则，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。

4　缩略语

下列缩略语适用于本标准。

IPSec：网络协议安全性（Internet Protocol Security）

Isakmp：密钥协商握手协议（Internet Security Association Key Management Protocol）

PDU：分包数据单元 （Package Data Unit）

SSL：安全套接层（Secure Socket Layer）

TLS：传输层安全（Transport Layer Security）

VPN：虚拟专用网（Virtual Private Network）

5 VPN 设备应用合规性管理体系

5.1 体系结构

VPN 设备应用合规性管理体系遵循 GM/T AAAAA，其体系结构如图 1 所示。

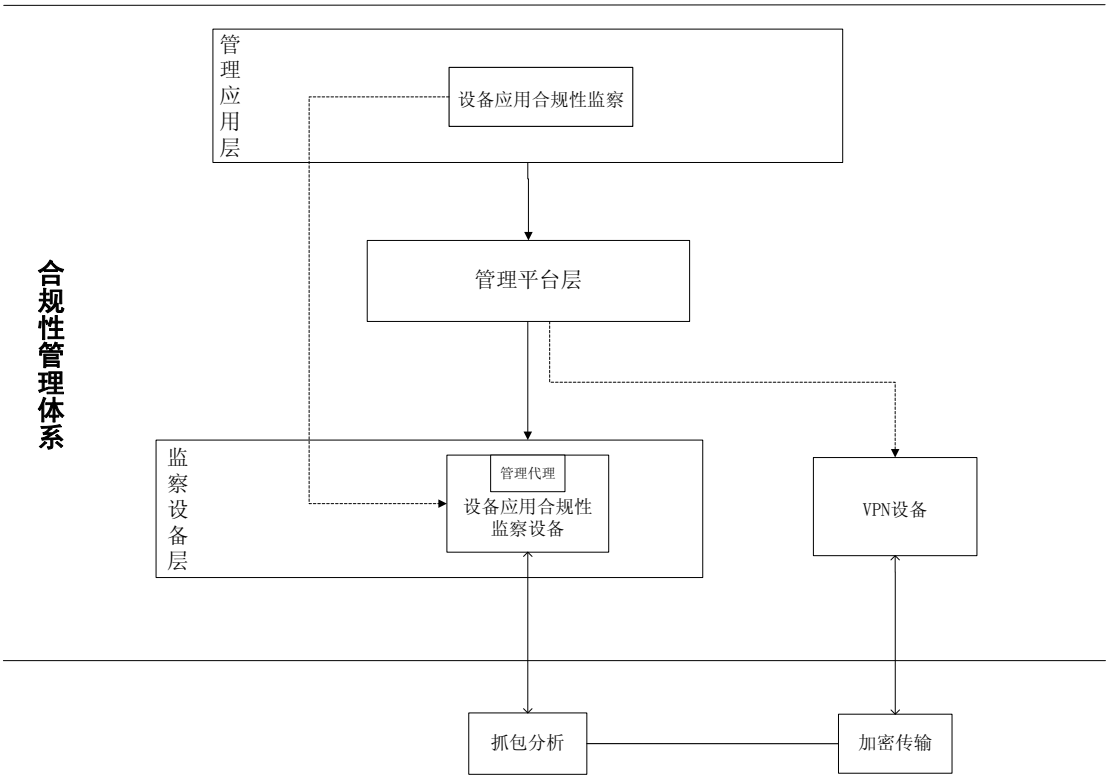

图 1 VPN 设备应用合规性管理体系结构图

以下 5.3、5.4、5.5 章节详细描述图 1 中的各层内容。

5.2 功能要求

合规性管理系统的功能要求为：

a) 在线获取VPN设备的合规性检查数据；

b) 分析判断获取的数据信息是否合规；

c) 发现不合规的VPN设备，进行实时告警和取证分析；

d) 维护(新增、修改和删除)非法算法的列表；

e) 维护过滤IP列表，建立白名单机制；

f) 对全网中VPN设备的通信次数进行统计；

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 设备应用合规性监察。

对于 VPN 设备应用合规性的监察管理，应通过抓取 VPN 密钥协商阶段的数据包，进行深度检测，分析网络中 VPN 设备的合规性状况，对非法 VPN 设备告警，确保 VPN 设备的合法合规。

5.4 管理平台层

对合规性管理平台层的要求遵循 GM/T AAAAA 的 5.4。

5.5 监察设备层

VPN 设备应用合规性监察设备接受管理代理的管理，并遵循 GM/T AAAAA 的 5.5.1 和 GM/T BBBBB。

VPN 设备应用合规性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合规性监察，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。

监察设备的逻辑结构如图 2 所示。

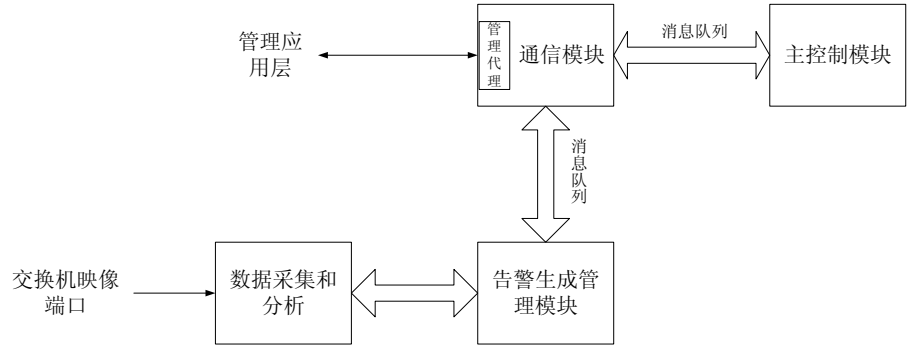

图 2 监察设备示意图

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、TLS/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，进行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。对非法的VPN设备信息，记录到非法设备数据库中。

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

f) 管理及维护功能，支持合规性管理应用层对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的管理指令，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。

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 AAAAA 的第 6 章。

管理应用层与监察设备的交互信息包括两个方面：

a) 监察设备上报给管理应用层的信息，包括非法VPN报警信息等；
b) 管理应用层下发给监察设备的信息，包括监察设备的配置信息、过滤规则信息等。

5.7 VPN 设备应用合规性管理流程

对在国密局备过案的 VPN 设备，管理应用层建立白名单列表。

合规性管理系统工作流程如下：

a) 将合规性监察设备部署到网络骨干节点，进行初始化，配置好上联IP地址；
b) 合规性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) 合规性管理应用层通过合规性监察设备的身份认证后，对监察设备进行初始化配置；
d) 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) 提取密码算法id，如果提取不到，则转到h);
f) 将提取的算法ID，对照国家密码管理局发布的技术规范中关于算法id的定义；
g) 如果提取的算法id符合规范中定义的，则VPN设备合规；否则，继续下一步；
h) 监察设备将采集到的“非法”VPN信息转换成统一格式，向管理应用层发送；
i) 管理应用层解析数据，检查上报的VPN数据是否在白名单列表中；
j) 如果上报的“非法”VPN数据在白名单列表中，则遵循GM/T BBBBB检验设备合规性；否则，进行实时报警；
k) 管理应用层将报警信息处理入库。

其流程图如图3所示。

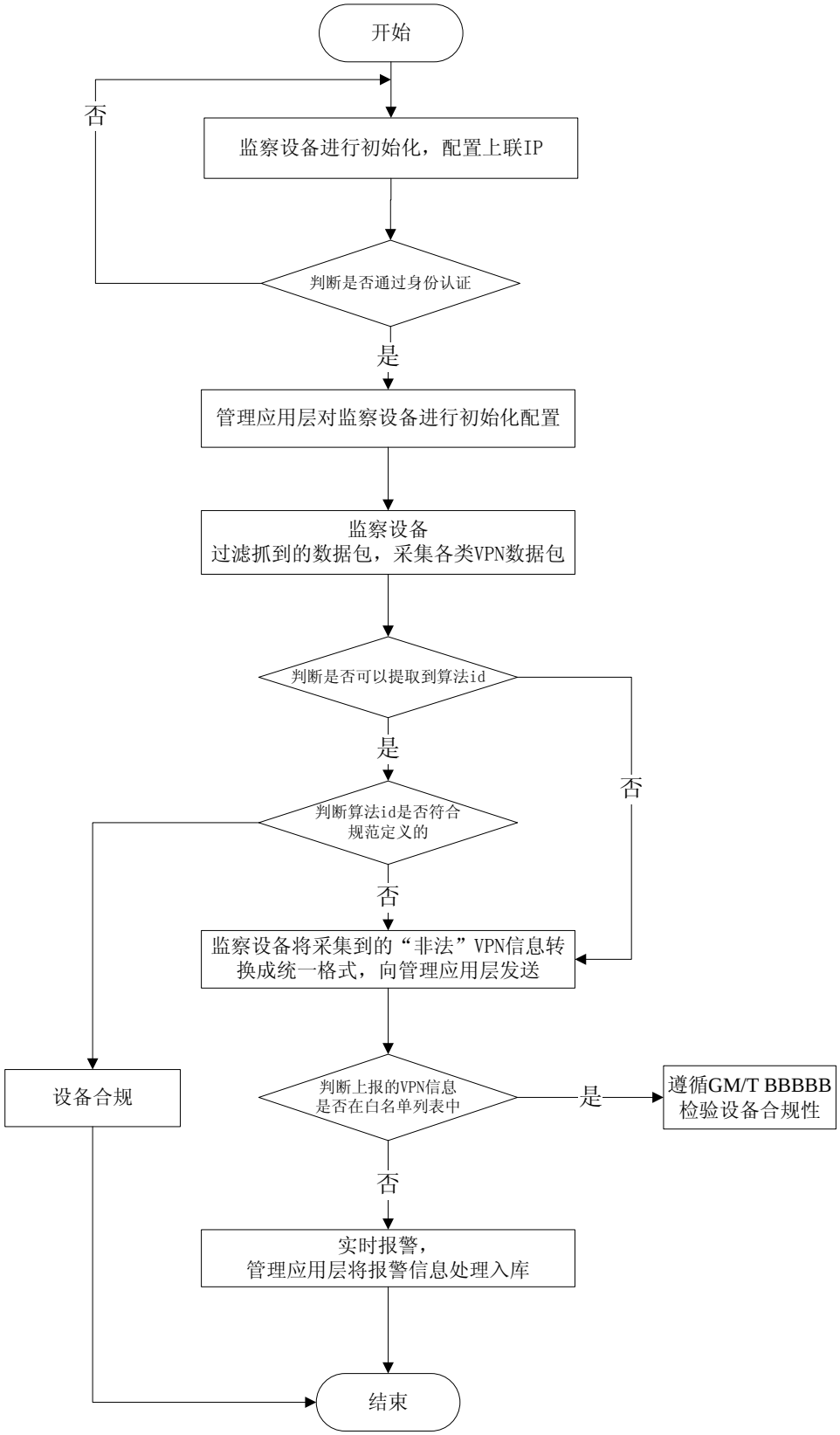

图 3　合规性管理系统工作流程图

6 VPN 设备应用合规性数据采集规则

6.1 过滤规则

对采用私有协议加密的VPN设备，应在国密局备案，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 BBBBB。对于其他 VPN 设备，则根据本章节的数据采集规则来监察其应用的合规性。

管理应用层向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合规性管理应用层。

管理应用层下发的默认报文过滤规则，是 TCP 协议的 443 端口和 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（密钥协商握手协议），

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伯克利封包过滤器（Berkeley Packet Filter，缩写 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 的合规性监察包括设备的合规性监察和设备所用算法的合规性监察，具体监察步骤为：

a) 提取密码算法id，包括对称算法id、非对称算法id、杂凑算法id。如果提取不到，则转到d)；
b) 将提取的算法ID，对照国家密码管理局发布的GM/T 0022-2014中关于算法id的定义；
c) 如果提取的算法id符合规范中定义的，则IPSec VPN合规；否则，继续下一步；
d) 监察设备将采集到的“非法”VPN信息转换成统一格式，上报管理应用层。

其算法合规性监察流程如图4所示。

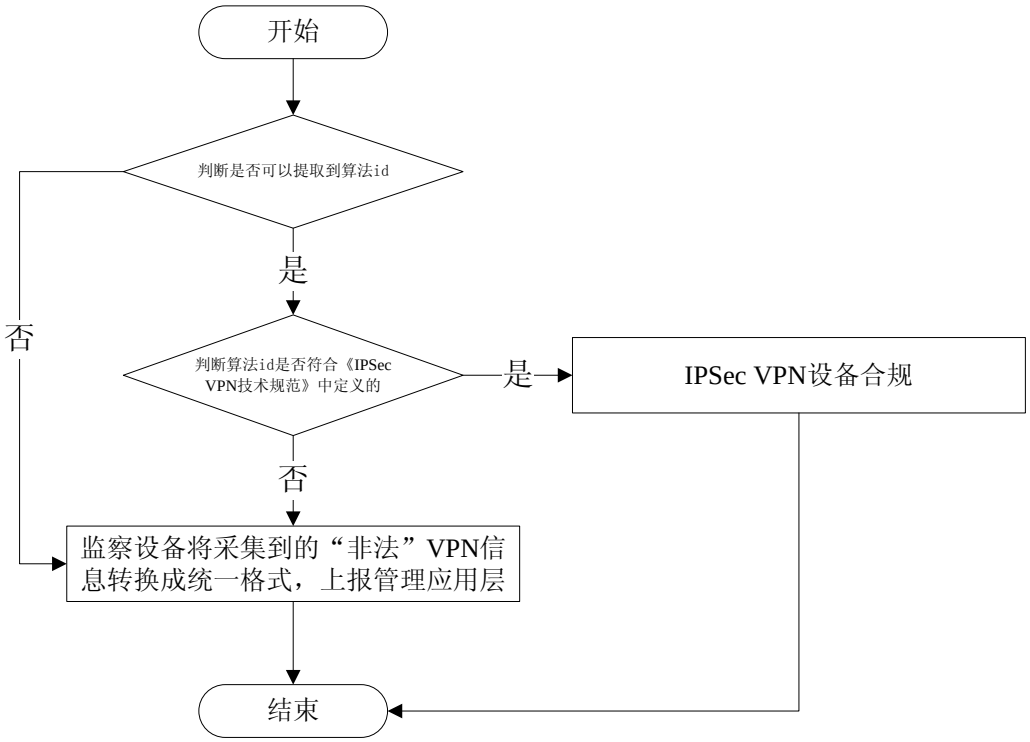

图 4　基于 IPSec VPN 协议的检测流程图

对野蛮模式也可以进行同样操作。

6.3　基于 SSL　VPN 协议的检测规则

对 SSL VPN 的合规性监察包括设备合规性监察和设备所用算法的合规性监察，具体监察步骤为：

a) 提取密码算法id，包括对称算法id、非对称算法id、杂凑算法id。如果提取不到，则转到d)；

b) 将提取的算法ID，对照GM/T 0024-2014中规定的密码算法套件；

c) 如果提取的算法id符合规范中定义的，则SSL VPN合规；否则，继续下一步；

d) 监察设备将采集到的“非法”VPN信息转换成统一格式，上报管理应用层。

其流程图如图5所示。

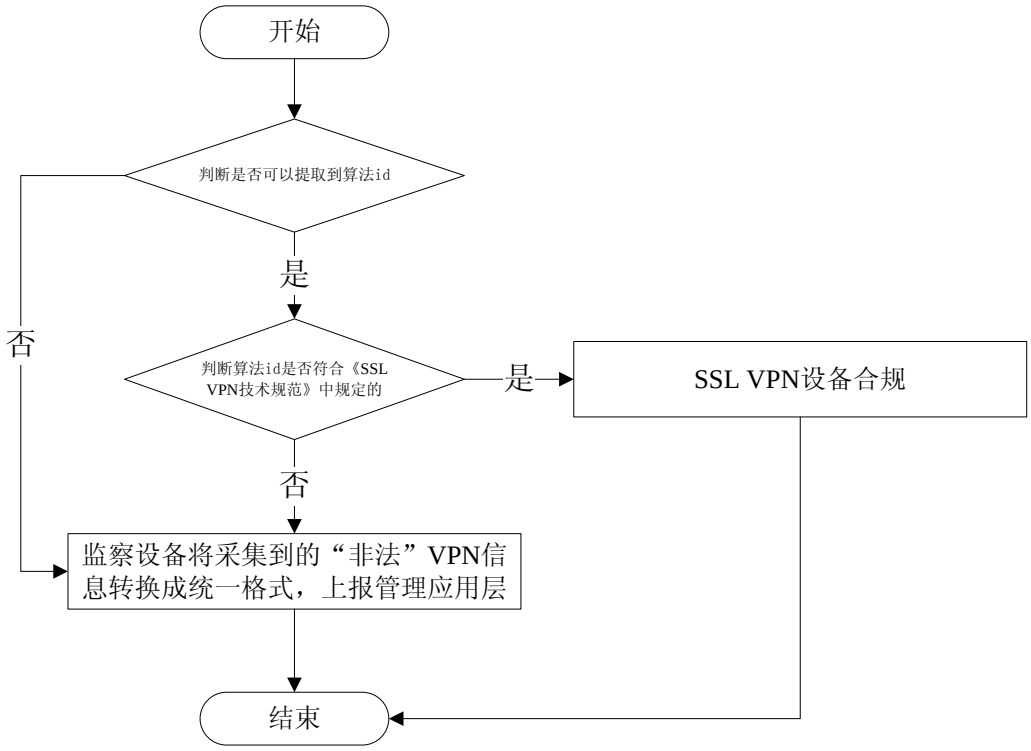

图 5　基于 SSL VPN 协议的检测流程图

7　VPN 设备应用合规性管理消息定义

7.1　合规性管理消息概述

VPN 设备合规性管理的通信过程主要包括管理应用层与合规性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。

消息交换格式采用 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进行拓展，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 中定义了监察设备的唯一 ID 标识、IP 地址及其它描述信息，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，如果格式有误，则拒绝处理并指示监察设备重发。

VPN 设备应用合规性管理消息调用 GM/T AAAAA 第 9.8 节 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　应用合规性管理消息格式

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 指设备应用合规性管理。

本章节对管理应用标识 0xC5 后面的管理消息 PDU 做出规范。

VPN 设备应用合规性管理的操作类型有 agent-config（监察设备配置消息）、agent-rule（监察设备规则消息）和 agent-alert（监察设备告警）等。

7.2 监察设备配置消息

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，主要涉及合规性管理应用层对多个合规性监察设备的管理、配置维护、策略规则下发等，定义了服务器 servers、心跳间隔、信息报告时间窗、时间戳等子类，servers 中应包含多项 server 子类，通过 sever 的元素值决定用于主用服务器还是其它用途，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）|| 监察设备配置（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="监察设备名称" id="监察设备 id" ip="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="监察设备名称" id="监察设备 id" ip="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>
```

详细消息定义参见附录 A.1。

7.3 过滤规则消息

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 4500 端口，而且，如果抓到的算法 id 在过滤规则中已经定义，则认为属于合规的 VPN 连接，不需要上报到合规性管理应用层。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 ID ‖ 哈希算法 ID ‖ 认证算法 ID}

```
<?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>
```

详细消息定义参见附录 A.2。

7.4 监察设备告警消息

监察设备告警消息 agent-alert 是 alert-reports 的子类， VPN 设备合规性监察设备将违规及非法 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 ={合规性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 ID||哈希算法 ID||认证算法 ID||组算法 ID||监察设备 IP||上联设备 IP ||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="监察设备 IP"   id="监察设备 id"   name="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 ID</arithmetic-enc>
        <arithmetic-hash>杂凑算法 ID</arithmetic-hash>
        <arithmetic-auth>非对称算法 ID</arithmetic-auth>
        <arithmetic-group>组算法 ID</arithmetic-group>
        <sourceAddress>监察设备 IP</sourceAddress>
        <destAddress>上联设备 IP</destAddress>
        <sourcePort>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：如果 IPSec、SSL 标识位为 SSL，那么算法 ID 这里是 SSL 算法套件 ID。

附 录 A

（资料性附录）

消息的 XML 定义举例

A.1 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 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)</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 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/