VPN 系统反馈调整和实时监控集成解决方案①

马宗萼[1,2]，李晓风[1]，谭海波[1]

[1](中国科学院 合肥物质科学研究院信息中心，合肥 230031)
[2](中国科学院研究生院，北京 100049)

摘 要：传统 VPN 系统存在不能根据状态自动调整运行，而且缺乏对运行状态的监控的问题，为此以 OpenVPN 为基础，提出一个 VPN 系统自动管理和实时监控解决方案，通过编写程序分析和理解服务运行状态，根据反馈触发执行相应管理程序，与管理端口进行通信调整服务行为，同时使用 SNMP 协议构造监控代理程序，对系统性能进行实时监控，使得管理员能够通过 Cacti 监控平台实时了解系统运行参数，达到保障 VPN 服务持续可靠和高效运行的目的。实验结果表明，该系统能够根据当前状态所设定的规则优化运行，并为管理员提供直观实时的性能视图。

关键词：OpenVPN；CACTI；SNMP；反馈调整；监控

Integration of Feedback Adjustment and Real-time Monitoring for VPN System

MA Zong-E[1,2], LI Xiao-Feng[1], TAN Hai-Bo[1]

[1](Information Center, Hefei Institutes of Physical Science, Chinese Academy of Sciences, Hefei 230031, China)
[2](Graduate University, Chinese Academy of Sciences, Beijing 100049, China)

Abstract: VPN system generally lacks the ability to adjust to the feedback from status and performance monitoring. To deal with this problem, an integration of feedback adjustment and real-time monitoring solution is introduced based on OpenVPN, which understands the status of VPN service, communicates with the management interface to adjust its behaviors, executes the administrative procedures according to the feedback automatically, and uses SNMP protocol to make an agent to provide real-time monitor, make the administrator understand system parameters through Cacti, ensures a continuous, reliable and high-efficiency vpn service. The experiments show that system can optimize the operation according to the status and rules, and provide a real-time performance view.

Key words: openvpn; cacti; snmp; feedback adjustment; monitoring

VPN 网络是企业“内网”区域在 Internet 范围内的延伸，随着企业信息化的发展，它的规模不断扩大，也由此带来了复杂的管理和安全问题。每个 VPN 用户都拥有自己的内网身份，它们经由 VPN 系统调度与内网进行通信，为了规范用户行为，必须制定严格的管理策略，设计相应的服务管理程序分析系统运行状态，在一定的条件下触发执行这些策略；同时 VPN 网络承载着重要的企业内部应用和数据，迫切需要对其服务质量进行监控，以便在出现问题时及时通知管理员进行处理，提高系统的可靠性和安全性。

1 研究现状

当前商用 VPN 系统大多基于 IPSec 协议或 SSLVPN 协议，在认证授权、隧道安全、日志审计方面的技术趋于成熟，但是用户和连接管理依赖于人为操作，而且这些系统难以实施二次开发进行功能性扩展，对于规模日益庞大的 VPN 网络，无疑是一个不小的负担。同时由于商用软件对自身状态的监控能力非常有限，造成系统的异常状态难以被及时发现和跟踪，无法对 VPN 网络行为实施有效监控[1]。

开源 VPN 系统通常仅具备基本的身份验证、隧道

① 收稿时间:2011-03-17;收到修改稿时间:2011-04-04

加密功能，缺乏友好的用户界面和管理元素，但是搭建方便，使用免费，并且提供了丰富的外部接口，可以编写应用程序获取和分析系统的运行反馈，然后通过系统接口调整其运行。此外，通过开发 SNMP[2,3]代理程序，周期性地获取系统状态信息，同时对历史数据进行存档分析，根据所设置的状态参数阈值主动预警，可以达到系统性能实时监控的目标。

这里主要围绕反馈调整和实时监控两方面，基于 OpenVPN[4]平台构架 VPN 系统，为系统接口编写连接程序，根据获取到的状态信息选择执行相应的处理规则，使系统自行调整其运行；同时开发 SNMP 监控代理程序[5]，为系统制定合理的监控方案。系统在自行调整、监控预警、功能扩展等方面具有更好的性能，更符合生产环境的需要。

2　系统设计与实现

2.1　关键技术

2.1.1 OpenVPN

OpenVPN 是基于 SSL 安全机制的 OSI 二层或三层网络隧道解决方案[6,7]，它在控制通道中使用 SSL/TLS 协议，为所创建的隧道结合了 RSA 身份验证，Diffie-Hellman 密钥协商，HMAC-SHA1 完整性检查，Blowfish 数据加密机制确保数据安全[8]。除了完善的安全机制，OpenVPN 还提供了身份验证、隧道控制的外部程序接口以及服务接口，满足功能扩展需求。

2.1.2 CACTI

CACTI[9]是一个基于 SNMP 的开源监控框架，采用 C/S 结构的监控模式，通过在受监控端运行 SNMP 代理程序暴露 MIB 信息，由监控服务端向受监控端周期性地发送 SNMP 查询命令收集所需数据，CACTI 将收集到的数据保存到本地 RRD 数据库中，并提供图形化的监测和分析工具。

2.2　系统架构

系统由 VPN 服务端和 CACTI 监控端两部分组成，体系结构如图 1 所示。

VPN 服务负责建立和维护 VPN 网络；审计程序在隧道的建立和撤销期间获取重要的用户信息和环境变量并存档备案；管理程序从审计数据库、运行日志和管理接口获取信息，从规则库中提取满足条件的规则形成命令提交到管理接口，管理系统的运行；Web UI 为用户提供注册激活、账户变更操作，为管理员提供用户管理、日志分析界面；监控代理进程通过 SNMP 协议监测系统性能数据，然后将这些数据暴露给监控端。

CACTI 周期性地执行 SNMP 查询获取系统性能数据，通过 Web 页面展现当前和历史监控图像；在 CACTI 中为系统的重要状态数据设置阈值，一旦采集到的数据不在阈值范围内，就会触发告警功能，以邮件和短信的方式第一时间通知管理员。

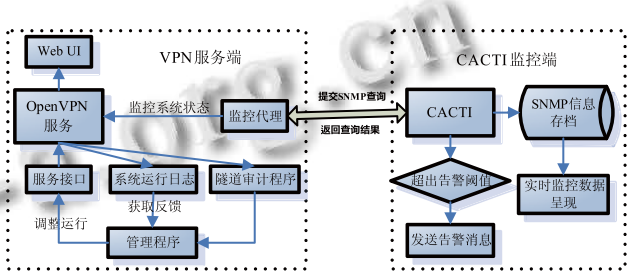

图 1　系统结构图

2.3　系统反馈调整

管理程序程序的处理流程如图 2 所示。

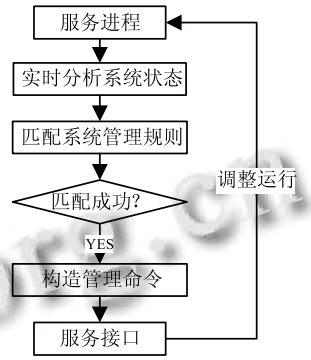

图 2　管理程序处理流程

管理规则在 XML 类型的文件中设定，用于定义用户行为规范，优化和调整系统运行。在系统运行过程中，管理程序读取这个文件获得系统管理规则并加以分析，将规则的触发条件与在线用户参数或者系统状态变量进行匹配，如果匹配成功，则根据规则的内容构造管理命令，发送至服务接口修改系统运行参数，调整服务进程的运行，实现自动系统管理。

例如需要对 UserA 用户实施如下访问控制：不允许与 UserB 和 UserC 之外的用户建立连接，不允许访问 10.10.0.0/16 这个网络中除 10.10.100.0/24 子网外的其他部分，允许访问 10.10.0.0/16 之外的其他网络，每

月下行总流量不得超过 5GB，上行总流量不得超过 2GB。

在规则库文件中设定如下规则：

```
/*================================*/
<User name=”UserA”>
<Rule name=’TC_1’ event=’TrafficControl’>
<period>monthly</period><download>5G</download><upload>2G</upload>
</Rule>
<Rule name=”AC_1” event=”AccessControl”>
<Clients action=“DENY“>
<Client>UserB</Client>
<Client>UserC</Client>
</Clients>
<Subnets action=“ACCEPT“ >
<Subnet>10.10.100.0/24</Subnet>
<Subnet action=“DENY“>10.10.0.0/16</Subnet>
</Subnets>
</Rule>
</User>
/*================================*/
```

当 UserA 用户建立隧道时，管理程序在规则库中识别出”TC_1”这条的规则，其事件属性为”TrafficControl”。于是管理程序对 UserA 用户隧道进行实时统计流量，将统计结果与规则中所设定的值进行比较，一旦不满足约束，将向管理接口发送”kill UserA”命令断开隧道。

接下来规则”AC_1”也被识别出来，其事件属性为”AccessControl”，于是查询 UserA 用户的隧道标识 CIDA，然后把规则转换为系统可识别的包过滤器：

```
/*================================*/
client-pf CIDA
[CLIENT DENY]
+UserB
+UserC
[SUBNETS ACCEPT]
+10.10.100.0/24
-10.10.0.0/16
[END]
END
/*================================*/
```

把上面的包过滤器提交到服务接口，系统将对 UserA 用户应用相应的访问控制策略。

通过在规则库文件中构造管理程序可理解的规则，可以灵活制定对用户的访问控制、连接流量和在线时间限制、证书的撤销和重建等服务接口所支持的策略，然后通过管理程序为系统自动实施这些策略。

2.4 实时监控

监控代理用于实现系统监控和告警功能，它包含两个进程，一个是数据采集进程，在固定时间周期内收集系统性能数据；另一个是 SNMP 代理进程，负责将系统性能属性注册到 MIB，暴露数据采集进程获取的数据，并响应来自 CACTI 的 SNMP 查询请求，返回所查询的监控数据。监控代理工作流程如图 3 所示。

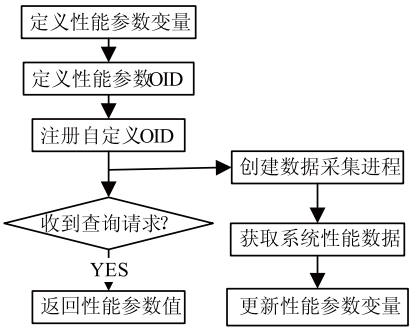

图 3 监控代理工作流程

首先定义所需监控的性能参数变量，创建两个私有 OID[10]结点：.1.3.6.1.4.1.1113.2.1 和.1.3.6.1.4.1.1113.2.2，分别对应服务端负载和服务进程性能数据集，然后在这两个 OID 结点下定义具体的性能参数子节点，把这些 OID 子节点与性能参数变量一一关联起来，注册到 SNMP 代理进程所维护的 MIB 树中，代理进程监听来自监控管理端的 MIB 查询请求，将对这些私有 OID 子节点的查询请求转化为对性能参数变量的访问。

数据采集进程通过周期性地在服务端运行操作系统命令返回的网络接口流量、磁盘利用率、CPU 和内存使用率负载信息，以及与系统管理接口交互得到的在线用户数、虚拟网络接口流量等服务进程信息，更新性能参数变量的当前值，同时将这些信息赋予对应的 OID 结点。这样，CACTI 监控管理端就可以通过 OID 标识周期性轮询性能信息，根据系统监控代理返回的结果，实时了解系统的运行状态。

3　系统测试与结果分析

实验在广域网环境中进行，首先在客户机安装 OpenVPN GUI，在连接配置文件中指定服务端的地址和端口，确保加密算法和认证方式与服务端一致，正常情况下可以看到在交换证书，服务端完成用户身份验证后客户机将获得对应权限的 IP 地址，从而以特定的内网身份访问内网资源。图 4 为实验的网络结构图。

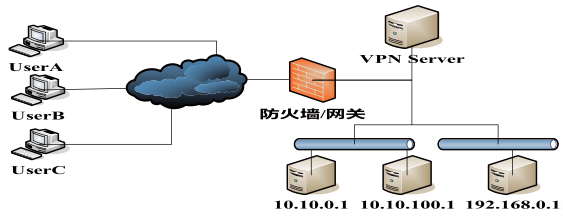

图 4　实验网络结构图

在客户机以 UserA 身份登录后，无法连接 10.10.0.1，也无法连接除 UserB 和 UserC 外的用户，可以连接 10.10.100.1 和 192.168.0.1，说明所设定的 ACL 规则已经起作用。

此时在 CACTI 上可以看到对应虚拟网络接口流量的变化，如图 5 所示。当 UserA 用户的累积流量达到所允许的上限时，服务管理程序将向系统发送命令撤销该隧道，客户端显示连接被断开，在图中可以看到随着该连接的断开，流量开始恢复正常水平。

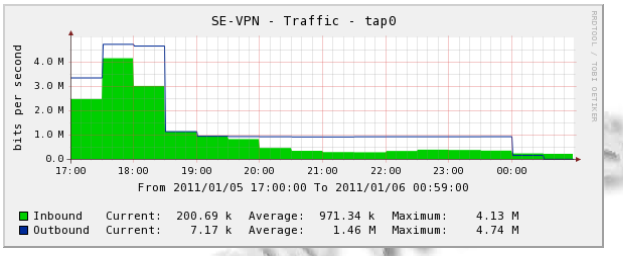

图 5　虚拟网络接口流量监控图

之后在客户机再次尝试以该用户身份登录，在识别用户身份后，服务管理程序根据审计数据库中的信息计算出该用户的可用流量小于等于 0，于是拒绝用户连接请求。在客户机上，会在通过验证后收到“连接失败”的消息，无法建立隧道。

图 6 为一个 VPN 用户组对应 IP 地址池的使用率，同时也反映了该用户组某一时段的在线用户数。如果使用率居高不下，甚至出现达到 100%的情况，CACTI 将通过阈值告警在使用率超过 95%时通知管理员检查系统的运行是否存在异常情况，必要时对地址池进行扩容；而如果使用率偏低，许多地址长时间闲置，就可以考虑缩小地址池的规模。

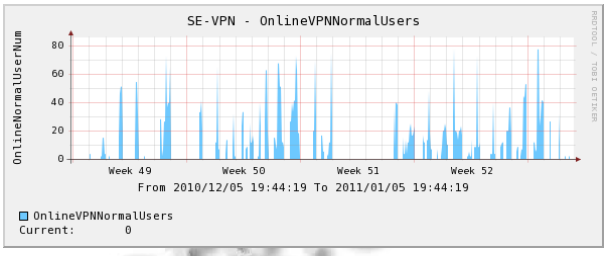

图 6　IP 地址池使用率

此外，管理员还可以根据监控图像所反映出来的系统负载变化规律，制定相应的规则应用到服务管理模块中，提高工作效率，使得系统能够根据自身状态及时做出相应调整，从而优化系统性能。

4　结语

针对规模庞大的 VPN 系统缺乏自动系统管理以及状态监控功能的缺陷，文章给出了基于 OpenVPN 和 CACTI 的 VPN 反馈调整和实时监控一体化实现方案，详细介绍了系统反馈调整和实时监控的实现方式，对特定的管理和监控应用情形，进行了验证性测试。结果表明系统能够根据预定义规则实现自动管理，同时通过监控代理实时反映自身状态，对系统重要性能参数进行监控和阈值告警。鉴于 OpenVPN 功能强大的服务接口，SNMP 丰富且可自定义的监控指标，无论在系统管理或是监控方面，系统都具有良好的扩展性。下一步要开展的工作，将为系统应用制定更全面的自动化管理策略，同时结合流量和包分析工具对来自 VPN 隧道的用户行为进行更细粒度的监控。

参考文献

1 黄勇,陈小平,潘雪增,陈红洲,蒋晓宁.基于 SNMP 的 VNP 集中管理若干关键技术研究.计算机工程与设计,2008,29(9):2186–2188,2400.

2 李明江.SNMP 简单网络管理协议.北京:电子工业出版社,2007,78–162.

3 Stevens WR, Wright GR. TCP/IP 详解(卷 1).陆雪莹,等译.北京:机械工业出版社,2000,270–292.

4 Yonan J. OpenVPN. http://openvpn.net

(下转第 66 页)

有相容答题状态进行比较后，分别求出它们相似概率，可知与 L2（00111）拥有最大相似概率的相容答题状态为 L23（10111），相容概率为 0.5288。即当受测者测试得到答题状态为（00111）时，我们认定他由于某些原因，在答题状态（10111）上出现了失误，答错了第 1 题，他的实际技能状态为（a,c,d,e）。

表 2　相容答题状态集

Li	$q_1q_2q_3q_4q_5$	θ	答题状态
L_0	00000	-1.2675	Φ
L_2	00011	-1.2800	{d,e}
L_8	01000	-0.4625	{b}
L_{10}	01010	-0.2215	{b,d,e}
L_{12}	01100	-0.2299	{b,c}
L_{14}	01110	0.6881	{b,c,d,e}
L_{15}	01111	1.5620	{b,c,d,e}
L_{16}	10000	-0.4625	{a}
L_{18}	10010	-0.2215	{a,d,e}
L_{20}	10100	-0.2299	{a,c}
L_{22}	10110	0.6881	{a,c,d,e}
L_{23}	10111	1.5620	{a,c,d,e}
L_{24}	11000	-0.4303	{a,b}
L_{26}	11010	0.4422	{a,b,d,e}
L_{28}	11100	0.4904	{a,b,c}
L_{30}	11110	1.4355	{a,b,c,d,e}
L_{31}	11111	2.4400	{a,b,c,d,e}

4　结论

本文结合扩展知识空间理论和认知诊断理论建立新的认知诊断模型，在认知诊断过程中，考虑到受测者的答题过程并不是完全理性的，通过计算“最大相似概率”来得到受测者的真实技能状态。根据项目反应理论中的方法可知，试题的技能结构可影响 IRT 模型中的公式结果，也就是影响相似概率，如何通过建立试题的技能结构提高诊断精度是本文未解决的问题。

参考文献

1 Doignon, JP, Falmagne JCL. Knowledge Spaces. Berlin: Springer Verlag,1999.50–55.

2 孙波,傅骞.扩展知识空间理论研究.中国电化教育,2004,(25)4:74–77.

3 刘艳花.基于扩展知识空间理论的技能自适应测试过程.计算机系统应用,2010,19(7):69–74.

4 林伯成.利用知识地图诊断数学问题之研究[硕士学位论文].台湾:中原大学资讯工程所,2002.

5 Steinberg L, Thissen D. Item response theory in personality research. Personality research, methods, and theory: A Festschrift honoring Donald W.Fiske. Hillsdals NJ: Lawrence Erlbaum Associates,1995,161–181.

6 胡麒,何华灿.基于试题空间的学习诊断方法.微计算机信息, 2007,23(10):238–240.

7 Albert D, Hockemeyer C, Wesiak G. Current Trends in e-Learning based on Knowledge Space Theory and Cognitive Psychology. Psychologische Beiträge, 2002,44(4):478–494.

(上接第 26 页)

5 赵林海,李晓风,谭海波.基于 CACTI 的分布式 ORACLE 监控系统的设计与实现.计算系统应用,2010,19(9):134–137,133.

6 Honser C.OpenVPN and the SSL VPN revolution. Sans Institute, 2004.

7 Yonan J. Understanding the User-Space VPN: History, Conceptual Foundations, and Practical Usage. Linux Fest Northwest, 2004.

8 郭学超,翟正军.OpenVPN 体系安全性研究.科学技术与工程,2007,7(8):1742–1745.

9 岑锐坚.使用 Cacti 监测系统与网络性能.开放系统世界,2006,(7):69–72.

10 Case J, McCloghrie K, Rose M, et al. Textual conventions for Version2 of the simple network management protocol (SNMPv2). RFC2579. IETF, 1999.