文章编号：1005-8451（2015）02-0022-06

基于正则表达式的防火墙安全配置核查方法研究

汤　飞
（中国铁道科学研究院　电子计算技术研究所，北京　100081）

摘　要：本文以铁路车站客票网防火墙为研究对象，提出了一种基于正则表达式的防火墙安全配置核查方法。此方法使用正则表达式匹配代替人工评判，提高了核查的效率；同时，该方法的安全配置基于信息安全国家标准要求和实际业务需求制定，降低了核查的主观性。

关键词：防火墙；配置；配置核查；正则表达式
中图分类号：U29-39　**文献标识码：**A

Method of firewall configuration checking based on Regular Expression

TANG Fei
(Institute of Computing Technologies, China Academy of Railway Sciences, Beijing　100081, China)

Abstract: This paper proposed a method based on Regular Expression to check configurations through studying firewalls in TRS network of railway station. The method adopted Regular Expression matching instead of manual judging, made checking process more efficient. In addition, configuration checking lists were made based on national standards of information security and practical requirements of TRS network, which made checking process less subjective.

Key words: firewall; configuration; configuration checking; Regular Expression

防火墙安全配置是防火墙执行访问控制功能依据的规则集合，可分为安全策略配置和安全管理配置。其中，安全策略配置是防火墙决定网络数据是否通过的规则集合[1]，它从数据报文安全层面为信息系统安全提供保障，防止网络数据威胁信息系统安全。安全管理配置指定防火墙工作和管理方式，是防火墙运行和维护时应遵循的规则集合[2]，它从设备管理安全层面为信息系统安全提供保障，避免防火墙自身安全问题威胁信息系统安全。作为保护信息系统安全的重要手段，防火墙自身的安全核查和测评也应得到验证。

1　问题提出

随着国家信息安全等级保护工作的推进，需对信息系统安全等级实施测评和定级。铁路客票系统作为涉及社会公共秩序的计算机系统，是国家信息安全等级保护第四级要求确定的系统，它在逻辑上分为铁路总公司级安全域、地区级安全域、车站级安全域，不同安全区域间通过防火墙等设备实现安全区域边界防护[3]。为验证铁路客票系统安全保护能力，需对防火墙开展安全配置核查工作，从配置制定和配置实施两个层面进行检查分析。在配置制定层面，需检查分析防火墙安全配置是否合理、完备；在配置实施层面，需实地核查防火墙是否启用配置。

传统上，防火墙配置核查多采用基于人工评判的 Web 界面配置核查方法，该方法需人工判断，且无法深入底层对防火墙配置进行全面核查。另外，也有人采用基于人工评判的命令行配置核查方法，该方法解决了不能查看防火墙底层配置的缺陷，但复杂防火墙命令对核查人员提出了较高的技术要求，而以上方法对待查安全配置结果的认定会受到核查人员主观意识和工作经验的制约，不一定具有合理性和完备性。Gawanmeh 等人曾研究了一种使用域限制 (domain restriction) 技术模拟和验证防火墙规则的方

收稿日期：2014-10-08
作者简介：汤　飞，在读硕士研究生。

法[4]，通过查看防火墙的反应以核查其安全配置，但该方法需要搭建复杂的测试环境且工作量大。

本文以铁路客票系统车站级安全域 H3C 防火墙为研究对象，依据等级保护要求和客票业务需求，引入正则表达式，提出了一种基于正则表达式的防火墙安全配置核查方法。

2　正则表达式

2.1　正则表达式简介

正则表达式是一种字符串，擅长操纵字符序列和处理结构化数据[5]。它由代表特定含义的元字符及其组合构成，这些元字符及其组合按照一定的语法规则结合起来，来表达对字符序列的过滤匹配逻辑。

如“\d”、“\s”、“\w”为 3 个不同的元字符，分别表示任意一位数字字符、任意一个空格或回车或换行符、任意一个可构成单词的字符。可以分别使用“\d\d\d\d”表示任意相连的四位数字，“\d\w\w\w\d”表示第 1 位及最后 1 位为任意数字、中间 3 位为任意可成单词字符的长度为 5 的字符序列。

2.2　正则表达式功能及应用

正则表达式的主要功能是字符（或序列）匹配，其使用可分为 3 个环节：输入、处理和输出。输入环节的输入内容包括两部分：描述预期字符或字符序列的正表达式、待处理字符序列；处理环节是正则表达式引擎依据输入的正则表达式代表的句法规则，对另一输入—待处理字符序列进行匹配过滤的过程；输出环节是将处理环节产生的结果输出，输出内容为包含在待处理字符序列中满足句法规则的字符或字符序列。正则表达式的主要应用对象是文本，它在基于文本的编辑器和基于文本的搜索工具中应用广泛。

2.3　正则表达式与配置核查

在基于人工评判的防火墙安全配置核查过程中，核查人员依据防火墙的展示信息，确定核查结论。若将该过程的参与要素抽象为核查人员、防火墙展示信息和核查结论，那么可将核查人员和防火墙的展示信息视为该过程的输入，核查人员对展示信息的评判视为该过程的处理，核查结论的确定视为该过程的输出，如图 1 所示。

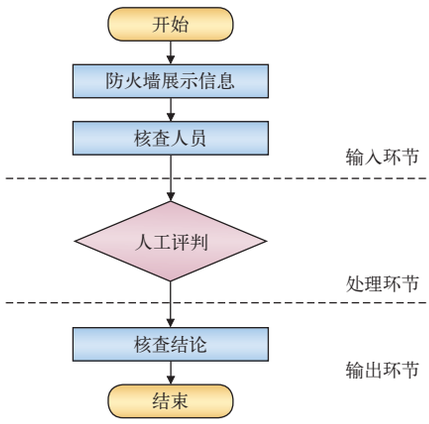

图1　基于人工评判的防火墙配置核查过程

可以发现，上述核查过程与正则表达式的使用过程类似。

由此，不妨将正则表达式引入配置核查过程，使用预先编制好的正则表达式代替核查人员，对防火墙的展示信息进行自动匹配评判，免去人工评判工作，提高核查效率。

3　防火墙安全配置要求

安全配置是防火墙发挥网络安全防护功能的关键。防火墙依据自身安全配置，执行访问控制功能，允许符合规则的正常数据流通过，拒绝不符合规则的非正常数据流通过。

传统的安全配置基于核查人员知识水平和工作经验得出，具有明显的个人主观性和不规范性。本文从国家标准要求和业务需求出发，提出对防火墙的安全配置要求。

3.1　信息安全等级保护要求

信息安全等级保护国家标准 GB/T 28448-2012[6] 及 GB/T 22239-2008[7] 第 3 级要求，从访问控制、安全审计、网络设备防护、备份和恢复 4 个方面对防火墙的安全能力作出了规定。《标准》对防火墙的安全能力提出了以下要求。

3.1.1　访问控制

防火墙依据安全策略允许或拒绝数据报文通过；能对应用层协议如 HTTP 进出网络的信息内容进行过滤；对已连接的会话应在其处于非活跃状态一段时间或会话结束后终止连接；应限制网络最大流量数和网络连接数；采取措施如 IP/MAC 绑定防止地

址欺骗；对受控资源的访问按用户和系统之间的允许访问规则进行；对进入内网的用户数进行限制。

3.1.2 安全审计

防火墙应对设备的运行状况、网络流量、用户行为等进行日志记录；审计记录应包括事件的时间和日期、用户、事件类型、事件是否成功等信息；能够进行审计数据分析并生成审计报表；应采取措施对审计记录加以保护以防止未预期的删除、修改、覆盖。

3.1.3 网络设备防护

防火墙应对登陆用户进行身份鉴别；限制管理员登陆的 IP 地址；不允许出现共享账号；重要防火墙应采用组合鉴别技术进行身份鉴别；鉴别信息应具有不易被冒用的特点；具备登陆失败处理功能；远程管理应采用 SSH、HTTPS 等加密协议防止鉴别信息被窃听；不同类型管理员仅分配业务需要的最小权限。

3.1.4 备份和恢复

应定期对防火墙的配置文件进行备份以防止防火墙因意外导致策略丢失影响系统正常运行；主要的防火墙设备，应提供硬件冗余，保证系统的高可用性。

3.2 铁路客票系统业务需求

铁路车站客票网防火墙，部署于车站客票网边界，对铁路局中心客票网与车站客票网间的交互数据执行检查过滤。车站客票网与铁路局客票网的部署结构如图 2 所示 [8]。

铁路局中心客票网与车站客票网间存在数据交互的业务有 [9]：

（1）车站窗口售票业务：包括窗口售票终端执行售票、退票、废票、换票、改签、互联网取票、财务统计等。

（2）车站自动售票业务：包括在自动售票机上旅客自助购票和电子票取票。

（3）车站检票业务： 包括铁路局中心向本站闸机下发检票计划，闸机上传检票信息至铁路局检票服务器。

（4）车站补票业务 [10]：包括车站到站补票，收入统计，结账等。

3.3 铁路车站级安全域防火墙安全配置内容

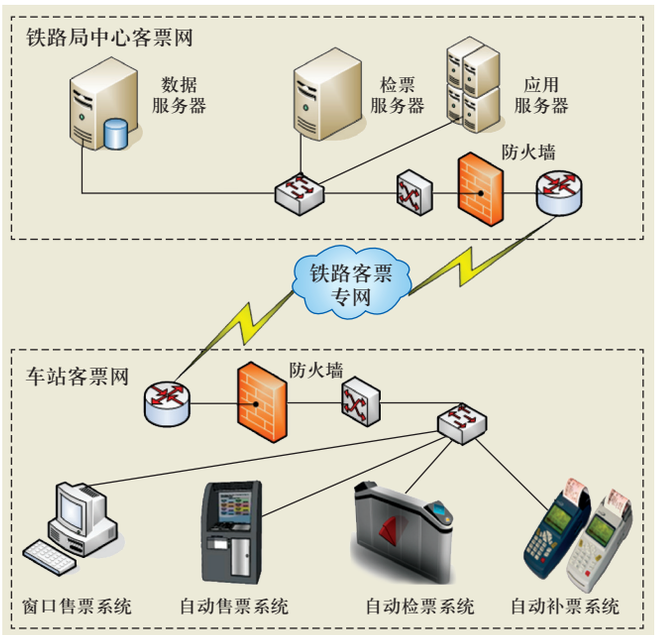

图2 车站与铁路局客票网部署示意图

按照上述等级保护要求及铁路客票网业务需求，总结出防火墙安全配置内容如下。

3.3.1 访问控制

（1）开启默认禁止策略，默认禁止未明确规定的数据通过；

（2）开启常用应用层协议如 HTTP、FTP 等的过滤策略；

（3）启用会话超时自动断开连接策略；

（4）启用最大流量数及最大连接数限制；

（5）重要应用启用 IP/MAC 地址绑定策略；

（6）支持并启用用户与资源的允许访问规则，特定用户只能访问特定资源；

（7）限制具有拨号访问权限的用户数。

3.3.2 安全审计

（1） 启用对防火墙自身运行状态、网络流量、用户行为的日志审计策略；

（2）审计记录应包括：事件日期、事件时间、用户、事件类型、事件成功状态等；

（3）能够对审计日志数据进行分析，生成审计报表；

（4）启用审计记录保护策略，防止日志受到未预期的删除、修改或覆盖。

3.3.3 网络设备防护

（1）对登陆防火墙的用户进行身份鉴别；

（2）启用防火墙登陆地址限制策略；

（3）防火墙用户标识名唯一；

（4）重要防火墙采用组合鉴别技术进行身份鉴别；

（5）身份鉴别信息应不易被冒用，口令满足复杂度要求，并定期更换；

（6）启用登陆失败处理功能，多次登陆失败锁定账号、网络连接超时自动退出；

（7）采用加密的 SSH 或 HTTPS 等协议进行远程管理，防止鉴别信息被窃听；

（8）为不同管理用户分配满足业务需求的最小权限，实现特权用户权限分离。

3.3.4　备份和恢复

（1）启用防火墙配置备份策略，定期对防火墙配置进行备份；

（2）重要防火墙启用硬件冗余策略，实现双机热备。

3.3.5　业务需求配置

若 3.2 中窗口售票、自动售票、自动检票及到站补票业务执行时，业务数据的参数如表 1 所示。

表1　铁路客票网不同业务数据参数

参数类型 / 业务类型	源 IP	源端口	目的 IP	目的端口	协议类型
窗口售票	src_ip_1	src_port_1	dst_ip_1	dst_port_1	protocol_1
自动售票	src_ip_2	src_port_2	dst_ip_2	dst_port_2	protocol_2
自动检票	src_ip_3	src_port_3	dst_ip_3	dst_port_3	protocol_3
到站补票	src_ip_4	src_port_4	dst_ip_4	dst_port_4	protocol_4

则防火墙应新增 4 条安全策略配置规则，允许符合上表描述的数据报文通过。

4　基于正则表达式的防火墙安全配置核查方法

4.1　传统防火墙安全配置核查方法

传统防火墙安全配置核查方法分为基于人工评判的 Web 界面配置核查方法和基于人工评判的命令行配置核查方法。

在前者中，核查人员登入防火墙 Web 管理界面，以查看 Web 页面的方式，对待查安全配置予以核查确认。该方法原理简单、易于操作，但不能深入底层对防火墙配置进行全面核查。

在基于人工评判的命令行配置核查过程中，核查人员登入防火墙，输入防火墙命令，依据防火墙返回的提示信息，判定防火墙当前的配置状况。该方法从开发级深度，深入底层对防火墙配置进行全面核查，核查过程如图 3 所示。

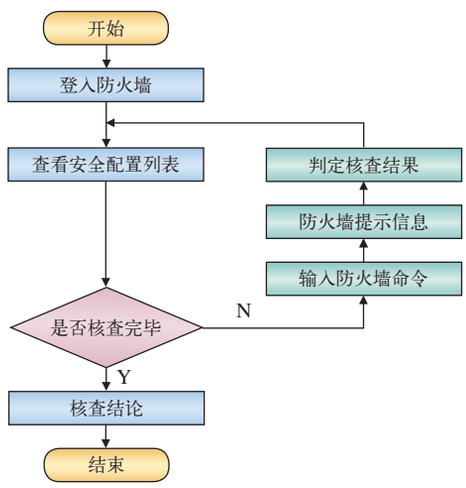

图3　基于人工评判的命令行配置核查过程

4.2　基于正则表达式的防火墙安全配置核查方法

类似于图 3 所述过程，若将配置查看命令提交远程防火墙执行，然后使用预设正则表达式对防火墙提示信息进行匹配，由匹配结果便得核查结果。这即为基于正则表达式的安全配置核查方法的基本思路。

安全配置、防火墙命令、正则表达式是该方法的 3 要素。安全配置为核查提供核查条目，是核查过程的指导和依据；防火墙命令为核查提供实施指令，是核查工作执行的承载者；正则表达式为核查判定结果，是核查结论的确立者。

在该方法的实施过程中，可将安全配置对应的防火墙命令和正则表达式保存于本地，逐条取命令提交远程防火墙执行，然后使用正则表达式对防火墙的返回信息予以匹配，依据匹配结果得出核查结果。

若将上述实施过程程序化，则核查人员只需事先将安全配置对应的防火墙命令和正则表达式作为参数输入程序，之后便可不做任何人工干预，程序即能一次性完成配置核查工作，从而极大提高核查工作的效率。基于正则表达式的配置核查模型如图 4 所示。

在该模型中，安全配置是防火墙命令和正则表达式完成配置核查过程的基准和依据，防火墙命令和正则表达式是实现配置核查过程的手段和方法。

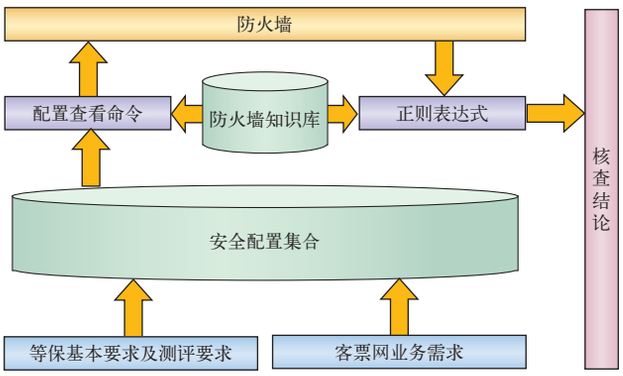

图4 基于正则表达式的配置核查模型

4.3 基于正则表达式的防火墙安全配置核查内容

将 3 要素逐一总结（正则表达式为配置符合要求时的匹配规则），得到基于正则表达式的配置核查内容如下[11]。

4.3.1 访问控制

依据 3.3 中访问控制的各项要求，得到对应配置核查内容如表 2 所示。

表2 防火墙访问控制类配置核查内容

安全配置	防火墙命令	正则表达式
（1）未明确规定的数据默认禁止通过	display current-configuration	(\#\s*(.*\s*)*)*firewall\s*packet-filter\s*default\s*deny(\#\s*(.*\s*)*)*
（2）开启应用层协议的过滤策略	display aspf all	Detect\s+protocols:\s+http(\s|.)*ftp(\s|.)*
（3）设置会话超时断连策略	idle-timeout minutes	.*
（4）设置最大流量及最大连接数限制	Display domain	\bAccess-limit\s+=\s+Enable\b
（5）启用 ip/mac 绑定策略	display firewall mac-binding item statistic	.+\s*.+\s*((([1-9]?|1\d)\d|2([0-4]\d|5[0-5]))\.){3}(([1-9]?|1\d)\d|2([0-4]\d|5[0-5]))\s*(.*\s*)*
（6）启用用户与资源的允许访问规则	super level	(.+\s+)+
（7）限制拨号权限用户数	modem call-in	.*

4.3.2 安全审计

依据 3.3 中安全审计的各项要求，得到对应配置核查内容如表 3 所示。

4.3.3 网络设备防护

依据 3.3 中网络设备防护的各项要求，得到对应配置核查内容如表 4 所示。

4.3.4 备份和恢复

依据 3.3 中备份和恢复的各项要求，得到对应配置核查内容如表 5 所示。

表3 防火墙安全审计类配置核查内容

安全配置	防火墙命令	正则表达式
（1）对防火墙运行状态、网络流量、用户行为进行审计	display firewall statistic system	(.*\s*)*
（2）审计记录包括事件日期、时间、内容等信息	display firewall statistic system	(.*\s*)*
(3) 可生成审计报表	display logbuffer summary	EMERG\s+ALERT\s+CRIT\s+ERROR\s+WARN\s+NOTIF\s+INFO\s+DEBUG
(4) 启用审计记录保护措施	info-center loghost ipAddr	.*

表4 防火墙网络设备防护类配置核查内容

安全配置	防火墙命令	正则表达式
(1) 对登陆用户进行身份鉴别	authentication-mode password	\bauthentication-mode\s+[^none]
(2) 限制登陆防火墙的 ip 地址	display acl acl-number	rule\s+\d+\s+permit\s+source\s+\d+\.\d+\.\d+\.\d+\s+\d+\.\d+\.\d+\.\d+
(3) 用户标识名唯一	local-user user-name	\w*
(4) 启用组合鉴别技术	super authentication-mode scheme	\w*
(5) 登陆口令满足复杂度要求	set authentication password cipher password 、local-user password-display-mode cipher-force	.*、.*
(6) 启用登陆超时锁定、网络超时断开连接策略	idle-timeout 、modem timer answer seconds 、ssh server timeout seconds	.*、.*、.*
(7) 设置使用加密协议进行远程管理	protocol inbound ssh	(.|\s)*
(8) 实现不同级别用户权限分离	display users all	Userlevel\s+.+\d+

表5 防火墙备份和恢复类配置核查内容

安全配置	防火墙命令	正则表达式
(1) 启用防火墙配置文件备份策略	display vrrp	(.|\s)*
(2) 重要防火墙启用双机热备策略	display rdo	.+\s+1\s*backup\s+\d+Ethernet.*\s*(\w*\s*)*

4.3.5 业务需求策略

依据 3.3 中业务需求配置的要求，将表 1 中代表不同数据包类型的数值 1、2、3、4 以 X 替代，得到对应配置核查内容如表 6 所示。

表6 防火墙业务需求类配置核查内容

安全配置	防火墙命令	正则表达式
(1) 允许满足窗口售票、自动售票、自动检票和到站补票业务需求的数据流通过	display acl acl-number_X	(.+\s+)+rule\d+permit\s+protocol_X\s+source\s+src_ip_X\s+0\.0\.0\.0\s+destination\s+dst_ip_X\s+0\.0\.0\.0\s+source-port\s+eq\s+src_port_X\s+destination-port\s+eq\s+dst_port_X\s*(.*\s*)*

5　结束语

本文依据信息安全等级保护标准要求，以铁路车站客票网防火墙为研究对象，提出了一种基于正则表达式的安全配置核查方法，该方法同样可以推广应用于其他网络安全设备的配置核查工作，为信息安全等级保护配置核查工作的开展提供了一种新的思路。

参考文献：

[1] 任展锐 . 防火墙安全策略配置关键技术研究 [D] . 长沙：国防科技大学，2011.

[2] 杜　雨 . 防火墙远程配置管理系统的设计与实现 [D]. 成都：四川大学，2006.

[3] 祝咏升，丁　妍，张　彦 . 铁路客票系统信息安全技术方案设计 [J]. 铁道科学与工程学报，2012，9（5）：119–124.

[4] Gawanmeh Amjad，Tahar Sofiène. Modeling and verification of firewall configurations using domain restriction method [C]. 2011 International Conference for Internet Technology and Secured Transactions，Abu Dhabi United arab emirates，2011.

[5] Broberg Niklas, Farre Andreas, Svenningsson Josef. Regular expression patterns [C]. Proceedings of the Ninth ACM SIGPLAN International Conference on Functional Programming，Snowbird UT United states，2004.

[6] 中华人民共和国国家质量监督检验检疫总局，中国国家标准化管理委员会 . GB/T 28448-2012，信息安全技术—信息系统安全等级保护测评要求 [S]. 北京：中国标准出版社，2012.

[7] 中华人民共和国国家质量监督检验检疫总局，中国国家标准化管理委员会 . GB/T 22239-2008，信息安全技术—信息系统安全等级保护基本要求 [S] . 北京：中国标准出版社，2008.

[8] 中国铁道科学研究院电子计算技术研究所 . 京沪高速铁路客票系统实施方案 [Z] . 北京：中国铁道科学研究院电子计算技术研究所，2011.

[9] 张　彦，史天运，李仕达，李　超 . AFC 技术及铁路自动售检票系统研究 [J] . 中国铁路，2009，1（3）：50-55.

[10] 方　凯 . 铁路客运车站补票系统的设计与实现 [J]. 交通运输系统工程与信息，2008，8（5）：124–128.

[11] 华三通信技术有限公司 . H3C SecPath 系列安全产品命令手册 [Z]. 杭州：华三通信技术有限公司，2009.

责任编辑　方　圆

（上接 P21）

内部均维护一个数据采集线程池。通过线程池集中管理采集线程。采集线程在并发执行的过程中，根据某些业务的需要，需要进行线程间同步，在同步过程中要清晰标识临界资源，采用同步锁、临界区、信号量、条件变量及事务等技术手段保障同步逻辑准确无误，避免死锁或因同步带来的性能下降等问题 [5]。

3　平台特点

（1）监控范围广，全面涵盖物理安全的各个方面。（2）实现了对物理安全隐患及时、有效的监控及处理，提升信息安全防护水平。（3）报警准确及时，误报率低，免维护性强。（4）采用良好的架构设计，具有良好的扩展性与使用性。（5）平台拥有开放性，支持与第三方系统互联互通。（6）平台采用专业设备远程监控单元（RMU），实现现场总线组网。（7）平台采用无代理、非侵入方式进行设备监控。

4　结束语

物理安全监控平台已经初具规模，关键设备—远程监控单元（RMU）已经成功研发并投入实际应用。随着平台功能的不断完善与推广应用，在日常的机房管理工作中，必将发挥越来越重要的作用，成为广大管理人员的得力助手，显著提高管理工作的质量与效率。

参考文献：

[1] 中华人民共和国国家质量监督检验检疫总局，中国国家标准化管理委员会 . GB/T 21052-2007，信息安全技术—信息系统物理安全技术要求 [S]. 北京：中国标准出版社，2007.

[2] 中华人民共和国国家质量监督检验检疫总局，中国国家标准化管理委员会 .GB/T 22239-2008，信息安全技术—信息系统安全等级保护基本要求 [S]. 北京：中国标准出版社，2008.

[3] 中华人民共和国工业和信息化部 .GB50174-2008，电子信息系统机房设计规范 [S]. 北京：中国标准出版社，2008.

[4] 王　平，靳智超，王　浩 .EPA 工业控制网络安全测试系统设计与实现 [J]. 计算机测量与控制，2009,17（11）：2153-2155.

[5] 周　坤，傅德胜 . 基于 Windows Socket 的网络数据传输及其安全 [J]. 计算机工程与设计，2007，28（22）：5381-5386.

责任编辑　方　圆