CISCO

ciscopress.com

网络安全体系结构

Network Security Architectures

Expert guidance on designing secure networks

〔美〕**Sean Convery**，CCIE #4232 著
田果，CCIE #19036
刘丹宁，CCIE #19920 译

人民邮电出版社
POSTS & TELECOM PRESS

ciscopress.com

网络安全体系结构

Network Security Architectures

〔美〕Sean Convery，CCIE #4232 著
[illegible]，CCIE #19036 译
[illegible]，CCIE #19920

人 民 邮 电 出 版 社
北 京

图书在版编目（CIP）数据

网络安全体系结构 /（美）康维（Convery, S.）著；
田果，刘丹宁译. -- 北京：人民邮电出版社，2013.1
ISBN 978-7-115-29818-8

Ⅰ. ①网… Ⅱ. ①康… ②田… ③刘… Ⅲ. ①计算机网络－安全技术 Ⅳ. ①TP393.08

中国版本图书馆CIP数据核字(2012)第255979号

版 权 声 明

网络安全体系结构

◆ 著 [美] Sean Convery，CCIE #4232
译 田果，CCIE #19036 刘丹宁，CCIE #19920
责任编辑 傅道坤

◆ 人民邮电出版社出版发行 北京市崇文区夕照寺街 14 号
邮编 100061 电子邮件 315@ptpress.com.cn
网址 http://www.ptpress.com.cn
北京艺辉印刷有限公司印刷

◆ 开本：800×1000 1/16
印张：44.25
字数：942 千字 2013 年 1 月第 1 版
印数：1－2 500 册 2013 年 1 月北京第 1 次印刷

著作权合同登记号 图字：01-2011-7832 号
ISBN 978-7-115-29818-8

定价：118.00 元

读者服务热线：(010)67132692 印装质量热线：(010)67129223
反盗版热线：(010)67171154

内容提要

本书是一本安全网络的设计指南，旨在帮助读者设计出符合可满足不同安全需求的网络环境。

全书共分为 4 个部分和 3 个附录。第一部分介绍了设计安全网络的一些基础概念，提供了设计安全网络的先决条件以及进行安全网络设计所需的基本元素，为后续章节打下基础。第二部分全面讨论了可供安全设计人员使用的各类技术，以及使用不同技术来设计网络安全解决方案时需要予以考虑的因素。第三部分针对不同的网络环境，介绍了它们各自的设计方式。第四部分介绍了如何保障网络管理的安全性，同时对一些设计案例进行了研究，最后对全书做了总结。附录 A 对书中使用过的一些术语进行了介绍。附录 B 提供了各章测试题的参考答案。附录 C 则提供了安全网络设计中，一些设计文档的起草范例。

鉴于本书强调安全网络的“设计”，因此本书的主要目标群体是网络安全领域的售前工程师和企业网络的运维人员。此外，本书同样适合其他网络/安全操作工程师、IT 经理和 CIO 及各类对网络安全感兴趣的专业人士阅读和参考。

关于作者

Sean Convery，CCIE #4232，是 Cisco 公司 VPN 和安全业务部门的安全架构师，专注于新的网络安全技术的研究。他已在 Cisco 工作了 6 年，其中最为引人瞩目的工作是担任了最初 Cisco SAFE 安全蓝图的首席架构师，并且还是其中数个白皮书的作者。在 Cisco 工作时，Sean 曾为全球数以千计的 Cisco 客户进行了网络安全设计，并为很多不同网络规模的客户提供了安全设计方面的咨询。在加盟 Cisco 之前，Sean 已在 IT 和安全咨询公司有过 12 年的网络行业工作经验，并且担任过各种不同的职位。

在思考网络安全问题之余，Sean 喜欢使用（机动或非机动的）两轮交通工具与家人远足，并且喜欢几乎所有水上、水中或水下运动。

关于技术审稿人

Qiang Huang，CCIE #4937，是 Cisco 公司 WWW 安全服务实践团队的网络咨询工程师。他的主要职责是为客户进行安全状况评估、安全设计检查以及提供其他安全服务。在此之前，Qiang 在 Cisco 公司技术支持部门（TCA）的 VPN 和网络安全团队中担任技术主管。Qiang 对很多安全产品和技术都有着丰富的经验，包括防火墙、VPN、IDS 和身份认证系统。Qiang 拥有 ISP、路由交换以及安全 3 个 CCIE 证书。Qiang 拥有科罗拉多州立大学电子工程专业的硕士学位。

Jeff Recor 目前是 Olympus Security Group，Inc.的董事长和首席执行官，负责为大型客户提供安全战略、投资回报和风险转移方面的咨询。作为 Nortel Networks 全球专业服务安全部门的前任全球主管，Jeff 负责开发一套国际性的服务，以满足不断发展的系统安全和网络设计需求。Jeff 有大约 18 年为公司提供安全和网络设计咨询的经验。他的经历包括：在担任 Holtzman & Silverman 的 MIS 主管期间，他领导的一个自动化项目获得了密歇根州的最佳技术应用奖；在担任 Netrex 的 PSO 主管期间，他白手起家创建了一个为全球财富 500 强公司提供支持的安全咨询机构；在担任 Sargon Group, Inc.总裁期间，他成功打造并出售了（卖给 Nortel Networks）一家领先的安全服务公司。Jeff 是 Walsh College 的副教授（是新创建的信息保障学院的院长），同时也是安全和网络技术领域的作家和讲师。Jeff 已为全球多家组织机构讲授了很多安全方面的主题。他还发表了数篇论文，并且编写了三本书：*Realizing the Virtual Private Network*、*Information Systems Security* 和一本有关 Educause 提出的安全论题的专著。很多会议（比如 Gartner CIO 峰会和 CA World）都曾邀请他讲述有关网络安全方面的主题。Jeff 还是 ITAA 下属一个委员会的主席，是 COMPTIA Security + Certification 委员会的核心成员，是 FBI Infragard 计划的顾问，是 IT-ISAC 的赞助人之一，并且是 Partnership for Critical Infrastructure Protection 的委员。Jeff 已获得密歇根州立大学的学士学位，并于 2003 年从凤凰城大学获得硕士学位。他还获得了 CISSP 和 CISA 认证，目前他同时任职于两家不同的两个董事会。

Russell Rice 是 Cisco 公司 VPN 和安全业务部的技术销售经理，专注于新系统安全规划并为 SAFE 网络安全最佳做法设计指导方针。Russell 在网络安全技术方面有着 8 年的工作经验，包括在 Cisco 期间以及在 Global Internet 担任工程主管的经验。

1988 年从 UC Berkeley 获得计算机科学的学士学位后，Russell 在 ABB、Dow Jones 和 Garmer's

Den 先后工作了 7 年，分别任混合工程（assorted engineering）、营销和管理职务。Russell 是安全研讨会（包括 Networkers，他曾获得该会议的多个奖项）上 Cisco 公司的常客。

Roland Saville 是 Cisco 公司企业解决方案工程部的技术销售工程师。他在 Cisco 的 9 年间曾参与了各种安全项目，包括开发和扩展 SAFE 蓝图、对产品销售员工的支持，并提供路线图、战略和缺陷分析方面的公司间反馈。从 2003 年 7 月开始，他曾参与无线、IP 电话通讯和视频智能方面的项目。Roland 拥有 Santa Clara 大学的 MBA 学位，现居住在 Boca Raton。

献　　词

谨将此书献给我的妻子 Monica，我的女儿 Mia。没有她们的耐心，本书绝不可能问世。

还要感谢我刚出世的儿子 Ronan，没有他的到来，我今天可能仍在写作此书。

致　谢

如果没有很多同事以及 IT 行业内几位同仁在幕后的辛勤努力，就不会有本书。

我要特别感谢以下同仁：Bernie Trudel 为本书的筹划作出了贡献；Russell Rice 在本书的早期提供了很多的帮助，并且在我需要成熟的看法时随时为我提供意见；Steve Acheson 审核了本书的部分章节；Michele Guel 为第 2 章提供了建议；Mike Schiffman 审核了第 3 章；Dan Wing 对第 6 章中 NAT 部分提供了一些建议；Marco Foschiano 简直是第 2 层方面的百科全书；Darrell Root 为 DHCP 过滤提供了的示例；Rob Thomas 的网站非常值得推荐；John Bartlomiejczyk 对 DHCP 攻击进行了测试；Eliot Lear 审核了第 8 章；Jeff Hillendahl 提供了 AAA 的最佳做法；Mike Sullenberger 对第 10 章 IPSec 部分的内容作出了重要贡献；Barbara Fraser 帮我解决了 IETF 和 IPSec 的许多问题；Darrin Miller 为第 11 章作出了贡献，同时还对其他章节进行了认真的审核，Ross Anderson 则对本书提出了很多反馈意见，并为本书撰写了序言。

另外，我还要感谢过去 6 年中与我共同工作过的 Cisco 公司的所有同事。非常感谢我的 SAFE 蓝图合作者：Roland Saville、Jason Halpern、Bernie Trudel（再次感谢）、Darrin Miller （再次感谢），以及所有对 SAFE 作出过贡献的同仁。同样，我还要感谢在我写作此书时的诸位经理：Steve Collen、Ken Watson 和 Robert Gleichauf。还要感谢 Jim Ring 和 Brian Waller，是他们把我招进了 Cisco 公司，并在我转行成为公司内一名全职安全技术人员时给予了理解。感谢 Matthew Franz 和 Eloy Paris，他们有时候会在不知不觉中回答许多与本书相关的问题。

非常感谢我的几位主要技术审校人员：Russell Rice、Jeff Recor、Roland Saville 和 Qiang Huang，他们总是能够及时为我提出宝贵意见，如果没有他们的悉心审校，很难想象本书会是什么样子。

要特别感谢 Cisco Press 的同仁，他们在我一开始多次失败之后仍然给与了我信任。感谢 Michelle Grandin、Dayna Isley 和 Tammi Ross，他们分别使我按时、按要点和按合同完成了本书。特别感谢我的开发编辑 Grant Munroe，他对本书结构的洞察力和建议使本书在内容组织方面增色不少，同时还得感谢他允许我偶尔在书里开点无伤大雅的玩笑。我还想感谢 Patrick Kanouse 在本书最后准备印刷阶段所提供的帮助。

感谢 Topher Hughes 向我推荐 Miles Davis 的 Kind of Blue 作为工作时调节情绪的音乐。最后一次查看 MP3 播放器时，我发现这张 CD 我一共听了 39 遍。

感谢 Mike McManus 和 Chris Lawrence，他们分别为我提供了第一份计算机工作和第一份 IT 工作。

十分感谢 Michael Lucas 为我提供了一个可以确保本书能够按时完成的简易公式。

我要感谢在过去数年中我为之提供设计指导方针的所有企事业机构。我从你们那里轻松学到的东西与你们从我这里得到的一样多。

感谢在我写作本书期间很少见到我和听到我声音的所有家人和朋友。尤其要感谢我的母亲，她校对了我的学位论文，并督促我尽力做到最好。另外，还要感谢我的父亲，他使我开阔了眼界，并且总是在我需要他帮助的时候出现在我身边。

我最后要郑重感谢我的爱妻 Monica 和宝贝女儿 Mia。Monica 为不使我分心，承担了整个家庭的重担，要知道在我写作本书期间，她正有孕在身。非常感谢 Mia 在听到我说“我仍有工作要做”时很有耐心并且不是十分生气。我希望“爸爸正在工作”不再成为她的口头禅。

Cisco 公司关于 SAFE 蓝图和网络安全架构的说明

随着 Cisco 公司拓宽它的安全产品组合，并开始深化其路由器和交换机平台上可用的安全服务，Cisco SAFE 蓝图也开始启动。它的目标是当工程师设计或扩展网络以期解决网络中现存的威胁，以及不断出现的挑战时，能够主动描绘出安全方面的最佳做法，以帮助网络及安全架构师和实施人员完成他们的工作。SAFE 的核心由技术白皮书（列举出威胁）、缓解技术、网络功能模块化思想，以及大量示例设计和配置所组成。

Sean Convery 是原始 SAFE 蓝图的主要推动者，他参与的工作包括概念的制订、加固安全性需要考虑的因素、网络的扩展，以及 Cisco 发布的首批关键白皮书的编纂。SAFE 白皮书今天能够获得 100 多万次的下载，并在安全团体中得到广泛接受，很大程度上是由于他最初的努力。

本书旨在从实用的角度来描述安全网络的设计方法，这可以确保本书的内容直击要害、切合题旨并且方便实用。在本书中，Sean 大量扩充了 SAFE 白皮书中的基本信息。本书全面地提供了实际安全生命周期的考量因素、缓解技术与各种威胁的评估方式、设计时需要进行考虑的详细因素，同时还为示例中所使用的安全策略与技术提供了替代方案。

Russell Rice

产品营销经理

新系统安全技术

2004 年 2 月

序

现今，诸多公司投入大量 IT 预算用于网络安全经费。因 Internet 恐慌所致，业务成本成倍增加。

传统 IT 安全方面的书籍业已被现实世界甩在身后。机密性、完整性、可用性的次序亦被颠覆。DDoS 攻击使可用性的地位达到顶峰。而这些利用他人系统而非自身系统漏洞所发起之攻击又将如何解决？

传统的加密书籍也已捉襟见肘。对不同加密算法的机制以及它们的优缺点进行探讨诚然妙趣横生，但从业人员更需正视现实：真正的漏洞极少源自深奥的算理，却往往因实施细节不当而给人以可乘之机。由是，于从业者而言，配置管理无疑重于算法分析。

因 IT 安全领域日趋成熟，不妨将其与医疗领域稍加类比：医学专业的学生靠一本医书学习知识的时代早已一去不返。当今他们必须多方获取资料。解剖学和生化学的基础教义固不可少，但于临床读物中了解各类疾病的衍生与治疗亦不得偏废。

基础理论（关于加密算法和安全操作系统理论）的读物早已不胜枚举，但信息安全领域于“临床实践”方面仍少有著述——真实系统失效的实战经验极少被付诸笔端。

有鉴于此，Sean Convery 的著作令人颇感欣喜。Sean 是一名思科人，而当今正是 Cisco 路由器推动了 Internet 的运行。因此，他的著作视野之宽广、内容之博大、论理之精深，其他作者恐难于企及。而他在 Cisco 咨询业务领域的深厚经验亦将使同行业者颇有斩获。

经设计和配置，网络可在面临恶意攻击、错误和灾难时快速恢复，这至今仍似水中捉月。而其最终或将被广为理解并简化，当是时，Sean 之著作必将为此铺路引航。

Ross Anderson

英国剑桥大学　安全工程学教授

Security Engineering——A Guide to Building Dependable Distributed Systems　的作者

2003 年 7 月

译 者 序

《Cisco ASA 设备使用指南》付梓至今，陆续收到一些读者的电子邮件，也曾在晚上 10 点半左右接到一位读者直接向我们致电，其中大多是指出书中的一些翻译错误。更有一些读者就技术问题向我们求助。对于指出我们翻译错误的读者，我们全部进行了回复并由衷表达了我们的感激和歉意。对于向我们求助的读者，我们在个人能力及精力许可的范畴之内，也尽量就其中的一些问题进行了解答。

3 月 28 日，有一位读者向我们提出了 5 点技术错误，但由于今年 3～7 月，我们二人在家庭、工作和个人安排上，都遭遇了一些变故，因此，当我们第一次看到这封邮件时，已是 4 月底 5 月初之际。虽然当时我们身在 4400 英里之外的异国他乡，而且个人安排也不宽松，但我们仍然向本书的编辑傅道坤先生转发了这封读者来信，同时也对这位朋友表示了感谢。几天后，当我们再次收到这名读者的邮件时，看到的却是恶语相向——指我们是误人子弟的专家教授云云。失笑之余，难免也感失落。

有同样做过翻译的兄弟问我："把联系方式留在书里后悔了吧？"

"怎么会呢！"我答。

自始至终，这都是一个让我感到骄傲的决定，就像我做出的很多其他决定一样。但平心而论，既然有勇气把自己的邮箱和电话留在书中，就是想表达我们愿意对自己并不成熟的翻译水准负责的态度，同时我们也为此作好了接受读者的询问、质疑和指责的准备。我只是想说：我们真的不是什么专家教授，真的不是什么技术权威，我们只是两个不再年轻的 80 后，只是两个普通的技术工作者，只是两个从不相信所谓权威也从不打算冒充所谓权威的新古典自由主义者。我们也只是为了一个介乎爱好和功利之间的目标，利用自己不多的闲暇时光，把自己的作品推广到更多技术同仁之中。工作学习之余，我们也会去喂养流浪动物，也会看看小说或者搜搜网上的八卦新闻，也会趁着入春去买打折的羽绒服，也会对超市里某几样商品的价格如数家珍。

我们不想推卸责任却也问心无愧。根据读者来信中指出的错误提醒出版社同仁在再版时修改，我们当仁不让；对于读者来信中我们能够也有时间进行解答的技术问题，我们也会尽量回复。至于发给我们一些需求，请我们进行网络设计；或者给我们提供几条线索，让我们进行故障排除等，因为涉及太多因素，一时之间难以理清，邮件或电话交流又有太多障碍，请恕我们

实在力不从心。

感谢人民邮电出版社的李际老师、傅道坤、翟磊、张贞等各位编辑。在你们的理解和宽容面前，我的任性永远显得那么自私和狭隘。

此外，我们一如既往地感谢所有批评指教过我们的朋友，包括那位因为我们一时对您的来信处理不当，而导致您心生怨怼的兄弟。同时，由于瑕疵和差错绝难避免，因此我们先为本书有可能出现的所有疏漏向各位致以最诚挚的歉意，也恳请各位读者在发现之时能够不吝赐教。若出于某些无法预知的特殊原因，我无法及时回复您的邮件，可以通过电话或者手机短信和我联系，我们的联系方式和我们在《Cisco ASA 设备使用指南》中公布的一样，从未改变。

田果

2012 年 9 月 17 日

2012 年，或多或少由于我们在家庭、工作等方面的变动，我们开始格外热衷旅游。不知从何时开始，梦想着有朝一日，我们的足迹能够始自南非开普敦，穿越广袤的非洲大陆和地中海到达欧洲，越过巴尔干半岛和高加索，沿着俄罗斯延伸至远东，渡过白令海峡到达阿拉斯加，经加拿大、美国、墨西哥和加勒比海到达南美，并穿过麦哲伦海峡来到火地岛——南美洲的天涯海角。我们固然无法像关野吉晴博士那样利用十年连续的时光去完成这样的伟大旅行，但我们也更愿意利用有限的时间，一点一滴践行我们的梦想。在已经行走过的那些微不足道的旅途中，我们已经获得了太多欢笑和感动，正是这些美好而又弥足珍贵的回忆让并不热衷飞行的我们一再坚定信念，踏上旅程。

为此，我们都十分感激中西旅游的王崟老弟，有些国家必须通过旅行社担保申请个人旅游签证，除了此类鲜有利润的业务之外，我们身上几乎无利可图。明知如此，他依然不厌其烦地为我们提供各种有益的信息与帮助。还要由衷感谢朱佳妮和蔡晓峰等众多驴友为我们提供了大量极其宝贵的旅游信息。

此外，感谢崔豪根大哥、Cemal Bulunmaz 兄弟和 Francis Kinda 兄弟，以及所有在我们需要帮助时义无反顾竭力对我们伸出援手的朋友，虽然我们不知道你们中绝大多数人的姓名，但你们的爱与善意将会不断传递下去。

感谢我在中国电信的所有同仁，尤其是陈扬先生和邓喆先生，批准我很多任性的请假申请；感谢乔宏伟女士和人事部门的同仁，协助我办理申请签证所需的各类文件。我的远行曾为你们带来了或多或少的不便，而我却从未带回任何当地特产来与你们分享旅行的快乐，真挚希望这种无本万利的同事关系能够一直持续下去。

感谢我们的家人，还有亲似我们家人的冬冬（王祎冬）、卢铭、老余（余建威）、秦柯，你们在很多问题上对我们无条件的帮助与支持，我们将没齿难忘。

最后，祝福所有人心想事成。

刘丹宁

2012 年 9 月 17 日

前　言

设计网络安全和设计安全的网络有什么区别？

乍看之下，这就像一个文字游戏。但实际上，它们的区别之中包含了解决网络安全问题的方法。设计网络安全意味着网络安全可以独立地进行设计，而不需要太多考虑其所处的网络环境。而设计安全的网络则意味着要在一开始就把安全作为网络设计的一部分。

本书的主要目标是提供设计安全网络的系统方法。与 Cisco Press 的大多数书不同，本书的内容在很大程度上与厂商的选择无关。我希望没有使用 Cisco 设备（无论网络还是安全）的读者也能够利用本书设计出安全的网络。

有一些网络安全方面的书籍着重介绍黑客故事、安全技术或安全理论概念。虽然这些书中的某些信息也许本书中也会涉及，但是本书的重点在于如何组合不同的安全要素来解决当今网络中的现实问题。本书围绕创建我称为“安全系统”的概念进行组织，其中描述了一些实用而又可靠的方法，利用这些方法就可以利用当前可用的技术设计出安全的、可管理并且可部署的网络。我个人就曾在全球范围内的多家公司应用这些方法帮助它们走向更加安全的联网之路。

通过本书，你将会学到安全最佳做法和完美设计的原则，这会使你在保护网络不同部分时作出经过深思熟虑的决定。当接触真正的设计时，你不仅会理解每个设计背后的原因，还有可能自己得出类似的设计方案。你不仅能够理解书中的设计方案并针对自己的需要作出修改，而且能够学到在实际设备上配置一些网络安全核心技术的方法。通过阅读本书中所介绍的案例研究，你能够将所学概念应用到有实际业务需求和实际安全问题的示例网络中，从而进一步梳理自己的知识结构。

这绝不仅仅是另一本用迷人封面来诱惑你的网络安全书籍；此外，本书也不想以令人厌烦的、冗长的、关于安全技术的理论论述作为写作的宗旨。相反，本书会将很多实际应用中的例子与一些理论和幽默结合在一起，以强调书中所讨论的各种原则。最后，我希望给你提供一组工具来对自己设计的网络进行评估，并重新设计它们以改进其安全性。享受这一旅程吧。

本书与 SAFE 白皮书的关系

多年以来，我编写了一些关于网络安全的白皮书。如果通过下载量来衡量影响力的话，其

中作为 SAFE 系列一部分的那些白皮书最受欢迎。它们描述的是由 Cisco 开发的安全网络设计方案的蓝图。更多信息请访问 http://www. cisco.com/go/safe。

虽然我收到了很多关于 SAFE 白皮书的积极反馈，但是也有许多读者要求我向他们介绍如何才能在自己的网络中设计具有相同安全级别的具体方法。本书旨在向你介绍安全设计的范例，以及通过它们得出满足组织机构特定业务、策略和技术需求的设计方法。这是授人以渔和授人以鱼的区别。

此外，本书还会提供书中讨论的相关技术的配置方法。为便于理解，我们对配置进行了注释。

为什么需要网络安全

IT 安全的作用是保护系统、资源和信息不受无意的、未授权访问或操作失误的破坏。虽然定义像安全这样广泛的概念会招致批评，但无论安全的概念应该如何定义，都很少有企业的 CEO 或总经理忽略网络安全的问题。回顾这些年来见诸报端的大多数攻击，无不表明网络安全在实现其定义的目标时扮演着重要的角色。

此外，IT 应用程序，或者后来的 Internet 应用程序，对组织机构的重要性都在增强。这些应用程序的复杂性，以及它们所运行的操作系统和计算平台的复杂性，使得它们很容易受到各类攻击的影响。而由于应用程序往往会控制对信息的访问，因此应用程序的安全性同样非常重要。

网络为用户提供了与应用程序以及其数据进行交互的管道。它遵循着保护网络安全是保护 IT 安全的第一道防线的理念。没有安全的网络，应用程序和信息就可能持续受到大量攻击者的威胁。

网络安全的发展与网络技术的发展是并行的。由此验证了那句老话：一切规则都有漏洞。最早的网络由连接终端到中央服务器的串行点到点线路构成。要攻入这些简单的系统，就必须能够从物理上访问终端或者串行端口。因此，安全系统主要由物理安全机制组成。

为了增加用户访问的灵活性，在串口上增加了调制解调器。这使得用户和攻击者可以从电话线能够到达的任何地方进行访问。他们主要通过拨号式扫描战术来寻找应答调制解调器，从而获得未授权访问的机会。于是，安全系统开始使用回叫这类技术来对合法用户进行认证。密码技术也因此得到了改进。

对信息共享的需求，尤其是在学术和科研用户之间共享信息的需求，促成了很多网络的建立，其中一个最终发展成为 Internet。这不仅使计算机用户能够从某一个系统来交换和访问大量信息，也使得整个网络中的主机都暴露在黑客的攻击之下。TCP/IP 连接的简便性又使攻击的可能性上升到了一个新的级别。入侵者不仅可以攻击网络上的任何主机，有些人甚至将目光锁定