华为科技有限公司

信息安全完整解决方案

建议书

安氏中国 iS-One

安氏互联网安全系统(中国)有限公司

目 录

1 前言

本章将对华为科技有限公司(简称华为)IT 安全技术基础设施项目的目标、范围、宗旨以及 IS-ONE 的安全理念进行简要描述

1.1 项目目标

建立华为的 IT 安全技术架构，并制定需要实施的各个技术解决方案的优先级、实施计划。从层次上涉及到 3 块：网络安全、系统安全、数据安全

建立华为 IT 安全技术的评估/测评、报告、改善体系

按优先级、按计划实施各个技术解决方案，以提升华为 IT 安全的技术基础。项目要实施或改善的范围包括至少如下

DMZ 方案

防火墙和虚拟网络体系

身份认证和访问控制

服务器、数据库、操作系统、应用系统安全

电子商务/Web 安全解决方案

防病毒体系

信息加密

IDS

安全检查扫描、测评、审计和监控报警系统工具等。

1.2 项目范围

1.2.1 IT 安全技术架构方案设计咨询服务

在 IBM IT 安全策略与标准咨询工作基础上，设计出一个 IT 安全技术框架和体系，确定要实施和改进的安全工具和产品范围、产品选型标准，确定具体的实施目标、实施优先级，制订总实施计划。阶段相关主要工作任务有：

评估华为的 IT 安全技术现状和需求，审视现有的 IBM IT 安全标准和策略（IBM 项目输出），提出相关的建议，输出“ IT 安全技术标准和策略改进建议报告 ”；

安全技术需求与风险评估报告；

漏洞检测和补救措施报告；

与世界级安全技术相比，进行功能转化，形成安全功能分析报告；

根据华为安全现状，确定各功能实现的优先级和产品选型标准；

输出安全产品的比较分析报告（包括功能、性能、价格、服务等）；

制定各安全功能实现的策略、计划和可能的风险；

确定各安全功能测评实施的验收标准；

建立安全功能关注测评、报告、改进、外部服务支持的 持续改进体系。

1.2.2 阶段实施 IT 安全技术架构服务

根据第 1 阶段输出，选择安全功能产品和工具，制定实施计划，进行具体产品实施，并建立与产品运作相关的流程、制度和标准。 阶段主要工作任务包括：

根据产品选型标准、比较分析报告和考察，采购安全产品和工具；

制定各实施计划，完成产品的实施；

建立保障产品按目标要求运作的流程、制度和标准（包括各功能产品的售后服务与支持在内）。（在具体技术解决方案中，需要有相配套的 IT 标准和流程支持，对这些相关 IT 标准和流程的具体要求，要求顾问在具体解决方案中提出建议，可以由华为为主去推行并优化）；

产品实施文档和安全测试结果文档、验收验证文档。

1.2.3 相关其他项目

在本项目开展的同时，IT 安全标准推行项目、Tivoli 实施项目、WEB 平台建设项目、龙岗数据中心建设项目、全球网络建设项目同时也再开展，这些项目之间关系上需要界定、相互之间的影响和集成要有一定的考虑。

如以下问题：

与 IT 安全标准推行项目的范围界定和配合；

与 Tivoli 系统管理工具（目前主要是 NetView、TSD，以后会进一步拓展）的集成（特别是在问题监控方面）；

与 Web 平台、Web 应用的适应和要求。

1.3 IS-ONE 安全宗旨

IS-ONE 在为华为企业网的信息安全提供建设和服务的宗旨可以表述为：

1．依据最新、最先进的国际信息安全标准

2．采用国际上最先进的安全技术和安全产品

3．参照国际标准 ISO9000 系列质量保证体系来规范 IS-ONE 提供的信息安全产品和服务。

4．严格遵守中华人民共和国相关的法律和法规。

5．客户的安全就是我们的成功。

1.4 信息安全“三元论”

IS-ONE 的信息安全理念突出地表现为“三元论”——信息安全有三个要素：策略、管理和技术。

- 安全策略——包括各种策略、法律法规、规章制度、技术标准、管理标准等，是信息安全的最核心问题，是整个信息安全建设的依据；
- 安全管理——主要是人员、组织和流程的管理，是实现信息安全的落实手段；
- 安全技术——包含工具、产品和服务等，是实现信息安全的有力保证。

三元论将信息安全工作中的‘管理中心’的特性突出地描述出来。根据三元论的指导，IS-ONE 为华为企业网提供的信息安全完全解决方案不仅仅包含各种安全产品和技术，更重要的就是要建立一个一致的信息安全体系，也就是建立安全策略体系、安全管理体系和安全技术体系。

1.5 安全标准和规范

在整个项目的建设过程中，IS-ONE **将遵循和参照最新的、最权威的、最具有代表性的信息安全标准。这些安全标准包括：**

- ISO/IEC 15408[①] Information technology– Security techniques – Evaluation criteria for IT security **信息技术—安全技术—信息技术安全评估准则(等同于** Common Criteria for Information Technology Security Evaluation V2.1**，简称** CC V2.1**)**
- BS7799[②] Code of practice for information security management **信息安全管理纲要（即将被** ISO **采纳为** ISO17799**）**
- IETF-RFC—Requests For Comments **是** Internet Engineering Task Force **组织发布的** TCP/IP **标准及相关说明等资料。其中有许多有关安全的标准和说明作为本项目的参考标准和资料。**
- **我国的国家标准** GB**、国家军用标准** GJB**、公共安全行业标准** GA**、行业标准** SJ **等标准作为本项目的参考标准。**[③]

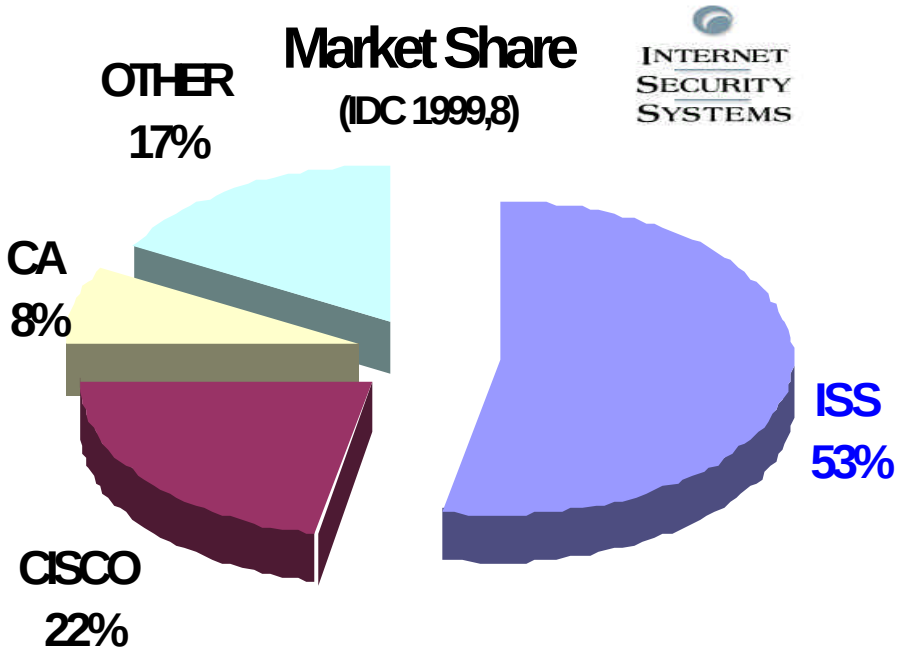
我国各级安全主管部门还颁布了一系列条例和规定。本项目要遵守国内的这些安全条例和规定。

[①] **参考附件** B **国际安全标准** ISO/IEC 15408 **简介**
[②] **参考附件** C **国际安全标准** BS7799 **简介**
[③] **参考附件** A **信息安全标准和规范介绍**

2 IS-ONE 公司简介

在 1992 年，安氏（Internet Security Systems）的创始人 Christopher Klaus 针对日益增强的对于网络安全的需求，推出了一项打破传统的信息安全产品。由此，安氏网络扫描仪产生了。这是业界第一个被设计用来检测网络安全的软件。它通过使用上百种漏洞测试，精确和全面地查找出网络中的弱点，同时对修补安全漏洞提供了详细的，逐步的指导。

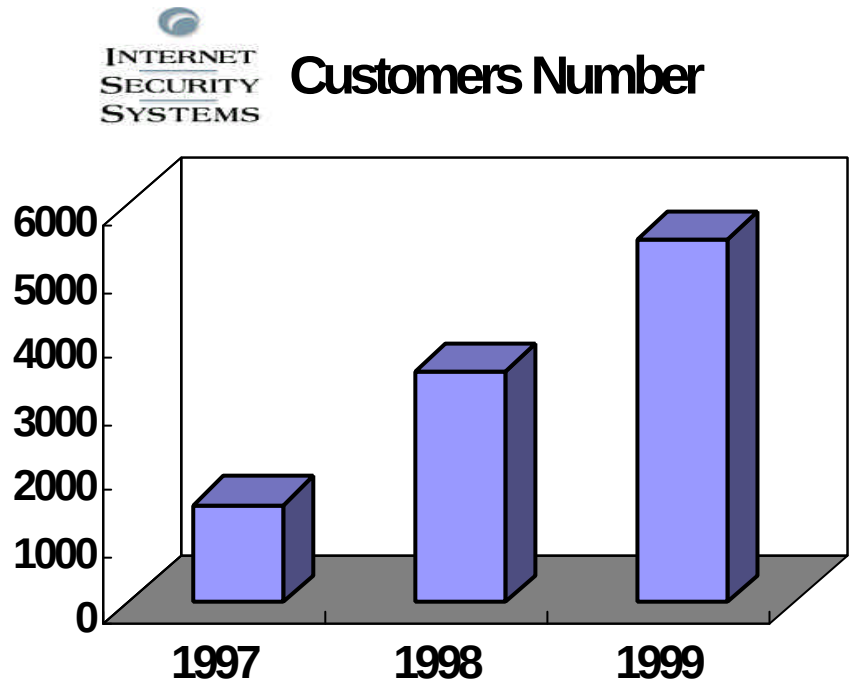
安氏公司由 Klaus 在 1994 年于美国亚特兰大创立。不久，在业界有丰富经验的专家 Thomas E. Noonan 成为安氏公司的 CEO。同时加盟的还有一组经验丰富的管理者和软件工程师。安氏公司于 1998 年在美国 NASDAQ 成功上市并已经成为世界上发展最快的软件公司之一。



安氏市值高达 60 亿美圆，在提供互联网安全整体解决方案综合市场占有率第一。安氏拥有一支世界上最强大的安全小组 X-Force，X-Force 紧密地跟踪计算机和互联网的最新技术，侦测世界上不断出

现的攻击手段，并及时制订出相应的解决方案。

安氏凭借自身专业的解决方案和优秀的售后服务赢得了广泛的客户。安氏其中包括美国前１０家电信公司中的９家，NTT、BritishTelecom、Cable & Wireless;前２５家商业银行的２１家，及超过３５家政府机构的用户包括美国政府、美国国防部、美国空军；等近 6000 家用户。



安氏互联网安全系统(中国)有限公司(Internet Security One Ltd)（简称安氏中国或 IS-ONE）依托安氏美国的技术优势，在中国成立了安氏安全实验室为中国用户提供全面的解决方案和完全本地化的技术服务。在短短两年的时间里我们在中国已获得了众多用户的信赖。我们的用户包括中国电信、中国联通、中国移动、中国工商银行总行、中国建设银行总行等等。安氏中国公司将以专业的解决方案、优秀的售后服务为中国华为网络安全提供满意的产品和服务。

安氏互联网安全系统(中国)有限公司(Internet Security One Ltd)是一家以技术开发及提供全面网络安全解决方案与服务为主的高科技企业。为中国广大的行业用户提供具有国际标准的 eSafeLink ™ 网络安全全面解决方案及服务，并向客户提供全面安全解决方案中所需

的各项安全工具，及提供安全解决方案管理所需的管理决策平台、安全咨询、教育培训以及卓越的售后服务。

经过两年多来对中国市场的大力开发，目前，安氏（中国）有限公司在中国的金融、电信、ISP/ICP、政府部门等行业已经拥有了非常广泛的客户，并在业届享有优秀的声誉。安氏（中国）有限公司目前已经成为国内最著名的网络安全产品和安全服务的主要提供商之一。其中，安氏（中国）在网络漏洞评估和入侵检测市场(IDS)的市场有领导地位。

安氏互联网安全系统(中国)有限公司，发展至今在中国大陆共有正式雇员 200 多人，其中 20%的员工具有高级职称，大专以上学历者占公司总人数的 98%，其中博士占 5%，硕士占 10%，本科学历占 80%。安氏这支高素质的队伍正在为中国的网络安全事尽自己最大的力量。

公司的历史：

安氏(中国)的前身是美国互联网安全系统公司（"安氏"）在中国和香港地区运营销售和产品本地化的载体；

1997 年 7 月在北京设立办事机构；

1999 年正式注册安氏互联网安全系统（中国）有限公司，即安氏（中国）；

针对不断扩大的网络安全市场，安氏互联网安全系统（中国）有限公司于 2000 年 11 月 8 日进行了重大结构和经营性调整，英文名称正式更名为 Internet Security One (China) Ltd.

全新铸造的安氏公司(iS-One Ltd.)汇集了在全球 IDS 市场占有率超过 50%（IDC 报告）的世界著名反黑客公司--美国安氏公司；世界最著名的企业级防病毒厂商--美国趋势科技（Trend Micro）公司(在全球互联网网关病毒防御市场占有率超过 54%，IDC 报告)；以及全球最大的 IT 风险投资基金 Softbank 等强大股东的技术和资金。从而拥有了更加强大的股东背景和技术支持力量，致力于成为业界最有权威的网络安全解决方案和服务提供商。

公司客户及业绩：

电信界：

中国电信、中国邮政、中国移动、中国联通、中国网通、中国

吉通

黑龙江公众多媒体通信网、辽宁公众多媒体通信网、

陕西省电信、天津移动通信局、江苏省电信、江苏移动、

浙江公众多媒体通信网、上海热线、安徽公众多媒体通信网、

湖南电信、贵州公众多媒体通信网、云南省电信、

广东省电信管局、广东省 163 **网、广东移动、**

海南公众多媒体通信、重庆电信、

中华网、搜狐网站（Sohu**）等等。**

金融届：

中国人民银行、中国银行、中国工商银行、中国建设银行、

中国农业银行、深圳招商银行、广东发展银行、

中国交通银行、深圳交易所、深圳银联 等等。

政府及企业：

公安部第三研究所、中国海关、

广东电力、天津电力

公安部金盾工程 等等。

3 IS-ONE 的信息安全方法论概述

IS-ONE 拥有自己独到的针对信息安全和信息安全服务的方法学。IS-ONE 的信息安全方法学可以简单地概括为以下几个范畴:

1. 信息安全表述模型
2. 信息安全实现原则和方法学
3. 多角度的安全需求分析
4. 安全要素分析和设计
5. 安全集成实施和安全服务
6. 安全评估

3.1 信息安全问题简介

信息安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的综合性学科。信息安全是指信息系统的硬件、软件及其系统中的数据受到保护，不受偶然的或者恶意的原因而遭到破坏、更改、泄露，系统连续可靠正常地运行，网络服务不中断。

从广义来说，凡是涉及到网络上信息的保密性、完整性、可用性、真实性和可控性的相关技术和理论都是信息安全的研究领域。

广义的计算机系统安全的范围很广，它不仅包括计算机系统本身，还包括自然灾害（如雷电、地震、火灾等），物理损坏（如硬盘损坏、设备使用寿命到期等），设备故障（如停电、电磁干扰等），意外事故等。

狭义的系统安全包括计算机主机系统和网络系统上的主机、网络设备和某些终端设备的安全问题，主要针对对这些系统的攻击、侦听、欺骗等非法手段的防护。以下所有的计算机系统安全均是狭义的系统安全范畴。

国际互联网络是跨越时空的，所以安全问题也是跨越时空的。虽然我们国家的网络不发达，但是我们遭到的安全危险却是同国外一样的，这是一个很严重的问题。

Internet 的不安全因素，来自几个方面。一方面，Internet 做为一种技术，是面向所有用户的，所有资源均通过网络共享；另一方面，Internet 是开放和标准的。Internet 过去主要用于科研和学术，现在已发展为商用阶段，但是它的技术基础是不安全的。

在不同的行业，所遭受的攻击因行业和网络服务的不同而不同。在电信或者 ICP 市场，进攻服务系统比较多；而在银行业，对数据系统的进攻相对更频繁。

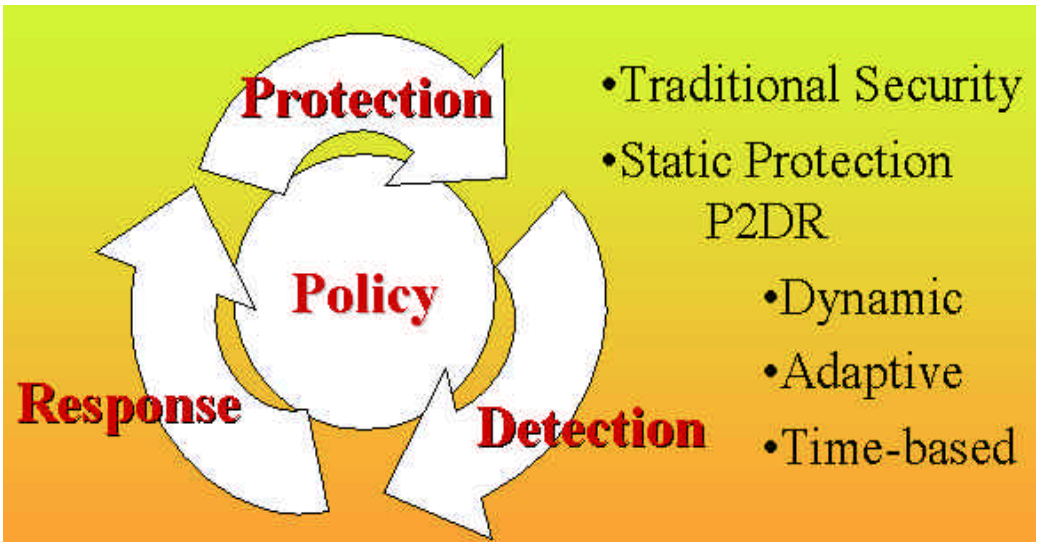
3.2 信息安全表述模型——P^2DR 模型

通过信息安全表述模型——P^2DR 模型的分析，我们可以对需要建设的整体解决方案有一个完整的概念。确定 Policy 策略、Protection 防护、Detection 检测和 Response 响应四个方面的安全需求。

3.2.1 P^2DR 模型概述[①]

IS-ONE 利用作为帮助各机构确定他们已有的信息技术风险和发展适当有效的信息安全控制与管理措施的基础。P^2DR 模型阐述了一个提供 7×24 不间断安全管理和保障的产品和服务的全部综合套件以及全面安全解决方案。

P^2DR 方案是一个超前的安全模型，它是由 IS-ONE 在对国际上安全方面可靠的权威著作进行多年研究的基础上独自发展出来的。它的指导思想比传统安全方案(传统安全在本质上是静态的，如防火墙和加固验证等)有突破性提高。



Policy 策略、Protection 防护、Detection 检测和 Response 响应组成的完整模型体系，可以描述和解释任何信息安全问题。P2DR 安全模型的特点就是动态性和基于时间的特性，可以说对信息安全的“相对性”给予了更好地描述：虽然没有 100%的安全，但是模型为进一

[①] 参考附件 C P2DR 动态安全模型简介

步解决信息安全技术问题提供了有益的方法和方向。

由 P^2DR 的数学模型我们得到结论：安全的目标实际上就是尽可能的增大保护时间，尽量减少检测时间和响应时间。

按照 P^2DR 模型，信息安全方案可以最大限度地保护信息不受诸多威胁的侵犯，目的是确保商务连续性，将商务损失和风险降低到最小程度，将投资回报和商业机会提高到最大程度。

下面我们从策略、保护、检测、响应四个环节分别加以讨论。

3.2.2 Policy(安全策略)

由于安全策略是 P^2DR 安全模型的核心，所以要想实施动态网络安全模型，必须首先制定企业的安全策略，所有的防护、检测、响应都是依据安全策略实施的，企业安全策略为安全管理提供管理方向和支持手段。

对于一个策略体系的建立包括：安全策略的制订、安全策略的评估、安全策略的执行等。

3.2.3 Protection（保护）

保护通常是通过采用一些传统的静态安全技术及方法来实现的，主要有防火墙、加密、认证等方法。通过防火墙监视限制进出网络的数据包，可以防范外对内及内对外的非法访问，提高了网络的防护能力，当然需要根据安全策略制定合理的防火墙策略；也可以利用 SecureID 这种一次性口令的方法来增加系统的安全性等等。

3.2.4 Detection（检测）

在 P^2DR 模型，检测是非常重要的一个环节，检测是动态响应的依据，它也是强制落实安全策略的有力工具，通过不断地检测和监控网络和系统，来发现新的威胁和弱点，通过循环反馈来及时作出有效的响应。

在我们采用了一系列静态安全措施后，比如设置了防火墙、进行

身份验证、采用了加密算法等等，我们是否就能认为我们的网络是安全的呢？应该如何来评估网络的安全性？实际上网络的安全风险是实时存在的，所以我们检测的对象应该主要针对构成安全风险的两个部分：系统自身的脆弱性及外部威胁。

漏洞检测

入侵者首先总是通过寻找网络中的安全漏洞来寻找入侵点。进行系统自身的脆弱性检查的主要目的是先于入侵者发现漏洞并及时弥补，从而进行安全防护。

由于网络环境比较复杂，一般利用工具来进行漏洞检查，检查可以针对网络层、操作系统层、数据库层、应用系统层多个层面上进行，可能是一些系统自身的漏洞也可能是一些管理、配置上的漏洞。漏洞检测的原理主要是通过查找安全漏洞库及采用一些模拟攻击的方法来发现漏洞，所以评价一个漏洞检测产品的好坏有一个很重要的因素就是安全漏洞库的大小。

因为网络是动态变化的，所以对于脆弱性检查应该定期执行，而在网络结构发生了变化、主机上新安装了软件等之后也应该执行脆弱性检查。

入侵检测

另一方面，也必须针对外部威胁进行实时入侵检测。

按入侵检测的策略来划分，入侵检测模型可以分为基于异常统计和模式匹配两类模型。模式匹配模型建立在已知的入侵特征库基础上，而异常统计模型则建立在已知系统正常工作模式基础上，异常统计模型包括两个方面：一是为用户和系统建立正常行为特征，二是观察实际的系统和用户活动与所建立的正常行为是否存在差异。模式匹配和异常统计两类模型具有互补性，异常特征模型能够精确地检测已知的入侵活动，误警率低；而对于一个确定的应用环境，异常统计模型会拥有一个比较精确的系统正常工作模式，从而发现一切偏离正常模式的活动，包括一些未知的入侵活动。

按入侵检测的手段来划分，入侵检测模型可以分为基于网络和基于系统两种模型。基于网络的模型通过实时监视网络上的数据流，来寻找具有攻击特征的数据包；而基于系统的模型则通过分析系统的审计数据来发现可疑的活动。这两种模型也具有互补性，基于网络的模

型能够客观地反映网络活动，特别是能够监视到系统审计的盲区；而基于系统的模型能够更加精确地监视系统中的各种活动。基于网络的模型受网络结构的限制，而基于系统的模型不受网络结构的影响。入侵检测必须实时执行。

网络是动态变化的，入侵者会利用不断发现的网络、系统的安全漏洞，采用各种新的方式、方法进行攻击，所以应该不断跟踪分析黑客行为和手法，研究网络和系统的安全漏洞，这些体现在安全检测产品上也就是入侵特征库及安全漏洞库，这也是评价一个安全检测产品比较重要的一个因素，当然入侵特征库及安全漏洞库更新的速度也很重要。

病毒检测

病毒和黑客入侵同样是对我们信息系统的动态的威胁。针对病毒的危害主要的解决方法有两种：

- 针对被感染的系统进行病毒扫描、清除检查；
- 对正在传输的文件和信息进行病毒检查
- WEB 浏览恶意代码过滤和邮件过滤

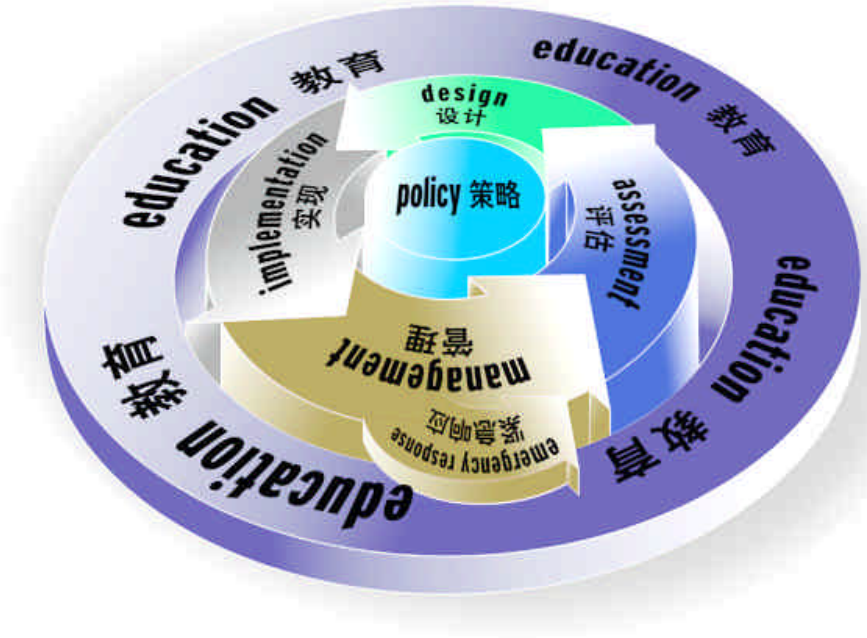
3.2.5 Response（响应）

紧急响应在安全系统中占有最重要得地位，是解决安全潜在性最有效的办法。在检测到安全漏洞和安全事件之后必须及时做出正确的响应，从而把系统调整到安全状态。从某种意义上讲，安全问题就是要解决紧急响应和异常处理问题。要解决好紧急响应问题，就要制订好紧急响应的方案，做好紧急响应方案中的一切准备工作。

> 一个信息安全完整解决方案必须对安全策略、安全防护、安全检测和安全响应有准确的描述。
>
> 必须针对 P2DR 的四个方面给出产品或者服务的解决方案。

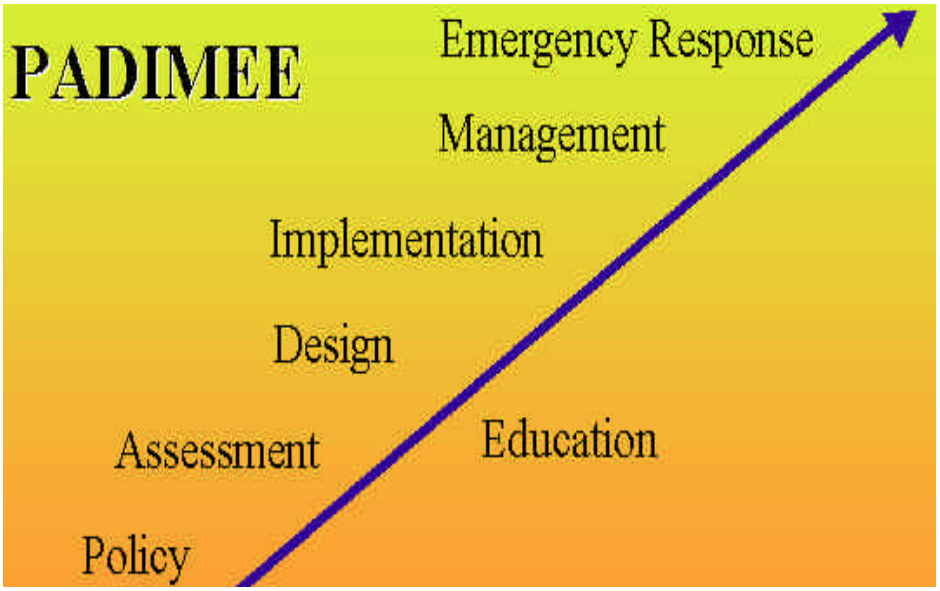
3.3 信息安全实现原则和方法学

为了降低风险和减少成本，IS-ONE 根据信息安全的生命周期特征，提出了一种按阶段实施的可操作的模型 SafeCycle（或者称为 PADIMEE）。IS-ONE 将信息安全的生命周期描述为下面各个阶段：



- Policy Phase 策略制订阶段：制订系统的安全目标；
- Assessment Phase 评估分析阶段：实现需求分析、风险分析、安全功能分析和评估准则设计等，明确表述现时状态和目标之间的差距；
- Design Phase 方案设计阶段：形成信息安全解决方案，为达到目标给出有效的方法和步骤；
- Implementation Phase 工程实施阶段：根据方案设计的框架，建设、调试并将整个系统投入使用。

- Management Phase **运行管理阶段：在管理阶段包括两种情况——正常状态下的维护和管理（**Management Status**），以及异常状态下的应急响应和异常处理（**Emergency Response Status**）。**
- Education Phase **安全教育：是贯穿整个安全生命周期的工作，需要对企业的决策层、技术管理层、分析设计人员、工作执行人员等所有相关人员进行教育。**



IS-ONE **认为** SafeCycle（PADIMEE）**模型应当成为实现信息系统安全的实施过程指南。所有的信息安全系统的建设都应当按照** SafeCycle **的过程来指导。**

一个信息安全完整解决方案必须对信息安全系统建设和运行的整个生命周期给予清晰的描述，不能仅仅局限于安全产品的集成。

SafeCycle 模型是指导安全完整解决方案制订和实施的方法学。

3.4 IS-ONE 安全完整解决方案结构

根据 P2DR 模型和 SafeCycle 模型的指导，IS-ONE 为华为构建安全完整解决方案是从对华为的安全需求进行分析和设计入手的。

在总体安全目标的要求下，IS-ONE 将会对此项目相关的信息系统进行信息安全评估服务。

IS-ONE 在安全评估阶段的主要工作是：

- 安全需求评估
- 安全风险评估（漏洞和脆弱性评估、入侵和风险评估、策略评估、风险综合分析）
- 安全功能分析
- 安全评估准则制订

在本建议书中的各个章节主要就是对应安全评估阶段的各个方面工作：

《第一章 前言》简单介绍安氏的安全宗旨和理念及此次项目的相关情况。

《第二章 IS-ONE 公司简介》简单介绍公司情况。

《第三章 IS-ONE 信息安全方法论概述》简要介绍了 IS-ONE 的如何构建安全完整解决方案的方法论。介绍了 P2DR 模型、SafeCycle 模型和需求分析的不同角度。

《第四章 安全需求分析》主要就是从各个角度对此项目相关的信息系统的安全需求和风险进行评估。

《第五章 安全功能要素分析和方案》主要就是从安全功能和安全要素方面，总结第四章对华为企业网的各方面安全需求分析形成的方案。

《第六章 安全服务体系》主要描述配合整个信息安全整体解决方案，从生命周期方面和全面技术方面 IS-ONE 为华为企业网提供的安全服务体系。安全服务体系是实现整个安全方案的有效方式，是安

全解决方案不可分割的一部分。

《第七章 安全集成方案》主要就是对第五章的安全功能要素进行集成性汇总。

《第八章 项目管理》主要描述整个项目的组织、流程、规划和实施的一些内容。

《第九章 质量保证体系》主要描述 IS-ONE 在实施此项目过程中要提供的质量保证体系。

制订一个信息安全完整解决方案不能仅仅局限于安全产品的集成，不能从罗列产品开始。

IS-ONE 的信息安全完整解决方案一定要基于对此项目相关的网络信息系统的安全需求、风险、功能、评级、服务等方面的全面评估开始。

3.5 多角度的安全需求分析和设计

信息安全问题是一个非常复杂的综合问题，信息系统有多复杂，信息安全就有多复杂。信息安全同样具有信息系统所具有的各种特性，同时也有自己的独特性。

分析此项目相关的信息系统的信息安全需求，需要从信息安全的不同特性和不同角度去分析，根据各方面分析的结果，形成综合的需求分析和解决方案设计。

信息安全最突出的特性包括：

- 相对性
- 动态性
- 潜在性
- 生命周期特性
- 分布性
- 层次性
- 业务相关特性
- 综合性、集成性
- 管理核心、策略核心等

对于安全的相对性、动态性、基于时间、潜在性等在 P2DR 模型中给予了充分的阐述。

安全的生命周期特性需要通过 SafeCycle 模型（PADIMEE）在信息安全体系的建立过程以及今后的维护过程中体现。

对于信息安全的策略核心、业务相关特性、分布性、层次性、集成性都在第四章的各节中给予详尽的描述和分析。

4 安全需求分析

本章就此项目相关的信息系统在安全方面的需求进行分析，分析从管理和策略、业务、分布式、层次性、集成性等多方面进行。

4.1 华为企业网安全策略和管理体系需求分析

在当前整个华为企业网系统的业务发展中，信息系统的作用毋庸置疑。随之带来的信息安全问题也同样占有重要的地位。要解决好信息安全问题的首要任务就是——制订完整的、切合实际的、具有前瞻性的信息安全策略，并能够落实执行。

前期已由 IBM 公司已根据需求定制了相关 IT 安全策略与标准咨询工作，设计出一个 IT 安全技术框架和体系，确定要实施和改进的安全工具和产品范围、产品选型标准，确定具体的实施目标、实施优先级，制订总实施计划。

但信息安全涉及信息系统的各个方面，又是一发展极为迅速的领域，单独一个标准、一个纲要是不能解决全部问题的。因此需要制订一个安全策略系列，策略系列在一个总则和总体纲要的指导下，各自解决一部分问题，我们将在原有基础之上在作一定的评估。

IS-ONE 建议信息安全策略系列应当包括：

信息安全总则

在总则中，从全局的、概要的角度对华为企业信息安全给予描述的规定。总则应当对安全策略系列的其他文档起到指导和规范的作用。这个总则就是整个信息安全策略系列的“宪法”。

总则的制订应当充分参考国际、国内以及本行业内的各种已经制定的标准、法规和制度等。建议参考的文本包括（但不限于）：

1. ISO 15408-1 Information technology – Security techniques – Evaluation criteria for IT security – Part 1：Introduction and general model

2. BS7799-1 Code of practice for information security management

3. IETF/RFC2196 Site security handbook

4. **其他行业的安全策略**

制定这个规范需要组织各方面的专家，包括技术的专家、法律的专家、银行业务的专家、安全管理的专家等共同制订。

信息安全人员组织管理规章

人员管理是信息安全管理的核心问题。人员管理主要通过组织的形式来体现。目前，需要尽快建立和完善华为/华为企业网信息安全的安全负责人和安全管理员体系。

这个管理规章的制定，主要参考以前相关的规定。

信息安全介绍和一般模型

在这个文档中，对信息安全的一般性定义、问题和模型，以及一般性的解决方案和步骤给予了描述。

此模型的制订应当充分参考国际、国内以及本行业内的各种已经制定的标准、法规和制度等。建议参考的文本包括（但不限于）：

1. ISO 15408-1 Information technology – Security techniques – Evaluation criteria for IT security – Part 1：Introduction and general model

2. BS7799-1 Code of practice for information security management

3. IETF/RFC2196 Site security handbook

4. **其他行业的规范**

制定这个规范需要组织各方面的专家，包括技术的专家、法律的专家、电信业务的专家、安全管理的专家等共同制订。

信息安全需求分析和功能分析

本标准对信息安全的需求和信息安全系统的功能给予了总体的全面的描述。制定这个标准主要参考以下标准：

ISO 15408-2 Security functional requirements

本建议书就是对信息安全的需求分析和功能分析给予了初步的描述。

信息安全管理纲要

信息安全管理纲要主要从管理的角度对信息安全给予了全面的描述，主要的参考标准就是：

BS7799-1 Code of practice for information security management

BS7799-2 Information security specification

信息安全评估准则

信息安全评估准则可以作为对信息安全产品、系统和服务的评估和评级标准。主要的参考标准是：

ISO 15408-3 Security assurance requirements

Common criteria for information technology security evaluation

ITSEC- Information technical security evaluation criteria

TCSEC- Trusted Computer Security Evaluation Criteria

信息系统安全保护等级划分准则

这个准则对华为企业网系统的安全保护等级要求给予了明确的表述。这个准则可以充分参照国家新制订的“计算机信息系统安全保护等级划分准则”。

信息安全教育培训和考核指南

本指南主要描述在华为企业网体系如何进行各级各类人员的信息安全教育培训。相应地还包括对人员的考核和上岗要求。各类人员包括：

安全负责人——总经理或总监级别

安全管理员——技术负责人

安全操作员——具体技术人员等

建议本指南的制定需要参考国际和国内已经开展的计算机安全培训工作的经验，包括：

公安部和人事部组织的培训体系

安氏公司的 SecureU 安全大学的课程

ICSA 国际计算机安全协会的教育课程

1999 年全国银行系统计算机安全大检查的教育培训经验

信息安全检查执行指南

1999 年的全国银行系统计算机安全大检查对促进整个银行系统的计算机安全工作起到了重要的作用。建议华为也借鉴这种管理制度，应当将这种检查变成一个制度化的、持续性的工作。本指南就是对这种检查工作给予描述和规范。

信息安全紧急响应指南

紧急响应在信息安全的保障体系中占有重要的地位，关于这个标准的制订应当充分参考国际和国内的相关紧急响应组织的建议和规定。可以参考的组织有：

CERT – Computer Emergency Response Team

FIRST – Forum of Incident Response and Security Teams

中国 CERT

信息安全实施和管理指南系列

这些指南对各种具体的安全技术给予描述，可以包括 :病毒防治、防火墙、漏洞扫描、入侵检测、加密等

通过对不同的技术进行深入的描述和规定，可以充分规范整个华为企业网系统的信息安全技术、产品和服务。

制订一个信息安全完整解决方案不能仅仅局限于安全产品的集成，不能从罗列产品开始。

IS-ONE 的信息安全完整解决方案一定要基于对此项目相关网络的安全需求、风险、功能、评级、服务等方面的全面评估开始。

4.2 华为企业网业务安全需求分析

4.2.1 内部办公

随着企业的业务拓展和规模的扩大，企业的内部办公网也会逐渐健全，员工对网络的依赖性越来越重，其地位也会变得越来越重要，安全性也就不容忽视。通常办公网分为两种类型：

- A 型，不连接到 INTERNET；
- B 型，连接到 INTERNET。

A 型网，不连接到 INTERNET

需要考虑的安全主要有以下几点：

a。子网划分

一般来说一个健全的内部办公网，应该根据不同的业务特征，划分为多个不同的逻辑子网。一般具有以下几个子网：管理网段，财务网段，业务网段，开发网段，公用网段。不同子网可以使用交换机或路由器等设备划分虚拟网段，或者采用更高安全级别的隔离措施，比如：使用路由器或防火墙等。

b。身份鉴别

内部办公网通常需要远程接入服务，以方便异地登录或家庭办公。对于远程接入的身份鉴别，通常使用用户名密码方式，主叫识别方式（回拨）。对于高强度的身份鉴别，应该使用动态密码验证。

c。访问控制

根据身份鉴别进行授权，对资源访问进行限制。访问控制是安全的一个重要环节，访问控制的关键在于策略的制定。策略制定使用最小安全原则。

d。数据加密

办公网重要数据传输应该使用加密方式。数据传输可以使用普通

电子邮件系统，可以使用 WEB 方式，也可以使用专用办公系统例如：NOTES。邮件数据加密可以使用专用软件实现。WEB 数据加密可以使用 SSL。

e。数字签名

数字签名主要作用是身份认证和防抵赖。最常用的是电子邮件的数字签名和文件的数字签名。数字签名是对签名者，签名时间，签署内容的合法性效验，可以使用专用数字签名软件来实现，例如 PGP。

f。结合具体办公系统或者 OA 系统，分析该系统的安全需求。

B 型网，连接到 INTERNET

需要考虑的安全除了 A 型网具有的以外，还有以下几点：

a。与 INTERNET 互连的安全策略设定

需要在办公网接入 INTERNET 处制定策略，实现单向办公网访出。需要对办公网的访出制定策略，实现选择性访问。需要对办公网的访入进行禁止，并进行记录，并在接入网络的边界，设置防火墙（FW）入侵检测（IDS）等软件。

b。透过 INTERNET 的 VPN 互连

对于透过 INTERNET 的网间办公网互连，需要使用加密传输信道，可以使用 VPN 技术，用防火墙或路由器实现功能。

4.2.2 平台业务

4.2.2.1 用户和子网接入

拨号接入

拨号接入服务安全主要有

a。拨号身份鉴别

对于用户拨号接入，身份鉴别应该使用 CHAP 方式，取代 PAP 方式，可以防止窃听

b。拨号服务器安全

拨号服务器策略制定应该限制 SNMP 使用，对拨号服务器登录应该取消缺省登录帐号，进行 AAA 认证。

专线接入

专线接入相对来说 ISP 需要提供给用户的安全服务要少。专线接入服务安全主要有

a。网段划分——专线子网权限策略制定。专线接入子网之间权限策略制定。

b。网络设备访问控制

4.2.2.2 应用业务系统

华为企业网是对整个企业内部提供全方位的信息服务，各种不同的服务具有不同的安全特征。

电子商务平台

电子商务平台涉及多方面的安全需求，其安全问题包括：电子商务安全系统架构，提供加密的数据传输，加密的数据存储，PKI 体系，系统安全，网络安全，防黑客攻击，防病毒，个人隐私等等。

因此，建议针对电子商务平台的安全，单独制订安全解决方案。

企业内部 IP 电话

需要提供实时性较强并且高带宽服务。所以要进行策略设定，对于 DoS 拒绝服务攻击进行防范，可以利用防火墙或路由器等包过滤设备完成功能。

IDC 系统

如虚拟主机业务，需要提供给虚拟主机的客户相应的访问权限。从安全管理方面由于涉及客户的复杂情况，会比较难于控制。

针对虚拟主机的安全，主要通过主机安全，身份认证，访问控制等方面实现。

如果金华为客户需要华为提供安全服务，需要另行制订《虚拟主机安全服务》。IS-ONE 可以协助华为进行此项服务。

客户将自己的主机托管在华为 IDC。这些主机的安全主要由客户自己负责。从业务上，华为考虑的安全主要在如何隔离客户的主机和网段，避免客户主机自身出现安全问题从而影响其他客户和华为企业网的骨干网络。

针对主机托管的安全，主要进行虚拟网段化分，需要进行包过滤级 DoS 拒绝服务攻击保护。

如果 IDC 的客户需要华为提供安全服务，需要另行制订《主机托管安全服务》。IS-ONE 可以协助华为进行此项服务。

建议针对 IDC 系统设计相应的安全解决方案。

WWW 主页服务

WWW 主页服务是 Internet 最基本服务项目。

针对 WWW 主页的安全，主要需要 WWW 服务器的主机安全，需要 HTTP 服务配置的安全，需要 CGI 的安全设置，需要 FILTER 设置，需要对抗 DoS 拒绝服务攻击，需要提供日志和审计，需要身份认证和访问控制，需要分权管理。

NEWS 新闻

News 新闻服务是 Internet 基本服务项目之一。

针对 News 新闻的安全，主要需要 News 服务器的主机安全，需要 INND/NNTP 服务安全配置，需要 FILTER 设置，需要对抗 DoS，需要日志和审计，需要身份认证和访问控制。

E-MAIL 电子邮件

E-Mail 电子邮件服务是 Internet 最基本服务项目。

针对电子邮件服务器的安全，主要需要邮件服务器的主机安全，需要 MAIL 服务(SMTP)配置的安全(主要包括服务器配置，拒绝，转

发，容量限制，数量限制等)，需要 POP3/IMAP 服务配置安全，需要对抗 DoS 拒绝服务攻击，需要域名服务器安全，需要提供日志和审计，需要身份认证和访问控制，需要分权管理

FTP 文件传输

FTP 文件传输服务是 Internet 基本服务项目之一。

针对 FTP 文件传输服务的安全，主要需要主机的安全，需要 FTP 服务配置的安全(主要包括服务器配置，权限设置，允许连接数等)，需要 FILTER 设置，需要对抗 DoS 拒绝服务攻击，需要日志和审计，需要身份认证和访问控制，需要分权管理。

4.2.3 辅助业务

企业生产辅助系统

a。需要主机安全

主机安全包括物理安全和操作系统安全。物理安全包括有硬件安全，屏保安全，软驱光驱安全，输入设备安全等。操作系统安全一般包括补丁程序，服务程序设置，系统 用户密码设置，进程合理配置，配置文件修改，漏洞扫描(发现)等。

b。需要数据库安全

数据库安全包括合理分区，分权管理，数据库灾难恢复，数据备份安全，数据存储安全，数据库操作安全等。

c。需要管理平台安全

管理平台需要分权管理。需要在管理策略中贯彻。

d。需要身份认证和访问控制

e。需要日志和审计

网络管理业务

a。需要主机安全

b。网络管理系统

需要网络管理协议安全配置，管理 KEY 设置，权限合理配置，分权管理等。

c。需要身份认证和访问控制

d。需要日志和审计

e。需要加密数据传输

网管数据加密传送，网管远程加密登录方式

DNS 域名服务

a。需要主机的安全

b。需要对抗 DoS 拒绝服务攻击

DNS 为提供给公众的服务器，需要不间断服务，需要高处理能力。

c。需要服务配置安全

安全最小化配置，需要提供正确 EMAIL 服务指向

d。需要日志和审计

4.3 分布式安全需求分析和设计

4.3.1 华为企业网络拓扑

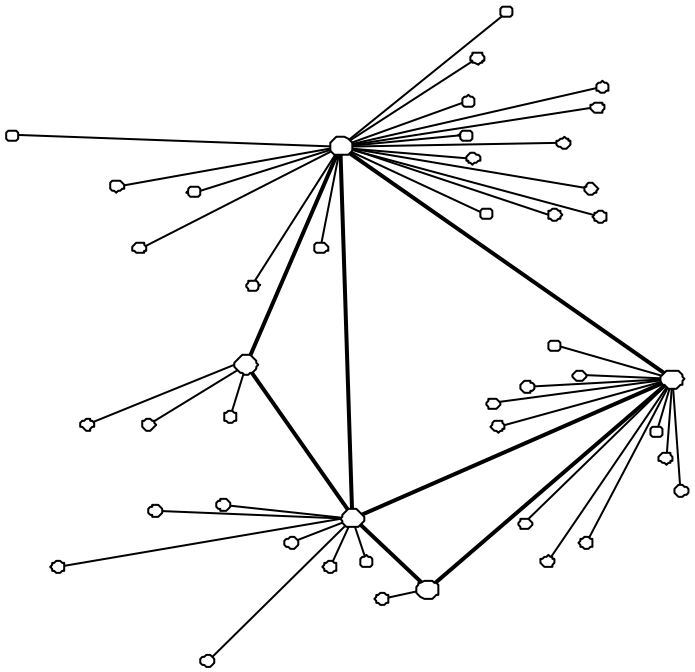
华为与 AT&T 合作，设计和构建华为全球网络。此项目 2000 年 10 月启动，设计方案部分目前已经全部完成，现正在实施中。

华为公司在总部及各分公司的办公网段利用华为网作为传输平台构成一个分布于全球的办公网。因为办公网对于主机安全和传输保密有较高的要求，本建议的方案在设计时对此有专门的考虑。

本建议书所提方案对不同类型的节点的各自特点进行分析，提出相应的最佳方案。同时需要和 AT&T 进行项目配合。

4.3.2 节点安全和路径安全

从网络的整体来分析华为企业网，可以将华为企业网看成各个网络节点和网络路径（干线）的组合。如下示意图。



节点地面线路拓扑

从节点和路径的角度分析华为企业网的安全需求主要表现在要能够持续地保证整个网络的畅通，保证承载服务的可用性。

4.3.3 子网安全和边界安全

华为企业网可以划分为不同的子网，子网之间和其他网络之间有连接。从子网和边界的角度可以对网络的安全需求进行分析。可以将这些安全问题归结为：

- 子网网接入 Internet（包括国际出口等）
- 子网网连接 Extranet
- 子网之间连接
- 拨号接入
- 子网内部安全

子网接入 Internet

子网网接入 Internet 必须考虑的安全部件有外层防火墙、内层防火墙、实时入侵检测系统、代理服务器，其他部件应根据实际需求选用。并解决好 DMZ 安全。

子网连接 Extranet

根据内部网连接 Extranet 安全技术规范，各级内部网连接 Extranet 可以采用防火墙技术，链路加密技术和入侵检测技术,实际业务中,外单位网络或主机接入内部网,在接入处设置防火墙保护内部网络安全.考虑到不同的业务，链路接入方式及安全风险，Extranet 连接可以采用三种模式:

- 只使用防火墙，这是最低的安全要求。所有 Extranet 接入都必须配置防火墙
- 使用防火墙和链路加密技术，只适用于 Extranet 接入经过安全风险较高的路径这种情况
- 使用防火墙，链路加密技术和入侵检测技术。适用于安全要求更高风险更大的 Extranet 接入情况。

子网之间连接

根据内部网经广域网互联安全技术规范的要求，考虑到不同安全级别的内部网安全需求和性能，各级内部网连接行内其他内部网可以有 4 种连接模式：

- 使用路由器的访问控制
- 使用防火墙
- 使用网络加密
- 同时使用防火墙和网络加密

拨号接入安全

参考华为企业网业务安全需求分析和设计中对拨号接入的描述和分析（4.2.2.1）

子网内部安全

子网的安全需求主要表现在：

- 子网的网段划分
- 子网中服务器的安全
- 子网中网络设备的可用性
- 子网中用户的身份认证和访问控制

4.3.4 各子网安全需求分析

核心子网

子网的安全需求主要表现在：

- 一些重要的服务器的保护，这些服务器都代表不同的重要业务。其中一些服务器的安全会影响整个网络的正常运行。
- 骨干网络设备的可用性保护
- 重要通路/边界的保护

节点子网

一级节点子网的安全需求主要表现在：

- 一些重要的服务器的保护，这些服务器都代表不同的重要业务。其中一些服务器的安全会影响整个下级网络的正常运行。
- 骨干网络设备的可用性保护
- 重要通路/边界的保护
- 拨号接入服务器的安全

二级节点子网

二级节点子网的安全需求主要表现在：

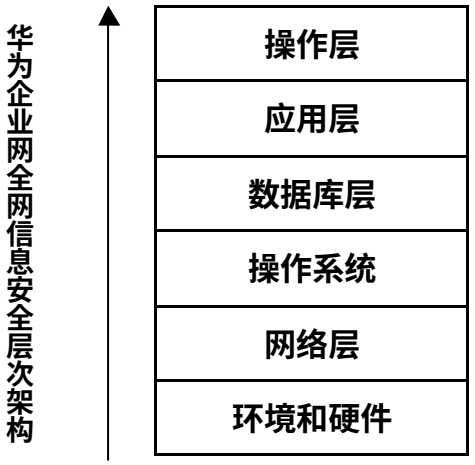
- 一些重要服务器的保护，这些服务器都代表不同的重要业务。其中一些服务器的安全会影响整个网络的正常运行。
- 骨干网络设备的可用性保护
- 重要通路/边界的保护
- 拨号接入服务器的安全

4.4 层次性安全需求分析和设计

网络安全方案必须架构在科学的安全体系和安全框架之上。安全框架是安全方案设计和分析的基础。为了系统地描述和分析安全问题，本节将从系统层次结构的角度展开，分析华为企业网各个层次可能存在的安全漏洞和安全风险，并提出解决方案。

4.4.1 层次模型描述

针对华为企业网的情况，结合《华为 IT 安全基础设施项目需求 RFP》的要求，IS-ONE 把项目相关的网络的信息安全划分为六个层次，环境和硬件、网络层、操作系统、数据库层、应用层及操作层。



4.4.2 环境和硬件

为保护计算机设备、设施（含网络）以及其它媒体免遭地震、水灾、火灾、有害气体和其它环境事故（如电磁污染等）破坏，应采取适当的保护措施、过程。

在本建议书中，环境及硬件的安全不做重点讨论。

4.4.3 网络层安全

安全问题

网络层是网络入侵者进攻信息系统的渠道和通路。许多安全问题都集中体现在网络的安全方面。

由于大型网络系统内运行的 TPC/IP 协议并非专为安全通讯而设计，所以网络系统存在大量安全隐患和威胁。网络入侵者一般采用预攻击探测、窃听等搜集信息，然后利用 IP 欺骗、重放或重演、拒绝服务攻击（SYN FLOOD，PING FLOOD 等）、分布式拒绝服务攻击、篡改、堆栈溢出 等手段进行攻击。

4.4.3.1 安全的网络拓扑结构

安全技术

保证网络安全的首要问题就是要合理划分网段，利用网络中间设备的安全机制控制各网络间的访问。

推荐产品和服务——网络拓扑安全评估服务

华为企业网的网络拓扑结构已经基本定型，为了保证当前系统的正常运行，保证系统的延续性等方面的要求，对于华为当前的网络拓扑结构，特别是网段划分方面，建议进行安全方面的评估。

4.4.3.2 网络扫描技术

安全技术

解决网络层安全问题，首先要清楚网络中存在哪些安全隐患、脆弱点。面对大型网络的复杂性和不断变化的情况，依靠网络管理员的技术和经验寻找安全漏洞、做出风险评估，显然是不现实的。解决的方案是，寻找一种能寻找网络安全漏洞、评估并提出修改建议的网络安全扫描工具。

推荐产品和服务——安氏网络扫描器 Internet Scanner

安氏网络扫描器 Internet Scanner 是全球网络安全市场的顶尖产品。它通过对网络安全弱点全面和自主地检测与分析，能够迅速找到并修复安全漏洞。网络扫描仪对所有附属在网络中的设备进行扫描，检查它们的弱点，将风险分为高，中，低三个等级并且生成大范围的有意义的报表。从以企业管理者角度来分析的报告到为消除风险而给出的详尽的逐步指导方案均可以体现在报表中。

结合使用 Internet Scanner 产品，还可以选用 IS-ONE 的网络安全漏洞评估服务。

4.4.3.3 防火墙技术

防火墙技术概述

防火墙的目的是要在内部、外部两个网络之间建立一个安全控制点，通过允许、拒绝或重新定向经过防火墙的数据流，实现对进、出内部网络的服务和访问的审计和控制。具体地说，设置防火墙的目的是隔离内部网和外部网，保护内部网络不受攻击，实现以下基本功能：

- 禁止外部用户进入内部网络，访问内部机器；
- 保证外部用户可以且只能访问到某些指定的公开信息；
- 限制内部用户只能访问到某些特定的 Internet 资源，如 WWW 服务、FTP 服务、TELNET 服务等；

推荐产品和服务——CheckPoint Firewall-1 防火墙

Firewall-1 防火墙是一种应用级防火墙，它的监测模块能监测和分析网络通信所有七层协议的内容。

推荐产品和服务——路由器安全配置服务

实际上路由器本身就可以实现包过滤防火墙的功能，对华为企业网中的各个路由器的配置进行检查和调整。保证整个网络中各个路由器的配置相互一致，并承担包过滤检查的功能。

4.4.3.4 网络实时入侵检测技术

安全技术

防火墙虽然能抵御网络外部安全威胁，但对网络内部发起的攻击无能为力。动态地监测网络内部活动并做出及时的响应，就要依靠安氏公司的基于网络的实时入侵监测技术。监控网络上的数据流，从中检测出攻击的行为并给与响应和处理。实时入侵监测技术还能检测到绕过防火墙的攻击。

推荐产品和服务——安氏网络入侵检测 RealSecure Network Engine

安氏实时网络传感器 (RealSecure Network Engine) 对计算机网络进行自主地，实时地攻击检测与响应。这种领先产品对网络安全轮回监控，使用户可以在系统被破坏之前自主地中断并响应安全漏洞和误操作。实时监控在网络中分析可疑的数据而不会影响数据在网络上的传输。它对安全威胁的自主响应为企业提供了最大限度的安全保障。

安氏网络入侵检测 RealSecure Network Engine 在检测到网络入侵后，除了可以及时切断攻击行为之外，还可以动态地调整防火墙的防护策略，使得防火墙成为一个动态的智能的的防护体系。

4.4.4 操作系统层安全

安全问题

操作系统安全也称主机安全，由于现代操作系统的代码庞大，从而不同程度上都存在一些安全漏洞。一些广泛应用的操作系统，如 Unix，Window NT，其安全漏洞更是广为流传。另一方面，系统管理员或使用人员对复杂的操作系统和其自身的安全机制了解不够，配置不当也会造成的安全隐患。操作系统自身的脆弱性

4.4.4.1 系统扫描技术

安全技术

对操作系统这一层次需要功能全面、智能化的检测，以帮助网络管理员高效地完成定期检测和修复操作系统安全漏洞的工作。系统管理员要不断跟踪有关操作系统漏洞的发布，及时下载补丁来进行防范，同时要经常对关键数据和文件进行备份和妥善保存，随时留意系统文件的变化。

推荐产品和服务——安氏系统扫描器(System Scanner)

安氏系统扫描器(System Scanner) 是基于主机的一种领先的安全评估系统。系统扫描器通过对内部网络安全弱点的全面分析，协助企业进行安全风险管理。区别于静态的安全策略，系统扫描工具对主机进行预防潜在安全风险的设置。其中包括易猜出的密码，用户权限，文件系统访问权，服务器设置以及其它含有攻击隐患的可疑点。

4.4.4.2 系统实时入侵探测技术

安全技术

为了加强主机的安全，还应采用基于操作系统的入侵探测技术。系统入侵探测技术监控主机的系统事件，从中检测出攻击的可疑特征，并给与响应和处理。

推荐产品和服务——安氏网络入侵检测 RealSecure System Agent

安氏实时系统代理 (RealSecure System Agent) 对计算机主机操作系统进行自主地，实时地攻击检测与响应。一旦发现对主机的入侵，RealSecure 可以马上可以切断系统用户进程通信，和做出各种安全反应。

安氏实时系统代理 (RealSecure System Agent)还具有伪装功能，可以将服务器不开放的端口进行伪装，进一步迷惑可能的入侵者，提高系统的防护时间。

4.4.5 数据库层安全

安全问题分析

许多关键的业务系统运行在数据库平台上，如果数据库安全无法

保证，其上的应用系统也会被非法访问或破坏。数据库安全隐患集中在：

- 系统认证：口令强度不够，过期帐号，登录攻击等。
- 系统授权：帐号权限，登录时间超时等。
- 系统完整性：Y2K 兼容，特洛伊木马，审核配置，补丁和修正程序等。
- 表、连接的权限设置

推荐产品和服务——安氏数据库扫描器（DataBase Scanner）

安氏数据库扫描器（DataBase Scanner）是世界上第一个也是目前唯一的一个针对数据库管理系统风险评估的检测工具。

该产品可保护存储在数据库管理系统中的数据的安全。Database Scanner 增强了安氏在安全领域的市场领先地位，并且目前安氏是唯一提供数据库安全管理解决方案的厂商。用户可通过该产品自动生成数据库服务器的安全策略，这是全面的企业安全管理的一个新的重要的领域。

Database Scanner 能通过网络快速、方便地扫描数据库，去检查数据库特有的安全漏洞，全面评估所有的安全漏洞和认证、授权、完整性方面的问题。

4.4.6 应用层安全

应用安全是指用户在网络上的应用系统的安全，包括 WEB、FTP、邮件系统、DNS 等网络基本服务，业务系统，办公自动化系统，电子商务系统等。

应用层安全的解决目前往往依赖于网络层、操作系统、数据库的安全，由于应用系统复杂多样，没有特定的安全技术能够完全解决一些特殊应用系统的安全问题。但对一些通用的应用程序，如 Web Server 程序，FTP 服务程序，E-mail 服务程序，浏览器，MS Office 办公软件等，安氏的 Internet Scanner 和 System Scanner 可以帮助检查这些应用程序自身的安全漏洞和由于配置不当造成的安全漏洞。

推荐产品和服务——安氏网络扫描器(Internet Scanner)

推荐产品和服务——安氏系统扫描器(System Scanner)

4.4.7 操作层（人，组织）

安全问题分析

层次系统安全架构的最顶层就是对华为企业网进行操作、维护和使用的内部人员。人员有各种层次，对人员的管理和安全制度的制订是否有效，影响由这一层次所引发的安全问题。

除按业务划分的组织结构以外，必须成立专门安全组织结构。这个安全组织应当由各级行政负责人、安全技术负责人、业务负责人及负责具体实施的安全技术人员组成。

此外，必须制订系列的安全管理制度和普及安全教育，包括：

- 用户守则制订，如应包括：未知请求一律禁止通过、只有网络管理员才可进行物理访问、分部不应使用单一标准的 Modem、只有网络人员才可进行软件安装工作、访问 Internet 必须通过代理、所有安全软件必须能保留完整的日志、重要系统应使用难猜测的口令并经常改换口令。
- 机房管理制度的制订
- 分层次的安全培训，对行政、技术的各级人员有针对地进行培训。

建立安全信息分发系统，对安全管理的阶段性结果，以可读性好的报告形式分发给各个结点的安全部门。应对具体的分发方式、分发渠道、保密措施做出规定。网络安全方案必须架构在科学的安全体系和安全框架之上。安全框架是安全方案设计和分析的基础。为了系统地描述和分析安全问题，本节将从系统层次结构的角度展开，分析华为企业网各个层次可能存在的安全漏洞和安全风险，并提出解决方案。

4.5 华为企业网安全集成需求分析

本节对此项目相关的网络的各个安全功能集成为一个完整的安全体系方面的需求进行分析。

4.5.1 安全要素总结

网络安全功能要素是组成整个网络安全体系的基本元素。在详细研究了华为公司网络安全需求、以及透彻了解洞悉业界最新网络安全技术的基础上，本解决方案中有效集成了网络拓扑结构安全服务、防火墙、主机系统安全服务、漏洞评估、入侵监控和防御、访问控制、日志和审计、身份认证、信息加密、防病毒和灾难恢复、安全管理工具等网络安全功能要素。

上述产品和服务安全要素实现了 P^2DR 动态安全模型（详见“P^2DR 安全模型”一节）。在整个安全解决方案的设计中，IS-ONE 公司选择了最优秀的产品以及本公司强大的专业安全技术服务。本建议书中第五章将详细描述上述安全功能要素的技术和性质。

4.5.2 安全集成需求

经济性

构建华为企业网的安全体系需要巨大的资金和投入。建立一个实际的安全体系必须对经济性和安全性之间进行权衡。

在本建议书中，在方案的制订、产品的选型、服务的选择方面都尽可能体现经济性的原则。

标准性

构建象华为企业网的这样庞大的安全体系，必须坚持遵循必须的标准。

策略性

建立华为企业的安全体系，需要首先制订完整的、一致的信息安全策略体系，并且将安全策略体系和其他企业策略相协调。

综合性、整体性

从系统综合的整体角度考虑此次华为企业网安全招标项目，制定有效、可行的安全措施，建立完整的安全防范体系。

一致性

IS-ONE **提供的安全解决方案应与华为企业网的网络，业务的安全需求相一致。**

用户界面

IS-ONE **提供的安全管理工具应提供友好的图形用户接口（**GUI**）管理界面。**

尽量降低对原有网络、系统性能的影响。

由于增加了安全设置后，必将影响网络和系统的性能，包括对网络传输速率的影响，对系统本身资源的消耗等。因此需要平衡双方的利弊，提出最为适当的安全解决建议。

避免复杂性

IS-ONE **提供的安全解决方案会尽力避免造成网络结构的复杂，操作与维护的复杂。安全体系的建立不会对华为企业网的结构做出根本性的修改。**

可用性

可用性包括两个方面，安全系统本身的可用性和建立在安全管理体系下的网络的可用性。对于安全系统来说，要求可提供方便、友好的图形化管理界面，能够持续地提供安全服务。对于网络来说，要求不影响原有业务的开展。

开放性

IS-ONE **提供的安全管理工具支持广泛的安全管理标准。提供的安全产品具有相应的接口，可以利于各种安全产品之间集成实用，并可以和其他信息产品高效结合。**

纵深性

IS-ONE **提供的安全解决方案是一个多层保护体系，各层保护相互补充，当一层保护被攻破时，其它层保护仍可起到安全防范的作用。**

适应性

IS-ONE **提供的安全解决方案能够随着华为企业网网络性能及安全需求的变化而变化，要容易适应、容易修改。**

集成性

IS-ONE **提供的安全管理工具应能够和其它系统管理工具有效集成。**

保障安全系统自身的安全

IS-ONE **提供的安全产品和系统都关注到系统自身的安全保护。**

5 安全功能要素分析和方案

根据第四章对华为企业网的安全需求进行了几个角度的分析，总结出一些安全要素，在本章将针对各个要素进行分析和方案设计。

针对每个安全要素都对详尽的描述该要素的技术和管理要求，介绍要素相关的产品和服务，并给出针对该要素的建议方案。

5.1 网络拓扑结构

网络分段是合理网络结构的重要的一部分，同时也是一项基本措施，其指导思想在于：将非法用户与网络资源相互隔离，从而达到限制用户非法访问的目的；通过合理的网段划分，帮助其他安全产品更加有效地发挥作用。

网络分段可分为物理分段和逻辑分段两种方式：

物理分段通常是指将网络从物理层和数据链路层（ISO/OSI 模型中的第一层和第二层）上分为若干网段，各网段相互之间无法进行直接通讯。目前，许多交换机都有一定的访问控制能力，可实现对网络的物理分段。

逻辑分段则是指将整个系统在网络层（ISO/OSI 模型中的第三层）上进行分段。例如，对于 TCP/IP 网络，可把网络分成若干 IP 子网，各子网间必须通过路由器、路由交换机、网关或防火墙等设备进行连接，利用这些中间设备（含软件、硬件）的安全机制来控制各子网间的访问。

在实际应用过程中，通常采取物理分段与逻辑分段相结合的方法来实现对网络系统的安全性控制。

鉴于华为企业网的网络结构已经基本建成，无法重新对网络结构进行重新规划，但是应该对现有网络结构进行一次检查，如发现问题严重的子网可以考虑重建，而且以后在新建网络的时候一定要注意这个问题。

推荐安全服务

网络拓扑结构安全分析服务——该服务是 eSafelink Professional 专业安全服务中的一项，是针对网络进行安全建设的一项基本服务。

服务的主要方式和内容包括：

- 分析网络的拓扑图结合华为公司网运行业务，对其安全性进行分析；
- 利用工具对网络的实际拓扑结构进行描述，对其安全性进行分析。
- 当发现安全拓扑结构方面的安全问题，给出网络拓扑结构调整建议。实际的拓扑结构调整由网络管理人员协助实施。

服务的主要成果是《华为企业网网络拓扑结构安全分析报告》。

建议方案

此服务是华为企业网全网信息安全完整解决方案中必须的一项服务。

5.2 防火墙

防火墙是解决子网的边界安全问题、实现网络访问控制的有效解决方法。

防火墙的主要功能

A。包过滤

包过滤（Packet Filtering）防火墙是出现最早的一类防火墙。事实上，路由器本身就具有包过滤防火墙的功能。理论上，包过滤器可以配置为根据协议报头的任何部分进行判断，但实际上，大多数的包过滤实现都针对最为有用的数据域：协议类型、IP 地址、端口号等。通常源地址、目的地址、协议类型、源端口、目的端口以及包到达或发出的接口等构成包过滤防火墙的基本安全控制和审计手段。

由于简单的包过滤防火墙在安全性方面的缺陷，当前基本上已经被基于状态检查的包过滤防火墙所取代。

状态检查（Stateful Inspection）是介于简单包过滤和应用级代理

之间的一种中间方式，它使用基于维持连接状态和协议信息的复杂过滤器来阻断或通过数据包，成为当前主流防火墙优先采用的工作方式。

B。网络地址翻译

网络地址翻译（Network Address Translation），又称 IP 伪装（IP Masquerade），它通过将内部主机的 IP 地址翻译到外部网络的 IP 地址，从而达到隐藏内部主机 TCP/IP 层次信息的目的。NAT 允许在内部网络中使用任何网络运行者希望的 IP 网络地址。NAT 技术的出现带来网络安全的同时，在很大程度也缓解了当前 Internet 中 IP 地址匮乏的问题，为网络设计和建设带来了巨大的方便。

按照地址翻译的工作方式，NAT 又可分为以下几种：

- 静态翻译（Static NAT），每一个内部地址对应一个外部地址，也简称为 1:1 NAT。此时，地址翻译带来的安全性、节约地址方面的优点全部消失。但是，在内部网络存在对外提供服务的服务器主机时，静态翻译非常必要。

- 动态翻译（Dynamic NAT），大段的内部网络地址对应于一个或者一小段外部网络地址。根据实施的细节又可分为 N:1 和 N:M(N>M)两种方式。

C。应用代理

应用代理（Application Proxy）防火墙的工作方式不同于包过滤防火墙，它首先对带有代理并且按照策略规则允许通过的数据包接收并重新产生，然后忽略掉那些没有相应代理的数据包。因为它阻断了内外的直接网络连接，在应用层，所以应用代理可以提供比包过滤防火墙更为细致的网络安全策略和更好的安全水平。

通常，最为常用的应用代理是 Telnet,FTP,SMTP,HTTP 等。

D。身份认证

身份认证（Authentication）技术能够识别从外部网进来访问的用户的身份，从而决定是否运行它们访问内部网络，达到在用户级进行访问控制、对安全策略进行细化的目的。

E。虚拟专网

虚拟专网（VPN）帮助用户在不安全的公网上面建设一个相对安全的、接近于专用网络的通信环境。虚拟专网使用以下几个基本安全功能来实现：IP 封装、加密的身份认证、数据包净荷加密等。

一般来说，局域网之间的虚拟专网可以通过服务器计算机、防火墙、路由器等来建立。单纯的虚拟专网并不能提供有效的保护，与防火墙的结合可以很大程度上提高虚拟专网的安全性。所以，虚拟专网成为当代防火墙的一个重要功能。

防火墙的分类

当前的防火墙主要包括三大类：包过滤型防火墙、应用级代理和混合型防火墙。它们各有所长，具体使用哪一种或是否混合使用，要看具体需要。

A。包过滤型防火墙

一般是基于源地址和目的地址、应用或协议以及每个 IP 包的端口来作出通过与否的判断。一个路由器便是一个"传统"的包过滤防火墙。大多数的路由器都能通过检查这些信息来决定是否将所收到的包转发，但它不能根据一个 IP 包的前后文进行判断。

先进的状态检查包过滤防火墙可以判断这一点，它可以判断连接状态和一些数据流的内容，把判断的信息同规则表进行比较，检查每一条规则直至发现包中的信息与某规则相符。如果没有一条规则能符合，防火墙就会使用默认规则。一般情况下，默认规则就是要求防火墙丢弃该包。

下面是某一包过滤防火墙的访问控制规则：

允许网络 123.0.0.1 使用 FTP(21 口)访问主机 150.0.0.1；

允许 IP 地址为 202.103.1.18 和 202.103.1.14 的用户 Telnet(23 口)到主机 150.0.0.2

允许任何地址的 E-mail(25 口)进入主机 150.0.0.3；

允许任何 WWW 数据（80 口）通过；

不允许其他数据包进入。

包过滤防火墙简洁、速度快，并且对用户和应用透明，但是因为

它只检查地址和端口，对网络更高协议层的信息无理解能力，对网络的保护有限。

B。应用级代理

应用级代理能够检查进出的数据包，通过网关复制传递数据，防止在受信任服务器和客户机与不受信任的主机间直接建立联系。应用级代理能够理解应用层上的协议，能够做复杂一些的访问控制，并做精细的认证和审核。但每一种协议需要相应的代理软件，使用时工作量大，效率不如包过滤防火墙。

应用级代理有较好的访问控制，是目前最安全的防火墙技术。但实现较为困难，而且有的应用级代理缺乏"透明度"，经常成为网络速度瓶颈。在实际使用中，用户在受信任的网络上通过防火墙访问 Internet 时，经常会发现存在延迟并且必须进行多次登录（Login）才能访问 Internet 或 Intranet。

C。混合型防火墙

该防火墙结合了包过滤防火墙和应用级代理的特点。它同包过滤防火墙一样能够通过 IP 地址和端口号，过滤进出的数据包，也能够检查 SYN 和 ACK 标记和序列数字是否逻辑有序。另一方面，它也能象应用级代理一样，在应用层上检查数据包的内容，查看这些内容是否能符合既定的网络安全规则。

目前在市场上领先的防火墙大多属于混合型防火墙，因为该防火墙对于用户透明，在应用层上加密数据，不需要修改客户端的程序，也不需对每个需要在防火墙上打开的服务额外增加一个代理。

5.2.1 推荐产品介绍——CheckPoint 防火墙

Checkpoint 公司是一家专门从事网络安全产品开发的公司，是软件防火墙领域的佼佼者，其旗舰产品 CheckPoint Firewall-1 在全球软件防火墙产品中位居第一（52%），在亚太地区甚至高达百分之七十以上，远远领先同类产品。在中国证券、银行等行业都有了广泛的应用。

CheckPoint Firewall-1 是一个综合的、模块化的安全套件，它是

一个基于策略的解决方案，提供集中管理、访问控制、授权、加密、网络地址传输、内容显示服务和服务器负载平衡等功能。主要用在保护内部网络资源、保护内部进程资源和内部网络访问者验证等领域。CheckPoint Firewall-1 套件提供单一的、集中的分布式安全的策略，跨越 Unix、NT、路由器、交换机和其他外围设备，提供大量的 API，有 150 多个解决方案和 OEM 厂商的支持。CP Firewall-1 由 3 个交互操作的组件构成：控制组件、加强组件和可选组件。这些组件即可以运行在单机上，也可以部署在跨平台系统上。其中，控制组件包括 Firewall-1 管理服务器和图形化的客户端；加强组件包含 Firewall-1 检测模块和 Firewall-1 防火墙模块；可选组件包括 Firewall-1 Encryption Module（主要用于保护 VPN）、Firewall-1 Connect Control Module(执行服务器负载平衡)Router Security Module （管理路由器访问控制列表）。

Checkpoint Firewall-1 防火墙的操作在操作系统的核心层进行，而不是在应用程序层，这样可以使系统达到最高性能的扩展和升级。此外 Checkpoint Firewall-1 支持基于 Web 的多媒体和基于 UDP 的应用程序，并采用多重验证模板和方法，使网络管理员容易验证客户端、会话和用户对网络的访问。

CHECKPOINT 防火墙功能要求

1）支持透明接入和透明连接，不影响原有网络设计和配置；

Check Point FireWall-1 是一款软件防火墙，是安装在现有的网关或服务器计算机上，对接入和连接都是透明的，不会影响原有网络设计和配置。

2）带有 DMZ 的连接方式；

Check Point FireWall-1 可以支持多个网络接口，所以客户可以很容易的按照需要设置 DMZ 分区。

3）支持本地和远程管理两种管理方式；

Check Point FireWall-1 中的 Enterprise Management Console 模块功能十分强大，支持本地和远程两种管理方式，减轻了网络管理员对网络的管理负担。

4）支持命令行和 GUI 方式的管理与配置；

Check Point FireWall-1 中的管理控制台支持命令行和 GUI 方式的管理与配置；可以在 Windows 95/98/NT 上安装 Windows GUI 界面，

在 Unix 操作系统下可以安装 Motif GUI 图形用户界面进行管理与配置。

5）对分布式的防火墙支持集中统一状态管理；

Check Point FireWall-1 中的管理控制台支持对分布式防火墙的集中统一状态管理。它可以同时管理多个防火墙模块。

6）规则测试功能，支持规则一致性测试；

Check Point FireWall-1 中的策略编辑器中有一命令，可以对已经配置好的规则进行测试，可以检测其一致性。

7）透明代理功能；

Check Point FireWall-1 支持代理功能，而且功能强大，可以支持本身自带的预定义的超过 150 多种的常用协议。

8）地址转换功能，支持静态地址转换、动态地址转换以及 IP 地址与 TCP/UDP 端口的转换；

Check Point FireWall-1 支持 NAT 地址转换功能，支持 Static Mode(静态转换)和 Hide Mode(动态转换) 两种方式；目前不支持 IP 地址与 TCP/UDP 端口的转换。

9）访问控制，包括对 HTTP、FTP、SMTP、TELNET、NNTP 等服务类型的访问控制；

Check Point FireWall-1 可以通过制定策略来进行访问控制，可以支持超过 150 多种的常用协议，并可以自定义各种不常用的协议。

10）用户级权限控制；

Check Point FireWall-1 可以指定用户对象，在其属性中有各种认证方式可供选择，加强了用户级的权限控制。

11）防止 IP 地址欺骗功能；

Check Point FireWall-1 提供了防止 IP 地址欺骗的功能，可以在设定防火墙网关的网卡属性时激活该功能。

12）包过滤，支持 IP 层以上的所有数据包的过滤；

Check Point FireWall-1 中的对象以 IP 地址或 TCP/UDP 端口号来识别，所以可以对 IP 层以上的所有数据包进行过滤。

13）信息过滤，包括 HTTP、FTP、SMTP、NNTP 等协议的信息过滤；

Check Point FireWall-1 可以通过 OPSEC 接口，与第三方厂商的软件或硬件产品无缝结合起来对 HTTP、FTP、SMTP 等协议进行信息过滤。

14）地址绑定功能，实现 MAC 地址与固定 IP 地址的绑定，防止 IP 地址盗用；

Check Point FireWall-1 目前为止不能实现 MAC 地址与固定 IP 地址的绑定。

但是可以利用各节点处的路由器来进行 MAC 地址与固定 IP 地址的绑定。

15）抗攻击性要求，包括对防火墙本身和受保护网段的攻击抵抗；

防火墙本身的抗攻击能力与其所运行的操作系统的安全级别有关。操作系统的安全级别越高，防火墙本身的抗攻击的能力也越高。

16）审计日志功能，支持对日志的统计分析功能；

Check Point FireWall-1 中自带有日志功能，可以对符合预定规则的网络流量事先规定的方式进行记录；在 Check Point FireWall-1 4.1 产品中更带有一个 Reporting Module，可以对记录的日志进行分析统计。

17）实时告警功能，对防火墙本身或受保护网段的非法攻击支持多种告警方式（声光告警、EMAIL 告警、日志告警等）以及多种级别的告警；

Check Point FireWall-1 的策略中有一个报警功能，其中包括了 E-mail 告警，日志告警等多种告警方式。

CheckPoint 防火墙技术性能指标

1）时延；

在每个包大小平均为 512 字节的情况下，在 3DES 加密方式下 Unix 的时延是 1.8msec，NT 是 1.2msec；在 DES 加密方式下 Unix 的时延是 1.3msec，NT 是 1msec。

2）吞吐量；

在没有数据加密情况下，不同的操作系统可以分别达到

152M~246Mbps；在数据加密情况下，可以达到约 55Mbps。

3）最小规则数；

在防火墙概念中无此提法。按照我们的理解，此概念如果是指策略中的规则数的话，则无限制。

4）包转发率；

10~15Mbps

5) 最大位转发率；

在防火墙概念中无此提法。按照我们的理解，此概念类似吞吐量。

6) 并发连接数；

理论上没有限制。

5.2.2 推荐产品介绍——LinkTrust™ 防火墙

安氏中国集多年的网络安全产品开发及工程实施经验，采用源自硅谷的，当今世界先进的防火墙开发模型及相关的核心技术，与国内外有关的科研机构及著名高等院校合作，遵循软件开发工程理论，由数名博士参与组成的开发团队协同工作，完成了 LinkTrust™ 放火墙的设计，开发，测试等方面的工作。

安氏中国的“入侵检测（ISS Realsecure）”和“漏洞评估（ISS Internet Scanner）”是国际著名品牌。LinkTrust™ 防火墙可与 RealScure 紧密耦合，协同工作。防火墙可以保护自己和 IDS 系统不受网络攻击和入侵的危害，IDS 系统检查到的攻击和入侵信息可以实时地通知防火墙，相应的修改安全策略，起到进一步保护内部网络的目的。

LinkTrust™ 防火墙通过了 ISS Internet Scanner 的强力扫描测试。

LinkTrust™ 防火墙能够与业界领先的病毒防火墙 InterScan 互相合作，为用户建立完整的企业级反病毒体系。

LinkTrust™ 防火墙属于基于状态检查的包过滤和应用级代理的混合型防火墙，带有一个集成的网络地址翻译器和一组专用安全过滤

器，以及大多数常见的应用层网络协议的代理，集状态检查防火墙的灵活高效与应用代理的安全性于一身。秉承安氏产品一贯的高、精、尖品质，LinkTrust™ **防火墙帮助用户建立完善的安全防御体系。**

LinkTrust™ **防火墙虚拟专网的设计可以帮助用户低成本的建立符合国际标准的安全网络。**

LinkTrust™ **采用专门设计硬件搭载平台，符合国际通用的电气标准。**

下面将分别介绍各个特色功能。

基于状态包过滤

▶ LinkTrust™ **防火墙采用基于状态包过滤和应用代理的混合模式，集两种方式防火墙的优点于一身，同事照顾到了安全性。**

▶ **基于源/目的** IP **地址，服务，用户，组（网络，服务）的精细粒度的访问控制**

应用代理

▶ **提供丰富全面的应用代理，覆盖大多数用户常用应用程序，包括** Telnet,FTP,HTTP,SMTP **等**

▶ **多线程的代理提供高性能的连接速度。**

网络地址翻译

▶ **支持多种方式的网络地址翻译，包括静态地址翻译（**1:1**）、动态地址翻译（**N:1,N：M N>M**）。**

用户认证

▶ **支持多种认证方式，包括普通密码，一次性密码（**S/KEY **和** MD5**）**

▶ **会话认证**

▶ SMTP **服务认证扩展（**RFC 2254**）**

内容安全过滤

LinkTrust™ 防火墙提供强大的、细微粒度的网络内容安全控制手段，包括：

- URL 屏蔽、监控（HTTP 代理）
- Web 邮件控制（HTTP 代理）
- Java/Active-X 过滤封堵（HTTP 代理）
- 邮件大小控制（SMTP 代理）
- 邮件地址传输（SMTP 代理）
- SMTP 命令控制(DEBUG, VRFY, EXPN)
- 双重 DNS 查找（SMTP 代理）
- E-Mail 过滤封堵（域，关键字，邮件大小，接受者的数量等）
- FTP 命令控制(GET, PUT, MKDIR 等)

与业界技术领先的趋势科技公司的病毒防火墙 InterScan VirusWall 配合，LinkTrust™ 防火墙可以为用户提供强大的、完整的反病毒保护。详见下节《LinkTrust 防火墙安全设计》。

日志、审计

LinkTrust™ 防火墙提供强大、完整的系统运行日志以及相关的处理、检索、报告等：

- 日志搜索 （标准字符串，日期/时间，IP 地址，服务，通过/阻塞包）
- 统计标准：源/目的 IP 地址，服务，日期/时间，通过/阻塞包等等。

告警

LinkTrust™ 防火墙支持多种事件告警方式，包括：

- 控制台
- SNMP

- 用户定义的其它程序

虚拟专网

- 符合业界标准(IPSec)的虚拟专网（VPN），利用公网建立自己的安全的企业网，降低整体安全成本（TCO）。

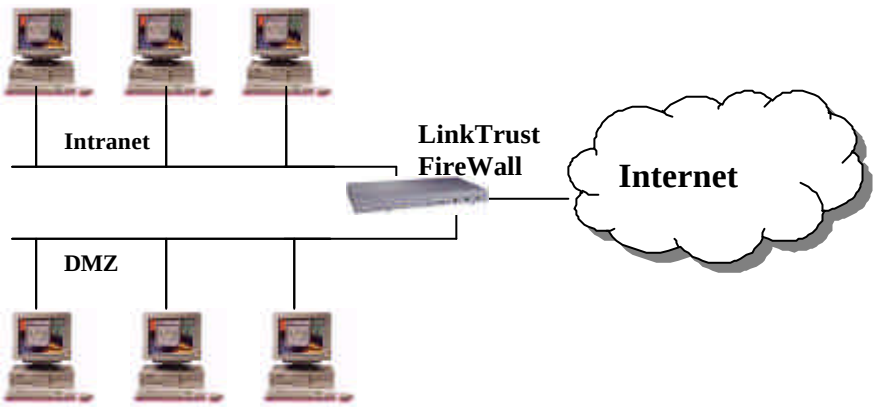
图形界面（GUI）配置管理

LinkTrust™ 防火墙提供安全的、友好的、易用的图形用户界面配置管理手段：

- 基于 Web 的远程管理和命令行界面
- 基于目标管理（网络，服务，用户，组）
- 支持 128 位 SSL（安全套接字层）加密
- 系统备份，提供安全应急能力

LinkTrust™ 防火墙安全设计

a。基本安全体系设计



图一：LinkTrust 基本配置示意

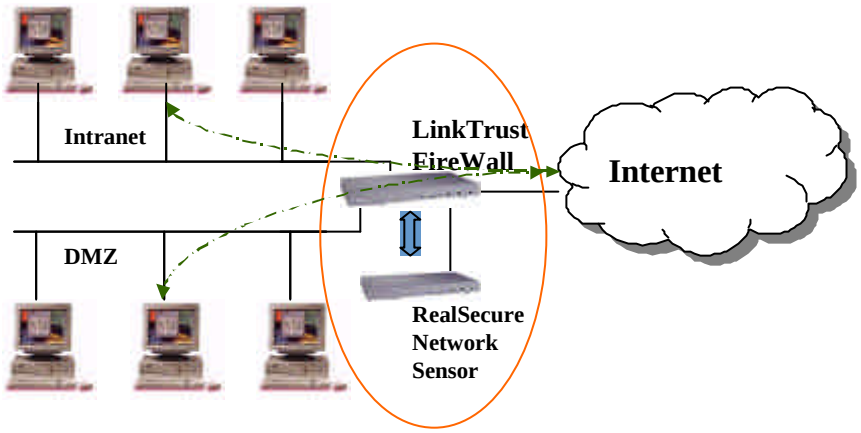
基本的防火墙安全防御体系配置如图所示。

LinkTrust 防火墙系统提供多种网络接口，标准配置的三个接口分别为：Intranet（内部网）、DMZ（Demilitarized Zone）以及外部网。其中 Intranet 是不对外开放的区域，外部用户检测不到它的 IP 地址，难以对它进行攻击，DMZ 区又称为停火区，或安全网络（SSN），它

对外提供服务，系统的开放信息都放在该区（如 HTTP、SMTP、DNS、FTP 等）。由于 DMZ 和内部网是互相隔离的，所以即使受到攻击也不会危及内部网。这种安全的体系结构使得 Intranet、DMZ 和外部网分工明确，界限分明，防止其中一部分瘫痪而影响整个网络。

b。入侵监测体系（IDS）

入侵监测能力是衡量一个防御体系是否完整有效的重要因素。强大的、完整的入侵监测体系可以弥补防火墙相对静态防御的不足。但是，传统的设计中，防火墙和 IDS 各成体系，互不相通，难以提高整体防御体系的智能性和及时性。



图二：使用 LinkTrust™ 防火墙构建入侵监测体系示意

LinkTrust™ 防火墙在设计中利用安氏公司在 IDS 技术方面深厚的积累，充分考虑了用户系统的实际需求，独特的设计可以使防火墙与 IDS 系统完全融为一体。

通过可选的 RS 网络接口，LinkTrust™ 防火墙可以将网络中指定的一部分流量镜像到 RealSecure Network Sensor 系统，RealSecure 系统将处理后的结果通知防火墙系统，要求相应修改安全策略，并可以根据既定策略实时做出响应，利用其强大的入侵监测能力共同保护防火墙和内部网络。

LinkTrust™ 防火墙与 RealSecure 系统一起构成了具有独特设计和强大防护能力的新型网络安全堡垒。

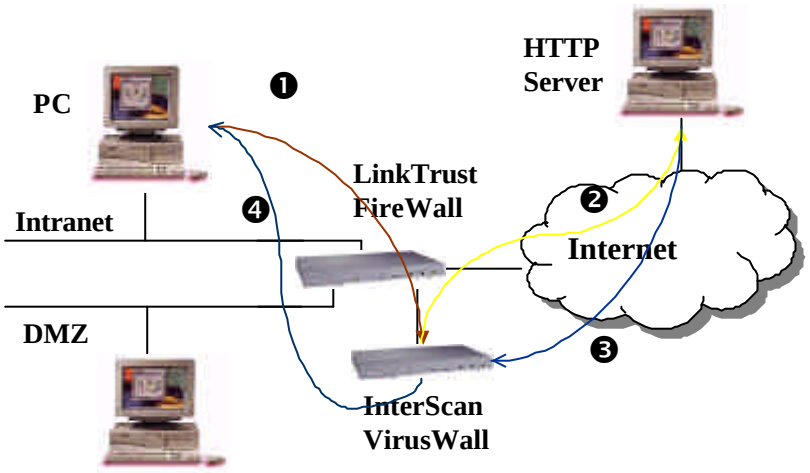
c。病毒保护体系（Anti-Virus）

病毒是当前网络安全体系应该面对的最重要的安全威胁，病毒防

护体系的失败会导致重要文件、数据的丢失、损坏以及重要服务的崩溃。所以，如何解决病毒带来的威胁是网络安全体系必须面临的重要课题之一。LinkTrust™ 防火墙在设计中充分考虑了这一功能需求。

权威数据显示，企业网络中的绝大多数病毒来源于互联网，而病毒传输过程中需要防护的关键点通常有三个：防火墙，用户桌面机以及各种服务器，其中，防火墙更是处于“一夫当关、万夫莫开”的要点，优良的防火墙反病毒能力可以大大减少整个企业网络病毒的威胁。

安氏中国与自己的战略伙伴 - 趋势科技一起利用业界领先的趋势病毒防火墙 InterScan 的专业服务与 LinkTrust™ 防火墙共同设计构建了具有高超反病毒能力的防火墙体系。



图三：使用 LinkTrust™ 防火墙构建反病毒体系示意

通常，带来病毒威胁最大的三种服务分别是：HTTP，FTP，SMTP。图三中是利用 LinkTrust™ 防火墙与 InterScan 共同构成针对 HTTP 服务的反病毒体系的示意图。处于企业内部网的一台 PC 机需要访问互联网中的 HTTP 服务器，并下载文件。这时，通过合理的 LinkTrust 和 InterScan 配置形成的数据流入图所示，这样能够保证所有的内外交换文件都通过病毒检测，避免内部网络受到互联网病毒的威胁。

LinkTrust™ 技术支持

安氏中国为 LinkTrust 防火墙提供专业的防火墙策略制定和管理

服务，以及完善的售前、售后技术支持服务。

安氏中国作为专业的网络安全公司，提供出色的防火墙产品，并致力于成为广大用户的安全合作伙伴和顾问。安氏中国通过提供完善的、多元化的技术服务，竭诚为广大用户服务，满足用户不同程度的需要，最大限度地保障用户的信息安全。

任何购买安氏中国网络安全产品的用户，都能够享受安氏中国全面周到的产品技术服务。

为了保证购买安氏中国安全产品的用户能够更好地使用安氏中国产品，建议用户配套采用安氏中国提供产品技术服务。

安氏中国的承诺：

- 正版承诺——保证向用户提供正版的安氏中国产品；
- 产品到货期承诺——根据合同，保证在用户提出交货申请后 4 周内，安氏中国产品到货；
- 公安部销售许可证承诺——保证产品拥有中华人民共和国公安部颁发的销售许可证；
- Y2K 承诺——保证产品没有计算机两千年问题；
- 中文手册承诺——安氏中国将为用户提供的中文产品手册。

技术支持服务承诺

- 请求渠道畅通承诺——安氏中国承诺用户可以通过热线电话、热线手机、电子邮件、传真等方式，将用户的技术支持服务要求有效地传达到安氏中国的技术支持中心。
- 现场服务响应时间承诺——在上述服务中的‘ 立即启程 ’是指：如果用户所在城市有安氏中国的分公司或者办公机构，安氏中国工程师将立即出发赶赴用户现场 ;如果用户所在城市没有安氏中国的分公司或者办公机构，安氏中国工程师将在有飞机、火车、汽车等交通条件下，选择实际可能的最快方式到达用户现场。
- 问题解决承诺——安氏中国技术支持工程师将及时、准确地回答用户提出的问题。对于一般技术问题，做到当时解决；对于无法立即答复的问题，做到 4 个工作日内给予响应；对于无法解答的问题，

安氏中国工程师将对用户提出的问题备案，在寻求到解决方案后通知用户。

▶技术支持体系承诺—安氏中国技术支持拥有有效的支撑体系，面对用户的技术支持人员背后有多层的支持，包括：当地的技术支持中心，设在北京的技术支持总中心。

▶安氏中国将为用户提供一年时间的免费硬件维修服务。

产品升级服务承诺

▶及时升级承诺——安氏中国承诺在产品的升级版本发布的 3 天内，向用户发出产品升级通知。如果没有收到用户的确认信息，安氏中国将每周试图联络 1 次，直到用户收到升级通知并给予确认。如果联系到用户，对于需要递送介质的用户，升级的产品介质将在联系到的 1 周内寄出或送出。

▶最新安全消息承诺——安氏中国将把用户主要联系人员的邮件地址添加到用户升级邮件列表中，定期向用户发布产品最新动态、产品升级内容、最新安全信息、最新黑客攻击手法警告等，最大限度地保证用户的网络安全，使用户紧跟安全技术的发展。

▶方便升级承诺——安氏中国将把最新的软件产品和相应的补丁、插件、策略库公布在安氏中国网站上，方便用户及时下载。

LinkTrust 防火墙技术性能指标

1）时延；　设计最大策略负载时延为 2~3ms
2）吞吐量；　设计最大策略负载时的吞吐量：79.3M；
　　最小策略负载时为：98.7M
3）最小规则数；　设计性能最大规则 512 条；许可策略 4096 条
4）包转发率；　最大帧长时：65148/秒
5）最大位转发率；98.7Mbps
6）并发连接数；　250000 条

5.3 主机安全

主机系统是网络通信的重要组成部分，是业务和关键信息的主要

承载体。对主机系统的保护成为网络安全防御中的重中之重。多数的网络攻击和入侵目标是网络中的主机系统。本建议书中的主机系统是指华为企业网中用以内部办公、提供平台服务以及辅助服务的 UNIX 类、WINDOWS 9X/NT/2000 类服务器、工作站以及个人 PC 机。

结合 IS-ONE 公司丰富的电信网络安全经验，本建议书认为经过安全加固配置的主机操作系统构成了保护主机系统的基础。通常缺省安装配置下的主机网络操作系统面临着来自网络和内部恶意用户的收集信息攻击、猜测口令攻击、拒绝服务攻击、（远程和本地）缓冲区溢出攻击等巨大威胁，缺省配置下的操作系统服务无法有效识别系统中的特洛异木马程序和入侵者安装的黑客后门程序等，无法准确记录和定位攻击和入侵者的“足迹”。

考察华为企业网的实际组成运行情况后，IS-ONE 公司在本次安全工程将提供强大的、高度专业化主机系统加固配置服务。主机系统加固配置安全服务覆盖了安装系统补丁、系统服务和帐号的安全化、安全配置系统内核参数、配置访问控制策略（详见“访问控制”一节）、集中式的日志审计（详见“日志和审计”一节）、关键文件完整性检测等。

下面将分别对华为网中运行的 UNIX（以 SOLARIS 为代表）、WINDOWS NT/2000、WINDOWS 9X 等三类主要网络操作系统和数据库（SQL Server、Sybase Server、Oracle Server）的安全加固配置进行陈述。

5.3.1 推荐安全服务——UNIX 类主机安全加固服务

该服务是 eSafelink Professional 专业安全服务中的一项。

UNIX 类服务器和工作站由于其出色的稳定性和高性能而成为电信级的网络操作系统，当前承担着电信级网络的关键任务。缺省安装的 UNIX 操作系统（以 SOLARIS 为例）会存在以下安全问题：

- 打开 FINGER（泄露系统信息）
- 打开各类 RPC（存在大量的远程缓冲区溢出、泄露系统信息）
- 打开 SENDMAIL（许多安全漏洞、垃圾邮件转发等）
- 打开 NAMED（远程缓冲区溢出、拒绝服务攻击等）
- 打开 SNMP（泄露系统信息）
- 操作系统内核中的网络参数存在许多安全隐患（IP 转发、堆

栈参数等）

- 存在各种缓冲区溢出漏洞
- 存在其它方面的安全问题

IS-ONE 公司将详细分析华为企业网络中的 UNIX 类主机的任务和生产关系，准确制定服务操作细则。通常会包括以下内容：

- 分析主机系统的任务和服务类型
- 检查分析现有系统的安全漏洞和黑客后门等
- 分别制定操作细则
- 安装最新的操作系统补丁
- 关闭系统缺省打开的不必要服务
- 删除系统缺省设置的、以及其它原因设置的不必要帐号
- 修改安全化操作系统内核参数
- 修改安全化系统缺省日志体系（详见“日志和审计”一节）
- 安装加密通信工具（详见“信息加密”一节）
- 配置访问控制策略（详见“访问控制”一节）
- 系统关键文件数字签名、定期完整性检测配置

5.3.2 推荐安全服务——WINDOWS NT/2000 类主机安全加固服务

该服务是 eSafelink Professional 专业安全服务中的一项。

WINDOWS NT 操作系统由于其简单明了的图形化操作界面以及逐渐提高的系统稳定性和性能等成为电信级企业中的辅助性网络操作系统，并且在企业办公网络中占有重要地位。WINDOWS NT 系统的安全水平取决于管理员在安装过程、补丁安装过程、应用服务配置过程中的安全修养和实际考虑。缺省安装的 WINDOWS NT 操作系统的安全问题不能通过安装最新的服务包（SERVICE PACK）完全解决，它们通常会出现下述安全问题：

- 最新的 SERVICE PACK 没有解决的安全漏洞
- 缺省安装的服务程序带来的各种安全问题
- 系统注册表属性安全问题
- 文件系统属性安全问题
- 缺省帐号安全问题
- 文件共享方面的安全问题
- 其它方面的安全问题

IS-ONE 公司将详细分析华为企业网网络中的 WINDOWS NT/2000 主机的任务和生产关系，准确制定相应的服务操作细则。通常会包括以下内容：

- 分析主机系统的任务和服务类型
- 检查分析现有系统的安全漏洞和黑客后门等
- 分别制定操作细则
- 安装最新的服务包（SERVICE PACK）
- 选择安装适当的安全漏洞补丁（HOTFIX 等）
- 关闭系统缺省打开的不必要服务
- 安全配置 IIS
- 删除系统缺省设置的、以及其它原因设置的不必要帐号
- 安全配置操作系统注册表参数
- 安全配置文件属性
- 安全配置系统缺省日志体系（详见“日志和审计”一节）
- 安装加密通信工具（详见“信息加密”一节）
- 配置访问控制策略（详见“访问控制”一节）
- 系统关键文件数字签名、定期完整性检测配置

5.3.3 推荐安全服务——WINDOWS 9X 类主机安全加固服务

该服务是 eSafelink Professional 专业安全服务中的一项。

当前 WINDOWS 9X 操作系统是办公网络、网络管理和监视等的重要组成部分。借助 WINDOWS 95/98 系统中存在的漏洞，攻击和入侵者可以直接窃取用户口令、窃取重要数据文件、安装木马程序、采用逐渐参透方法入侵其它主机等。一方面，网管人员习惯使用 WINDOWS 9X 系统进行日常的电子通信、文件编辑、资源共享、文件打印、登录其它主机、浏览网页等；另一方面，WINDOWS 9X 系统的安全问题容易受到忽视而导致安全管理方面的松懈。因此，由此导致的网络安全威胁不容忽视。

- WINDOWS 9X 系统通常存在的安全问题包括以下方面：
- WINDOWS 9X 系统经常出现的拒绝服务攻击漏洞
- IE 浏览器出现的各种安全问题
- WINDOWS 资源共享导致的安全问题
- 电子邮件携带的病毒和木马程序

- IRC、ICQ、OICQ 等网络联络工具带来的安全问题
- WINDOWS 9X 系统中存在的其它安全问题

IS-ONE 根据自身丰富的安全管理经验和专业技术，从华为企业网的实际安全需求出发，在对 WINDOWS 9X 系统提供防病毒保护（详见“防病毒”一节）之外，将提供以下内容的安全服务，并帮助制定相应的安全管理制度。

- 制定详细的操作细则
- 检查分析现有系统的安全漏洞和黑客后门等
- 安装最新的 WINDOWS 9X 补丁
- 安装安全加密通信工具
- WINDOWS 9X 用户安全咨询

5.3.4 推荐安全服务——数据库服务器加固服务

数据库服务器上的数据是企业的信息系统的“生命”

5.3.5 推荐安全服务——风险评估和服务

eSafeLink 风险评估和服务是主机安全加固服务的基础。参见 5.4 安全风险评估。

5.3.6 建议方案

各类主机安全加固服务是华为企业网全网信息安全完整解决方案中必须的一项服务。

在服务范围方面可以根据华为企业网的具体情况分步骤实施：首先解决相关核心子网和其他骨干节点网络中的主机安全加固，之后再实施节点、二级节点的主机安全加固。

5.4 安全风险评估

5.4.1 风险评估技术

风险评估（Vulnerability Assessment）是网络安全防御中的一项重要技术，其原理是根据已知的安全漏洞知识库，对目标可能存在的安全隐患进行逐项检查。目标可以是工作站、服务器、交换机、数据库应用等各种对象。然后根据扫描结果向系统管理员提供周密可靠的安全性分析报告，为提高网络安全整体水平产生重要依据。在网络安全体系的建设中，安全扫描工具花费低、效果好、见效快、与网络的运行相对对立、安装运行简单，可以大规模减少安全管理员的手工劳动，有利于保持全网安全政策的统一和稳定。风险评估技术基本上也可分为基于主机的和基于网络的两种，前者主要关注软件所在主机上面的风险漏洞，而后者则是通过网络远程探测其它主机的安全风险漏洞。安氏公司开创了风险评估技术新的领域，即基于数据库的风险评估技术，使风险评估内容更加完善。

由于网络采用的通信协议并不是为安全通信而设计的，这些协议和网络设备存在一些固有的安全隐患，入侵者可利用这些漏洞，通过网络实施攻击。基于网络的风险评估技术，主要是模拟黑客攻击的方法，检测网络协议、网络服务、网络设备等方面的漏洞。

现代操作系统代码数量巨大，成百上千工程师的共同设计编制，很难避免产生安全漏洞。随着及计算机技术的发展，操作系统的功能越来越强大，但配置越来越复杂。面对横跨多种平台、不同版本、不同种类的操作系统，系统管理员显得力不从心，经常会造成配置上失误，产生安全问题。系统安全漏洞涉及口令设置、文件权限、账户管理、组管理、系统配置等。基于主机的风险评估技术，主要检查操作系统本身固有的安全漏洞和系统文件的不安全配置。并指示用户如何修补漏洞以使操作系统安全风险降到最小，也就增加了整个网络系统的安全性。

越来越多的关键业务系统和宝贵的信息资源依赖于数据库平台，数据库本身的漏洞和错误配置同样会引起严重的安全问题。数据库风险评估技术主要针对数据库系统的授权、认证和完整性方面进行安全漏洞检测。

5.4.2 推荐安全产品—安氏网络漏洞扫描器 Internet Scanner

产品简介

该产品的时间策略是定时操作，扫描对象是整个网络。它可在一台单机上对已知的网络安全漏洞进行扫描。截止 Internet Scanner6.01 **版本，**Internet Scanner **已能对** 900 **种以上的来自通讯、服务、防火墙、**WEB **应用等的漏洞进行扫描。它采用模拟攻击的手段去检测网络上每一个** IP **隐藏的漏洞，其扫描对网络不会做任何修改和造成任何危害。**

Internet Scanner **包括三个组成部分：**

- Web Security Scanner:**针对** Web **站点的漏洞扫描**
- Firewall Scanner：**针对防火墙的漏洞扫描**
- Intranet Scanner：**针对通讯和服务的漏洞扫描**

Internet Scanner **每次扫描的结果可生成详细报告，报告对扫描到的漏洞按高、中、低三个风险级别分类，每个漏洞的危害及补救办法都有详细说明。用户可根据报告提出的建议修改网络配置，填补漏洞。**

可检测漏洞分类表：

Brute Force Password-Guessing	**为经常改变的帐号、口令和服务测试其安全性**
Daemons	**检测** UNIX **进程（**Windows **服务）**
Network	**检测** SNMP **和路由器及交换设备漏洞**
Denial of Service	**检测中断操作系统和程序的漏洞，一些检测将暂停相应的服务**
NFS/X Windows	**检测网络网络文件系统和** X-Windows **的漏洞**
RPC	**检测特定的远程过程调用**
SMTP/FTP	**检测** SMTP **和** FTP **的漏洞**
Web Server Scan and CGI-Bin	**检测** Web **服务器的文件和程序（如** IIS,CGI **脚本和** HTTP**）**
NT Users, Groups, and Passwords	**检测** NT **用户，包括用户、口令策略、解锁策略**
Browser Policy	**检测** IE **和** Netscape **浏览器漏洞**
Security Zones	**检测用于访问互联网安全区域的权限漏洞**
Port Scans	**检测标准的网络端口和服务**
Firewalls	**检测防火墙设备，确定安全和协议漏洞**
Proxy/DNS	**检测代理服务或域名系统的漏洞**
IP Spoofing	**检测是否计算机接收到可疑信息**
Critical NT **安氏** ues	**包含** NT **操作系统强壮性安全测试和与其相关的活**

	动
NT Groups/Networking	检测用户组成员资格和 NT 网络安全漏洞
NetBIOS Misc	检测操作系统版本和补丁包、确认日志存取，列举、显示 NetBIOS 提供的信息
Shares/DCOM	检测 NetBIOS 共享和 DCOM 对象。使用 DCOM 可以测试注册码、权限和缺省安全级别
NT Registry	包括检测主机注册信息的安全性，保护 SNMP 子网的密匙
NT Services	包括检测 NT 正在运行的服务和与之相关安全漏洞

配置方案

在华为企业网络相关各骨干结点或网络安全管理中心，分别配置一套 Internet Scanner。建议产品安装在笔记本电脑中，由各结点或网络安全管理中心专人负责，定期对本结点及所辖范围的下级结点进行全面的网络安全评估，包括所有重要的服务器、防火墙、路由设备等。

漏洞报告分发：由安全管理部门统一下发至相关设备几节点的负责单位和个人。

产品运行环境要求

Windows NT 4.0 Workstation 系统需求

项目	最小系统需求
处理器	200MHz Pentium Pro（推荐 300MHz Pentium）
操作系统	安装了 Service Pack 6 的 Windows NT 4.0 Workstation(强烈建议使用独立、专用系统进行扫描） 注意：互联网扫描器不支持Windows NT 3.51， Windows NT 4.0 Server，Windows 2000 Server， 或Windows 2000 Advanced Server 同RealSecure协同工作：推荐Windows 2000 Professional
其他软件	Microsoft IE 4.X 或更高版本用于运行 HTML 帮助 Adobe Acrobat Reader 4.x 或更高版本用于查看..\Scanner6\Manuals 目录下的 PDF 文件
内存	通常扫描：80MB 大规模扫描：128MB（推荐 256MB）
硬盘	从文件安装需要 180MB，从 CD 安装需要 60MB。 运行时：55MB + 2.5MB 每 100 个主机 推荐 NTFS 分区
用户权限	本地或域管理员
网络	连接到一个活动网络中的 Ethernet 或 Token Ring
协议	TCP/IP
MDAC	2.1 或更高版本
显示	支持最少 256 色、800x600 分辨率的显示器

Windows 2000 Professional 系统需求：

项目	最小系统需求
处理器	200MhzPentium Pro（推荐 300MHz Pentium）
操作系统	Windows 2000 Professional（强烈建议使用独立、专用系统进行扫描） 注意：互联网扫描器不支持Windows NT 3.51， Windows NT 4.0 Server，Windows 2000 Server， 或Windows 2000 Advanced Server同RealSecure协同工作：推荐Windows 2000 Professional
其他软件	Microsoft IE 4.X 或更高版本用于运行 HTML 帮助 Adobe Acrobat Reader 4.x 或更高版本用于查看..\Scanner6\Manuals 目录下的 PDF 文件
内存	通常扫描：80MB 大规模扫描：128MB（推荐 256MB）
硬盘	从文件安装需要 180MB，从 CD 安装需要 60MB。 运行时：55MB + 2.5MB 每 100 个主机 推荐 NTFS 分区
用户权限	本地或域管理员
网络	连接到一个活动网络中的 Ethernet 或 Token Ring
协议	TCP/IP
MDAC	2.5
显示	支持最少 256 色、800x600 分辨率的显示器

增加软件和硬件

项目	地点	数量
Internet Scanner	网络各骨干结点	
笔记本电脑	网络各骨干结点	

5.4.3 推荐安全产品—安氏系统漏洞扫描器 System Scanner

产品简介

该产品的时间策略是定时操作，扫描对象是操作系统。System Scanner 包括引擎和控制台两个部分。引擎必须分别装在被扫描的服务器内部，在一台集中的服务器上安装控制台。控制台集中对各引擎管理，引擎负责对各操作系统的文件、口令、帐户、组等的配置进行检查，并对操作系统中是否有黑客特征进行检测。

其扫描结果同样可生成报告。并对不安全的文件属性生成可执行的修改脚本。

配置方案

该产品可实现远程扫描管理。在华为企业网络的骨干结点或网络安全管理中心，配置一套 System Scanner Console。建议安装在笔记本电脑中（可以与 Internet Scanner 安装在同一台电脑内），由各结点专人负责保管。在各结点的重要服务器内安装 System Scanner Agent，每个结点的 System Scanner Console 分别管理本结点及管辖范围内的下级结点的各个 System Scanner Agent。定期对本结点及所辖范围的二级结点进行全面的操作系统安全评估，包括所有重要的服务器，如 WWW 服务器、FTP 服务器、E-mail 服务器、News 服务器、DNS 服务器、RADIUS 服务器和生产系统服务器等。

漏洞报告分发：由安全管理部门统一下发至相关设备或子网的负责单位或个人。

产品运行环境要求

Console 系统需求

平台	最小系统需求
Windows NT	200 MHz Pentium II 处理器（推荐300MHz或更快的处理器） 64 MB内存（推荐128MB或更大的内存） 安装了Service Pack 4或5的Windows NT 4.0 Workstation或Server Windows NTFS磁盘分区 100M剩余磁盘空间 2GB磁盘空间用于存储漏洞扫描结果和报告

	256色、1024x768图形分辨率 Microsoft IE 4.0，Netscape 4.0及以上或相对应的其他浏览器 MDAC 2.0.3 或者 2.1 SP2 注意：系统扫描器控制台 4.0 不支持 MDAC（微软数据库访问组件）2.5 安装 TCP/IP 协议，并且能够直接解析代理和控制台的主机名

Agent 系统需求

平台	最小系统需求
Windows NT	安装了Service Pack 4或5的Windows NT 4.0 Workstation、Server或Enterprise Server Windows NTFS磁盘分区 64 MB内存 35M剩余磁盘空间 50M磁盘空间用于存储扫描结果 安装 TCP/IP 协议，并且能够直接解析代理和控制台的主机名
Windows 2000	Windows 2000 Professional、Windows 2000 Server Windows NTFS磁盘分区 64 MB内存 35M剩余磁盘空间 50M磁盘空间用于存储扫描结果 安装 TCP/IP 协议，并且能够直接解析代理和控制台的主机名
UNIX (包含系统扫描器3和4版本的系统需求)	32 MB内存/交换内存 10M剩余磁盘空间 50M磁盘空间用于存储扫描结果 安装 TCP/IP 协议，并且能够直接解析代理和控制台的主机名

增加软件和硬件

项目	地点	数量
System Scanner Console	各骨干结点或网络安全管理中心	
System Scanner Agent	骨干结点的重要服务器内 结点的重要服务器内 各二级结点的重要服务器内	
不需增加硬件		

5.4.4 推荐安全产品－安氏数据库漏洞扫描器 DatabaseScanner

产品简介

该产品可保护存储在数据库管理系统中的数据的安全。Database Scanner **增强了安氏在安全领域的市场领先地位，并且目前安氏是唯一提供数据库安全管理解决方案的厂商。用户可通过该产品自动生成数据库服务器的安全策略，这是全面的企业安全管理的一个新的重要的领域。**

Database Scanner **具有灵活的体系结构，允许客户定制数据库安全策略并强制实施，控制数据库的安全。用户在统一网络环境可为不同数据库服务器制定相应的安全策略。一旦制定出安全策略，**Database Scanner **将全面考察数据库，对安全漏洞级别加以度量的控制，并持续改善数据库的安全状况。**

Database Scanner **能通过网络快速、方便地扫描数据库，去检查数据库特有的安全漏洞，全面评估所有的安全漏洞和认证、授权、完整性方面的问题。**

Database Scanner **漏洞检测的主要范围包括：**

- 2000 **年问题 — 分析数据环境并报告数据和过程中存在的** 2000 **年问题。**
- **口令，登录和用户 — 检查口令长度，检查有登录权限的过去用户，检查用户名的信任度。**
- **配置 — 验证是否具有潜在破坏力的功能被允许，并建议是否需要修改配置，如回信，发信，直接修改，登录认证，一些系统启动时存储的过程，报警和预安排的任务，**WEB **任务，跟踪标识和不同的网络协议。**
- **安装检查 — 提示需要客户打补丁及补丁的热链接。**
- **权限控制 — 检查那些用户有权限得到存储的过程及何时用户能未授权存取** Windows NT **文件和数据资源。它还能检查“特洛伊木马”程序的存在。**

配置方案

针对华为企业网数据库服务器，配置的扫描服务器，即笔记本电脑中安装 DBscanner 软件。定期对 4 套数据库服务器软件进行漏洞评估，并将软件生成的漏洞报告分发给数据库管理员，对数据库系统中的安全问题及时修复。

产品运行环境要求

项目	最小系统需求
操作系统	Windows 2000 Professional; 安装了 Service Pack 3 或更高版本的 Windows NT 4.0
浏览器	安装了 Service Pack 1 或更高版本的 Microsoft IE 4.01
处理器	Pentium 以上处理器
内存	16MB+15MB×同时扫描的系统数
硬盘	60M 剩余磁盘空间
数据库网络连接	使用一个具有足够访问权限的帐号对每种数据库进行安全扫描检测，每种数据库的需求细节请参照该“数据库访问需求”

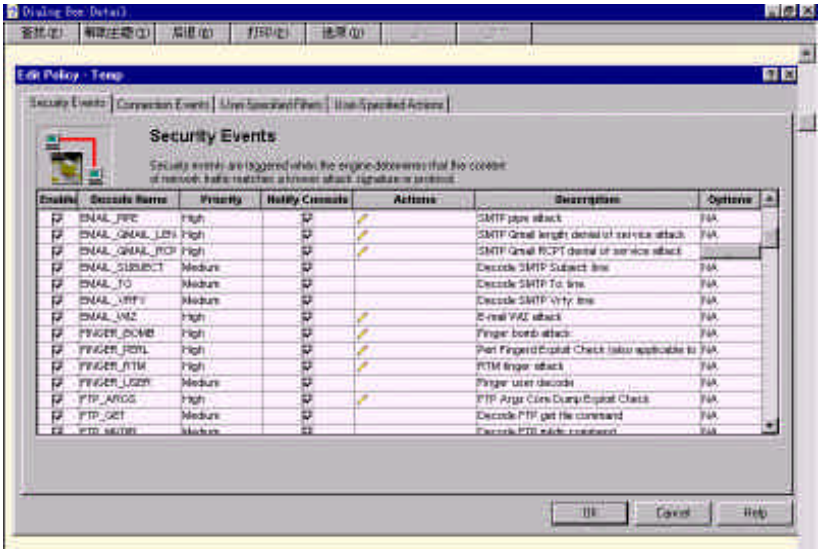
增加软件和硬件

项目	地点	数量
Dbscanner 硬件		

5.4.5 安氏产品特点

方便、易用

安氏产品提供统一的图形用户界面，用户可在集中的控制界面上对整个网络进行安全管理。扫描策略、监控策略的配置均通过简单易学的鼠标操作实现。



强大的日志、报警能力

安氏产品后台均有数据库系统支持，对扫描、监控的结果都以统一数据库格式存储。

Internet 扫描记录如下内容：

- 扫描起始、结束时间
- 被扫描主机的用户名
- 被扫描的主机和网络设备的 IP 地址，操作系统类型
- 网络系统中存在漏洞
- 每台主机提供的服务端口；

System Scanner 扫描记录如下内容：

- 扫描起始、结束时间
- 被扫描的主机的 IP 地址
- 操作系统类型，存在的安全漏洞

- 系统中是否有特洛伊木马程序驻留

对于监控能够根据用户的配置记录如下内容：

- 记录攻击发生的时间，IP 地址，MAC 地址
- 网络系统内新增加设备的 IP 地址、域名等信息
- 攻击的击键过程
- 正常网络操作的源、目的 IP 地址，源目的服务端口号

报警有如下形式：

- Internet Scanner 运行时对扫描的主机发消息，告之正在被扫描
- 监控到网络事件时，给网络管理员发电子邮件
- 监控到网络事件时，向网管软件发 SNMP 陷阱
- 监控到网络事件时，向 CheckPoint 防火墙、Lucent 防火墙的控制台发警告，并重新配置防火墙
- 监控到网络事件时，通知监控控制台
- 监控到网络事件时，执行用户指定的脚本

丰富的报告格式

安氏产品提供各种报告格式，并允许用户定制客户化的报告格式，可满足不同层次的要求。

- 行政级报告：以图表为主，提供漏洞趋势分析、各级风险漏洞占比分析，网络安全漏洞摘要，企业经理对网络安全状况可一目了然；
- 部门级报告：以图表和辅助文字说明为主，提供主机、服务端口、漏洞等报告，帮助部门经理了解漏洞分布情况；
- 技术级报告：提供详细的技术报告，可按照 IP 地址、服务、漏洞级别等各种方式索引生成报告。报告中对每个漏洞提供详细说明及补救漏洞办法，网络安全管理员可根据技术报告的详尽描述实施网络安全。

性能稳定

安氏 产品技术成熟，已经过全球 3000 家以上的大型企业的网络

环境的考验，产品性能稳定。在实施网络安全管理的过程中，安氏产品不会增加网络负载，不影响业务系统的正常运转，确实能有效地保护网络的安全，将网络风险降为最小。

网络安全工业标准

安氏中 Ineternet Scanner 被国际计算机安全委员会 ICSA 用于防火墙产品出厂前的检测工具，只有经过 Ineternet Scanner 检测合格的防火墙产品才具备 ICSA 认证资格。因此，安氏产品已经成为网络安全工业标准

5.4.6 推荐安全服务—安全风险评估服务

安氏依靠雄厚的技术力量和业界最优秀的产品为用户提供广受赞誉的漏洞评估服务，该服务为用户提供：

- 关键信息系统广泛深度的漏洞探测。
- 测评系统弱口令，系统配置缺陷，系统潜在危险操作等等。
- 对发现漏洞及可能造成的风险给出详细，按危险等级排序的详细总结报告。
- 给出系统风险修正措施以及系统安全指导性架构。
- 安全专家提供安全意识，知识培训。

上述风险评估给用户带来的收益：

- 明确界定公司/组织网络的关键信息系统，服务器等等。
- 获得第三方公正，客观的网络安全状况评估。
- 测评安全漏洞并且不对系统产生不良影响。

安全风险评估的步骤

安氏公司的漏洞评估服务通过可回溯，螺旋循环进行的三步过程组成。利用安氏享誉业界的专门技术以及最可靠，最先进的自动化安全评估工具，通过安氏富有经验的网络安全专家的全面监控和测评，对用户关键网络系统给出准确的安全风险评估。

步骤 1：资料收集与准备

在这个环节，安氏向客户解释测评所需的所有要素。特别是用户的漏洞扫描要求通过问卷和需求表的形式收集。确定要评估的网段及系统，确认所需的场地和设备，所有条件确认后双方商定测评时间。

步骤 2：扫描及安全知识讲座

安氏的网络专家将在客户现场进行一个评估前的知识交流，包括：漏洞评估的概要，评估要求概述等等。安氏专家随后将根据客户要求配置扫描工具并启动对客户网络的漏洞扫描工作。

同时，安氏网络安全专家为客户提供两个层面的知识讲授。第一层面包括公司/组织的网络安全意识和企业网络安全管理事宜。第二个层面从技术上对测试工具的安装和特点进行讲解。

步骤 3：分析与建议

安氏专家完成扫描以后，对扫描报告进行分析，并按照系统中危险程度和潜在的影响级别给出风险等级报告。依据测试报告，安氏安全专家将给客户给出有优先顺序的解决方法和防卫措施，来最大限度的减低客户网络的风险。

安氏安全专家将针对扫描发现和建议措施给出草拟陈述性报告以及一份最终正式的评估讲解。草拟报告有利于安氏和客户沟通发现的问题并讨论给出符合用户特殊要求的解决方案。正式报告在最终讲解后 5 天内送达客户。

风险评估的技术实施环节

漏洞扫描服务通过综合的安全分析和漏洞检查帮助客户了解现有的安全状况。这个评估根据运行需求，安全策略和商业需求来建立当前的设计方案，从而确定实施一个信息安全管理方案（例如危险管理）的适当需求。这个阶段包含以下工作：

1 检查现有网络技术结构

了解华为公司的逻辑网络，由什么物理网络组成以及网络的关键设备的位置所在对于保持网络的安全是非常重要的。另外，鉴定关键网络拓扑，对于成功地一个实施基于网络的危险管理方案是很关键的。基本信息包括网络带宽，协议，硬件（例如：交换机，路由器等）

Internet 接入，地理分布方式和网络管理。这项工作将使项目团队对华为公司和企业需求更熟悉。如果有必要，在华为公司的网络结构内的关键网络位置出要进行网络流量分析。

2 检查现有信息安全策略

将要对现在的信息安全策略、标准和指导方针进行一次检查，这个检查将提供适当的信息，以便构造一个与那些文件的要求相一致的风险管理方案。另外，安氏将和华为公司一道工作，开发一个用在华为公司操作中心内的合适的升级管理程序，对事件通知方法和事件紧急性进行评估来决定联系谁。工作人员信息和责任结构将由华为公司提供。以帮助决定在发生何种类型事件应联系何人。

3 要确定实施一个安全方案（如风险管理）的当时操作环境，进行一个操作评估是基本条件，以下的信息将会通过检查和分析得到：

A 鉴定关键设备和企业职能——包含或提供对于企业是关键性的系统和资源应被恰当地鉴定出

B 鉴定信息技术商业战略和关系——企业战略和关系在确定适当合理的控制措施方面起到关键性作用，这些控制措施要求提供最高等级的风险管理，并且对效率的影响最小。

C 确定影响和需要保证的程序——基于通过以上措施确定的企业目标，保证等级能被确定，并能够提供风险的范围和等级以及需要的适当控制措施：

● 紧急性等级	服务中断时间（举例）
● MC：最紧急／大量用户	不超过２小时
● C： 关键的企业职能	２到４小时
● R： 需要的企业职能	４到６小时
● N： 必要的企业职能	６到时１２小时
● I： 重要	１２到２４小时

D） 检查边界网络控制措施——这项工作的目的是检查当前实施的边界网络控制措施，这个检查将包括防火墙、路由器和远程访问服务器。特别是，安氏将检查这些现有的控制规则，措施。

- 访问控制配置和验证机制
- 过滤规则
- 日志、通知系统日志和审计功能
- 代理配置（作为可用的）

- **周边设备安全等级（如** B2，B1，SecureOS **等）**

E）选择性漏洞扫描分析样例——安氏将选择一个与实施危险胁管理方案相关的系统范例，并进行一次基于网络的漏洞评估以获得对华为公司服务器，安全状态的总体认识，这个信息对于确定反映华为公司当前安全状况，便于安氏实施威险管理方案的基准配置是很有用的。

使用工具：

安氏 互联网扫描器 Internet Scanner6.01

安氏 系统扫描器 System Scanner4.0

安氏 数据库扫描器 Database Scanner4.0

5.5 入侵监控和防御

5.5.1 入侵检测技术

大多数传统入侵检测系统（IDS）采取基于网络或基于主机的办法来辩认并躲避攻击。在任何一种情况下，该产品都要寻找“攻击标志”，即一种代表恶意或可疑意图攻击的模式。当 IDS 在网络中寻找这些模式时，它是基于网络的。而当 IDS 在记录文件中寻找攻击标志时，它是基于主机的。每种方法都有其优势和劣势，两种方法互为补充。一种真正有效的入侵检测系统应将二者结合。本节讨论了基于主机和基于网络入侵检测技术的不同之处，以说明如何将这二种方式融合在一起，以提供更加有效的入侵检测和保护措施。

基于网络的入侵检测

基于网络的入侵检测系统使用原始网络包作为数据源。基于网络的 IDS 通常利用一个运行在随机模式下网络的适配器来实时监视并分析通过网络的所有通信业务。它的攻击辩识模块通常使用四种常用技术来识别攻击标志：

- 模式、表达式或字节匹配
- 频率或穿越阀值
- 低级事件的相关性
- 规统学意义上的非常规现象检测

一旦检测到了攻击行为，IDS 的响应模块就提供多种选项以通知、报警并对攻击采取相应的反应。反应因产品而异，但通常都包括通知管理员、中断连接并且/或为法庭分析和证据收集而做的会话记录。

基于主机的入侵检测

基于主机的入侵检测出现在 80 年代初期，那时网络还没有今天这样普遍、复杂，且网络之间也没有完全连通。在这一较为简单的环境里，检查可疑行为的检验记录是很常见的操作。由于入侵在当时是

相当少见的，在对攻击的事后分析就可以防止今后的攻击。

现在的基于主机的入侵检测系统保留了一种有力的工具，以理解以前的攻击形式，并选择合适的方法去抵御未来的攻击。基于主机的 IDS 仍使用验证记录，但自动化程度大大提高，并发展了精密的可迅速做出响应的检测技术。通常，基于主机的 IDS 可监探系统、事件和 Window NT 下的安全记录以及 UNIX 环境下的系统记录。当有文件发生变化时，IDS 将新的记录条目与攻击标记相比较，看它们是否匹配。如果匹配，系统就会向管理员报警并向别的目标报告，以采取措施。

基于主机的 IDS 在发展过程中融入了其它技术。对关键系统文件和可执行文件的入侵检测的一个常用方法，是通过定期检查校验和来进行的，以便发现意外的变化。反应的快慢与轮询间隔的频率有直接的关系。最后，许多产品都是监听端口的活动，并在特定端口被访问时向管理员报警。这类检测方法将基于网络的入侵检测的基本方法融入到基于主机的检测环境中。

将基于网络和基于主机的入侵检测结合起来

基于网络和基于主机的 IDS 方案都有各自特有的优点，并且互为补充。因此，下一代的 IDS 必须包括集成的主机和网络组件。将这两项技术结合，必将大幅度提高网络对攻击和错误使用的抵抗力，使安全策略的实施更加有效，并使设置选项更加灵活。

有些事件只能用网络方法检测到，另外一些只能用主机方式检测到，有一些则需要二者共同发挥作用，才能检测到。

5.5.2 推荐安全产品——安氏的入侵检测产品 RealSecure

安氏实时网络引擎 (RealSecure Network Sensor) 对计算机网络进行自主地，实时地攻击检测与响应。这种领先产品对网络安全轮回监控，使用户可以在系统被破坏之前自主地中断并响应安全漏洞和误操作。实时监控在网络中分析可疑的数据而不会影响数据在网络上的传输。它对安全威胁的自主响应为企业提供了最大限度的安全保障。

安氏 网络入侵检测(RealSecure Network Engine)在检测到网络入侵后，除了可以及时切断攻击行为之外，还可以动态地调整防火墙的防护策略，使得防火墙成为一个动态的智能的的防护体系。

安氏实时系统代理 (RealSecure System Sensor) 对计算机主机操作系统进行自主地，实时地攻击检测与响应。一旦发现对主机的入侵，RealSecure 可以马上切断的用户进程，和做出各种安全反应。

RealSecure Workgroup Manager 是 RealSecure 系统的控制台。可以对多台 RealSecure 网络引擎和系统代理进行管理。对被管理监控器进行远程的配置和控制，各个监控器发现的安全事件都实时地报告控制台。

安氏 RealSecure 是一个完整的，一致的实时入侵监控体系。

5.5.2.1 功能描述

安氏 Realsecure 对来自内部和外部的非法入侵行为做到及时响应、告警和记录日志，并可采取一定的防御和反入侵措施。它能完全满足《华为企业网全网安全解决方案招标书》所提要求：

支持统一的管理平台，可实现集中式的安全监控管理；

RealSecure Workgroup Manager 是 RealSecure 系统的控制台。可以对多台 RealSecure 网络 Sensor 和系统 Sensor 进行管理。对被管理监控器进行远程的配置和控制，各个监控器发现的安全事件都实时地报告控制台。

在华为企业网中可以利用这一特点，实现对各结点的集中监控管理。例如，从核心骨干结点或网络安全管理中心的 RealSecure

Workgroup Manager，对其下级各结点进行统一的 Sensor 监控策略配置，Sensor 所发现的安全事件将实时地报告给 Manager；对各个 Sensor 安全特征库的升级也可以从 Manager 统一分发完成。

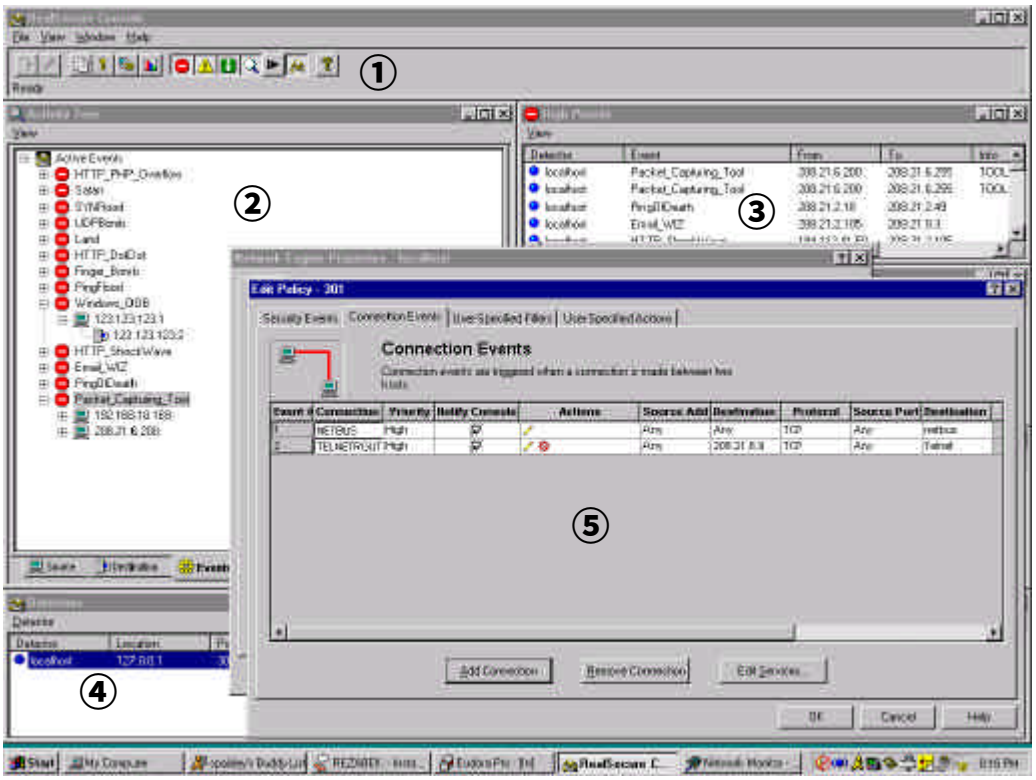


图 RS-1 RealSecure Workgroup Manager 的工作界面

①主菜单和工具栏
②监控安全事件的综合窗口
③按安全级别分成高、中、低三个事件窗口
④列出所有被管理的网络 Sensor 和系统 Sensor
⑤对被管理的网络引擎和系统代理进行配置的弹出窗口

自动识别类型广泛的攻击；

网络 Sensor 能够识别以下种类的攻击和误用行为：

类型	说明
拒绝服务攻击	通过消耗系统资源使目标主机的部分或全部服务功能丧失。例如，SYN FLOOD 攻击，PING FLOOD 攻击，WINNUK 攻击等。
分布式拒绝服务攻击	检查分布拒绝服务攻击的主控程序和代理之间的通讯和通讯企图。例如，TFN、Trinoo 和 Stacheldraht 等。
未授权访问攻击	攻击者企图读取、写或执行被保护的资源。如 FTP ROOT 攻击，EMAIL WIZ 攻击等。
预攻击探测	攻击者试图从网络中获取用户名、口令等敏感信息。如 SATAN 扫描、端口扫描、IP HALF 扫描等。
可疑行为	非“正常”的网络访问，很可能是需要注意的不安全事件。如 IP 地址复用，无法识别 IP 协议的事件。
协议解码	对协议进行解析，帮助管理员发现可能的危险事件。如 FTP 口令解析，EMAIL 主题解析等。
普通网络事件	识别各种网络协议包的源、目的 IP 地址，源、目的端口号，协议类型等。

系统 Sensor 能够监控并识别的攻击类型有：

类型	说明
安全事件	监控 NT 或 Unix 系统事件 login 成功/失败，logout，管理员行为异常，系统重启动等； 监控特殊的系统事件，包括对重要文件的读写、删除行为，系统资源情况异常现象等； 监控 Windows 环境下的未授权事件，如企图访问未授权文件，访问特权服务，企图改变登录权限等。
对未用端口监控	监控对未提供服务端口的连接企图，这种连接企图应视为可疑行为。例如，对未提供 FTP 服务的主机尝试 FTP 连接被认为是可疑的。
远程 UNIX Syslog 事件	对远程的 UNIX 主机进行监控。监控用户的 login 成功/失败，logout，管理员行为异常等；监控的服务包括 IMAP2bis，IPOP3，Qpopper，Sendmail 和 SSH 等。
自定义事件	用户自定义的基于系统审计事件的监控

支持按行为特征的入侵检测；

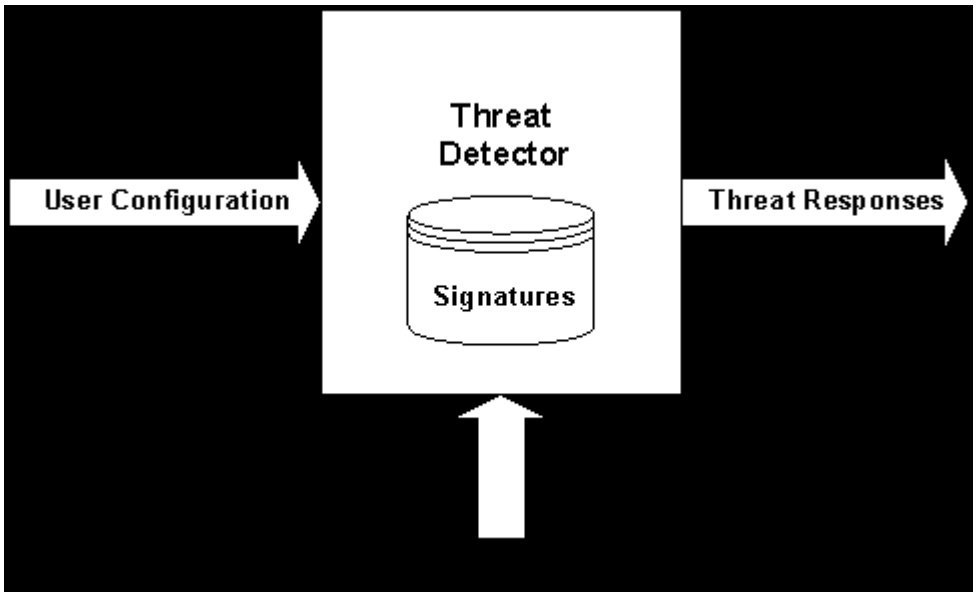


图 RS-2 RealSecure Sensor 工作过程示意图

如图所示，Realsecure 的入侵检测主要是依据用户事先定义的监控策略，将发生的入侵事件与已有的安全事件特征库进行特征匹配，匹配成功，则认为是有威胁事件发生，采取适当的响应动作。

具体分析：

过程的输入包括：

- 用户或者安全管理人员定义的配置规则；
- 以及作为事件检测的原始数据。对于 Network Sensor 来讲原始数据是原始网络包；对于 OS Sensor 来讲原始数据是操作系统日志项。

过程的输出包括：

- 系统发起的对安全事件的响应。

过程：

- 监控器在收到数据后，将数据和特征库进行对比，如果匹配会发出对应的响应。特征数据库主要来源于安氏的 Xforce 研究开发小组，而且是目前业界最全面的攻击特征数据库。另外，Network Sensor 和 System Sensor 都支持用户自定义特征。
- Network Sensor 检测过程——安装 Realsecure Network Sensor 主机的网络适配卡连接到被监控的网段上。Realsecure 将网络适配卡设成 Promiscuous 模式，可收到本地网段上的所有数据流。当一个包符合了

当前有效的过滤规则时，会被解码并进行攻击特征识别分析。每个活动的过程都被保持和跟踪，这样跨越了许多包的攻击特征就可以被检测出来。因此，当一个“感兴趣事件”被检测到时，Realsecure 会采取合适的动作。

- OS Sensor 检测过程——RealSecure OS Sensor 在被保护服务器上运行一个进程。每当操作系统产生一个新的日志记录项，操作系统会向 System Agent 发出中断。System Agent 读取新的日志记录项，与监控特征进行对比，如果匹配会发起适当的响应。由一些特征会涉及多个日志记录项，因此 System Agent 会同时维护和监控一些用户活动流的状态。

提供对特定网段的实时保护，支持高速交换网络的监控；

对重要网段的保护，如公共服务器群，为了避免来自网络其它边界的入侵，需要在该子网的入口处安装 Realsecure Network Sensor，并在各个服务器内配置 Realsecure OS Sensor，由集中的 Realsecure Workgroup Manager 统一管理。

RealSecure 运行在交换式网络中，有以下三个解决方案：

- 策略性地布置 RealSecure Network Sensor——如果一个交换机的端口与连接其它网络的路由器相连，那么就应当在交换机和路由器之间连接一个小 HUB，将 RealSecure engine 连接在这个点上。这样就可以防护来自 Internet 的攻击，而不处理网络的其它部分。

- 另外，还可以使用交换机的管理端口甚至一个 VLAN。一些交换机（比如，Cisco Catalyst）有一个管理端口（有时称为 span 端口）可以镜像一个或多个指定端口的数据流。可以将 RealSecure Network Engine 配置在这样的管理端口上，通过镜像的方式获得多个端口的数据流。如果交换机的一个端口里连接 Internet 路由器，则可以镜像连接路由器的这个端口。如果交换机连接多台重要内联网服务器，则可以镜像连接服务器的这几个端口。现在，已经有很多交换机支持这种功能。

- 使用 RealSecure OS Sensor——由于 Systen Agent 是基于主机的工作方式，因此完全不会受到交换方式的影响。在连接交换环境的服务器上安装 System Agent，对每个服务器进行

保护。将 network Sensor 和 OS sensor 结合使用，会达到很好的防护效果。

提供对关键服务器，如 Web、E-mail、DNS、FTP、NEWS 等的实时保护；

华为企业网中的某些关键服务器主要是 Solaris 和 HP 平台，安氏的 Realsecure 完全支持以上平台。对各结点关键服务器的保护，采取 Network Sensor 和 OS sensor 结合使用的方式，在网段的入口处配置 Network Sensor，从网络层阻断一切可能的入侵行为；在服务器内配置 OS sensor，从系统级对服务器的访问行为进行严密监控。

能够在检测到入侵事件时，自动执行预定义的动作，包括切断服务、重起服务进程，记录入侵过程信息等；

1. 首先，当一个攻击或事件被检测到，RealSecure 可以做出以下几种响应：
   - 自动终止攻击
   - 终止用户连接
   - 禁止用户账号
   - 重新配置 Check Point™ Firewall-1®防火墙阻塞攻击的源地址
   - 向 Lucent 防火墙安全管理服务器(SMS)发出实时警报
   - 向管理控制台发出警告指出事件的发生
   - 向网络管理平台（off-the-shelf）发出 SNMP trap
   - 记录事件的日志，包括日期、时间、源地址、目的地址、描述以及事件相关的原始数据。
   - 实时观看事件中的原始记录（或者记录下来过后再回放）
   - 向安全管理人员发出提示性的电子邮件
   - 执行一个用户自定义程序
2. 其次，可以为 RealSecure OS Sensor 自定义一些特征。OS Sensor 允许用户指定一个关键字或正则表达式，在发现操作系统日志文件项对应特征时，会做出相应的响应。
3. 第三，用户可以为 RealSecure Network Sensor 自定义连接事件。一个连接事件可以定义为基于 IP 的连接，可以对下面信息进行匹配：
   - 协议
   - 源 IP 地址
   - 目的 IP 地址

- 源端口
- 目的端口

4．第四，一些 RealSecure 预定以攻击特征可以根据网络的具体情况进行参数调整。比如，有些网络中 PointCast 下载会引发 SYN Flood 特征，此时可以通过调整 SYN Flood 的阀值来减少误报。
5．第五，用户可以定义 RealSecure network engine 过滤规则来忽略某些类型的数据流。可以通过指定协议、源 IP 地址、目的 IP 地址、源端口、目的端口定义忽略的数据流。对于规则匹配的数据流不进行预定义或用户定义特征分析。通过这种方式，可以将 RealSecure 配置得更适合用户的网络。
6．最后，用户可以建立自己的响应选项。任何可以从命令行发起的动作（如：可执行程序、批处理文件、Shell Script 等），都可以作为 RealSecure network engine 或者 system agent 对攻击的响应。

支持集中的攻击特征和攻击取证数据库管理；

Realsecure 真正实现集中管理，也体现在对攻击特征和攻击事件的数据库管理。

- Realsecure Workgroup Manager 运行在 MS NT 或 Win2000 平台上，在默认情况下，其管理数据库格式为 MS Access 文件格式。Realsecure 的数据库接口支持标准的 ODBC，因此可以灵活选择其后台管理数据库类型。
- 在 Realsecure 的管理数据库中，有一组数据库表格式，分别用于记录所有最新版本能够识别的攻击特征，及从各个远程的 Sensor 汇总来的攻击事件的记录。

支持攻击特征信息的集中式发布和攻击取证信息的分布式上载；

Realsecure 中包含升级组件 X-press Updates，利用这一组件，可以从 Workgroup Manager 集中分发攻击特征信息。

当分布在网络中的各个 Sensor 监控到攻击事件时，依据 Sensor 的策略定制，Sensor 将执行一系列的动作，包括实时在 Workgroup Manager 的屏幕上显示，并执行切断连接或重新配置防火墙等动作，为了方便管理员查询并记录犯罪证据，Sensor 必须将监控的事件记录到日志中。在 Workgroup Manager 可以采取手工干预或自动两种方式对 Sensor 的日志进行上载和汇总。上传后的日志将统一以数据库形式保存。

提供对监视引擎和检测特征的定期更新服务，更新方式可有多种，包括厂家的直接服务和联网更新操作；

安氏拥有实力雄后的 X-Force 小组，该小组专门研究和发现新的攻击手段，是业界独一无二的安全小组。作为入侵检测产品，其 Sensor 和攻击特征库的升级能力直接反映了产品的功能，而安氏的系列安全产品包括Realsecure的升级速度都是其它厂商无法比拟的。

安氏承诺对用户的升级服务，详见安氏服务承诺。从产品本身提供的功能看，Realsecure 中提供了 X-press Updates，利用这一组件，可以直接从安氏站点下载升级包，并可以从 Workgroup Manager 集中分发攻击特征信息至所管理的每个 Sensor。

网络访问控制；

Realsecure 的主要功能用于对恶意入侵事件和误用行为的监控报警。可以根据实际需要，对 Sensor 进行策略配置，用于特殊的网络访问控制。

如可以用 Network Sensor 对办公环境员工上网浏览 Web 页面进行限制；

可以对某个重要的服务器进行特殊保护，限制某个地址或某个范围的地址段对该服务器指定端口的访问；

通过对 E-mail 主题或内容的特殊字符串的监控，限制某些 E-mail 的非法传送。

等等。

可疑网络活动的检测，对带有 ActiveX、 Java、JavaScript、VBScript 的 WEB 页面、电子邮件的附件、带宏的 Office 文档中的一些可以执行的程序（包括通过 SSL 协议或者加密传输的可疑目标）进行检测，隔离未知应用，建立安全资源区域；

Realsecure Network Sensor 除了对恶意的入侵行为进行识别以外，还能够对可疑的不安全事件报警和阻止，包括对带有 ActiveX、Java、JavaScript、VBScript 的 WEB 页面，可疑的 Arp 事件，IP 地址复用事件等报警。

支持与防火墙的配合监控；

Realsecure 与防火墙功能互补

适当配置的防火墙可以将非预期的信息屏蔽在外。然而防火墙为提供一些级别的获取权的通道可能被伪装的攻击者利用。防火墙不能制止这种类型的攻击，RealSecure 却能够制止。RealSecure 对防火墙后面的网络的信息流监控，能够检测到并终止获取权限的企图。

另外防火墙的错误配置也有可能发生。尽管防火墙的错误配置能够迅速更正，网络内有了 RealSecure 则能捕获许多溜进来的未预料的

信息。即便不选择切断这些连接，RealSecure 所发出的警告的数量仍能迅速表明防火墙没有起到作用。

- Realsecure 与 CheckPoint 协同工作

CheckPoint 公司通过它提供的 OPSEC（Open Platform For Secure Enterprise Connectivity， 安全企业连通性开放平台）向第三方提供 API，使得其他厂商可以使用这些 API 开发能集成到 FW-1 防火墙中的产品。由于安氏是 CheckPoint 的 OEM 厂商，所以 Realsecure 能够对 FW-1 进行安全操作。

Realsecure 重新配置 FW-1 有两种响应方式：冻结指定的时间长度 和 完全关闭。每种响应方式根据需要又细分四种模式：针对源地址操作，针对目的地址操作，针对源和目的同时操作，针对服务操作。

- Realsecure 与 Lucent 防火墙协同工作，Realsecure 的报警动作之一是通知 Lucent 防火墙的管理控制台。

RealSecure Network Sensor 可以完全透明

RealSecure network Sensor 可以配置为完全透明的方式。一个 RealSecure Network Sensor 可以采用 Out-of-band 方式和管理控制台进行通讯。这种情况需要配置两块网络适配卡：一块网络适配卡用来监控本地网段，另一块用来和控制台通信。由于这种方式使得 RealSecure Network Sensor 采用了专门的通信通道和控制台通信，会大大加强 RealSecure 的安全性。

另外，用来监控本地网段的网络适配卡并不需要一个协议栈。因此，RealSecure Network Sensor 并不需要一个外部可见的 IP 地址或者外部可见的 IP 服务。这样 RealSecure Network Sensor 可以做到从被监控网络上不可见。

当然，RealSecure Network Sensor 需要 TCP/IP 协议与管理控制台通讯。因此，与管理控制台通讯的接口卡需要 IP 地址。

Realsecure OS Sensor 可疑连接监控

一个攻击者首先会刺探主机提供了什么服务。“可疑连接监控”使得一个没有服务的端口看起来是活动的，这样入侵者可能会误以为系统开启了某种服务，在刺探中浪费时间而一无所获。这个功能对防范一些自动攻击工具十分有效。

对不存在服务的连接企图或者是一个错误，或者是故意的攻击。System Agent 将这些连接作为入侵检测判断的数据。持续的对不存在服务的连接企图会产生高风险报警。

安全管理人员可以对这种连接企图设置响应提示。可以设置为法律警告指出入侵是非法的，或者可以设置成欺骗性连接提示（比如，登录提示）。

可疑连接监控的功能能延长攻击者发现可攻击端口的时间，为防护者抓住他争取更多的时间。

5.5.2.2 产品运行环境要求

Network Sensor(Engine)系统需求

平台	最小系统需求
Windows NT	300 MHz Pentium II或更高的处理器 至少128 MB内存（推荐256MB） 150MB磁盘空间，用来存放日志文件和数据库记录 10MB用于软件安装 安装了Service Pack 6.0a的Windows NT 4.0 Workstation（从Service Pack3到Service Pack 6.0a都支持） 一个PCI网卡（具有混杂模式能力，并能连接到被监控的网段） — 以太网 — 快速以太网 — Token Ring — FDDI 选项：第二块网络接口卡（NIC）。控制台通过第二块网络接口卡与一个安全网络连接，进行额外的通信
Solaris SPARC	UltraSPARC 2 或更好的处理器 至少128 MB内存（推荐256MB） 至少150MB磁盘空间 Solaris SPARC 2.5.1， 2.6， 2.7 Sbus或PCI具有混杂模式能力的适配器（推荐PCI） 选项：第二块网络接口卡（NIC）。控制台通过第二块网络接口卡与一个安全网络连接，进行额外的通信

OS Sensor(Agent)系统需求

平台	最小系统需求
Windows NT	安装了Service Pack 6.0a的Windows NT 4.0（NT 4.0 Workstation和NT 4.0 Server都支持） 从Service Pack3到Service Pack 6.0a都支持 至少64 MB内存（推荐128MB） 25MB磁盘空间用于软件安装 50MB磁盘空间用于软件运行 Pentium II系列或更高的处理器
Solaris SPARC	Solaris SPARC 2.5.1， 2.6， 2.7 注意：Solaris 2.5.1操作系统探测器不支持在线升级 UltraSPARC2 至少50MB磁盘空间用于软件运行
IBM AIX	AIX 4.3.2或者AIX 4.3.3 至少50MB磁盘空间用于软件运行
HP-UX	HP-UX 11.0 至少50MB磁盘空间用于软件运行 从HP网站http://www.hp.com下载Patches #PHCO_16127， Patches #PHCO_19666， 和Patches #PHCO_20765

WorkGroup Manager(Console)系统需求

平台	最小系统需求
Windows NT	300 MHz Pentium II 或更好的处理器 至少128 MB内存（推荐256MB） 100M磁盘空间用于控制台管理每个探测器 注意：数据库使用（和需要的）磁盘空间取决于各种因素，包括网络上通信量的多少、监控事件的种类、写入数据库的内容和同步数据库的频率 20M磁盘空间用于软件安装 安装了Service Pack 6.0a的Windows NT 4.0（推荐NT 4.0 Workstation） 支持从Service Pack3到Service Pack 6.0a 安装了Service Pack1 的Microsoft IE 4.01或更高版本用于查看关于攻击和怎样处理攻击的帮助信息 从微软站点http://www.microsoft.com/Data/download_250RTM.htm下载MDAC（微软数据库访问组件）2.5 RTM 系统管理员权限 支持最少256色、800x600分辨率的显示器

5.5.3 建议配置方案

Realsecure 是一个真正的集中管理的入侵检测系统。它由一个或多个（可选）管理控制台，即 Workgroup Manager，统一、集中管理分布在网络中的 Sensor。

建议在华为企业网各个骨干结点各安装一套 Workgroup Manager，用于对各地区的入侵检测管理和监控的平台。

如图所示，在某各个 INTERNET 入口处，配置 Network Sensor，用于对子网进行网络一级的入侵检测。在各个子网内的重要服务器上，如 WWW 服务器、E-mail 服务器、DNS 服务器、FTP 服务器 NEWS 服务器和 RADIUS 服务器等，安装 OS Sensor，对这些关键的服务器进行系统一级的实时防护。

增加软件和硬件

项目	地点	数量
Realsecure Workgroup Manager + Manager 服务器（PC Server） Realsecure Network Sensor + Network Sensor 服务器(PC Server) Realsecure OS Sensor		

5.6 访问控制

根据电信企业网络服务和生产运行需要，制定详细的网络资源访问控制策略，以及管理落实制度是安全防御的一个重要内容。制定网络访问控制的原则是细致全面、实用有效。细致全面不会给攻击入侵者留下可以利用的空间；实用有效方便落实和管理。过于简单不能实现有效保护，过于繁杂的访问规则由于难于管理落实同样会流于形式，不能实现有效保护。

访问控制具有基于 IP 地址、域名和用户身份等几种形式。

身份认证技术（详见“身份认证”一节）是实现基于用户身份的访问控制的基础。

路由器（交换机）、防火墙、主机是实现访问控制的主要网络手段。

IS-ONE 拥有丰富的电信企业网络的安全管理经验，并由此出发为华为企业网安全解决方案设计了细致全面、实用有效的网络访问控制体系。

路由器（交换机）

路由器（交换机）是实现网络资源访问控制的基本手段。接入层路由器和网管系统、办公系统的交换机是实现网络资源访问控制的主要位置。按照制定的华为企业网安全策略配置访问控制列表（ACL）可以实现有效的基于 IP 地址的访问控制。

防火墙

防火墙可以实现比路由器（交换机）更加细化的访问控制，合理配置的防火墙是保证访问控制策略的有力手段。防火墙可以实现基于 IP 地址、域名和用户身份等的访问控制。具体细节详见“防火墙”一节。

主机

UNIX 类主机和 WINDOWS NT 主机本身的资源访问控制手段是整个访问控制体系的最后堡垒。下面分别说明 UNIX 类和 WINDOWS NT 主机设备的访问控制手段：

- UNIX 类主机通常使用用户、组实现文件和网络资源的访问控制，能够使用的具体手段包括：
- Tcpwrapper（可以针对多数 TCP 服务实现基于 IP 地址、域名的访问控制）
- /etc/shells，/etc/ftpusers，/etc/security/access 等配置文件（可以实现基于用户的访问控制）
- 合理设置的属主（owner）、组（group）的写、读、执行操作
- 其它有效的配置

WINDOWS NT 实现资源访问控制的主要手段包括：

- 用户（实现资源的读、写、执行、添加、等控制）
- 用户组（实现资源的读、写、执行、添加、更改等控制）
- 注册表
- 网络属性高级配置（控制面版-网络-网卡属性-高级配置）（实现基于网络 IP 地址、域名等的访问控制）
- Windows IIS Server 高级配置（基于 IP 地址、域名的控制、本地资源的发布等）

推荐安全服务——访问控制安全服务

访问控制安全服务——该服务是 eSafelink Professional 专业安全服务中的一项，是针对网络进行安全建设的一项基本服务。

服务的主要方式和内容包括：

- 根据华为企业网的要求，制订整体的访问控制策略。
- 利用工具切实落实访问控制策略的要求。
- 对整体的访问控制状态进行评估。

服务的主要成果是《华为企业网访问控制策略和实施报告》。

5.7 日志和审计

合理设计日志和审计体系能够提供有效的入侵检测和事后追查机制，是整个安全解决方案中的重要组成部分。当前应用中的主要网络操作系统（包括主要路由器、交换机、UNIX 类、WINDOWS NT 操作系统等）都能够提供基本的日志记录功能，用于记录用户和进程对于重要文件的更改和对网络资源的访问等。通常的操作系统日志体系失败的重要原因是日志系统的设计和审查没有充分考虑网络安全的特性，导致日志记录不够细致、没有考虑日志系统的备份、日志被入侵者篡改，而失去对入侵和攻击者的定位和追查功能。

在透彻考察华为企业网实际运行的安全需求后，IS-ONE 充分利用操作系统本身具备的日志和审查能力，在安全方案中设计了实用有效的集中日志体系。作为入侵监控和防御系统（详见“入侵监控和防御”一节）的重要补充。

本解决方案中设置两台专门的日志服务器，分别集中存放华为企业网络中的重要网络设备和主机系统中的系统日志。日志服务器采用 SUN 服务器硬件、运行 SOLARIS 操作系统。考虑到日志服务器本身任务的关键性，方案中对日志服务器本身和日志审计体系进行下述安全保护：

- 单独网段划分
- 主机系统加固配置
- 安装入侵监控和防御系统
- 合理配置日志服务器前端防火墙（路由器）的访问控制策略，只接收指定的网络地址的日志信息
- 制定完备的日志服务器安全管理制度
- 安全管理员对所记日志进行定期地、有效的备份
- 安全管理员对所记日志进行定期、详细的审查

推荐安全服务——日志和审计安全服务

日志和审计安全服务——该服务是 eSafelink Professional 专业安全服务中的一项，是针对网络进行安全建设的一项基本服务。

服务的主要方式和内容包括：

- 根据华为企业网的要求，制订整体的日志和审计策略。
- 利用工具切实落实日志和审计策略的要求。
- 为华为企业网构建日志和审计体系
- 对整体的日志和审计状态进行评估。

服务的主要成果是《华为企业网日志和审计策略和实施报告》。

推荐解决方案——设备 SYSLOG 记录和审计

备份和记录----采用一台 PC Server 安装 LINUX，由它来收集重要的网络设备和重要 UNIX 系统的 SYSLOG，以备将来发生网络安全事件，可以对事件进行跟踪和分析。

日志的审计----在日志服务器上安装 RealSecure System Sensor（见 5.5.2），由该软件对所记录的日志进行实时的日志审计，一旦发现设备异常，便可作出报警。

5.8 身份认证

认证（Authentication）技术的目的是确保网络资源按照企业的安全策略被正确的用户访问。对于电信企业来说，网络管理系统对网络元素的访问、对应用服务器系统的访问、办公系统之间的资源访问等都需要身份认证技术的保护。当前主要应用的认证技术包括 UNIX 类主机、WINDOWS NT 主机、路由器等操作系统自带的本地认证以及 RADIUS、TACACS+等远程认证技术。

S/KEY（或 SecureID）一次性口令认证技术可以有效地防御口令窃听等网络攻击，减小口令泄露带来的安全威胁，是对上述认证技术的有效增强。

身份认证技术是实现资源访问控制的重要手段，是落实企业网络安全策略的保证。

最大可能地利用简单明了的认证技术是实现安全的重要原则，“复杂容易导致安全体系失败”。

考虑到大企业管理运行的安全需求特点，IS-ONE 认为，对路由器、交换机等网络设备结合使用 RADIUS、S/KEY（或 SecureID）、对主机设备使用本地认证技术可以在“实用有效”的原则下，建立起一套简捷明了、行之有效的大网络身份认证体系。下面分别就网络设备和主机设备的身份认证技术进行说明。

网络设备

电信级大企业网络的一个重要特点就是拥有大量的路由器和交换机等网络设备，网管工程师需要经常地从网管网段（或办公网段，根据企业的安全策略决定是否允许）登录。此时，本地认证有以下不足：

- 网管人员需要维护大量的登录口令和超级用户口令
- 口令表丢失或内容泄露会导致大量的网管工作量
- 很难保证口令不会因网管人员的变动而泄露
- 不容易掌握网管工程师对路由器等网络设备的登录和配置情况

本建议书提出利用 RADIUS 和 S/KEY（或 SecureID）技术相结合的集中认证办法可以很好地满足华为企业网对于网络设备身份认证的需求。

主机设备

UNIX 类和 WINDOWS NT 主机设备是网管系统和应用服务器系统的主要组成部分，也是网管工程师的主要工作对象。考虑到电信级大企业网络管理的特点，通常每个网管工程师会根据网管的安全策略或者运行维护中的“包机维护”原则登录管理相对稳定的主机功能设备。此时，口令的维护管理工作相对网络设备大幅度降低。此时，采用单点认证（Single Sign-On）技术、集中认证技术等有以下不足：

- 成本高
- 技术复杂
- 管理维护复杂
- 许多网管操作仍然需要本机登录验证
- 容易失败

IS-ONE 根据自身具有的丰富的电信网络安全运行维护经验，认为使用主机设备本地认证和加密通信（详见“信息加密”一节）相结合的方法，可以防止口令窃听等网络攻击，在保证网络身份认证安全有效的原则下，最大限度的利用网络资源，节省企业开销。

推荐安全服务——身份认证安全服务

身份认证安全服务——该服务是 eSafelink Professional 专业安全服务中的一项，是针对网络进行安全建设的一项基本服务。

服务的主要方式和内容包括：

- 根据华为企业网的要求，制订整体的身份认证策略。
- 利用工具切实落实身份认证策略的要求。
- 为华为企业网构建身份认证体系
- 对整体的身份认证状态进行评估。

服务的主要成果是《华为企业网身份认证策略和实施报告》。

5.9 信息加密

加密（Encryption）技术是保护信息安全的主要手段之一，也是当前网络安全技术重要发展方向。加密技术能够保护信息的机密性（Confidentiality）、提供完整性检测、身份验证能力等安全保护，防止信息被窃取、篡改和假冒。

当前，加密技术在国防、金融、证券等行业已经得到普遍采用。为满足上述行业对机密性、完整性和认证等高度需求，通常使用专用通信加密机、私有加密算法等手段完成通信加密。但是，上述解决办法在提供高强度加密的同时，具有投资强度大、需要修改网络设计、不易升级换代等不利之处，并不完全适用于电信企业。

充分考察和研究华为企业网的特点后，IS-ONE 认为在网络管理通信过程中采用适当加密通信手段（SSH、IPSEC-VPN）可以有效地保护网络安全，防止网络窃听带来的口令和其它重要信息泄露等安全威胁，同时具有节省开支，容易配置和部署、管理等特点。

SSH

众所周知，网络管理活动中使用最为频繁的通信过程 TELNET、FTP、RCP 等完全是明文传送的。由此，入侵者成功入侵并控制网络中的某些主机和网络设备后，经常使用网络窃听器（Sniffer）来窃取口令等重要信息，来扩大和加深入侵程度。SSH（Secure Shell）正是上面这些通信过程的加密替代品，是客户端-服务器端网络通信中的强大、有效的加密措施。SSH 具有以下特点：

- 软件程序（包括服务器和客户端）完全免费
- 支持多种 UNIX、WINDOWS 平台
- 支持多种强加密算法（3DES，RC4，TWOFISH 等）
- 支持多种消息摘要算法（MD5，SHA1 等）
- 支持多种认证方式（PublicKey，Password 等）

- 加密的端口定向转发（Port Forwarding）
- 可完成 TELNET、FTP、RCP 等多种通信的加密

IPSec-VPN

IPSec 协议是在 IP 基础上发展而来，具有加密和认证、不可抵赖等能力。RFC2401、RFC2402、RFC2406 等 12 个文件定义了 IPSec 的主要内容。它包含认证头（AH）和安全净荷封装（ESP）两部分，其中 AH 能够提供认证和完整性检查能力，ESP 能够提供机密性、认证、重发保护和完整性保护能力。

当前，IPSec 获得了业界广泛的支持，包括 CISCO 路由器、多种防火墙、LINUX、FREEBSD、WINDOWS2000 等操作系统。使用 IPSec 技术建立加密通信渠道和虚拟专网（VPN）不仅具有可行性，并且具有投资节省、方便配置、高强度加密安全环境等特点。

考虑到华为企业网规模大、分布式的特点，使用 IPSec 技术在分布各处的网管系统、主要应用服务器系统和办公系统之间建立 VPN 加密通信环境无疑是恰当的。这种架构与华为企业网公用网络可以作到无缝集成，为网管系统、应用服务器系统和办公系统之间提供了适用有效的加密手段。为以后华为企业网向用户提供加密、VPN 等增值服务打下基础。

推荐安全服务——加密安全服务

加密安全服务——该服务是 eSafelink Professional 专业安全服务中的一项，是针对网络进行安全建设的一项基本服务。

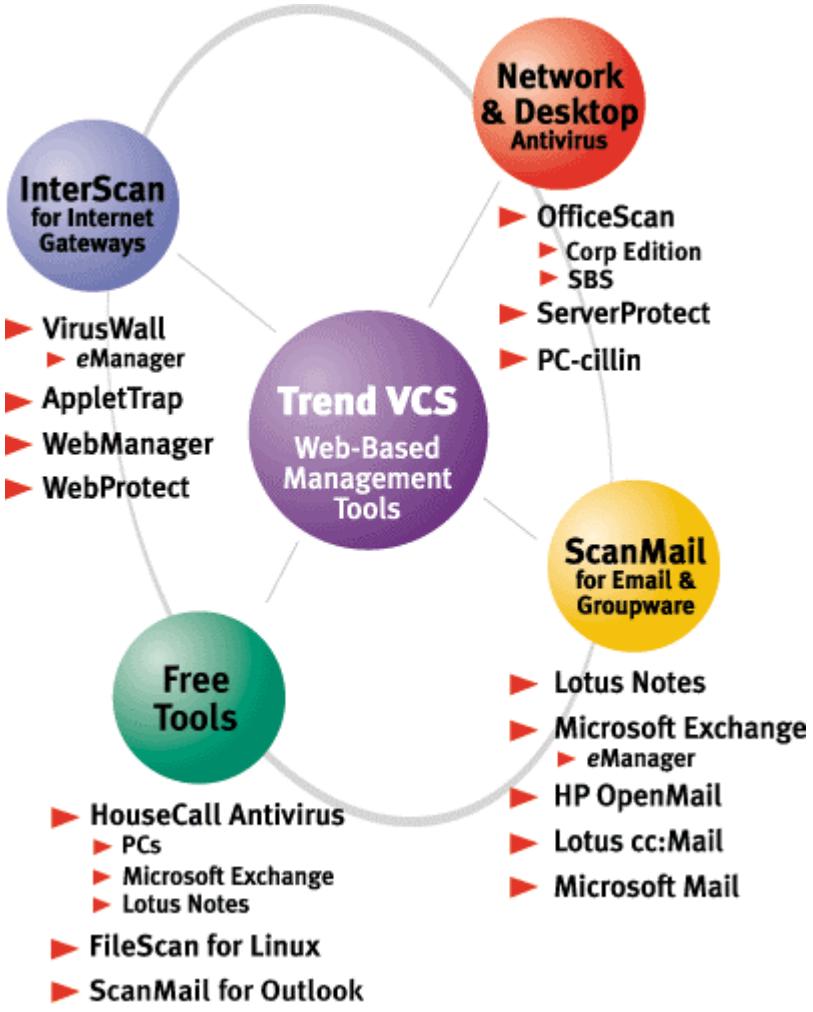
服务的主要方式和内容包括：

- 根据华为企业网的要求，制订整体的加密策略和规划。
- 对当前系统的加密技术状态和需求进行评估。

服务的主要成果是《华为企业网加密策略和规划报告》。

5.10 防病毒

5.10.1 推荐安全产品——Trend Micro 防病毒产品



5.10.2 TrendMicro 性能指标

支持对网络、服务器和工作站的实时病毒监控；

1. **对于** Internet **类型的网络，包括** Extranet **和** Intranet**，趋势科技提供基于网关处的防毒产品：InterScan 系列。产品都含有纯** web **方式的管理界面。**

   - **因特网病毒防火墙——InterScan VirusWall :在网关处实时监控通过** SMTP、HTTP **和** FTP **协议传输的信息内容，检查其是否存在病毒或恶意程序，并根据管理员的设定采取相关的处理方式，以保证通过网关出入企业的信息的安全性。支持对** 16 **种以上的压缩类型、压缩深度最多达** 20 **级的文件进行病毒扫描工作。支持的平台：**Windows NT(2000)、Solaris、HP-UX、Linux。
   - **电子邮件安全管理——InterScan eManager :基于** InterScan VirusWall NT **版和** Solaris **版的外加（**Plug-in **）的电子邮件管理工具，属于** InterScan VirusWall **的因特网安全（**Internet Security **）系列产品之一。**eManager **电子邮件安全管理软件可以过滤垃圾邮件及大量推销性质的电子邮件，并可扫描由内部使用者寄出的邮件内容，若有敏感性内容可就进行拦阻；此外也能够自定邮件传递时间，延迟递送较大的邮件、国际信件或其它自定规则范围内的邮件，避免在网络带宽使用高峰时段造成邮件阻塞。支持的平台：**Windows NT(2000)、Solaris。
   - **网站安全管理软件——InterScan WebManager：集** web **访问的管理限定和防病毒与一身。除了对传入的** web **页面进行防毒之外，还可以对访问的内容及带宽进行管理。可弹性设定对** 14 **种不同类型的网站内容进行过滤。**WebManager **应用** Cyber Patrol **所开发出全球数十万个网站的数据库，阻止内部使用者通过因特网进入色情或其它的不良网站。可依据个人及部门的特殊需求，过滤不良网站和设定下载文件的大小限制。管理员可依每日、每周或每月，设定个人或部门对于** Web **下载文件的最大流量，从而控制网络的使用带宽。支持的平台：**Windows NT(2000)。

2. 对于企业内部的电子邮件和群件系统，如 Lotus Notes 和 Microsoft Exchange，由于企业内部用户间的通讯可能并不通过 Internet 网关，因此光靠在网关处防毒并不能控制病毒在企业内部的传播。趋势科技针对此类系统提供了相应的防毒产品：ScanMail 系列。

   - ScanMail 系列在对邮件系统内的邮件和公用文件夹内的文件进行病毒防护的同时，还可以对含有敏感性内容的邮件进行隔离等处理，以保护企业内部信息流的安全。产品都含有纯 web 方式的管理界面。
   - ScanMail 支持对 19 种压缩类型、压缩深度最多达 20 级的文件进行病毒扫描工作。
   - ScanMail for Lotus Notes：完全支持 Lotus Domino R5。支持的平台：Windows NT 4.0 and above; Sun Solaris 2.5 and above; IBM AIX 4.1.3 and above; OS/2 Warp 3 or above，IBM S/390 2.4 and later， IBM AS/400 V4R2 and above。
   - ScanMail for Lotus CC:Mail
   - ScanMail fro Microsoft Exchange：真正支持微软建议的 AVAPI 接口，以获得更高的工作效率，减少对系统资源的占用。完全支持 Exchange 的群集技术。支持的平台：Windows NT(2000)。
   - ScanMail for HP OpenMail

3. 针对目前企业广泛使用的文件型服务器——NT 和 NetWare，趋势科技提供了相应的服务器防毒软件：ServerProtect 系列。ServerProtect 可以有效地捍卫文件服务器和网域内的信息安全，免于计算机病毒的攻击，并且利用趋势科技新一代的防毒集中管理软件 TVCS 的技术，让管理员可以从单一的主控台来安装并且管理 ServerProtect。有关病毒的报警信息可通过信箱、寻呼机、打印机、e-mail、SNMP 通知或写入到 Windows NT 事件记录文件来传送。

   - ServerProtect 可支持扫描下列压缩格式的文件：ARJ、Diet、LZEXE、LZH、PKLITE、PKZIP 和 Microsoft Compress，也支持译码 UUENCODE 及 MIME 等编码格式的文件并进行扫描工作。
   - ServerProtect 采用独特的三层结构，使对服务器防毒的管理工作变得轻松自如。（1）普通服务器：安装了 ServerProtect

防毒模块的服务器<NT/NetWare>；（2）信息服务器：安装了 ServerProtect 防毒模块和信息服务模块的服务器<NT/NetWare>，通过它可实现对防毒信息的集中分发和管理；（3）控制台：安装了 ServerProtect 管理控制模块的机器，可以是 win95、98 或 NT 机器，管理员只要在这台机器上即可完成对所有服务器防毒的管理和监控。

4. 对于企业内的各类工作站——NT(2000)， win3.x/95/98，趋势科技提供了工作组级的防毒软件产品：OfficeScan。采用 OfficeScan 可以大大降低企业在防毒工作上的总体成本。只需将 OfficeScan 安装在一台 NT 服务器上，就可实现对所有上述工作站的防毒管理工作。企业的每个用户无需再为自己的机器如何防毒而操心。管理员可设置自动或手动对所有的机器进行杀毒工作，每个用户也可以在需要的时候对自己的机器进行杀毒。通过 OfficeScan 实现了管理员对所有工作站防毒工作的集中监控。

5. 防毒工作中央监控系统：TVCS——Trend Virus Control System。为了让企业能对所有的防毒产品和工作进行集中管理，趋势科技提供了产品 TVCS。上述的趋势科技的防毒软件产品都可集成 TVCS 的客户端组件—TVCS Agent。当企业安装了 TVCS 系统后，即可实现对上述产品的集中控制和管理。同时，TVCS 也可以显示出其他一些防毒软件产品的信息，以便让管理员统一监控。

- TVCS 采用纯 web 的管理界面，管理员不论在何时何地，只需有 Web 浏览器即可实现对整个企业的防毒管理工作。
- 完善的日志记录和统计信息功能。
- 支持弹出窗口、e-mail、寻呼机等报警方式。

能够在中心控制台上向多个目标系统分发新版杀毒软件；

防毒工作中央监控系统 TVCS 提供统一而且自动的产品组件更新功能，通过它可实现趋势科技所有防毒产品的扫描引擎及病毒码更新功能。

能够在中心控制台上对多个目标系统监视病毒防治情况；

防毒工作中央监控系统 TVCS 使管理员通过浏览器即可实时监视趋势科技所有防毒产品的工作情况，以及病毒防治情况。由于采用了客户/服务器的时间驱动模式进行工作，因此有效的避免了对

网络带宽的过多占用。

支持多种平台的病毒防范；

趋势科技是一家专注于企业安全的产品供应商，具有十分完善的产品系列，考虑了企业内从工作站到因特网网关，几乎所有需要防病毒的平台和网络连接点。

能够识别广泛的已知和未知病毒，包括宏病毒；

作为作早进入计算机防毒领域的厂商之一，趋势科技在防毒技术上始终保持着领先的优势。早在 1995 年趋势科技即开发出了基于人工智能（Rule-based）的扫描引擎，采用陷阱方式探测恶意程序可能出现的破坏动作，以及探测出变形病毒的真面目，从而实现对未知病毒的拦截。经过不断地完善，目前的引擎中已设下了多达 12 道以上的陷阱，根据传统方式制作的各类新病毒根本逃不过被检测出的命运。1996 年趋势科技又率先推出了自己的专利技术——MacroTrap™，解决了对已知或未知的宏病毒的探测问题。

支持对 Internet/Intranet 服务器的病毒防治，能够阻止恶意的 Java 或 Active X 小程序的破坏；

趋势科技的因特网网关病毒防护产品——InterScan 系列，能够有效阻止恶意的 Java、Active X 程序以及一些黑客程序通过因特网对企业进行的入侵。InterScan 在网关处实时监控通过 SMTP、HTTP 和 FTP 协议传输的信息内容，检查其是否存在病毒或恶意程序，并根据管理员的设定采取相关的处理方式，以保证通过网关出入企业的信息的安全性。

支持对电子邮件附件的病毒防治，包括 WORD/EXCEL 中的宏病毒

趋势科技的产品系列中，InterScan、OfficeScan、ScanMail 等都支持对电子邮件附件的病毒防护。趋势科技的扫描引擎中含有自己的专利技术—MacroTrap™，由于采用了人工智能的陷阱技术，还可以检测出部分未知的宏病毒。

支持对压缩文件的病毒检测；

趋势科技的产品对压缩文件的扫毒支持是同类产品中最为完善的。其中的 InterScan 和 ScanMail 更是支持 16 种以上的压缩格式和 20 级的压缩深度。

支持广泛的病毒处理选项，如对染毒文件进行实时杀毒、移出、删

除、重新命名等；

针对企业和个人用户的需要，趋势科技提供了灵活的处理选项。如对于网络防毒，一般提供：带警告通过（pass）、隔离转移（move or quarantine）、删除（delete）、清除病毒（auto clean）等选项。其中对于 auto clean 方式，由于有些文件本身即是病毒或黑客程序，或者带有不能随意删除的病毒类型，因此当选择 auto clean 方式时，将会针对不能清除病毒的文件提供给用户额外的选项，其中又包括：pass， move， delete 方式。

支持病毒隔离，当客户机试图上载一个染毒文件时，服务器可自动关闭对该工作站的连接；

趋势科技的产品都支持文件隔离方式，让管理员可以对染毒文件进行分析，或是发往趋势科技的支持中心以得到针对新型病毒的最新解药。考虑到应尽量简化企业的防毒管理工作，以降低 TCO，趋势科技不主张采取关闭客户连接的做法。如果采用这种方式，企业将需要有专职的防病毒管理员来处理每次的连接中断，用户也会觉得十分麻烦。

提供对病毒特征信息和检测引擎的定期在线更新服务；

趋势科技的全线防毒产品都提供此类功能。其中大多数产品更是能自动通过因特网更新其病毒码、扫描引擎和产品升级包。通过使用 TVCS，所有的防毒产品更新工作都可从中央进行集中管理，并只需建立 TVCS 和趋势科技间的 Internet 连接，而不需要各个产品各自去连接因特网。

支持日志记录功能；

趋势科技的全线产品都提供日志记录功能。通过使用 TVCS，所有的防毒产品的日志可以从单点进行管理和浏览，并可通过 TVCS 得到企业所有防毒工作的各类统计信息和日志。

支持多种方式的告警功能（声音、图像、e-mail 等）；

趋势科技的全线产品都提供告警功能。通过使用 TVCS，对企业内所有的中毒情况都会有综合的报警提示，包括弹出窗口、e-mail 和寻呼机报警。其中的 ServerProtect 更是提供了包括：讯息信箱、寻呼机、打印机、Internet 电子邮件、SNMP 通知或写入到 Windows NT 事件日志的多种报警方式。

5.10.3 解决方案

根据目前网络产品的发展趋势和客户的普遍需求，Trend 公司开始为客户提供软硬件集成的基于 Linux 平台的产品（Trend 把其命名为 estation）。对客户而言，购买集成的软硬件产品和服务将大大减少产品安装、配置等工作的复杂度，对于企业内网络设备和软件的正常运行影响也较小；另外由于采用了 Linux 操作系统，客户将省去支付服务器操作系统的额外费用，节省了系统运行的开支。目前趋势科技对于其因特网网关防毒产品——InterScan VirusWall，建议客户考虑采取这种新的购买思路。

建议方案（标准功能）：

1. 因特网网关处防毒软件：Trend InterScan VirusWall for Unix/Linux or NT

i. 针对企业自身网络

a) 其中包括的模块：E-Mail viruswall、Web viruswall、FTP viruswall、TVCS（Trend Virus Control System）agent。

b) 作用：对从 Internet 上通过 SMTP、HTTP、FTP 标准协议传入的各类信息进行防毒处理。其中 E-Mail viruswall 还可对传出的信息进行防毒；FTP VirusWall 还可用来保护内部的 FTP 服务器不受外部 upload 的信息的病毒侵扰（为实现该功能应将其安装在 FTP 服务器上或单独安装）。

c) 安装建议：原则上在出现防火墙的网关处都应该部署 VirusWall。InterScan VirusWall 产品包中内含两个版本——标准版和 CVP 版。其中 CVP 版是专门针对与采用 CVP 协议的防火墙进行集成设置而设计的，InterScan 完全遵从 OPSEC 规范（TREND 公司是 OPSEC 联盟的成员之一）。如果企业部署的防火墙采用了 CVP 协议，建议使用 InterScan 的 CVP 版本。这样部署 InterScan 会更简便，并且能够更好地与防火墙协同工作。

d) 购买使用许可证方式：按照子网内的客户工作站台数计算用户数量，按用户数计算总价格。

ii. 针对 Internet 接入的虚拟主机服务

a) 如果虚拟主机放置于单独的子网内，电信企业可以考虑是否需要为其提供防毒服务。如果需要提供该服务，则应采用同上述类似的方式为该子网安装独立的 InterScan VirusWall。

iii. 针对 Internet 接入的主机托管服务

a) 由于各个客户的服务器单独放置，电信企业可以考虑为需要防毒的客户提供服务。原则上应把需要防毒的客户和不需要防毒的客户分在两个不同的子网内，对需要防毒的客户子网安装 InterScan VirusWall。电信企业可以将其做为增值服务向客户收费或免费提供。采用此种方式时，产品购买方式可与软件销售商进行商榷而定。

iv. 如果客户考虑 Dedicated Server 的模式，Trend 公司可以为客户与软件产品一起提供硬件平台。软硬件由 Trend 公司或集成商进行整体维护。

2. 企业内部网络防毒软件：Trend ServerProtect，Trend OfficeScan

i. ServerProtect for NT and NetWare

a) ServerProtect 安装时分为三部分：普通服务器模块、信息分发服务器模块、管理控制台模块。

b) ServerProtect 应安装在所有的 NT 和 NetWare 服务器上，其中的一台将做为信息分发服务器（Information Server），由它对所有服务器上的 ServerProtect 进行管理和控制。

c) 管理控制台模块可安装在 win95/98/NT 上，管理员可以在安装有控制台模块的机器上对整个 ServerProtect 系统进行中央管理。

ii. OfficeScan

a) OfficeScan 是单机产品的企业版软件，整个软件只需安装在一台 NT 服务器上，客户机上的防毒模块可以自动地、透明地分发到各个客户机上，包括 win3.x、win95/98、winNT/2000 等平台的机器。所

有客户机的防毒工作由服务器管理，管理员籍此可以实现对所有客户机防毒工作的集中管理和配置。

3. 防毒软件中央控制系统：Trend Virus Control System——TVCS

i. 趋势科技的所有防毒产品都可以选装 TVCS 的客户端代理模块，一旦企业安装了 TVCS 系统，就可以实现不论何时何地都可以从某个 WEB 浏览器上对整个防毒系统进行管理和控制，为管理工作提供了极大的便利性。

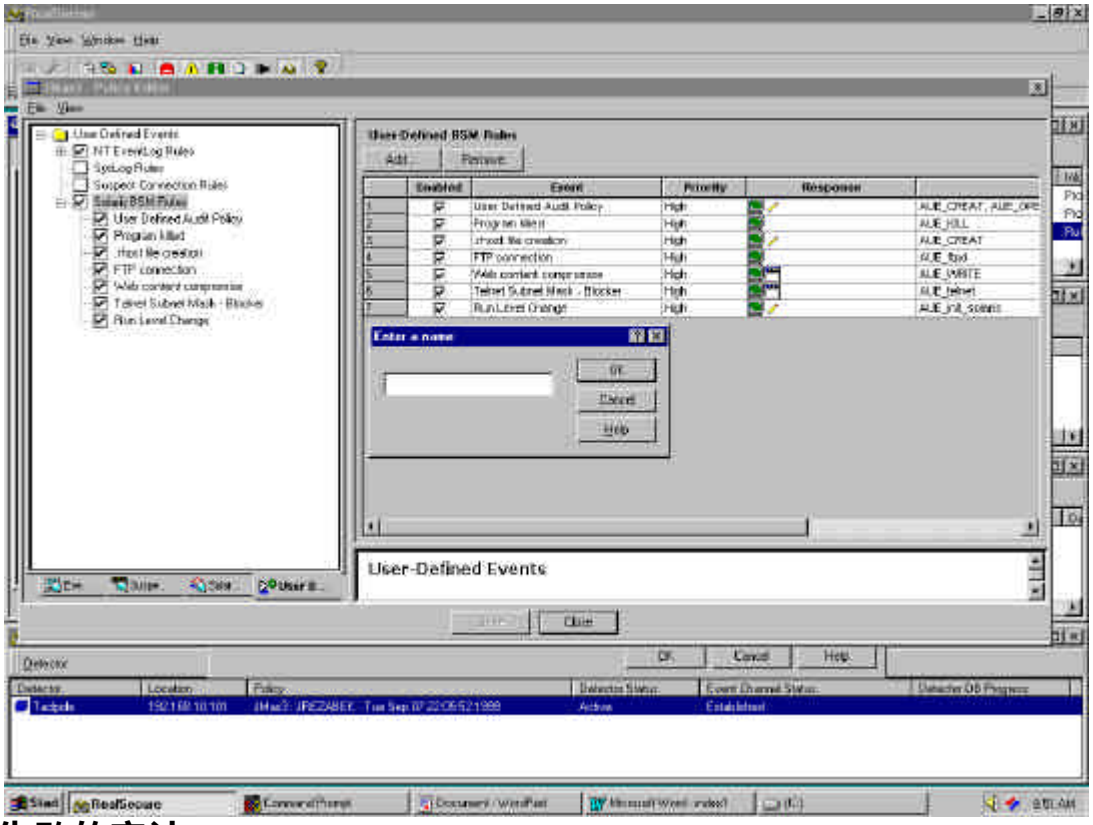
5.11 灾难恢复

当系统已经遭到攻击，迅速地恢复到被攻击之前的状态是相当重要的，也是入侵检测系统必备的重要功能之一。Realsecure OS Sensor 特有对系统审计事件的监控功能。当系统审核到某个文件有成功的读取、修改或删除操作时，OS Sensor 检测这一数据源，并对预先定制的策略比较，一旦发现是所关心的事件，立刻采取响应动作。

它能够有选择地对关键服务器的文件进行不同级别的监测，报告并记录所有非授权的内容修改；按照预先配置的策略自动恢复到被修改以前的状态。

Realsecure OS Sensor 能对文件进行审计监控。以 Web 服务器的主页恢复为例，说明 OS Sensor 如何迅速恢复被篡改的主页。

首先，需要对保护的主页文件配置系统审计，如修改操作的成功、失败的审计。



第二步，在 OS Sensor 的策略中自定义一个安全事件，指定对主页文件的操作审计事件进行监控，如上图示；

第三步，编写一个脚本文件，将备份的主页文件拷贝回原来的目录，将被修改的文件恢复；

第四步，在 OS Sensor **策略中的监控事件中，定义响应动作为执行该脚本文件。**

如上描述，当 Web **服务器的主页被恶意篡改后，**OS Sensor **能够自动恢复主页文件，使遭到攻击的损失降到最低。**

基于同样的原理，可以对其他服务器的重要系统文件进行灾难恢复的安全配置，利用 Realsecure OS Sensor **对操作系统日志审计文件监控的能力，保护关键服务器。**

推荐安全服务——安全紧急响应服务

安全紧急响应服务——该服务是 eSafelink Professional **专业安全服务中的一项，是针对网络进行安全建设的一项基本服务。**

服务的主要方式和内容包括：

- **根据华为企业网的要求，制订整体的紧急响应策略和规划。**
- **对当前系统的安全状态和需求进行评估。**
- **实施紧急响应的准备工作**
- **运用工具设置部分自动紧急响应机制，比如通过** RealSecure OS Sensor **设置主页自动恢复等。**
- **在紧急的状态** IS-ONE **可以提供紧急的在线和现场紧急安全服务。**

服务的主要成果是《华为企业网紧急响应策略》和建立紧急响应体系。

5.12 安全管理工具

5.12.1 推荐安全产品——安氏 Safesuite Decision 安全决策支持系统

SAFEsuite Decision 将安氏 SAFEsuite 产品的价值定位于能提供一个完整的可适应性企业网络安全体系，用于实时探测和预保护。

SAFEsuite Decision 将安氏的互联网扫描器、实时监控和第三方的防火墙产生的重要安全数据综合成一个封闭的自闭合的环。通过安全分析和取证信息帮助识别严重的安全热点。管理员不必再去收集和分析数据，而直接集中精力去实施能改善整个企业安全的措施。SAFEsuite Decision 是一个新的起步，它实现了企业安全风险的有效管理，加强了大规模网络和基于互联网的商务应用的安全性。

基于安氏的 SAFElink 技术， SAFEsuite Decision 能够浏览到企业安全风险条件的变化。SAFElink 实际上是从网络中的安全产品中收集和存储信息的一组软件，它把这些收集的信息合并到一个数据库中，称为 SAFEsuite 企业数据库，其中安全产品主要包括安氏的 Internet Scanner、RealSecure 以及第三方的防火墙比如 Checkpoint Firewall-1，根据 SAFEsuite 企业数据库，SAFESuite Decisions 能产生报告分析和评估企业安全策略，这些报告可以帮助用户决策如何持续提高网络的安全。

SAFELink 由 SAFELink Manager、SAFELink Console 以及 SAFELink Agent 几个组件构成。

SAFELink Manager：是一个软件组件，它告诉 SAFELink Agent 什么时候从它们的产品数据库或日志文件中取出和发送信息到 SAFEsuite 企业数据库

SAFELink Console：是一个 GUI 软件，它允许你从本地或远程配置 SAFELink Manager

SAFELink Agent：是驻留在每个安装有安全产品的计算机上的软件，Agent 等待从 Manager 发来的命令，它从安全产品的数据库或日志文件中取出数据，利用安氏拥有的加密方法安全的传送数据到

SAFEsuite 企业数据库。

查看、计划、运行报告的方式有下面三种：

1）Crystal INFO Desktop

2）InfoDesktop for HTML

3）Java Desktop(accessed through a web browser)

如果使用 Crystal INFO Desktop，**必须在用户的机器上安装软件，如果使用** InfoDesktop for HTML 、Java Desktop，**用户有合适的浏览器即可。报告具有灵活的输出选项，可以产生** HTML、Excel、Word **和透明的报告，可以发邮件或存入文件中，可以从** UNIX **和** Windows NT **平台上浏览报告。报告还可以存入“报告库”中以便重新阅读，也可以把报告的不同部分分发给不同的人或网络上的不同地方。**

集中的安全信息

- **综合从多个网络运行的多个源中得到的重要安全数据，来改善企业的整个安全面貌。**
- **将安氏** X-Force **的知识库和多年的可适应性网络安全的经验用于一个企业的应用。**
- **提供内部和外部的分析并在实际网络中发现风险源和直接响应。**

管理功能

企业安全风险管理报告---- SAFEsuite Decision **提供基于统一、相互关联、协调的从产品而来的分析信息的有价值的安全报告。报告集中于重要的风险管理范围，如实时风险、攻击条件、安全漏洞和攻击分析。**

报告的定制执行---- SAFEsuite Decision **报告的执行和分布是自动的并且是可以预定的。这样保证了重要安全信息的快速有效的传播。**

企业安全数据的集中管理---- SAFEsuite Decision **的** SAFEsuite **企业数据库组件是一个具有一定规模的关系数据库，它成为企业安全数**

据的一个集中且永久的数据存储。SAFEsuite Decision 依赖于 Microsoft SQL Server 或 Oracle 关系数据库。

安全数据采集---- SAFEsuite Decision 的 SAFElink Loader 组件使得来自于安装在世界各地的产品如安氏 SAFEsuite 应用和第三方产品的安全信息能够安全转移到 SAFEsuite 企业数据库中。

5.12.2 建议方案

建议在华为企业网安全建设的前期阶段主要进行安全管理工具体系的设计和相关产品的评测。

5.13 安全测评

安全测评是贯穿整个华为企业网全网信息安全完整解决方案的一个重要环节。安全测评的目的是对华为企业网全网的安全状态进行评估，使得决策人和安全建设人员能够对系统有一个清晰的认识。

华为企业网安全建设中安全评测的主要内容包括：

- 安全需求分析
- 安全风险分析
- 安全测评规范制订
- 安全测评过程制订
- 安全内部测评
- 外部第三方权威机构测评

5.13.1 推荐安全服务

安全需求分析和安全风险分析服务请参考第七章安全服务体系中有关安全评估阶段的描述

安全测评规范和过程的制订，以及内部安全测评请参考第七章安全服务体系中有关安全测评的描述。

5.13.2 推荐权威测评机构——CNISTEC

IS-ONE 建议由中国国家信息安全测评认证中心（CNISTEC）来对华为企业网的安全建设成果进行测评。

CNISTEC 的测评结果是对华为企业网安全状态的测评和评级，同时也是对 IS-ONE 的安全产品、安全集成和安全服务水平的评价。

CNISTEC 的测评过程由 CNISTEC、华为、IS-ONE 共同协商制订。

6 安全服务体系

IS-ONE 提供系列化的安全服务体系，再服务体系中主要包括下面几个方面：

安全顾问服务体系 eSafeLink Consulting

专业安全服务体系 eSafeLink Professional

安全方案服务体系 eSafeLink Solution

6.1 专业安全服务 eSafeLink Professional 体系

IS-ONE 提供系列化的专业安全服务，针对不同的安全功能需求，不局限于提供产品的解决方案，主要通过服务的方式解决华为企业网的安全问题。

这些安全服务包括：

- 网络拓扑结构安全分析
- 主机安全服务
- 访问控制安全服务
- 信息加密服务
- 身份认证安全服务
- 日志和审计安全服务
- 灾难恢复安全服务
- 紧急响应服务

6.2 安全方案服务体系

安全方案服务主要围绕 IS-ONE 为华为企业网提供的顶尖安全产品所提供的服务。

安全方案服务包括：

- 安装和调试服务
- 产品技术支持服务
- 产品应用解答热线服务
- 产品升级服务等

安氏产品的安全服务参考《安氏安全方案服务建议书》。

6.3 安全顾问服务体系

安全顾问服务体系主要遵循 SafeCycle 模型的指导，为华为企业网的安全建设在整个生命周期的过程中提供持续的服务。

在下面的小节中将给予进一步介绍。

6.4 企业信息安全策略顾问服务

制订华为企业网有关信息安全方面的核心策略。

在本阶段，IS-ONE 将和华为企业网的安全负责人一同制订华为企业网的信息安全策略系列的核心文档。整个策略将包括：

- 《华为企业网信息安全总则》——此文档应当是一个概要性的，高层次的，纲要性的文件。此文档要指导其他策略的制订，规范全局的信息安全工作，明确信息安全的工作方向。
- 企业信息安全发展规划——信息安全发展规划的制订主要以华为企业网自身的业务发展规划和公司发展规划为基础。IS-ONE 就信息安全的发展趋势给出意见，使得信息安全发

展规划能够符合信息安全的发展方向,同时也能够与公司的整体发展规划相吻合。

- 企业信息安全人员组织管理规章——建立管理体系框架,定义每一个信息安全管理岗位。对每一个岗位给出责任、业务、水平要求等细节内容，通过管理框架将各个岗位联络起来。 信息安全管理体系必须和华为企业网已有的管理框架相一致。帮助制订《华为企业网的信息安全组织管理》和《华为企业网的信息安全人员岗位指南》。
- 《信息安全管理纲要》是企业实施信息安全管理工作的指导文件，纲要充分体现了信息安全总则提出的原则，执行信息安全总体发展规划的各项步骤，规范各个岗位的职责和管理。

华为企业网的信息安全策略系列文档是一个需要在持续的安全工作中不断修正、补充和完善的文档系列。

再其他工作阶段，也会涉及到各方面的策略。策略制订会渗透到各个工作阶段。

6.5 ASS—安全评估顾问服务

6.5.1 ASS-SNA—安全需求分析

帮助华为企业网进一步明确作为整个体系的安全目标什么；整个安全体系需要保护的对象是什么;并且对要保护的对象能够有比较量化的描述。

信息安全需求的主要体现在三个特征：

a.机密性——保证只有被授权访问的人才可以获取信息。

b.完整性——保证信息和处理方法的准确与完整。

c.可用性——保证授权用户可以获取信息，在被要求时，可以访问相关设备。

在本阶段，IS-ONE 的安全技术顾问将和华为企业网的安全负责人和安全技术人员一起，对华为企业网的业务和信息系统的具体情况进行充分分析后，将提供一个《华为企业网信息系统安全需求分析说明书》。说明书将详尽地分析华为企业网的具体安全需求。此说明书将作为整个安全服务和华为企业网进行安全管理的目标依据。

对于华为企业网的安全需求分析是一个需要在持续的安全工作中不断修正、补充和完善的文档。

服务过程主要有以下几项工作：

- 向华为企业网的相关人员进行需求分析的教育和沟通。
- 华为企业网提供信息系统结构等相关文件
- 通过会议和讨论的形式，对华为企业网的信息系统的安全需求进行分析和论证
- 形成正式的安全需求分析说明书

6.5.2 安全风险分析

对华为企业网的信息安全风险能够从自身脆弱性、潜在威胁、策略和管理的评估等多方面综合分析，对于公司的风险有一个全面的认识。

需要对华为企业网可能存在的信息安全风险进行定量和定性两方面的分析。

安全风险分析包含 6 个方面：

- 当前脆弱性和漏洞审计
- 自身脆弱性和漏洞评估分析
- 当前威胁和入侵审计
- 潜在威胁和入侵评估分析
- 整个体系的策略和管理评估
- 风险综合分析

系统脆弱性和漏洞审计

对华为企业网系统的当前安全脆弱性进行评估，通过检测对华为企业网的信息系统进行定量的漏洞检测。

对华为企业网的网络和系统，通过漏洞检测工具进行定量的检测，形成检测报告。检测可能在网络、操作系统和数据库管理系统三个层次上进行。此项工作是定量的检测。

自身脆弱性和漏洞评估分析

对华为企业网系统的当前安全脆弱性进行评估，通过综合的安全脆弱性分析和漏洞检查帮助客户了解现有的安全状况。

这个阶段包含以下工作：

1．检查现有技术体系结构

体系结构的检查以网络结构检查为主，结合业务体系、系统体系等结构的检查。

了解华为企业网的逻辑网络，由什么物理网络组成以及网络的关键设备的位置所在对于保持网络的安全是非常重要的。另外，鉴定关键网络拓扑，对于成功地一个实施基于网络的风险管理方案是很关键的。基本信息包括网络带宽，协议，硬件（例如：交换机，路由器等）Internet 接入，地理分布方式和网络管理。

这项工作将使项目团队对华为企业网和企业需求更熟悉。如果有必要，在华为企业网的网络结构内的关键网络位置出要进行网络流量分析。

2．应用脆弱性评估

对华为企业网的应用系统的脆弱性进行定性评估

3．脆弱性和漏洞综合评估

对根据前面各种定量和定性的检测和评估，综合形成对整个华为企业网信息系统的脆弱性和漏洞评估分析。

当前威胁和入侵审计

充分了解当前的安全威胁状况。利用工具对华为企业网信息系统

可威胁进行定量评估。

本阶段任务包括：在华为企业网系统某部份中安装“入侵监测系统”。在经过 10 天到 30 天的监测之后，将系统获得的安全事件汇集成为一个报告。

潜在威胁和入侵评估分析

能够对华为企业网的信息安全方面潜在威胁和可能入侵给出全面的评估。通过综合的威胁预测和分析，帮助客户了解现有的潜在安全威胁。

根据定量的对当前威胁和入侵审计，结合定性分析，对华为企业网潜在的信息安全威胁和可能的入侵进行评估和分析。

本阶段任务包括：

1．深入分析《当前威胁和入侵审计报告》的内容

2．对没有在审计报告中表现出来的潜在威胁和可能的入侵给与分析和预测。

3．综合形成华为企业网信息安全的威胁分析

策略评估

对企业的所有涉及 IT 的策略进行全面的评估，以便使得所有策略能够共同确保信息安全策略的执行。

将要对现在的信息安全策略、标准和指导方针进行一次检查，这个检查将提供适当的信息，以便构造一个与那些文件的要求相一致的风险管理方案。另外，IS-ONE 将和华为企业网一道工作，开发一个用在华为企业网操作中心内的合适的升级管理程序，对事件通知方法和事件紧急性进行评估来决定联系谁。工作人员信息和责任结构将由华为企业网提供。以帮助决定在发生何种类型事件应联系何人。

综合风险分析

分析所有的人和技术的因素造成的当前的风险，及可能潜在的风险，针对华为企业网作一个系统的分析，为风险管理的实施准备资料。

工作的主要形式是对已有的脆弱性评估、威胁评估、策略评估进

行分析和汇总。

综合风险分析的主要理念可以用下图表示：

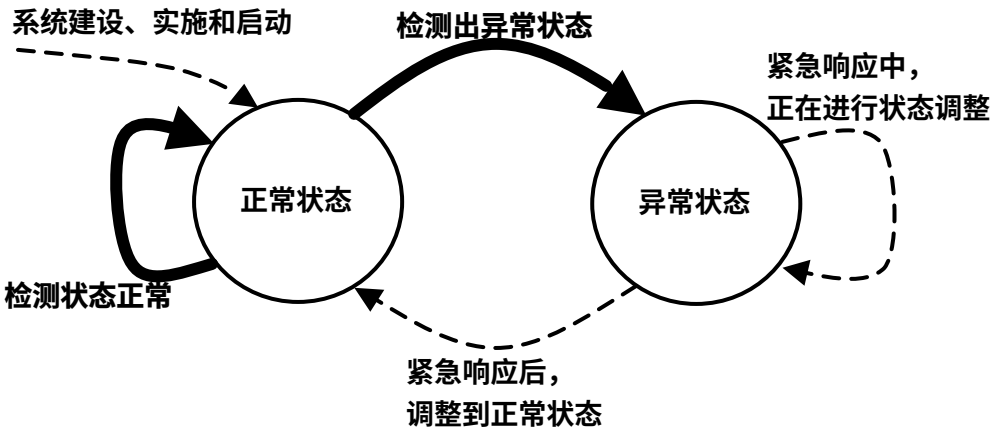
$$\frac{\text{自身脆弱性} \times \text{潜在威胁}}{\text{安全策略和措施}} = \text{安全风险}$$

通过分析和汇总最终形成一个综合性的风险评估报告。

6.6 安全管理维护方案

对华为企业网的信息系统安全整体解决方案的实施完成之后的持续管理和维护给出指南：

- 《华为企业网安全系统管理维护指南》
- 《华为企业网安全威胁管理指南》



本任务主要对安全状态转换模型中的对正常状态的检测过程给出指南。这个检测过程就是安全系统的实施完成并启动运行之后，需要进行的持续管理和维护工作。

在安全需求分析、安全策略制订和安全风险分析的基础上，IS-ONE 将向华为企业网提供实施一个围绕上述需求作出的风险管理方案的建议设计书。

1．入侵管理

互联网安全系统顾问将紧密地与客户在一起，保证他们已经为任何可能发生的入侵或攻击做好准备。安全保护程序的成功与否，关键要取决于意外事件响应程序是否能在事故发生之前就已经处在它应该在的位置上。

安氏中国顾问将会帮助华为企业网建立网络安全防护体系，检测保护措施能够防止入侵企图得逞，并进行管理。

2．漏洞管理

安氏中国安全顾问将于客户一起，帮助华为企业网建立网络漏洞管理体系，此任务包括确定每一系统的风险，以及机器上的资产价值。在此数据与已经找的漏洞之间建立相关关系，客户可以准确的找出哪些地方最需要进行修补，并且在该处修补最有效。

3．威胁管理

威胁管理包括入侵管理和漏洞管理两种形式。将这两种形式的结果关联起来，你可以看到企业的安全状况的全貌。

4．重复评估

安氏中国将根据技术的发展最新动态，为用户定制好完善的循环重复的评估体系。

6.7 安全紧急响应服务

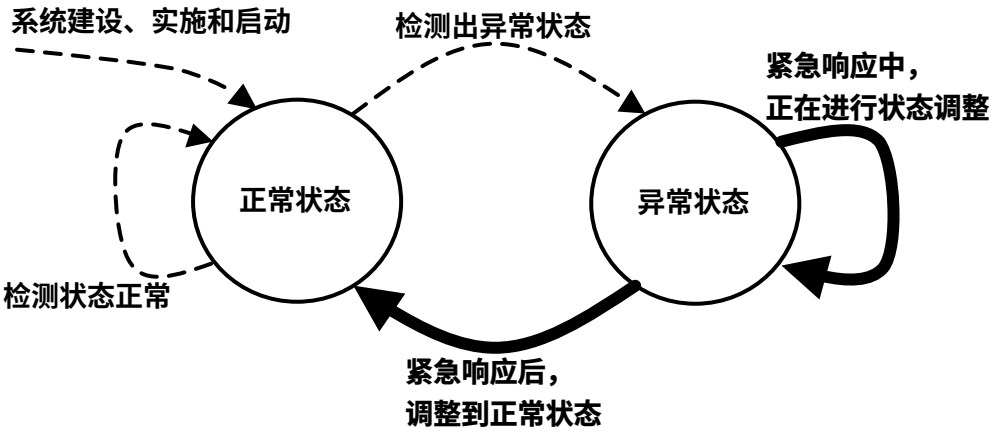
华为企业网必须从上而下地建立独立运作的系统安全员队伍，为整网可能发生的安全问题做到尽快响应，确实保障系统安全。

作为系统安全服务的一部分，我们可以帮助建立华为企业网独立的、由上而下的、反应迅速的系统安全员队伍，从安全管理上锻炼人员自身素质，对黑客入侵事件采取最迅速的反应，为 华为企业网中存在的异地攻击提供相互系统管理员支持的根本条件。

因为网络服务必须每周 7 天 24 小时提供，具有不可间断性，快速反应体系在华为企业网在遭到攻击时，能及时作出响应，解决问题，

维持服务的延续，处理问题的方式可以采取通过网络远程维护，在出现重大情况下可以前往本地解决或者通过电话协助本地管理员解决。

对华为企业网的信息系统安全整体解决方案的实施完成之后，进入管理和维护阶段，当发现异常情况而进入紧急状态后的响应和处理工作给出指南。



本任务主要对安全状态转换模型中的对异常状态的紧急响应和处理过程给出指南。这个响应和处理过程就是安全系统在运行、管理和维护状态出现异常之后，做出的紧急响应处理，以及在响应和处理完成之后的状态调整。

建立紧急响应体系的主要工作：

- 制订紧急响应指南。
- 建立紧急响应队伍

IS-ONE 安全顾问将根据华为企业网的人员配置情况，帮助华为企业网建立紧急响应队伍，随时应付将出现的紧急情况。

1．准备

- 评估现有的安全状况
- 建立入侵响应小组
- 制订一个紧急响应的报告流程
- 正常工作时间提供信息安全支持

- 为 WINDOWS NT/2000 和 SOLARIS 系统提供 SAVANT 安全信息服务
- 每季度或每月的用户的安全培训

2．响应

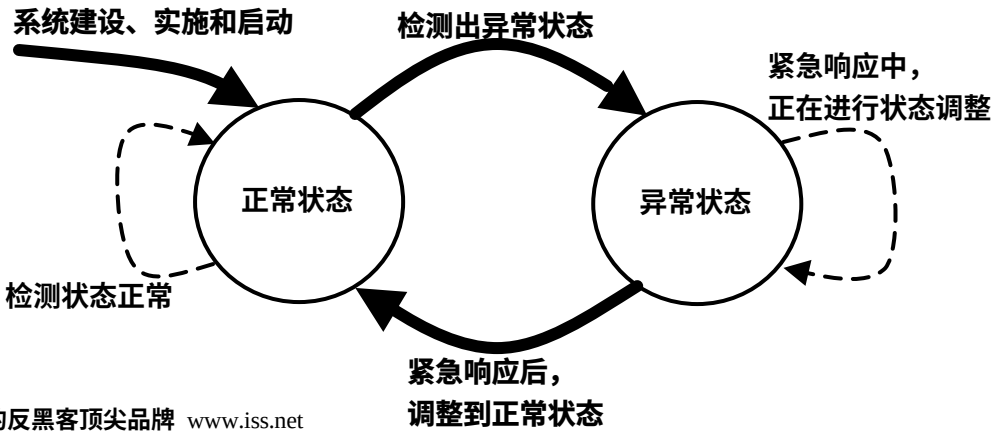
- 7*24 小时紧急实践响应服务
- 入侵分析
- 消除被破坏的和非法的文件
- 恢复正常的操作
- 消除今后的入侵隐患
- 对系统的安全进行重新评估

《华为企业网安全系统应急响应指南》

6.8 安全测评服务

6.8.1 制订安全测评准则和测评过程

明确描述安全测评过程。对如何测评华为企业网的信息系统的安全等级给出测评过程。制订出的测评过程将成为实施阶段中内部测评和外部测评的实施依据。



本任务主要对安全状态转换模型中的状态转换的条件给出描述。状态转换的条件实际上就是安全测评的依据。本任务将具体的测评标准落实为详细的测评过程。

最终形成《华为企业网安全系统测评过程说明书》

6.8.2 安全体系内部测评

本阶段的主要工作是对华为企业网的信息安全体系进行内部测评。工根据制订的测评准则，对华为企业网信息系统安全进行内部测评，作的主要形式是按照测评过程，对相关的文档进行审查。通过会议、讨论和评审的方式进行工作。

最终形成《华为企业网信息系统安全内部测评报告》并完成对华为企业网信息系统安全的内部测评。此测评安全工作的最后验收。

6.8.3 安全体系外部测评

向国内权威安全测评机构申请对华为企业网的信息系统安全进行测评。

可以申请的第三方测评有多个选择。华为企业网可以选择其中一个，或者多个。

最终希望该权威机构出具的测评报告。

推荐中国国家信息安全测评认证中心作为华为企业网的第三方权威测评认证机构。

6.9 教育培训服务

系统管理员是直接和系统打交道的高级计算机工作者，在整个网络维护中的地位非常重要。国内系统安全面临的最大问题是有着丰富系统安全经验尤其是主动发现黑客的系统管理员非常少，系统管理员在和黑客交锋的战斗中经常吃亏。由于和黑客的战斗是一场智力的斗争，也是计算机网络知识的交锋，所以需要迫切地给各种系统管理员进行有效的系统安全培训，掌握计算机安全的高级知识，了解黑客使用的流行手段，并能采取必要的防范措施。

在企业各部门工作的普通员工是能够接触主要服务系统的工作人员。为了确保安全，建议对所有的职工，从信息主管到一般的工作人员都要加强安全意识，需要对信息主管和普通工作人员的安全培训课程。

教育培训服务的主要内容包括：

- 教育培训体系建议
- 具体的一些培训课程
- 制订信息安全人员考核标准

6.9.1 教育培训体系

本任务的主要工作是：为华为企业网建立信息安全教育培训的制：

- 安全教育政策制订
- 安全教育计划制订
- 安全教育实施支持方案

最终形成《华为企业网信息安全教育培训体系》

6.9.2 教育培训课程

提供并帮助华为企业网安排信息安全培训课程。制订培训大纲。并具体安排一些培训课程：

- 安排华为企业网的人员参加 IS-ONE 提供安氏认证培训。
- 安排华为企业网的人员参加在美国安氏举办的安氏认证培训。
- 安排华为企业网的人员参加防火墙、防病毒、加密等技术方面的培训课程

6.9.3 安全人员考核服务

协助华为企业网建立信息安全人员考核体系。包括：

- 制订信息安全人员考核标准
- 帮助华为企业网建立安全相关人员的定期的评估和考核制度。

形成《华为企业网信息安全人员考核体系》

7 安全集成方案

7.1 方案一：强健型方案（推荐）

该方案适用于电信级大企业的完全安全解决方案。具有高可靠性（HA）、高安全性、最优性价比等特点。参照第五章安全系统功能要素表述，本方案如下配置：

网络拓扑结构	**采用网络拓扑结构安全分析服务** **参考** 5.1
防火墙	**采用双机冗余设计，无单点故障。在节点网段配置双机备份的** CHECKPOINT **防火墙。** **参考** 5.2**，针对高速骨干链路和** IDC
主机系统	**采用主机安全服务（包括** UNIX **类和** WINDOWSNT/2000 **类）。** **参考** 5.3
漏洞评估	**采购安氏** Internet Scanner **网络漏洞扫描器，** System Scanner **系统漏洞扫描器，** Database Scanner **数据库漏洞扫描器。并建立华为企业网的漏洞评估体系。** **采用** IS-ONE **的风险评估服务。** **参考** 5.4.6 **和** 6.5
入侵监控和防御	**采购安氏** RealSecure **入侵监控产品，在重要网段和重要服务器上配置** Network Sensor **和** OS Sensor**。** **参考** 5.5

访问控制	**采用** IS-ONE **访问控制安全服务** **参考** 5.6
日志和审计	**采用** IS-ONE **日志和审计安全服务** **参考** 5.7
身份认证	**采用** IS-ONE **身份认证安全服务** **参考** 5.8
信息加密	**采用** IS-ONE **加密安全服务，提出华为企业网的加密体系。** **参考** 5.9
防病毒	**每个节点配备** TrendMicro Neatsuite **防病毒套件** **参考** 5.10
灾难恢复	**采用** IS-ONE **安全紧急响应服务** **参考** 5.11
安全管理工具	**设计安全管理工具体系** **参考** 5.12
安全测评	**请中国国家信息安全测评认证中心对华为企业网安全系统进行测评。** **参考** 5.13 **和** 6.8
安全策略	**采用** IS-ONE eSafeLink **安全策略顾问服务。** **参考** 6.4
安全管理维护	**采用** IS-ONE eSafeLink **安全管理维护顾问服务。建立安全系统运行维护体系。** **参考** 6.6

教育培训	**采用** IS-ONE eSafeLink **安全教育培训服务。建立完备的安全教育体系和考核体系。** **参考** 6.9

7.2 方案二：经济型方案

安全是相对的，经济型方案是为了适应在华为企业网安全建设方面的不同资金投入，提供一个投资方面比较精简，安全性比强健型相对较弱，但是也是一个可以满足基本要求的安全方案。

经济型方案和强健型方案的主要区别是：

防火墙	采用 LinkTrustTM 防火墙，在骨干节点不采用双机热备方式。 参考 5.2.4
主机系统	减少主机安全服务的设备数量。优先对骨干节点的重要主机进行安全加固服务。
入侵监控和防御	减少监控点的配置数量。优先对骨干节点的重要主机进行安全加固服务。
访问控制、日志和审计、身份认证、信息加密	短期内只进行体系、策略的制订
安全测评	请中国国家信息安全测评认证中心对华为企业网安全系统进行测评。 但是在评级方面申请较低级别。

7.3 安全建设规划和规划型方案

由于华为企业网是一个庞大的、复杂的信息系统。需要一个长期的建设和管理。

从安全建设规划方面，华为企业网的建设可以分为多个阶段。可以分期建设部分核心骨干节点、节点和二级节点；在安全产品的选择和安全服务的采用方面，首先选择最基本的服务和产品，其次在配置加强服务和产品。

在强健型方案的基础之上，为华为企业网全网的信息安全建设提出一个规划型方案。规划型方案与强健型方案的主要区别为：

- 全面采用安全管理工具——Safesuite Decision。
- 全面采用主机安全加固服务
- 采用更加强健的访问控制、加密和认证产品，并配合相应的服务
- 加强灾难恢复能力

7.4 安全系统自身安全说明

本建议书中安全解决方案是建立在 IS-ONE 公司丰富的电信企业网络安全经验基础之上的，提供的产品、技术服务都已经过严格的电信级企业网络的实际生产环境考验。本方案安全系统自身安全采取了以下措施保证：

- 安全系统主机经过主机操作系统加固配置
- 安全系统主机处于入侵监控（IDS）系统保护下
- 安全系统主机处于路由器、防火墙、主机本身联合访问控制保护下
- 经常性的、定期的风险评估（VA）保证安全系统自身的安全水平
- 安全系统控制台和被控制主机、代理之间的网络通信全部通过强加密方式进行
- 安全系统中的产品都经过电信级运行环境的考验

7.5 集成性说明

本建议书所提出的方案是全面考虑了华为网的全网安全需求、业务要求而提出的，各部分之间有机结合构成一个整体的全面解决方案。其特点是：

提出了完善的安全管理体制，它是在安氏公司多年的安全实践及理论研究基础上，结合华为网的当前实际网络结构、业务类型及其未来发展而提出的，具有很强的可操作性和实用性。

简单有效而灵活的安全软、硬件产品配置，所选产品及其配置都经过仔细考虑，在保证自身功能的前提下对华为网全网的网络结构、性能及所承载的业务没有任何实质性的影响，并且可以通过软件配置、升级或硬件升级、扩容，平滑地适应未来华为网网络及业务的大规模发展。

工程方案易于实施，在华为网这样的全国性的提供综合业务的大网中进行全网性的工程时，可能会出现一些复杂情况，部分操作在实施时可能会暂时影响到网络及业务的正常运行，某些操作如果失误可能影响整个节点甚至全网的正常运行，因此方案在设计时充分考虑到这是一个系统工程，把工程实施的易操作性放在重要位置。在工程实施前还将与甲方管理及技术人员、第三方产品提供商共同制订详细的工程实施方案。

所配置的安全软、硬件产品本身具有较强的自我防护能力所配置的安全软、硬件产品（包括入侵检测、安全扫描、防火墙、防病毒等）都能满足集中配置、集中管理和集中监控的要求所配置的安全软、硬件产品都可以通过易学易用的图形化界面进行配置、管理和监控所配置的安全软、硬件产品互相之间功能互补，构成一个多层的保护体系一些重要的产品遵循最新的国际标准，因而能提供良好的互操作性及其它功能，如 CHECKPOINT 防火墙与 TREND 防病毒软件

8 项目管理

8.1 项目运作方式

针对华为企业信息安全顾问服务，安氏公司提出两类项目运作方式：企业安全顾问方式和顾问服务项目方式。

企业安全顾问方式就是在安氏公司和华为公司双方签署全方位的信息安全合作。华为公司选择安氏公司作为华为的信息安全顾问公司。安氏公司将在合作协议确定的工作范围内，为华为公司全面地提供安全服务。安氏公司将站在用户的角度，循序渐进地、有计划地协助华为公司构建自身整体/定制信息安全体系。

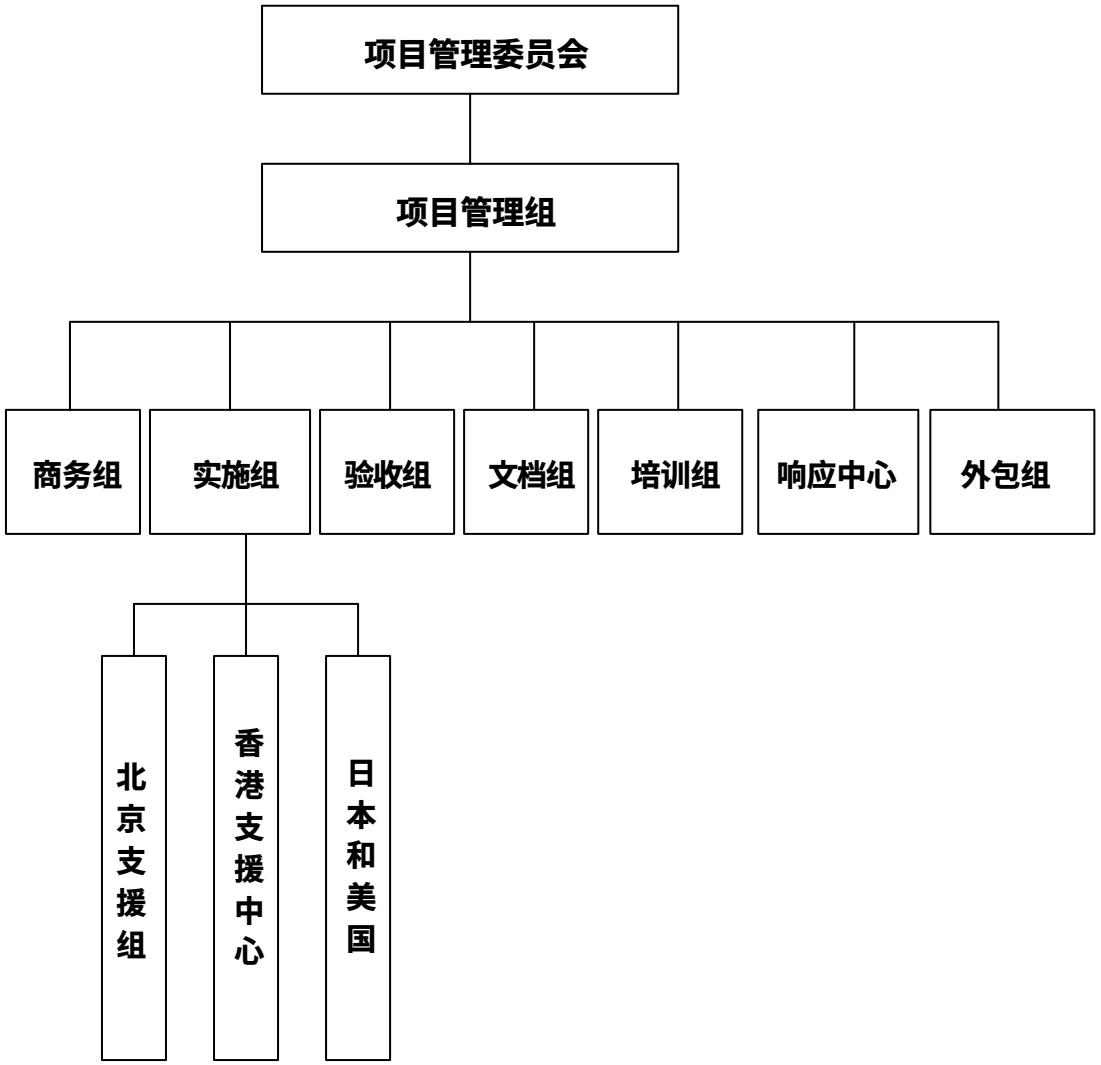
顾问服务项目方式就是将华为公司的信息安全工作定义为一些明确的项目，由安氏公司来承担相应项目的服务和产品工作。这方面的服务项目可以包括以下几个方面：

- 信息安全管理框架服务：主要侧重在企业信息安全管理框架的建立和实施。
- 专业安全技术顾问：主要侧重在特定安全技术领域的支持，比如黑客攻防技术服务，紧急重大安全事故响应和处理等。
- 教育培训服务：主要侧重协助华为公司实施全员信息安全培训。
- 技术服务：具体的信息安全技术服务，比如漏洞探测服务、系统漏洞修复服务、入侵监控服务、防火墙管理服务等。

项目的运作和管理流程将由安氏公司和华为公司共同完成。

8.2 项目实施组人员组织结构

8.2.1 组织结构图



8.2.2 人员职责说明

项目管理委员会

对项目的实施提供高层的支持和帮助。

由华为、安氏和其他可能的合作伙伴的各一位高层管理人员组成。

项目管理组

全面负责项目的实施进度，负责项目组之间的协调和沟通；定期召开审查会议，把握项目的实施进度，及时发现问题解决问题，并定期地向项目委员会报告项目的实施进度。

由安氏公司高级项目管理员担任

商务组

负责项目中所有硬件、软件保质保量到达用户现场。

由安氏公司一位高级商务人员组成

实施组

负责顾问服务项目的实施工作。参考“顾问资源”章节。

验收组

负责对各个服务项目的实施情况加以验收。

验收组的成员组成在不同的验收阶段有所不同。

培训组

负责对用户提供所有的课堂培训。

由安氏公司培训部的专业培训人员组成，人员数量配合不同的实施阶段有所不同。

文档组

负责收集和整理华为安全项目实施过程中产生的所有文档资料（书面的和电子的）。

由 1 位安氏公司项目管理中心的管理人员组成。

响应中心

负责提供给用户及时准确的帮助，包括使用方面的热线咨询、故障的修复。

由安氏公司客户服务中心 3 位工程师组成。

外派技术人员

如果客户需要，安氏公司可以派出技术人员到客户现场实施外派服务。

由安氏公司客户服务中心的工程师组成，具体人员数目需要进一步视需求而定。

8.3 项目实施管理

安氏公司对项目管理非常重视，因为项目管理直接关系到整个项目的成败。

8.3.1 项目管理的目标

安氏项目管理的目标不是单方面的。它由五个方面构成，这五个方面同时也是安氏评价项目管理成功与否的依据。

用户满意

这是安氏项目管理追求的首要目标，如果这个目标没有达到，安氏认为这个项目就是失败的。

完成合同规定的所有任务

安氏与客户签订的供货及服务合同是具有法律效力的。我们会象客户那样尊重它。我们信守所作的承诺。不折不扣地完成合同规定的所有任务。如果合同执行过程中出现任何变化，我们会主动友好的与用户协商讨论，保障用户利益的前提下，双方达成一致。确保合同完成，让用户满意。

按时完成任务

安氏一贯重视合同执行期，我们会千方百计的确保合同按时完成。我们会制定备用方案，以防发生不测事件。

项目各参与方满意

在项目实施的过程中，安氏会邀请合作伙伴参与。其目的是发挥

他们的专长确保工程质量。这些合作伙伴是经安氏考核，满足安氏在选择合作伙伴的标准。安氏非常尊重他们。安氏会兼顾各方利益，使各方心情愉快地参与项目的实施。

符合预算

考核项目预算是安氏自我监督的重要步骤，目的在于提高项目管理水平。合理运用资源，达到上述五个目标是我们的目的。但是如果没有用户的大力支持是不可能的。因此安氏公司希望客户能在以下几方面配合我们。

- 制定专人组成用户方的项目小组。
- 任何在需求上的变化，如果将影响合同时间期限，双方需协商一致。
- 及时提供反馈意见。

8.3.2 项目管理的方法论介绍

- FocusPM(简称:注重项目管理法)
- CPLC(Customer Product Life Circle, 简称:客户化生命周期法)
- TCM(The Consulting Methodology, 简称:咨询方法论)

这些方法论有效地指导我们在项目管理中作出正确的决定，圆满地履行合同。这些方法论的共同特点是将理解用户的需求放在第一位，从针对行业的特点和项目的规模上可以区别他们各自的应用领域。

FocusPM 是一种通用的方法，它可以适用于通讯、信息、金融和制造等众多行业，适用的项目规模也比较灵活。

8.3.3 项目的管理方法

针对华为安全项目的特点，及 FocusPM 的原理，我们将整个项目的实施分成几个方面，包括:

- 分析和研讨
- 计划与总体设计
- 试点与培训
- 实施和验收
- 支持与维护

在整个实施过程中，坚持下面三个管理重点.

- 降低风险
- 项目合作方的管理
- 质量控制

降低风险

注重风险管理是西方管理理论的一个特色。任何事件的发展都会有一定的意外，它的发生是不可定的，这种脱离常规的意外称之为风险，若我们充分重视风险会造成的影响，就可以避免遭受较大的损失，风险管理主要从三方面着手：

- 确定风险因素

- 阻止不可承受的风险发生
- 制定风险发生的解救方案

风险因素的确定要根据项目的具体情况。在项目实施中，存在实施参与方多，实施时间较长，推广工程量大等等风险。

针对客户会关心的风险，我们制定了避免风险的措施:

风险事例	避免措施
项目参与方多	项目参与方资格认证 明确项目参与方职责 建立项目高级委员会
合作方对项目重视不够，人员投入不足，人员素质不够，产品质量不高	合作各方资格认证 合同严格保证 人员能力认证 人员先期培训 建立质量规范 建立项目实施监督计划
合作伙伴人员不稳定，如出国或跳槽	强化软件规范 规范设计和技术文档 培训后备人员 技术转移

依据安氏公司的项目管理经验，我们认为除上面提到的风险之外，还有一些包括货运等在内的其他风险，在项目中，三个对项目影响最大的风险是:

风险事例	避免措施
大量设备按期到货风险	各点设备按期到货 设备发运无差错 组织安装验收
客户需求的变化和厂家对客户需求的理解的不易致，尤其是本地化业务	严肃项目需求分析阶段，共同制定严格的需求书 分阶段验收
系统质量不符合规范	共同制定开发质量监督实施规范 加强监督 严格测试

项目合作方的管理

安氏在项目合作方的管理上主要从几个方面着手:

- 选择项目合作方的必要性
- 选择项目合作方的资格要求
- 明确分工职责
- 监督项目实施

我们将通过合同明确合作方的职责范围，确定定期监督检查方式，确保项目合作方达到项目对其要求.。

质量控制

质量控制的重要性在项目管理中如何强调都不过分，我们正是通过质量控制来保证项目的顺利实施，不会出现任何形式的返工。包括：

- 清晰的安装配置手册
- 明确验收方式
- 强化实施方法
- 监督操作过程

8.3.4 项目的实施原则

安氏的宗旨是满足用户的需求，保证项目的成功。

定期项目审查会议

定期的项目审查会议贯穿整个项目的实施过程，由项目管理员负责召集相关人员定期召开，目的包括：

- 审查项目进程
- 解决存在问题
- 检查落实后续的工作

项目分阶段性验收

由项目管理员将所有的阶段性验收排入项目计划之中，目的是为了保证项目的计划和项目质量，同时强化用户对系统的熟悉程度。

全过程文档记录

由项目管理员和总体设计组确定在各个阶段要提交的所有文档，以及相应编写人员、文档模板、提交及认可方式。

8.4 项目实施进度安排

[TBD] 根据华为公司的需求进一步确定。

8.5 阶段性详细实施计划

[TBD] 根据华为公司的需求进一步确定。

9 质量保证体系

9.1 概述

IS-ONE 非常重视质量保证工作，在 IS-ONE 的各方面工作中，要坚决贯彻 ISO-9000 系列质量管理标准。在本项目的质量方针是“质量第一，用户至上，服务一流”。

IS-ONE 通过自身非常健全、有效的质量保证体系，保障此项目的研制、开发、设计、采购、生产、检验、试验、安装、调试、交付和服务的全过程实施有效的质量控制，使项目质量得到保证。

9.2 项目执行人员的质量职责

项目开发、设计人员——项目开发、设计人员的质量责任主要是，贯彻公司质量方针、目标，执行质量体系文件的各项有关规定和要求，确保设计工作始终处于受控状态；积极运用优化设计技术和可靠性、可维护性、安全性等工程技术，确保设计满足质量要求；为产品研制、物资采购、系统安装、调试、检验等活动提供技术支持和配合。

项目质量师——质量师配合项目经理开展工作，其主要职责和权利是：制订本项任务的质量工作计划，并贯彻实施；负责对工程任务的全过程的质量活动进行监督检查，参与设计评审和其他重要的质量活动，其质量业务工作受公司质量部的指导监督。

项目标准化主管师——标准化师由标准化工作人员兼任，负责贯彻国家有关标准和公司的质量方针、目标，制订标准化大纲并监督其贯彻实施，负责设计图纸和其他技术文件的标准化的审查，参与设计评审工作。

项目实施人员——项目实施人员应贯彻公司的质量方针、目标、执行质量体系文件的有关规定和要求，熟练掌握本岗位的工作技能，严格按照项目设计要求及有关标准进行实实施作，对其实施质量负责，并负责有关设备的日常维护工作。

后勤保障人员——后勤保障人员应经过业务培训、考核合格、持证上岗，应熟悉本职业务。

9.3 项目质量控制措施

9.3.1 合同评审

合同评审的控制要求：

- **合同的各项要求明确，并形成文件**
- **合同规定的要求合理，符合国家有关法律、法规，双方的风险和利益适宜**
- **任何与投标不一致的合同要求或双方不一致的意见都已得到解决**
- **公司已具备满足合同要求的能力**

9.3.2 设计控制

9.3.2.1 对设计工作策划的控制要求：

- **对每一项工程任务制定设计开发计划，划分设计阶段，规定每一阶段的设计任务，应开展的质量活动及控制措施和验证方法等；**
- **编制的设计开发计划可确保前一阶段的活动未达到要求，不能转入下一阶段；**
- **设计人员应按相应的设计，实验规范开展设计、实验工作，并依此作为控制和评价设计工作的准则；**
- **设计人员应运用优化设计和可靠性、可维护性技术，开展设计工作；**
- **应执行设计文档和技术文件的审查制度，保证设计质量满足**

规定要求；

9.3.2.2 对设计评审的控制要求：

- 在设计的适当阶段，应有计划地对设计结果进行正式评审，评审结果应形成文件并予以保存；
- 应根据项目的功能级别和管理级别，实施分级、分阶段设计评审合同要求时，应邀请用户方或其他代表参加评审；
- 每次评审的参加者包括与被评审的设计阶段有关的所有职能部门的代表，需要时也包括其他专家；

9.3.3 采购、检验和试验

9.3.3.1 对采购的控制要求：

- 评定分承制方。按有关程序的规定，评价分承制方的质量保证能力，确定对承制方的控制方式和控制程度。建立和保存合格分承制方的质量档案；
- 按有关程序的规定，编制采购文件，明确采购要求；
- 按有关程序的规定和采购文件的要求采购所需产品；
- 对采购产品进行验证；
- 对采购产品的入库、保管及发放的每个环节进行有效控制，以满足质量保证的要求；

9.3.3.2 对进货检验和实验的控制要求：

- 按有关程序、标准和技术文件规定的方法，对外购产品进行检验和试验，确保未经检验或未经验证合格的产品投入使用；
- 在确定进货检验的数量和性质时，应当考虑在分承制方处所

进行控制的程度和提供和提供的合格证据；

9.3.4 搬运，贮存，包装，防护和交付

9.3.4.1 运输、包装及交付的控制要求:

- 应根据产品的特点采取相应的防止损坏或变质的搬运方法；
- 产品贮存应使用指定的贮存场地或库房，应按规定的管理方法接受和发放产品，应定期检查库存品状况，以便及时发现情况；
- 应采取适当的防护和隔离措施，以防止产品混淆或遭受环境的不良影响；
- 产品交付时，应提供有关检验和试验结果；
- 产品交付时，符合合同规定，有按规定签署的产品合格证，经使用方或其代表验收合理，有产品使用维护说明书，产品包装符合有关规定和合同要求；

9.3.5 过程控制

过程控制的实施要点是，制定并执行文件化的过程控制程序，对系统质量形成过程的 4M1E 五个基本要素实施全面控制与管理，一旦发生偏离能够立即发现和纠正，确保过程输出质量符合规定要求。

4M1E 五个要素是指：人（man）、机（machine）、物（matter）、料（material）、环境（environment）。

9.3.5.1 控制要求：

- 要确保直接影响系统质量的生产、安装和服务过程处于受控状态；受控状态主要包括：

a． 对生产、安装和服务的方法制定相应的程序文件。现场使用的所有技术文件均应文文一致、完整、清晰并现行有效。

b． 使用合适的生产、安装和服务设备，并安排适宜的工作环境。

c．严格按有关标准/法规、质量计划和程序文件的规定操作。

d． 对适宜的过程控制参数和产品特性进行监视和控制。

e． 需要时，对某些过程和设备是否满足要求进行认可。

f．操作人员的技术水平必须满足规定的要求，并持有考核合格证书。

g． 按规定周期对试验设备、工艺装备和检测器具进行检定，并作出检定合格标志。

- 对特殊过程应按工艺文件或专用的质量控制程序，由具备资格的操作人员来完成和/或要求对过程参数进行连续监视和控制，以确保满足规定要求。
- 对关键工序应制定并执行专用的质量控制程序，以确保满足规定要求。

9.3.5.2 控制措施

9.3.5.2.1 三检制

各实施小组要严格执行实施过程中的自检、互检、专检制度，实施过程中要做到“以预防为主”，将质量隐患消灭在实施过程中，实

施人员在分部、分项工程完成后，首先进行自检，再由班组长进行互检合格后，通知专职质量师进行专检。

9.3.5.2.2 质量样板制

- 在全面开展分部、分项实施前，组织技术熟练的实施人员按实施文档和实施规范进行典型分项工程的操作示范。经专职质量师检验认可后，进行样板交底，并填写样板工程鉴定单，一式三份。主管实施的项目负责人、实施小组、专职质量师各一份。
- 分部分项工程的三检均以样板作为质量评定的依据

9.3.5.2.3 技术质量通知单：

专职质量师发现违反实施程序，不按设计文档和规范规程实施，系统和设备不符合质量要求时，首先向项目经理部负责人反映，限期解决，如影响到实施质量时应填写技术质量通知单，一式三份，写明主要问题和解决意见，实施小组一份，质量师一份，并报项目经理根据公司有关质量奖惩规定进行处理，并责成实施小组提出纠正措施，限期整改。如是严重危害工程质量行为应上报公司质量部。

9.3.5.2.4 项目预检：

项目预检主要是对实施前或实施过程中的重要技术工作、部位进行检查或核实，一般工程部位由班组长负责，质量师参加签署检查意见，重点工程及重要实施部位由项目经理、实施小组组长、质量师共同检查，合格后办理签证。

9.3.5.2.5 质量事故处理

凡属一般质量事故由项目经理部组织检查处理，重大质量事故和特殊项目质量事故由公司质量部组织有关部门进行检查处理。处理质量事故必须本着“三不放过”的原则办事。事故应按国家有关规定及

时逐级上报，不得拖延，重大质量事故的返修要专题报告，经公司批复后才能进行返修工作。

9.3.5.2.6 验收预检

a. 验收预检是单位工程在正式验收前一次全面检查，对存在的问题没有全部解决前，不得报请验收。

b. 预检条件

●各系统分项工程基本完成

●各系统设备安装、调试完毕，达到试运行。

●竣工技术档案资料基本齐全。

9.3.5.2.7 项目验收

a．项目验收是在修复验收预检存在的问题基础上，由项目经理部并报请甲方进行交付使用前的正式验收。

b．项目验收具备的条件：

●验收预检时提出的问题全部解决

●各分系统试运行达到设计要求并具备甲方使用条件

●各系统工程技术资料齐全，全部分类整理装订线册，达到移交甲方的程度。

9.3.6 服务

服务内容和服务质量已成为业主非常关心的重要内容，能否提供优良、丰富的技术支持与系统保修、维护服务，已成为衡量安全服务商能力和水平的重要标准。

服务控制要求

- **在规定有服务要求时，各有关部门应执行程序文件的规定与要求，制定服务实施计划，配备必要的资源，认真负责地做好所需要的服务工作；**
- **对用户方反映的意见和质量问题应及时处理，并将有关信息处理的结果报质量部门备案；**
- **质量部门对用户方反映的质量问题进行归口管理和统计，并及时向总经理及其它有关部门和领导汇报。**

10 项目产品及服务价格