动态网络安全模型综述

1　可适应网络安全模型

可适应网络安全理论主要有 PDR 模型和 P2DR 模型[1]，它能够根据网络动态变化的情况及时做出相应的调整，以维持网络系统相对安全稳定的状态。PDR 模型通过防护(protection)、检测(detection)和响应(response)三位一体来保障网络系统动态和整体的安全性(图 1)。P2DR 模型在 PDR 模型的基础上增加了策略(policy)。但是，PDR 模型和 P2DR 模型都没有考虑网络安全的管理和控制要素，因此缺乏管理、人为处理因素，不便于网络系统信息安全整体的监视和控制。

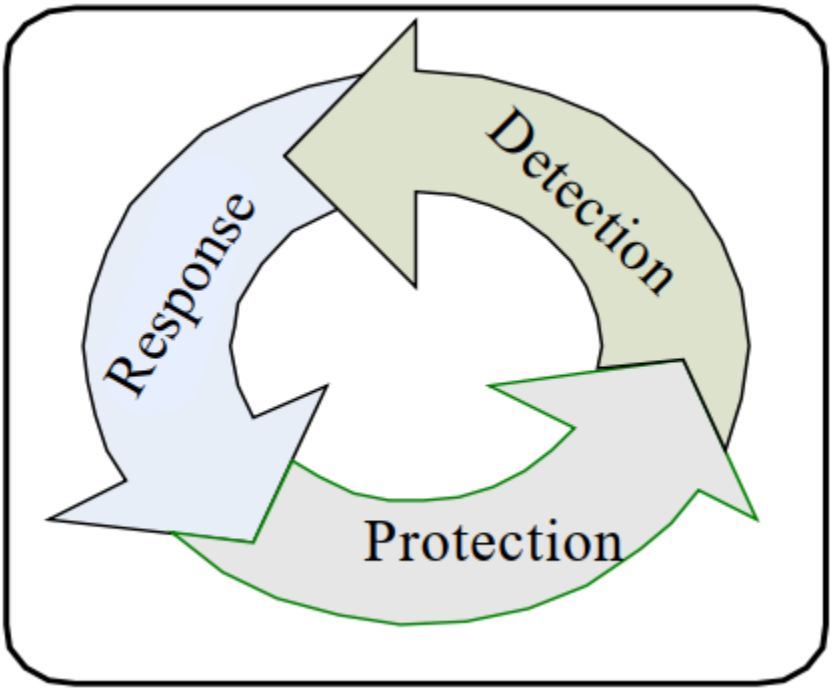


图 1 PDR 模型

2　可适应网络安全模型的改进

在 PDR 模型和 P2DR 模型中，将管理因素加入，将原来的模型扩展成为 P2DRM 网络信息安全模型(图 2)，用于北京烟草的网络安全综合管理系统。该系统架构具有动态响应机制，能使多种网络安全技术分工合作、有机结合，通过检测、决策、响应三位一体的联动，有效提高系统入侵检测、防御、保护的能力[2]。

通过多种类型的网络防御、人工管理和协同工作机制，共同完成网络系统的安全目标，实现网络系统信息安全多层次的监视和控制。策略、防护、检测和响应 4 种要素及各种安全措施都需要在安全管理的指导下实施。在此体系框架下将来源于分布式人工智能领域的 Agent 技术融入网络安全系统体系中。同时，系统通过多 Agent 的之间的协作、交互等手段构成一个基于安全管理的动态网络安全模型。系统总体框架如图 3 所示。

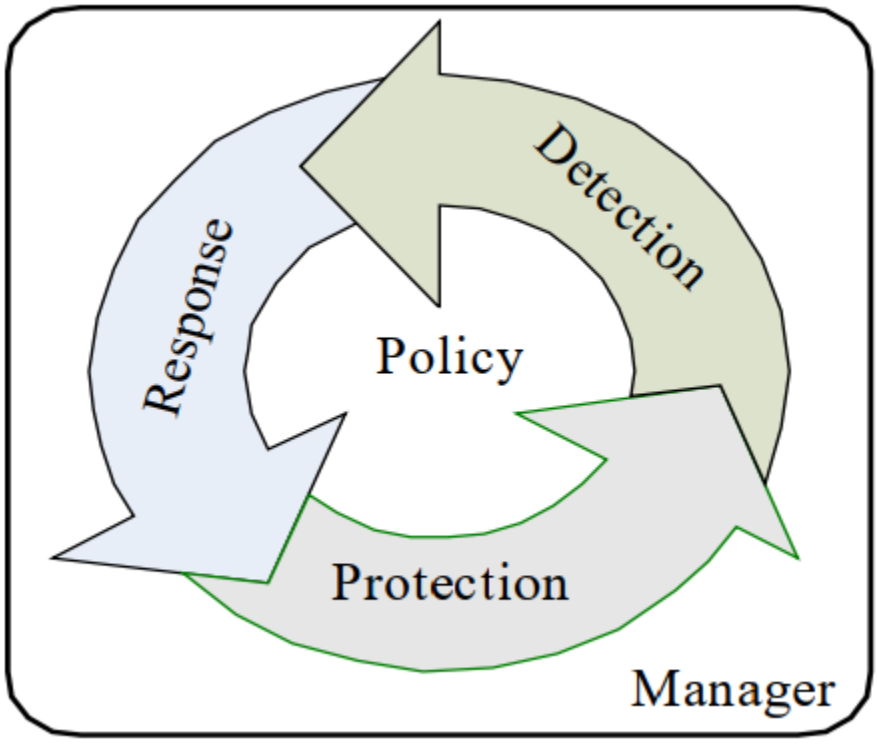
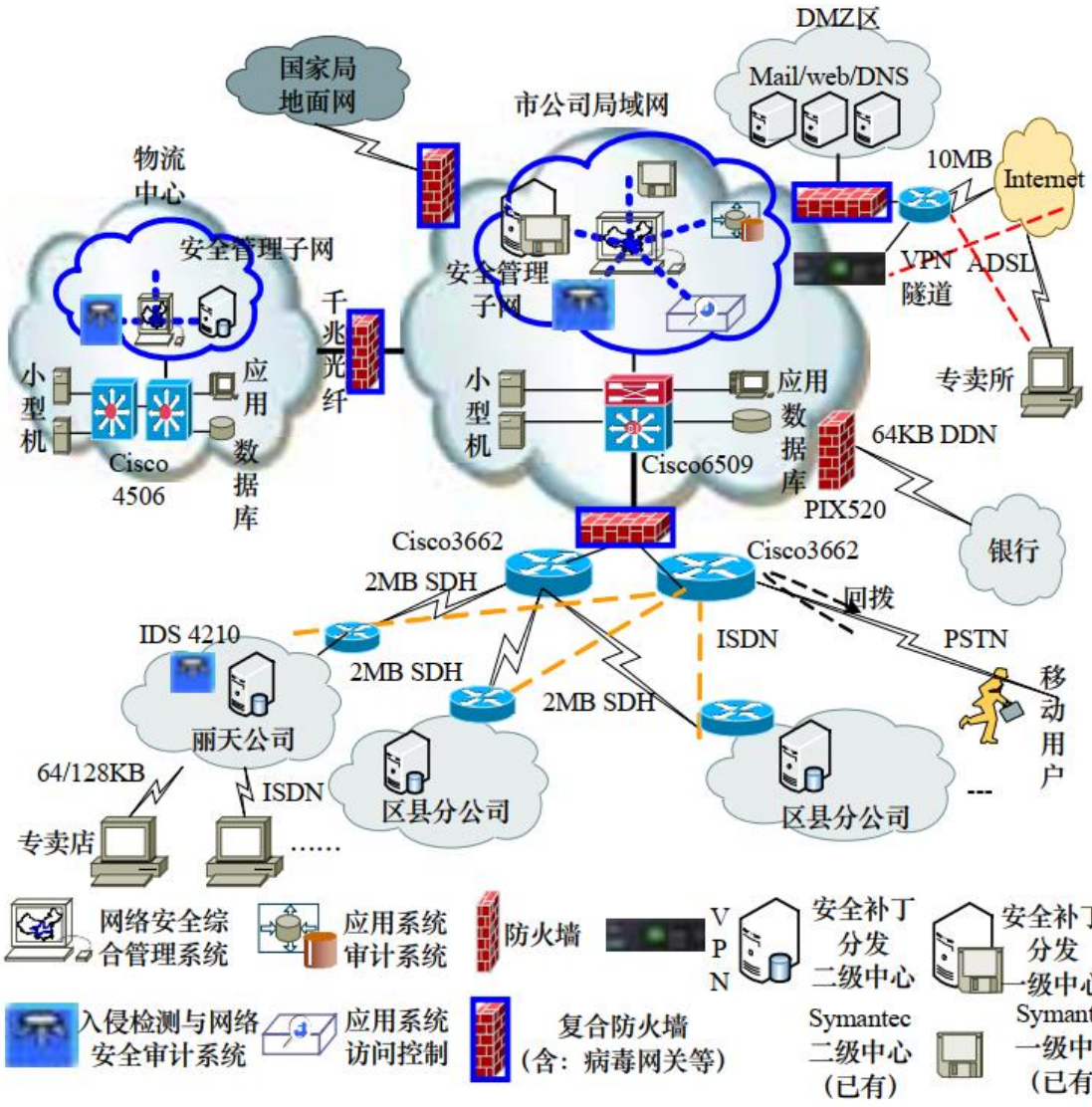


图 2 P2DRM 模型


DMZ区
Mail/web/DNS
国家局
地面网
市公司局域网
物流
中心
10MB
Internet
安全管理子网
安全管理
子网
VPN
隧道
ADSL
千
兆
光
纤
小
型
机
应
用
数
据
库
Cisco
4506
小
型
机
应用
数
据
库
Cisco6509
专卖所
64KB DDN
PIX520
银行
Cisco3662
Cisco3662
2MB SDH
回拨
IDS 4210
2MB SDH
ISDN
PSTN
移
动
用
户
2MB SDH
丽天公司
区县分公司
区县分公司
64/128KB
ISDN
专卖店
……

网络安全综
合管理系统
应用系统
审计系统
防火墙
V
P
N
安全补丁
分发
二级中心
安全补丁
分发
一级中心
入侵检测与网络
安全审计系统
应用系统
访问控制
复合防火墙
(含：病毒网关等)
Symantec
二级中心
(已有)
Symantec
一级中心
(已有)

图 3 系统结构

3　全网动态安全体系 APPDRR 模型

全网动态安全体系可由下面的公式概括：

网络安全 = 风险分析 + 制定策略 + 防御系统 + 实时监测 + 实时响应 + 灾难恢复

即网络的安全是一个“APPDRR”的动态安全模型，如图 4 所示。

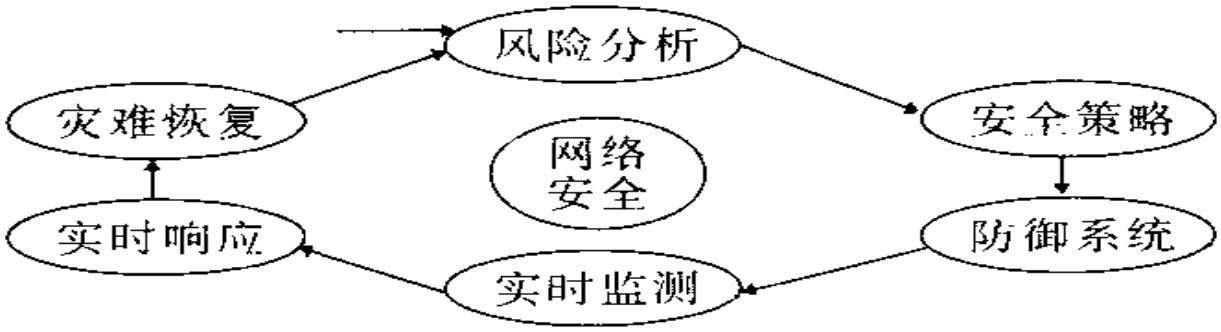


图 4 动态安全体系 APPDRR 模型

从安全体系的可实施、动态性角度，动态安全体系的设计充分考虑到风险评估、安全策略的制定、防御系统、监控与检测、响应与恢复等各个方面，并且考虑到各个部分之间的动态关系与依赖性。

进行风险评估和提出安全需求是制定网络安全策略的依据[3]。风险分析(又称为风险评估、风险管理)，是指确定网络资产的安全威胁和脆弱性，并估计可能由此造成的损失或影响的过程。风险分析有两种基本方法：定性分析和定量分析。在制定网络安全策略的时候，要从全局进行考虑，基于风险分析的结果进行决策，建议公司究竟是加大投入，采取更强有力的保护措施，还是容忍一些小的损失而不采取措施。因此，采取科学的风险分析方法对公司的网络进行风险分析是非常关键的。

一旦确定有关的安全需求，下一步应是制定及实施安全策略，以保证把风险控制在可接受的范围之内。安全策略的制定，可以依据相关的国内外标准或行业标准，也可以自己设计。有很多方法可以用于制定安全策略，但是，并不是每一组安全策略都适用于每个信息系统或环境，或是所有类型的企业。安全策略的制定，要针对不同的网络应用、不同的安全环境、不同的安全目标而量身定制，各公司应该按照自己的要求，选择合适的安全体系规划网络的安全。制定自己的安全策略应考虑以下三点内容：①评估风险；②企业与合作伙伴、供应商及服务提供商共同遵守的法律、法令、规章及合约条文；③企业为网络

安全运作所订立的原则、目标及信息处理的规定。

图 4 的安全模型为网络建立了四道防线[4]：安全保护是网络的第一道防线，能够阻止对网络的入侵和危害；安全监测是网络的第二道防线，可以及时发现入侵和破坏；实时响应是网络的第三道防线，当攻击发生时维持网络“打不垮”；恢复是第四道防线，使网络在遭受攻击后能以最快的速度“起死回生”，最大程度上降低安全事件带来的损失。

安全管理贯穿在安全的各个层次实施。实践一再告诉人们，仅有安全技术防范，而无严格的安全管理体系相配套，是难以保障网络系统安全的；必须制定一系列安全管理制度，对安全技术和安全设施进行管理[5]。从全局管理角度来看，要制定全局的安全管理策略；从技术管理角度来看，要实现安全的配置和管理；从人员管理角度来看，要实现统一的用户角色划分策略，制定一系列的管理规范。实现安全管理应遵循以下几个原则：可操作性原则；全局性原则；动态性原则；管理与技术的有机结合；责权分明原则；分权制约原则；安全管理的制度化。

参考文献

[1]Buddhikot M M, Suri S, Waldvogel M. Space Decomposition Technique for Fast Layer-4 Switching[C]//Proceedings of Conference on Protocols for High Speed Networks. 1999: 25-41.

[2]何翔, 薛建国, 汪静. 动态网络安全模型的应用[J]. 计算机工程, 2007.12: Vol.33 No.23, 173- 175.

[3]陈洪波. 如何实现动态网络安全[J]. 信息网络安全, 2001,1(2): 15-20.

[4]姜朋. 信息安全与 IA 计划[J]. 信息网络安全, 2001, 1(4): 43-44.

[5]赵战生. 我国信息安全保障体系结构框架的构想[C]. 上海: 2001 年上海首届信息网络安全高层论坛发言, 2001.