VPN 拓扑中关联控制技术的研究*)

欧阳凯[1] 周敬利[1] 董理君[2]

(武汉科技大学计算机学院 武汉 430081)[1] (华中科技大学计算机学院系统结构系 武汉 430074)[2]

摘 要 网络拓扑的安全性是保障网络服务安全的核心研究内容;尤其在虚拟私有网络(VPN:Virtual Private Network)拓扑中,由于 VPN 的隧道技术、私有路由技术和加密技术,一方面使得内部服务群暴露在 Internet 中,另一方面增加防火墙和入侵检测系统(IDS:Intrusion Detection System)保护内部网络的难度。为此,本文提出以 VPN 网关为中心,协同用户终端、防火墙、IDS 和内部的应用服务,构建的多层安全防护机制---关联控制机制(CCM:Correlative Control Mechanism)。CCM 将终端延伸、IDS 关联和应用引擎三者关联,使得 VPN 防护构成一个关联整体,提高了网络拓扑的安全性。

关键词 虚拟私有网络,关联控制机制,多层安全防护

Research for Correlative Control Technology in the VPN Topology

OUYANG Kai[1] ZHOU Jing-Li[1] DONG Li-Jun[2]

(College of Computer Science & Technology, Wuhan University of Science & Technology, Wuhan 430081)[1]

(Department of System Architecture, College of Computer Science & Technology, Huazhong University of Science & Technology, Wuhan 430074)[2]

Abstract The research of the security of the network topology is the core content for the guarantee for the security of the network services. Especially in the VPN(Virtual Private Network) topology, because of the VPN's tunneling, private routing and cipher technology, there are two embarrassments for the protection of the internal network. One is the internal services could be uncovered in the internet by the VPN's tunneling, the other is firewall and IDS(Intrusion Detection System) could not completely analyze the network packet content because of the VPN's private routing and cipher technology. Hence, we propose CCM(Correlative Control Mechanism) that is a multilayered security protection mechanism based on VPN gateway incorporating client end-point, firewall, IDS and internal services. By the correlation among terminal-extending, IDS-correlation and application-engine, CCM can make the VPN protection into one correlative whole and improve the security of the VPN topology.

Keywords Virtual private network, Correlative control mechanism, Multilayered security protection

1 引言

由于 Internet 已成为主流的低成本通讯构架,大量研究机构和公司利用公用网建立安全可靠的私有网 VPN[1]。通常,VPN 技术采用安全协议(如 IPSec[2]、TLS/SSL:Transport Layer Security /Secure Socket Layer[3])来实现数据的保密性、消息完整性和端点认证。但是,隧道技术使得内部服务群通过 VPN 网关暴露于 Internet 中,恶意人员便能够通过用户正在使用的客户终端(该终端和 VPN 之间建立了一条临时的、加密的通道)来攻击内部服务群;而且,VPN 的加密技术使得 VPN 前端的防火墙/IDS 无法对通信流分析实施有效的控制。因此,VPN 网络结构的安全保障需要通过多层次、深度检测的网络安全部件协同工作。本文通过分析 VPN 结构可能的安全隐患,提出在 VPN 结构中,以 VPN 网关为中心,协同用户终端、防火墙、IDS 和内部的应用服务,构建多层的安全防护机制,称之为关联控制机制(CCM:Correlative Control Mechanism)。

2 关联控制分析

在如图 1 所示的 VPN 拓扑中,VPN 网关是网络拓扑中唯一识别加密数据报文内容和实现私有路由的部件,包含了三类关联方式—终端延伸、IDS 延伸和应用引擎。

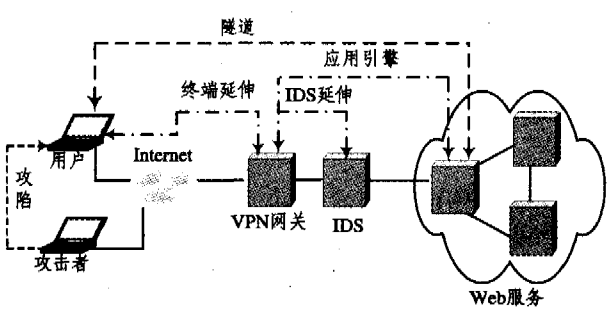

图 1 VPN 拓扑的安全关联

1)终端延伸:VPN 的根本意义在于使得远端用户能够安全地访问内部服务,但是用户终端设备可能被恶意人员利用来攻击 VPN 内部网络。欧阳凯等人曾对 SSL VPN 接入机制的安全性做了研究[4],该文只是对终端用户信任做了研究,并没有对用户终端安全性做探讨。如图 1 所示,假设用户接通 VPN,正在访问内部服务;攻击者通过攻陷用户的终端设备获得通过 VPN 隧道攻击网络内部服务的机会。通过检测

*)国家自然科学基金,编号 60373088。欧阳凯 博士,讲师,研究方向为安全操作系统、网络安全控制技术和网络存储技术;周敬利 教授,博士生导师,研究方向为高性能网络存储技术及安全模型;董理君 博士研究生,研究方向为网络安全结构与控制技术。

用户终端的安全状态，CCM能够获得当前接入用户设备的安全信息，协同CCM的系统策略规则来控制用户的访问能力，如图1中所示的用户设备和模型系统之间的终端延伸点分线。

2)IDS关联延伸：IDS事件分析器通常利用关联技术将可能的攻击报文和一定逻辑特征关联分析，从而发现攻击行为。在VPN结构中，由于VPN隧道、加密技术和私有路由技术的介入，IDS需要和VPN网关协同工作才能有效地进行事件分析，实施攻击控制和防范。如图1中VPN网关与IDS之间的IDS延伸点分线所示，一方面模CCM能够为IDS提供事件关联信息；另一方面IDS为CCM提供攻击信息触发系统策略规则。

3)应用引擎：在VPN结构(特别是应用层VPN技术)中，应用引擎技术是VPN支持复杂应用服务的关键技术。比如：FTP的PORT工作模式，其数据传输通道是从服务器反向连接客户端，如果VPN网关不能识别反向连接，将阻塞服务器连接；因此VPN结构必须能认知应用层协议。CMM通过VPN网关的报文控制和私有路由信息为应用引擎的实现提供了基础；同时，基于对不同应用协议的认知，CCM能够对不同服务做深度检测。如图1中所示的模型系统和Web服务之间的应用引擎点分线，CCM通过解析HTTP协议能对Web进行报文检测。

3 终端关联设计

CCM将用户终端设备安全状态作为VPN安全结构的安全因子进行检测，其根本原因是：VPN结构不仅需要信任用户，而且要信任用户所使用的终端设备。虽然客户使用的终端设备千差万别，但是CCM对终端设备的基本检测包含了3个方面：

1)操作系统类型及其最新的补丁。

2)个人反病毒软件运行状态，最近病毒库时间。

3)个人防火墙软件运行状态。

基于终端安全检测，CCM能够：(1)通过系统安全策略设置VPN结构对终端安全状态的需求；(2)将终端安全状态和VPN接入授权规则关联；(3)对终端安全状态进行安全等级分类，并与VPN内部服务群访问控制关联，进一步细化访问控制粒度。如图2所示的终端检测模型包含了：终端检测库、库同步模块、终端检测模块、策略规则转换模块和实时监控模块。其工作机制描述如下：

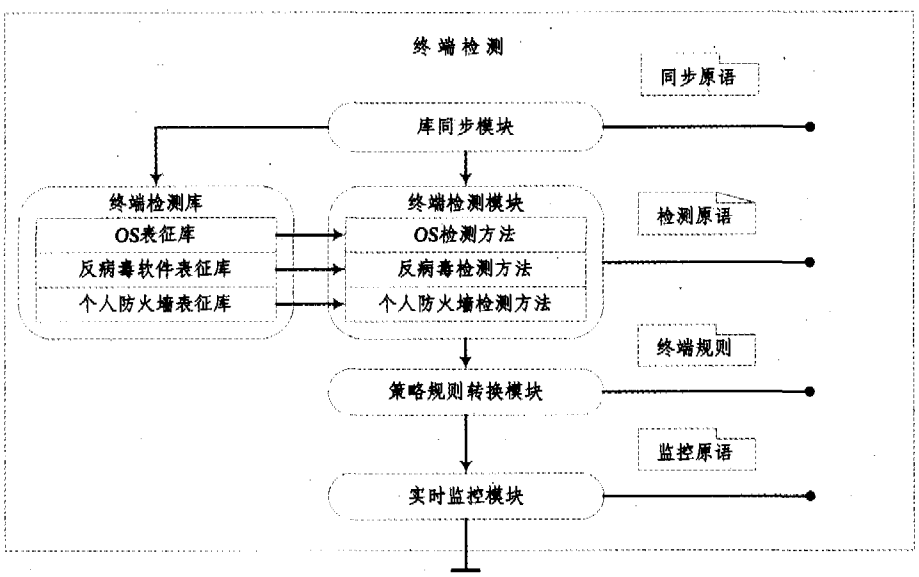

图2 终端检测模型

1)终端检测库——由于OS、反病毒软件和个人防火墙提供商的不同，其表征特点也不相同；CCM只相信具有良好信誉和知名的提供商所提供的产品服务。终端检测库记录了这些知名产品的表征，为终端检测模块提供鉴别素材。

2)库同步模块——随着产品的发展和补丁的发布，用户终端的检测机制不一定具备最新的表征信息，而检测机制能够通过库同步模块从CCM中获取最新的信息。CCM的实现者定义了同步原语用于更新检测机制的终端检测表征库。

3)终端检测模块——检测机制在完成库同步操作后，根据终端检测库的表征库，利用OS检测方法、反病毒检测方法和个人防火墙检测方法对用户终端扫描检测。另一方面，CCM的实现者定义了检测原语用于管理、指示用户终端的检测行为。

4)策略规则转换模块——在VPN结构允许接入的情况下(包含了用户的信任过程和用户终端的信任过程)，CCM将该用户所必须知道的策略规则以终端规则的形式发送给策略规则转换模块，该模块根据本地环境转换为VPN客户端识别的结构，用作检测机制以及该用户会话的各种控制参数。

5)实时监控模块——在整个VPN用户会话过程中，检测机制通过实时监控模块随时监视用户终端的监控状态；一旦发现行为异常，实时监控模块通过监控原语与模型系统通信，并根据预设指令或者CCM的指令做出相应的处理。

4 IDS关联设计

入侵检测系统是信息安全保障的关键技术之一，包括了防护(protect)、检测(detect)、反应(react)和恢复(recovery)4个层面[5]。最早的入侵检测模型是由Denning提出的[6]。该模型主要根据主机系统审计记录数据，生成有关系统的若干轮廓，并检测轮廓的变化差异发现系统的入侵行为。随着入侵行为的种类和范围不断扩大，IDS各功能组件之间以及各IDS之间共享这类攻击信息尤为重要。根据Dillis的IDS关联技术报告[7]，我们可以得知当前IDS的事件关联机制通常

是由如下7种基本关联技术组成：源IP关联(Source IP Correlation)、目的IP关联(Destination IP Correlation)、事件类别/命名关联(Event Class/NameCorrelation)、时间关联(Time Based Correlation)、攻击关联(Vulnerability Correlation)、开放端口关联(Open Port Correlation)和异类关联(Heterogeneous Correlation)。当前的IDS设备都集成了上述关联技术，但是在VPN网络中，有的IDS关联技术会失效(比如：源IP地址关联)，更进一步，VPN技术的部署并不是以孤岛的形式存在，为了保障整个网络拓扑的安全，必须和已有的安全技术(如IDS)整合，形成一个有机的整体，协同工作。如图3所示的CCM与IDS的关联通信，VPN网关和IDS之间通过协商好的通信机制交互信息。

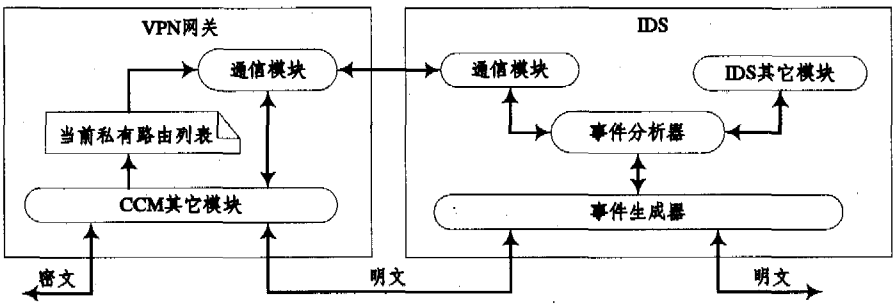

图3 CCM与IDS的关联通信

CCM能够为IDS提供：

1)在VPN结构中，只有经过VPN网关解密后的报文，IDS设备才能分析，目前IDS无法对密文进行解析。因此CCM为IDS设备提供可认知分析的报文。

2)由CCM记录下的经过VPN网关报文的私有路由列表，该列表包含了客户端的真正IP来源，能够利用通信模块告知IDS对应关系，便于IDS的事件分析器分析。

3)由CCM的资源属性记录下的外界可访问的内部资源信息，能够为IDS提供攻击关联、开放端口关联的必要信息。

IDS能够为CCM提供：

1)当IDS发现攻击异常后，利用通信模块通知VPN网关，CCM根据其提供的信息定位VPN用户会话，通过运行请求事件或者触发器终止用户会话。

2)为CCM提供动态设置、变更系统策略规则的依据。当IDS确认攻击后，CCM能够将该攻击关联的IP地址和用户加入黑名单，并提示管理员对其核查。

目前VPN网关与IDS之间关联通信的最大困难在于VPN提供商和IDS提供商各自为政，提供的密闭系统并没有对通信规则形成标准协议。一方面随着IPS(Intrusion Prevention System)结构[8]的提出，该领域的研究表明网络结构的关联技术正在逐步走向标准化；另一方面也可以基于开源IDS项目(比如：snort)研究设计关联通信模块。

5 应用服务关联设计

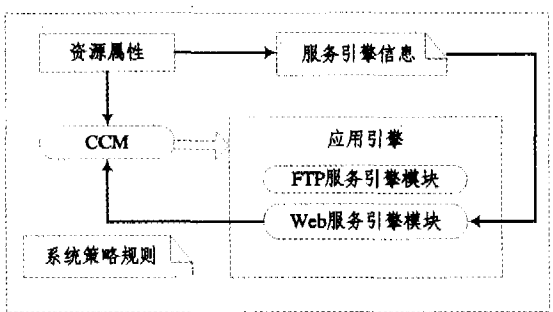

图4 应用引擎的逻辑设计

CCM通过应用引擎提供具体的应用服务管理，应用引擎的逻辑设计如图4所示：(1)从CCM的可扩展性考虑，应用引擎是以独立的二进制模块存在，不同应用服务的引擎模块更改、添加和删除不会影响CCM系统；(2)应用引擎通过系统策略规则向CCM注册；(3)创建、管理内部服务资源时，管理员通过资源属性的服务引擎信息关联具体的引擎模块(比如：Web服务引擎模块)；(4)在一个用户会话中，当该用户触发一个内部服务的数据区间时，CCM调用相应的服务引擎模块来控制数据区间内的报文传输。

由于Web服务是当前应用最为广泛的Internet服务之一，本文根据已知的Web攻击分析，以Web服务引擎为实例阐述应用引擎的设计思路。

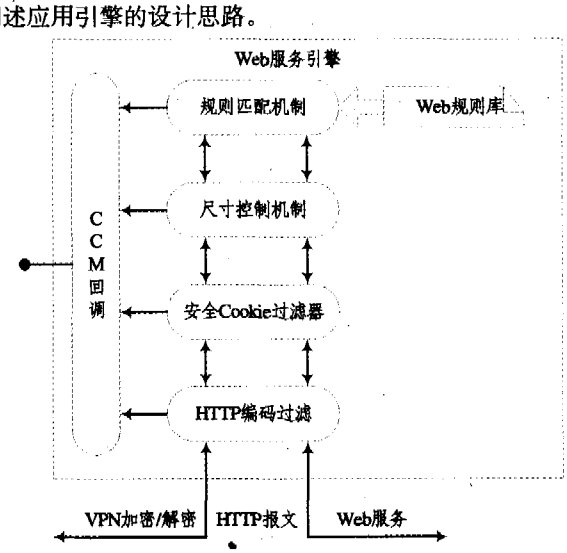

图5 Web服务引擎的逻辑设计

Web服务引擎逻辑设计如图5所示。通过VPN加密/解密技术保证了HTTP报文在Internet上以密文的形式传输；Web服务引擎为HTTP类型的内部服务提供了HTTP编码过滤、安全Cookie过滤器、尺寸控制机制和规则匹配机制四个逻辑功能以实现HTTP的深度检测，从而为VPN内部的Web服务提供安全保障。另外，Web服务引擎还包含了CCM系统的回调机制，用于实现引擎与CCM的耦合(如调用CCM系统的日志功能；在检测HTTP报文时发现异常，则通过回调机制控制该HTTP报文所属的数据区间甚至用户的会话)。

(下转第152页)

据A和B相互支持，说明它们都是真实的，可以用“交集”运算将证据的信度聚焦在它们的交集上；如果证据A和B相互冲突，表明不知道哪一条证据是真实的，那么，就可以用“并集”运算将信度聚焦在它们的并集上，即证据支持A或B中的一个，这种思路更符合人类的直觉。由于在目标识别系统中，最终决策是单元素，因此要用Pignistic概率转换法将多元素命题的BPA再分配给它的各个组合元素。使用本文方法时，证据的融合顺序对融合结果没有影响，因此可以很方便地编程实现。

参考文献

1 Dempster A. Upper and lower probabilities induced by a multivalued mapping. Annals of Mathematical Statistics, 1967,38:325～339

2 Yager R R. On the Dempster-Shafer framework and new combination rule. Information Science, 1987,41:93～137

3 孙全，叶秀清，顾伟康. 一种新的基于证据理论的合成公式. 电子学报，2000,28(8):1～3

4 Campos F, Cavalcante S. An extended approach for Dempster-Shafer theory. IEEE, 2003. 338～344

5 Smets P. The combination of evidence in the transferable belief model. IEEE Trans on Pattern Analysis and Machine Intelligence, 1990,12(5):447～458

6 吴根秀. 冲突证据组合方法. 计算机工程，2005,31(9):151～154

7 Prade D D H. On the combiniation of evidence in various mathematical frameworks. Reliability Data Collection and Analysis, 1992, EAFC: 213～241

8 Ferson S, Kreinovich V. Representation, propagation, and aggregation of uncertainty:[SAND Report]. [in progress],2002

9 向阳，史习智. 证据理论合成规则的一点修正. 上海交通大学学报，1999,33(3):357～360

10 潘巍，王阳生，杨宏戟. Pignistic概率算法设计. 计算机工程，2005,31(4):20～23

(上接第41页)

6 实现与性能测试

本文基于VSB-SSL VPN[9]设计实现了CCM机制。VSB-SSL VPN在实现标准SSL VPN的基础上提出了两项关键性技术：虚拟服务和基于VPN流的访问控制模型。CCM以VPN流的访问控制模型为信息交换中心；通过在虚拟服务中植入终端关联模块，从而能够动态检测客户终端信息实现终端认证；以IDS关联插件的形式在IDS设备实现了IDS关联的通信模块，从而到达与控制模型通信的能力；通过流分析实现应用服务关联。

由于在VBS-SSL VPN中添加了CCM功能，使得隧道建立过程开销有所增加。针对有CCM机制和无CCM机制两种情况，VBS-SSL VPN在不同并发隧道数目下的性能测试如表1和图6所示。

表1 VBS-SSL VPN通道建立平均时间

通道数	VSB-SSL VPN(无CCM)通道建立时间/s	VSB-SSL VPN(有CCM)通道建立时间/s
1	10.03	10.58
5	10.72	10.93
10	11.13	11.22
15	11.36	11.45
20	11.52	11.63
25	11.77	11.82

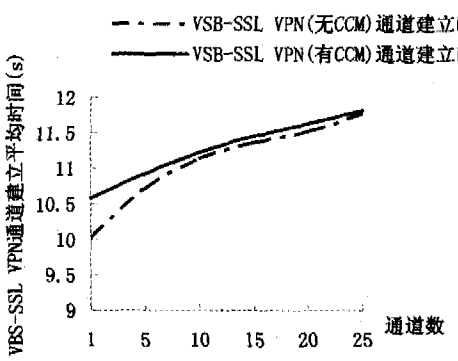

图6 CCM对VBS-SSL VPN性能影响的测试

由于CCM机制的加入，使得VSB-SSL VPN通道建立平均时间比无CCM时稍长，但是通道建立时间增加百分比的平均值$r<3\%$(r如下计算：先求出$d=$(有CCM时隧道建立时间－无CCM时隧道建立时间)/无CCM时隧道建立时间；$r=d$的平均值，即$r=((10.58-10.03)/10.03+(10.93-10.72)/10.72+(11.22-11.13)/11.13+(11.45-11.36)/11.36+(11.63-11.52)/11.52+(11.82-11.77)/11.77)/6))=1.74\%$)。而且随着连接通道数增多，每条隧道建立平均时间越来越接近无CCM时的值。这是因为随着隧道数的增加，CCM机制对隧道建立平均时间的影响越来越小，而SSL握手和加密解密耗时对隧道建立时间的影响占了主要。由此可见，虽然有CCM机制的VBS-SSL VPN系统会导致隧道建立时间稍微增加，但是CCM机制提高和完善了VBS-SSL VPN体系的安全性。

小结 本文针对VPN网络结构特点，从终端安全延伸、IDS关联延伸、应用引擎技术三个方面论述了VPN网络拓扑的关联技术——关联控制机制CCM。通过终端安全延伸将VPN客户终端状态纳入VPN网络安全策略中；通过IDS关联延伸将IDS与CCM系统关联，形成有机控制体；通过应用引擎技术实现上层协议的深度解析；从而实现高安全性的VPN网络结构。

参考文献

1 Cohen R. On the Establishment of an Access VPN in Broadband Access Networks. Communications Magazine, IEEE, February 2003,41(2): 156～163

2 Kent S, Atkinson R. Security Architecture for the Internet Protocol. RFC2401, November 1998

3 Dierks T, Allen C. The TLS Protocol Version 1.0. RFC2246, January 1999

4 欧阳凯，周敬利，夏涛，等. 基于SSL VPN接入机制的研究. 计算机科学，2005,32(5):59～64

5 卿斯汉，蒋建春，马恒太，等. 入侵检测技术综述. 通信学报，2004,25(7):19～28

6 Denning D E. An intrusion-detection model. IEEE Transactions on Software Engineering,1987,13(2):222～232

7 Dillis C D. IDS event correlation with SEC-the simple event correlator:[White paper]. Available at: http://www.giac.org. 2005

8 Zhang Xinyou, Li Chengzhong, Zheng Wenbin. Intrusion Prevention System Design. In: Proceedings of the Fourth International Conference on Computer and Information Technology. September 2004. 386～390

9 欧阳凯，周敬利，夏涛，等. 基于虚拟服务的SSL VPN研究. 小型微型计算机，2006,27(2):229～232