

文章编号:1001-9081(2005)08-1756-04

## 基于移动代理的虚拟专用网安全系统

胡宝芳,王 红,张 霞

(山东师范大学 信息管理学院,山东 济南 250014)

(hbf0509@126.com)

**摘 要:**针对现在网络信息交换中的安全问题,结合虚拟专用网(VPN)和移动代理这两大技术,提出了一种新的 VPN 安全体系结构——VPNAgent 系统,系统中有一个移动代理 VPNClientAgent,作为服务器端防火墙的一个代表作用在客户端,检测数据包并对合法的数据包签名,并护送数据包到防火墙处。防火墙上嵌有一个静态代理 StaticAgent,由 StaticAgent 检测数据包的签名,签名有效的数据包不用解密即可通过防火墙,从而达到提高安全性的目的。

**关键词:**虚拟专用网;移动代理;防火墙;加密;签名

**中图分类号:** TP393.08 **文献标识码:** A

## VPN security system based on mobile Agent

HU Bao-fang, WANG Hong, ZHANG Xia

(School of Information and Management, Shandong Normal University, Jinan Shandong 250014, China)

**Abstract:** Aimed at the security problem in network information exchange, combining Virtual Private Network(VPN) and mobile Agent technologies, a new VPN security architecture named VPNAgent System was presented which works at a virtual private network. The system has a mobile Agent named VPNClientAgent which is an analogy to the customs Agent in real life. It works at the client, inspects the packets, signs the legal ones and guards them to the firewall. There is a static Agent named StaticAgent. The StaticAgent inspects the signature of the packets and the packets with valid signature can go through the firewall without decryption to improve the security of the packets.

**Key words:** VPN(Virtual Private Network); mobile Agent; firewall; encryption; signature

### 0 引言

随着计算机网络的普及,各种企业和机构越来越依赖于计算机来进行管理和运营。与传统的封闭式的企业经营模式不同,现代企业常常表现为相对开放的组织结构,各种机构和人员可能分布在不同的地区,企业之间的合作及企业与客户之间的联系也日趋见密。在这种背景下,一种基于公共网络的、动态的、安全的链接解决方案就成为时代之需,虚拟专用网(Virtual Private Network, VPN)就是这样一种技术。

VPN 是指依靠互联网服务提供商(ISP)和其他网络服务提供商(NSP),在公网中建立的专用的数据通信网络,是通过特殊设计的硬件和软件,直接通过共享的 IP 网所建立的隧道来完成的。通过 VPN 可以实现远程网络之间安全、点对点的连接,它的基本点就是化公为私,使每个企业可以临时使用一部分公共网络的资源,是专用网络的延伸<sup>[1]</sup>。VPN 代表了当今网络发展的最新趋势。与以前租用专用线路方式相比,它以其更低的网络运营成本实现了更加灵活、更加自由的局域网延伸,提供了更为丰富的特性和功能。

VPN 必须具备广泛的安全性和高效性,尽管目前所有的 VPN 解决方案都能提供数据加密、身份验证和访问控制等功能,而且这些解决方案对一般用户已表现出良好的安全特性,但是,对于安全级别要求较高的用户,这些 VPN 方案还存在着安全隐患。VPN 中的加密机制和防火墙检测机制会产生冲突,因为信息通过防火墙时,防火墙为了检查流经信息的内

容,必须把 VPN 加密产生的密文转化成明文。也就是说 VPN 中的加密信息在传输过程中被解密过,这就有被攻击的可能,安全性就大打折扣。本文的目标就是在 VPN 中实现数据包通过防火墙时不必解密,这可以通过用移动代理技术构建的 VPNAgent 系统来实现。

移动代理是一段自主程序,可以在异构网络中按照自己的意愿从一台计算机迁移到另一台计算机<sup>[4]</sup>。也就是说这种程序可以选择何时迁移以及迁移的目的地,它能在任意点悬挂,把自己传送到另一台机器上恢复执行。它具有自主计算、平台无关性以及能够对环境变化做出感知和应变等优点,非常适合 VPN 对动态性和灵活性等方面的要求。

### 1 VPNAgent 系统

假定有两个国家进行贸易交换,A 国从 B 国按一定的进口条令进口货物,为了保证货物符合条令,A 国可以先派遣一个客户代理到 B 国去预先检测货物,如果货物检测合格,就给货物颁发签证,表示这个货物符合输入条令,然后客户代理就带着具有签名的货物返回 A 国。这样,当货物到达 A 国的边境时海关信任该签证,就无需再对货物进行检测。

由此可以考虑在虚拟专用网上构建一个 VPNAgent 系统来实现信息的安全交换。在这个系统中有一个类似于客户代理的移动代理 VPNClientAgent,如果客户端 B 想与在防火墙(边境)后面的服务器 A 交换信息,防火墙要先派遣一个移动代理去客户 B 处检测信息是否合法,如果合法则给其加密,

收稿日期:2005-03-10;修订日期:2005-05-10 基金项目:山东省中青年优秀科学家奖励基金资助项目(03BS009)

作者简介:胡宝芳(1979-),女,山东泰安人,硕士研究生,主要研究方向:移动代理、网络安全;王红(1966-),女,天津人,副教授,博士,主要研究方向:移动计算、网络安全;张霞(1982-),女,山东临清人,硕士研究生,主要研究方向:移动代理、网络安全。

颁发签名,然后再由移动代理护送信息到 A 的防火墙处,防火墙上嵌有一个静态通信代理 StaticAgent,它会验证签名是否有效,如果签名有效,就允许数据包进入内部网络。这一切都是在 VPNAgent 协议定义的规则下进行的。下面将介绍该系统的体系结构及其应用的协议。VPNAgent 系统包括 VPNClientAgent、StaticAgent 和 VPNAgent 协议。

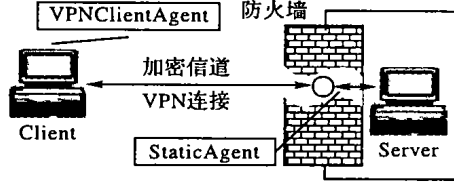


图 1 VPNAgent 系统的体系结构

### 1.1 VPNClientAgent

VPNClientAgent 是一个移动代理,能从防火墙(服务器)迁移到指定的客户处做一定的检测工作,这个代理包含代码和数据(特定检测目的代码和安全策略数据),它是和一个静态通信代理同时工作的。VPNClientAgent 作为防火墙的一个检测代表,是在各客户端进行检测的,它利用防火墙嵌入其上的安全规则进行数据包检测。

VPNClientAgent 是一个特殊场合的用户化的防火墙,它能按客户的需要和当前连接的需要产生,不能用于普遍或不同时间的其他场合。VPNClientAgent 在结构上有三个主要特征:

1) 应用级防火墙代理:每一个要检测的应用程序有特定的检测代码,VPNAgent 协议按每个应用程序所属的不同的 Internet 服务类别(SMTP、FTP、Telnet 服务或 WWW 服务)提供不同的 VPNClientAgent,如客户端进行 FTP 传输时,则派遣一个适合于 FTP 的 VPNClientAgent,来处理这些场合的检测过程,用于安全远程连接等。系统按用户的需要决定派遣哪个 VPNClientAgent。这就减轻了移动代理主机的负担。

2) 工作环境:一般的,由于本地网络是可信任的,要比全球网络安全得多。工作地点影响移动代理的结构。一个工作在本地机器上的 VPNClientAgent 和工作在全球机器上的有不同的结构。

3) 加密模式:加密协议有有效载荷加密和隧道模式两种加密模式。第一种模式加密数据,其他信息以明文方式;第二种是把整个数据包封装成一个新的数据包。VPNClientAgent 需要知道要用哪种模式来封装数据包。

#### 1.1.1 VPNClientAgent 的结构

VPNClientAgent 的任务主要是检测和签名,其结构包括检测单元、加密单元和签名单元。VPNClientAgent 和加密协议一起进行黑箱操作,代理检测信息,用一个默认的加密协议把信息分割成数据包,然后把数据包加密,传入签名单元。

图 2 描述了一个 VPNClientAgent 的工作流程图,数据包依次经过检测、加密和签名过程。下面将讨论 VPNClientAgent 的各个单元:

#### 1.1.2 检测单元

检测单元是防火墙的主要代表部分,它和作用在应用级代理防火墙的检测过程的工作相同。但是,检测单元虽然是防火墙的代表却工作在与防火墙不同的位置,它工作在客户端。

检测单元的结构如图 2 中所示,这个单元的输入是明文格式的信息,适合的安全策略已经嵌入。检测过程有两种结

果:

通过:意味着信息是合法的,签名后就准备交给通信代理。

失败:这种情况下信息会被丢弃,以后的工作需要基于安全策略。

这个单元的函数是:  $I(m) = I\{m\}_{security\_police}$

$I$  是检测函数,  $m$  是明文信息,  $security\_police$  是为合适场合选定的安全策略,检测函数就是在这些安全策略的作用下检测数据包的。

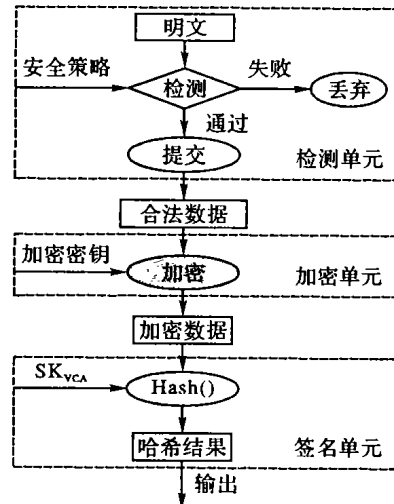


图 2 VPNClientAgent 的工作流程

#### 1.1.3 加密单元

加密和解密过程是和检测过程相独立的过程。加密之后就没有办法区分数据包,为了防止未检测的信息混入到检测过的合法信息中,加密协议必须嵌入到 VPNClientAgent 封装中。因此,VPNClientAgent 按安全策略执行检测后把数据包交给加密协议,加密后再为合法的数据包签名,在目的机解密前要先除去签名。

加密的数学公式是:

$$C = E(p)$$

$$E(p) = E\{p\}_{SK}$$

$C$  是加密后的数据包,  $p$  是明文形式的数据包,  $E$  是加密函数,  $SK$  是加密过程参与者的共享密钥。

#### 1.1.4 签名单元

它的作用是证明签名的数据包是已经经过检测,符合防火墙安全策略。VPNClientAgent 通过签名告诉 StaticAgent 某个数据包是被检测过的,这样通过防火墙时就无需再进行检测,这个过程可以靠一个数字签名方法实现。这个单元需要两个组件:一个签名数据包的算法;一个 VPNClientAgent 和 StaticAgent 的共享密钥( $SK_{VCA}$ )。

StaticAgent 和 VPNClientAgent 共享签名密钥和签名算法。在 VPNAgent 签名中,签名一个数据包的方法是对检测过的数据包用共享密钥执行一个哈希函数,然后把哈希结果和检测的数据包一起封装,然后由 VPNClientAgent 产生的护送 Agent 护送到防火墙处(如图 2 中的签名单元所示)。为了额外的安全,VPNClientAgent 会加密哈希结果产生一个检测数据包的 MAC,并将其放在数据包中。

这个单元的函数是:

$$h = H(p)$$

$$H(p) = hash(p) SK_{VCA}$$

$P$  是加密的数据包,  $H$  是哈希函数,  $SK_{VCA}$  是 VPNClientAgent 和 StaticAgent 的共享密钥。

表 1 描述了最后通过公网的数据包的格式。

表 1 数据包的格式

IP 头	TCP 头	VPN Client Agent 头	加密的包头	数据
------	-------	--------------------	-------	----

加密单元加密过的数据块被层层封装, 依次加上各种包头, VPNClientAgent 包头包括签名值, AgentID、时间戳和其他参变量。IP 包头表明了源和目标 IP 地址, TCP 包头表明了数据包传输信息。在隧道模式中加密协议可能还会加密 TCP 和 IP 信息。

## 1.2 StaticAgent

StaticAgent 是一个静态通信代理, 其职责是在防火墙上只为特定的合法的数据包打开一个通道, 它工作在防火墙上控制通过防火墙的数据包的路由过程。

StaticAgent 的职责大体上可以被归纳为三点:

- 1) 验证绑定到数据包上的通信 VPNClientAgent 的签名;
- 2) 确保 VPNClientAgent 起作用;
- 3) 将合法的数据包路由到目的地。

图 3 描述了 StaticAgent 的工作流程, StaticAgent 包括签名验证单元和路由单元。在签名验证单元中, StaticAgent 先确定过来的数据包有无签名, 然后验证签名是否正确, 如果正确则让其通过防火墙, 再路由到目的主机。

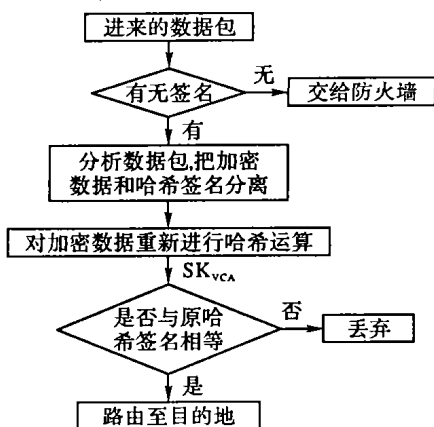


图 3 StaticAgent 工作流程

StaticAgent 和 VPNClientAgent 的签名算法共享密钥, 如果签名有效, StaticAgent 会将数据包的加密部分传到目的服务器, 否则丢弃。

## 1.3 VPNAgent 协议

下面是 VPNAgent 系统中所用到的主要协议:

身份证明与实体认证协议: 一个或多个信息的参与者需要彼此验证身份。系统假定每个参与者都有一个可信任的 CA (Certification Authority, 证书权力机构) 颁发的 X.509 证书, 其中表明用户的信息, 包括他的验证公钥和交换密钥。当然, 也可以用其他的证书。

密钥交换协议: VPNAgent 协议用对称和非对称算法来交换密钥。VPNAgent 协议用一个非对称密钥交换结构来作为验证方法的底层结构和初始化交换密钥来得到公钥。

哈希签名算法: 加密和解密协议作用于 VPN 网络, VPNAgent 会用数字签名算法, 来加密 Agent 的签名。

## 2 应用实例

以某企业的 VPN 网络系统为例来验证本系统的应用。

该企业的网络拓扑结构如图 4 所示, 包括企业内部网络、分公司网络、办事处和移动办公人员。分公司、办事处和移动办公人员与总公司之间实现的是 VPN 连接, 分公司与总公司之间是专线 VPN 连接, 办事处是非对称数字用户环线 (ADSL) 上网, 移动办公人员属拨号 VPN, 分公司、办事处和移动办公人员属于客户。每个客户是可信的, 有可信任的第三方颁发的数字 ID 证书, 不会修改移动代理的代码。客户端要求有一个和本地网络的加密信道, 客户用他的 ID 证书 (如 X.509 证书) 和其他信息如公钥等来向防火墙提交验证, 客户机允许移动代理在其机器上的运行。职员交流的信息通过防火墙传送, 有不同的安全级别。

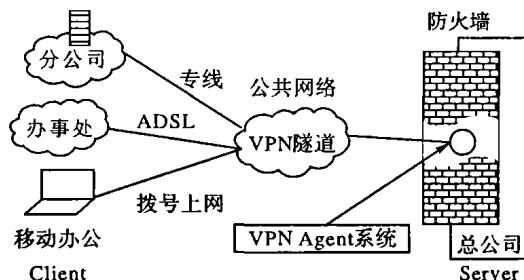


图 4 某企业风格拓扑结构

在企业内部网络的防火墙处安装 VPNAgent 系统, 客户如果与总公司网络建立连接, VPNAgent 系统就会去侦测连接的类型, 并派遣相应的 VPNClientAgent 到客户处, VPNClientAgent 负责检测数据包, 对合法的数据包签名, 并携带着数据包返回到防火墙处, 由防火墙处的 StaticAgent 验证签名的有效性, 最后传输到内部网络。图 5 是客户端与内部网络进行数据传输时的 VPNAgent 系统反馈给用户的界面。当客户端和服务端建立连接时, 信息显示与服务器端连接成功, 防火墙派遣 VPNClientAgent 到客户端, 信息显示收到 Agent, 并在迁移至此的 Agent 栏中显示 Agent 的 ID, 然后消息再显示 VPNClientAgent 的工作进程, 当 VPNClientAgent 产生的护送 Agent 带着数据包返回防火墙后, 信息显示工作结束。

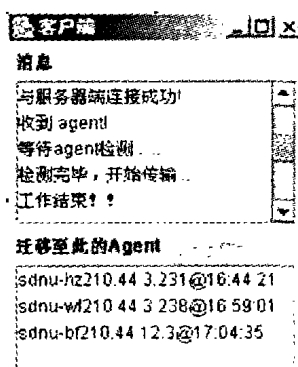


图 5 客户端界面

与现有的 VPN 解决方案相比, VPNAgent 系统具有以下优点:

1) 数据通过防火墙时无需解包, 只要出示其签名即可, 这种技术提高了传输数据的私有性和完整性, 其安全性要比单纯使用 VPN 连接时高得多。以前在对安全级别要求较高的场合, 我们一般是通过租用专用线路来连接, 但是这样的连接方式要支付昂贵的通信费用, 而且缺乏灵活性, 对于企业地理位置的改变不能很好地适应, 而利用本文提出的系统即满足了对安全性的要求, 又节省了开销, 还具有很高的灵活性。

2) 提高了网络通信性能。在以前的网络连接中, 所有数据都要在网络中传输, 只有到达本地网络的防火墙时才进行筛选, 这样不合法数据就进行了无效传输, 而本文提出的系统在数据传输之前就进行了筛选, 这样就消除了不合法数据在网络间的传输, 只有合法的、签了名的数据才能在网络间传输, 这样就减轻了网络通信负担, 提高了网络通信性能。

3) 减轻了防火墙的负担。在以前的网络连接中, 数据包

到达防火墙时才进行解包检测,此时防火墙的负担很重,而本文提出的系统把防火墙处的检测任务分散到各客户机上,数据包在客户机上检测后通过防火墙时仅由 StaticAgent 验证数据包携带的签名是否有效,防火墙无需再对数据包进行检测,仅作为一个通道,从而减轻了防火墙的负担,使得数据到达防火墙时能更快地通过,从而提高了传输效率。

### 3 结语

本文把移动代理技术应用到 VPN 安全机制中,提出了一种更为安全的系统结构—VPN Agent 系统,该系统实现了加密的数据包经过防火墙时不解包,而由护送该数据包的护送 Agent—VPNClientAgent 出示签名以证明该数据包是合法的,使现有的 VPN 解决方案更安全可靠。今后我们将致力于研究把 VPNAgent 系统应用到多个防火墙的网络环境中。

#### 参考文献:

[1] 王达. 虚拟专用网(VPN)精解[M]. 北京:清华大学出版社, 2004.

- [2] 戴宗坤,唐三平. VPN 与网络安全[M]. 北京:电子工业出版社, 2002.
- [3] 北京启明星辰信息技术有限公司. 防火墙原理与实用技术[M]. 北京:电子工业出版社, 2002.
- [4] 张云勇,刘锦德. 移动 Agent 技术[M]. 北京:清华大学出版社, 2003.
- [5] 王红,曾广周,林守勋. 一种高效的移动 Agent 控制机制[J]. 计算机工程和应用, 2002, (2): 250 - 252.
- [6] 周健. 基于移动代理的网络管理框架研究[J]. 计算机应用, 2002, 22(5): 48 - 50.
- [7] 叶盛,高海峰,张根度. VPN 的实现机制和系统评价[J]. 小型微型计算机系统, 2002, 23(9): 1053 - 1058.
- [8] FARINACCI D, LI T, HANKS S. Generic Routing Encapsulation (GRE). RFC 2784[S]. 2000.
- [9] DEERING S, HINDEN R. Internet Protocol, Version 6 (IPv6). RFC 2460[S]. 1998.
- [10] 许勇,张凌,郝志锋,等. 基于 VPN 的企业内联网[J]. 计算机工程与应用, 2001, 23: 33 - 34.

(上接第 1755 页)

3)在分布式环境中可靠的协同工作能力。MTS 中的中继区和网关 Agent 确保了分布式网络管理环境中各部分以及多个分布式系统之间的协同工作,它们提高了通讯的可靠性和可扩展性,也提供了可靠协同工作的通讯基础。同时体系结构对一系列被管元素提供统一的策略,相关的 Agent 根据这个统一的策略来协调完成管理服务。

4)模块级别和应用级别的可重用性。体系结构中 Agent 的产生是基于蓝图库中的蓝图和策略库中的策略,因此可以从现有系统中移植这些 Agent,从而比较容易地构建一个新的系统。基于体系结构中的协同工作能力,现有的网管系统可以成为更大分布式网管系统的一部分,也可以与新构建的其他分布式网管系统进行合作。

总的来说,我们提出的网络管理体系结构全面利用了基于策略的管理技术和基于多 Agent 技术的优点,弥补了各自的不足。使用策略,使该体系结构面向服务,具有系统全局性的视图,使缺乏全局管理视图的 Agent 能够协调完成全局性的任务。同时使用策略也弥补了 Agent 间通讯在安全性方面的部分缺陷。智能 Agent 的引入,使该体系结构更加灵活,更具智能性和扩展性,而且使网络元素实现部分自治管理。

### 4 实现

从实现的角度来说,我们的网管体系结构可以使用 Java 语言来构建。因为 Java 能够运行在不同的硬件和软件系统上,也能够实现易于理解的用户接口,因此 Java 非常适合于实现我们的网管体系结构。各个 Agent 包括移动 Agent 都能比较容易的用 Java 实现。

通讯技术的实现基于 SOAP 和 XML/XSL。为了便于体系结构中的各个 Agent 之间以 SOAP 通讯,我们以 XML 格式封装 ACL 消息,网关 Agent 可以根据相应的 XSL 文件把 XML 格式的消息转换为最终的 ACL(KQML 或者 FIPA)格式的消息。对于移动 Agent 的传输,我们使用 Java 的 RMI 机制来传送移动 Agent。为了减少编程的复杂性,移动 Agent 的迁移方式为弱迁移方式。

我们以此网络管理体系结构为基础,实现了一个网络计费系统,并已经在某城域网中进行测试,此项目起源于文献[1]。通过测试,与传统计费系统相比较,此计费系统在灵活性、扩展性、分布性、自适应能力以及管理的实时性方面,均优越于传统网络管理结构。

### 5 结语

策略驱动的基于多 Agent 系统的网络管理体系结构虽然较之传统网络管理体系结构有许多特点,但是它还存在一些不足:

- 1)策略只能通过管理员人工提炼并输入系统,不能通过智能 Agent 做到这一点。
- 2)面向 Agent 的编程工具还不完善,我们使用面向对象的 Java 语言编程来模拟实现,还不是完全意义上的 Agent 系统。
- 3)为了提高协同工作能力和可重性,我们采用了 SOAP 这样的高层通讯协议,使网络管理系统的资源占用率相对较高。

要解决上述问题,除了需要基于策略的管理技术和智能 Agent 技术的继续发展,还需要对网络管理体系结构做进一步深入的研究,以优化网络管理系统结构,提高网络管理系统的性能。

#### 参考文献:

- [1] 徐治国. 新型 IP 网络管理系统的研究和应用[D]. 浙江:浙江大学计算机系, 2001.
- [2] 卢世凤,刘学敏,刘淘英,等. 基于策略的管理综述[J]. 计算机工程与应用, 2004, 40(9): 85 - 89.
- [3] 王继成. 基于 Agent 网络管理模型的研究[J]. 小型微型计算机系统, 2004, 21(4): 57 - 59.
- [4] 史永林,樊晓桢,高德远,等. MAPBNM: 一种自动化的网络管理模式[J]. 计算机工程与应用, 2003, 39(27): 21 - 23.
- [5] 杨博,杨鲲,刘大有. 面向网络管理的移动主体安全设施[J]. 软件学报, 2003, 14(10): 1761 - 1767.