金融企业网络化服务的安全问题研究①
——流量清洗技术在金融网络中抵御DDOS攻击的研究

河北金融学院 何志强 崔新会 安文广

摘 要:在互联网应用日渐丰富的背景下,金融企业开发了很多基于互联网的业务,很多金融业务在网络化的支持下提升了服务效能的同时也会和其他企业网络一样,面临互联网上的各种安全风险。本文介绍了当前网上金融服务的特点,深入分析了其存在众多安全问题的根源,重点分析了网上金融服务中较难防范的DOS拒绝服务攻击,特别是分布式拒绝服务攻击(DDOS)的特点,提出了将路由牵引结合流量清洗技术应用在金融业务网络中的新思路,并结合互联网金融业务的特点,分析了流量清洗技术在金融业务网络中的应用可行性,并给出了应用方案的体系。

关键词:网上金融服务 拒绝服务攻击 路由牵引 流量清洗
中图分类号:F724.6 文献标识码:A 文章编号:1005-5800(2009)05(b)-154-02

目前,网上金融服务面临着和很多普通互联网服务相同的安全威胁,如信息监听、解密、盗取账号、拒绝服务等。金融企业在发布其基于互联网的产品时,已经在技术、管理等多方面对其服务的安全性做了大量的工作,很多的安全威胁可以在用户和金融企业的共同努力下将其危害程度尽量降低,但拒绝服务攻击(Denial of Service, DoS)在所有攻击形式中是比较特殊的一种,由于这种主动攻击方式往往利用的是正常的数据连接请求,通过消耗被攻击目标的资源达到攻击的目的,因此防范难度非常大。本文中详细介绍了网上金融业务的特点和拒绝服务攻击(DoS)的形式及其对网上金融业务的威胁,分析了几种防范攻击的方法,其中重点分析了流量清洗技术的实施原理及优势,并提出了一种金融网上服务系统中应用流量牵引技术的部署方案。

1 网上金融服务及其特点

网络的出现改变了传统银行的运行模式,发达的电子和通讯技术的应用到金融业务中使得金融企业有能力开发更加多样的金融服务,如电子货币、网上银行以及对电子商务更加方便的支持等等。网络条件下的金融业务活动相比传统的业务具有如下特点:

(1)服务更加直接、快速

由于网络技术的支撑,使得金融服务的地域差异变得微乎其微,信息传递的便利使得用户数据更新更加快速,服务的实时性提高使得金融业务服务质量有了显著提升,大型金融企业的业务可以方便的在全球范围推广。

(2)服务虚拟化

由于业务操作是基于互联网进行,现实的货币已经被排除在外,使得交易成本大大降低,同时这也在很大程度上提升了服务效率。

(3)风险性增大

前述两个特点可以给正常的用户开展业务时带来极大的便利,但这种开放的业务运行模式同样会给潜在的攻击者提供便利的攻击途径。由于金融网络业务相关的服务器需要将服务发布到互联网上,因此该服务相关业务和数据时刻面临着互联网上潜在的安全威胁,如信息监听、拒绝服务、数据篡改等常见的互联网威胁在网上金融业务运转过程中都不可能完全避免。

一旦金融企业的网络服务受到一次成功的攻击,由于其业务的特殊性,攻击造成的不良后果将比一般的网络服务受到攻击的后果严重得多。因此,网络化金融服务面临着不小的运行风险,如何保障网络金融业务的连续性和其数据的完整性也成为目前每个网上金融业务提供企业关心的重要问题。

2 拒绝服务攻击的防范手段

对于DDOS攻击来说,其主动权完全在攻击者手中,何时攻击、如何攻击都是无法预测的,且用于攻击的数据往往都是正常的数据,因此从数据包内容上判断DDOS攻击的可能性微乎其微。为了能够在发生DDOS攻击时网络能够保持运转并提供服务,很多企业往往会采取诸如更大的带宽、运算能力更强的服务器等手段来增强网络和服务器的抗打击能力,但这些技术手段只能在一定程度上减少DDOS攻击的效果,如果黑客发动更大规模的攻击这些手段就很难继续发挥作用了。为了能够从根本上截断DDOS攻击的途径,目前很多企业网络采用流量牵引技术对DDOS攻击数据进行截断和分流。

所谓流量牵引主要指将去往被攻击目标的流量重路由到一个用于攻击缓解的数据处理节点, 以便在该节点处理或丢弃攻击流量,目前主要的实现方法有黑洞路由技术和流量清洗技术两种。

2.1 黑洞路由技术

黑洞路由技术主要是通过宣告BGP最优路由改变原有流量的流向,将流量引入到空接口并丢弃。这样从路由层面看,就在网络中形成了路由"黑洞",吞噬这些异常流量的数据包。这种方法的优点是:

(1)部署实施简单、快速。一旦发现网络中存在异常,仅需改变路由,将异常流量牵引至空接口就可以实现对异常流量的疏导;而当异常流量消失后,可以快速地恢复至原来的正常路由状态。

(2)充分利用路由器的转发功能,效率高。路由器仅需将IP包头的目的地址与路由表进行比照就可以完成转发,对路由节点的性能影响较小。

(3)适合对大规模针对特定IP或IP段的DDOS攻击。

这种方式的缺点是不能对所牵引的数据包进行区别处理,只能全部丢弃。在这种情况下,网络仍然不能正常提供服务,网络业务仍然处于中断状态,这对于金融业务网络来说是无法接受的。

2.2 流量清洗

流量清洗技术是最近几年发展起来的技术,由于其对转发节点有较高的要求,早期的发展较为缓慢,随着计算机计算性能的不断增强,流量清洗技术也逐渐开始在信息安全领域实际应用。

①河北省教育厅课题。课题编号:2008437。

© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

目前，流量清洗主要用于城域网范围的恶意流量进行监控及过滤，在防范DDOS攻击上表现出了较好的性能。

流量清洗也使用了路由牵引，但与黑洞路由不同的是，这种方式将流量重定向到了专用的清洗设备上，利用清洗设备对流量进行“深度报文检测”(DPI)后将合法流量做回注操作。这种方式的优点是：

(1)对数据的检测可深入到应用层甚至应用层协议内部，因此甄别攻击流量和正常流量的准确率高，并在此基础上对攻击流量进行过滤，合法流量被转发到各自的最初目的地，最大程度保证了关键数据流不会中断或丢失。

(2)可按照实际需要，通过宣告特定路由条目，对遭受DDOS攻击的节点进行过滤，而在攻击消失后，又可以恢复原有的路由途径，使设备在过滤异常流量时，做到按需过滤，提高了设备的效率和应用的可扩展性。

(3)过滤系统设备可以旁挂在核心节点路由器上，部署方便，可靠性高，不易发生因过滤设备运行异常而导致的网络中断事故。

流量清洗主要缺点是对过滤设备的性能要求高，同时对攻击的判断准确度要求高，并且可能对旁挂设备造成潜在的性能影响。尤其是在旁挂的清洗设备上开启了多条ACL，而在流量需要进出该设备多次的情况下，对设备性能影响较大。

3 金融网络中流量牵引部署方案的提出

如前所述，流量牵引是在路由技术支持下实现的，因此为了能够在金融网络中实现抵御DDOS，实现数据流量的清洗，需要动态路由设备的支持。除此之外，流量牵引的实现需要智能检测设备和流量清洗设备的支持。考虑到目前互联网上的DDOS攻击几乎全部来自外网，且金融企业内部也已经采取了比较多的安全措施，因此流量牵引技术在银行网络等金融应用中需要重点部署在服务的互联网出口上。建议的网络出口结构如下：

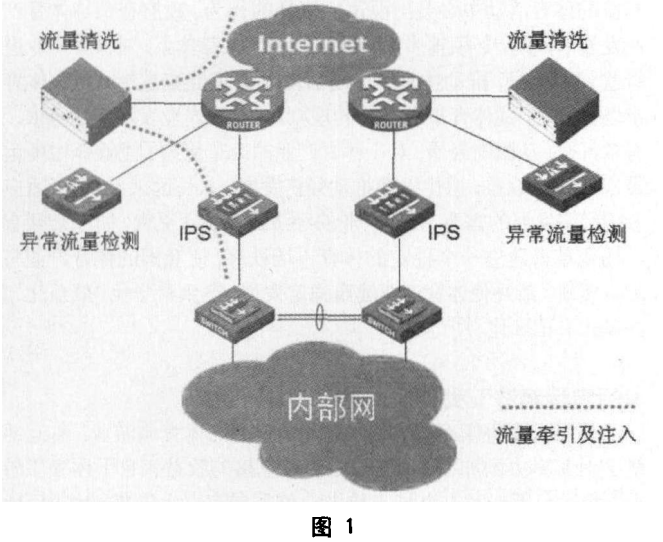

图 1

图中异常流量检测节点负责对DDOS攻击行为进行分析，区分出攻击行为和正常访问行为。当攻击行为被确认之后，监测节点将给清洗设备发出警报，以启动数据清洗工作，当然考虑到智能检测有可能出现漏判的情况，异常检测要保留手动工作功能。流量牵引在技术上可以通过防御设备向相邻的路由器发布BGP路由更新来实现，这样通过路由表的变化就可以将所有的攻击流量转发到流量清洗设备上。

流量清洗节点是流量牵引体系中的关键部分，当流量被牵引到该节点上后，该节点负责区别攻击流量和正常访问流量并根据策略过滤攻击流量，保留正常访问流量，并对正常流量回注以保证正常用户能够持续访问金融业务。典型的流量清洗的过程由五个步骤组成：

(1) 过滤：包括静态和动态的DDoS 过滤器。

(2) 反欺骗：用以验证进入系统的数据包是否包含欺骗信息。

(3) 异常识别：监测所有通过了过滤器和反欺骗模块的流量，并将其与随时间纪录的基准行为相比，搜寻那些非正常的流量，识别恶意数据包的来源。

(4) 协议分析：处理反常事件识别模块发现的可疑数据流，目的是为了识别特定的应用攻击，例如http-error 攻击。

(5) 速率限制：提供了另一个执行选项，防止不正当数据流攻击目标。

流量回注是本体系中的另一个重要环节，这也是流量清洗相对于“路由黑洞”技术的优势所在。在城域网流量牵引操作中，可以采用双链路、策略路由、隧道等较技术来实现。对于金融企业的服务发布网络来说，考虑到效率、性能等因素可以采用策略路由方式。其策略可以采用基于源地址的策略路由并将该策略应用到出口路由器上，该策略的功能可设置为为将来自清洗节点的数据从路由器的内网接口转发出去。这种方法一般情况下，仅仅给出口路由器增加了几条策略，路由器增加的负担并不明显，在效率上和性能上都可以接受。

4 结语

DDOS攻击是互联网上常见且破坏性明显的攻击方式，流量牵引技术和清洗技术的结合与其他技术相比在防范DDOS攻击方面具有明显的优势，特别是对于网络化的金融业务来说，流量清洗技术在过滤DDOS攻击的同时可以保持业务的持续畅通，这对于金融企业提升业务质量具有直接的现实意义，金融业务在该技术的支持下将会给用户提供更加高效、便捷、畅通的服务，在给用户提供更好服务的同时也会极大地提升企业的形象。

参考文献

[1] 清源计算机工作室.DOS 攻击基础 [M]. 科学出版社,2005:64~71.
[2] 吉根林 . 对 DDOS 防御 [M]. 科学出版社,2005:87~152.
[3] 向宏 . 信息安全管理 [M]. 机械工业出版社,2004:142~176.

© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net