网络安全系统在税务行业的实施和应用

The Deployment and Application of Network Security System In the Taxation Administration Area

丁 勇　汤晓霞　（浙江大学 浙江杭州 310027）

摘要：介绍了基于当今先进网络安全技术而构建的互联网接入网络安全系统在税务行业的实施和应用，阐述了SSL，IPSec VPN，防火墙，VRRP，NSRP 等网络安全技术。该系统上线后，网上报税、全程服务等互联网涉税业务运行稳定、畅通、快捷，取得了良好的社会和经济效益。

关键词：网络安全 防火墙 负载均衡 SSL VPN 入侵检测

1 引言

随着税收征管改革的深入进行，网上涉税业务已成为税务行业开展税收业务工作的主要工具，税收征管信息系统的安全问题，特别是网络安全问题已成为税务局重点考虑和亟待解决的问题。经过慎重地分析、研究、部署和实施，在税务系统内已成功建设完成了一个具有国内先进水平的互联网接入网络安全系统。

专家评审会通过对该系统认真论证后，一致认为：该系统起点高、设计合理、技术先进、实用性强；安全防范机制设计严密，能够保障税务信息系统安全可靠运行；系统在纳税户的规模设计上具有前瞻性，以 10 万纳税户的规模为标准选择设备档次和链路带宽，在今后若干年内可满足业务流量的需求。

2 系统描述

互联网接入网络安全系统在体系结构上充分考虑了设备和链路的冗余性，同时采用负载均衡技术，确保在意外故障和重负载情况下系统可靠稳定地运行。

该系统通过两条百兆光纤接入 Internet，选用了电信级的链路负载均衡器，合理分配两条链路的数据流量，并保证链路的互为冗余。系统采用了具有 25 万个并发会话连接数、1 万个虚拟专网（VPN）安全隧道建立数、支持多种加密算法的千兆级硬件防火墙，确保在业务高峰期间系统的快速响应。安全系统向网上报税的纳税人提供 SSL 数据加密方式，对重点纳税户提供 IPSec VPN 和 SSL 技术相结合的双重加密机制，进一步确保企业端和税务端的安全。

为了更好地防范黑客入侵，安全系统在使用防火墙作内外网隔离保护的同时，还部署了入侵检测系统、安全审计系统、以及在链路负载均衡器上配置了 SynApp 安全模块，自动监控、检查非正常请求，记录可疑事件并及时报警，记录访问日志，使网络在受到危害之前，能主动截取并防范非法入侵，最大限度地降低安全风险。

为增强系统的可靠性，安全系统所有核心安全设备均采用双机备份冗余结构，运用 VRRP 和 NSRP 冗余协议，互备的两台设备中任何一台设备出现问题，都能在合理的时间内自动切换至备份设备，从而保证了网络的 7×24 小时不间断服务，最大程度上避免了单点故障造成的危害。

2.1 系统拓扑结构

网络安全系统在逻辑上共分为 5 层：链路负载均衡层，防火墙负载均衡层，服务器负载均衡层，SSL 高速加解密层和内部应用服务器层（包括入侵检测系统和安全审计系统）。拓扑结构中共有三层采用了负载均衡技术，与当前其它网络安全系统的单一结构相比具有先进性和更高的稳定性、可靠性。

2.2 用户访问数据流程

Internet 用户访问涉税网上业务的整个数据流程如下：

（1）Internet 用户发起 https/http/VPN 请求访问各

项涉税网上业务，通过运营商提供的两条不同链路（记为 L1 和 L2）到达 Active LinkProof；

（2）LinkProof 选择最佳链路（假设选择链路 L1）；

（3）用户访问请求通过 L1 到达 Active LinkProof；

（4）LinkProof 选择最佳防火墙，并将流量定向到该防火墙，防火墙做安全处理。若用户采用 VPN 方式，则防火墙对 VPN 数据解密拆包，得到 HTTPS 数据（如果用户访问基于 HTTP 协议，跳至第 7 步）；

（5）HTTPS 请求到达 WSD，WSD 根据负载均衡原则，选择其中一台 CT100，将请求转发至该 CT100，由 CT100 完成与客户的 SSL 协议需要交换的内容，如证书、密钥等；

（6）CT100 将解密的 HTTP 请求数据转发至 WSD；

（7）WSD 根据一定的安全检查策略和负载均衡策略将 HTTP 请求数据转发至相应的服务器；

（8）服务器将 HTTP 响应数据转发回 WSD，（如果用户访问基于 HTTP 协议，跳至第 11 步）；

（9）WSD 将 HTTP 响应数据转发回 CT100；

（10）CT100 对 HTTP 响应数据进行加密后形成 HTTPS 数据，并转发回 WSD；

（11）WSD 将数据传送至防火墙；

（12）防火墙将数据传送至 LinkProof 主设备；

（13）数据经过 L1 返回至用户。

注：图中运营商提供的两条链路的网段分别标记为 A. B. C. 0 和 A. B. D. 0。LinkProof、WSD、CT100 依次分别为链路负载均衡器、服务器负载均衡器和 SSL 高速加解密设备。

3　系统功能及实现

3.1　链路负载均衡

运营商提供两条 Internet 接入链路，分别从城区骨干的两个不同 POP 点接入。由 POP 点直接引四路光纤到税务局机房，每路光纤均为 100M 的带宽。采用双链路接入，可以保证链路上的冗余，即使在一条链路出现故障，甚至一个 POP 点出现故障的情况下，仍保证有一条通路到达安全系统。

两台 LinkProof 链路负载均衡器互为主备，对 Internet 接入链路提供智能化的流量管理，实现 Internet 流量的双向负载均衡。同时通过启用 VIP（Virtual IP）功能，实现了内部两台 NetScreen 防火墙的负载均衡。

LinkProof 的"优化内容路由"技术能够确保通过最佳链路传递特定内容，在决定哪条链路能够为特定内容提供最佳性能时，会综合考虑与请求内容的网络就近性、链路的实时负载与链路的成本。因此，最终用户将充分享受到经过优化的服务和极快的响应时间。

LinkProof 连续监视每个 Internet 连接的状态。它通过定时检测网络内部和外部节点的状态来检查每个路由器接入 Internet 的路径。LinkProof 还自动检测各种故障，如链路、路由器、DNS 服务器和其它故障。通过检查可以确保只使用那些高效运转的接入链路。两台 LinkProof 设备冗余配置，保证即使主用设备发生故障的情况下也可以保证不中断的 Internet 链路流量管理。

3.2　SYNAPP 安全防范

为了加强系统安全性，在最外层链路负载均衡器设备上附加了 SYNAPPS 模块。该应用安全模块可以防范 1300 多种常见攻击和病毒，如拒绝服务（DOS）攻击、分布式拒绝服务（DDOS）攻击、缓冲区溢出/超限、利用已知的 bugs、利用错误配置和默认的安装问题来进行攻击、攻击前探测网络流量、未授权的网络流量和后门/特洛伊木马、端口扫描等。对流量进行双向监控——监控从外界进入的或者从内部往外发出的流量中的攻击信息，阻止攻击，补充了防火墙针对应用方面安全防范的弱点，有效保障了进出通道上的安全，从而更全面地保证网络系统的安全。

3.3　防火墙安全防范

该系统使用了两台高性能、高可靠、高速的防火墙设备 NetScreen 500 ES。NetScreen 防火墙运用了动态封包过滤（状态检测）技术，保护所有连接尝试的安全。对于从一个区段向另一区段（该防火墙设置了 Untrust 和 Trust 两个区段）传递的任何信息流，都必须有允许它的策略。当封包尝试从一个区段向另一区段传递时 NetScreen 设备会检查其策略组列表中是否有允许这种信息流的策略。缺省情况下，NetScreen 防火墙拒绝所有方向的所有信息流。该系统通过创建相应策略，定义允许通过或禁止通过的指定源地点到达指定目的地点以及指定端口的信息流种类。

为了保护区段的安全，避免来自其它区段的攻击，对防火墙的每个区段启用了防御机制（即 Screen 安全设置）来检测并拦截如 SYN Attack（SYN 攻击）、ICMP

Flood(ICMP 泛滥)、UDP Flood (UDP 泛滥)和 Port Scan Attack(端口扫描攻击)等常见的网络攻击。

3.4 服务器负载均衡

内部应用服务器前端架设的两台 WSD(服务器负载均衡器)对税务局内部网络中提供相同应用的服务器进行负载均衡。此外 WSD 还具有如下功能:

(1) 具备无限的扩充能力,可随时增加内部服务器数量;

(2) 增加新的服务器到服务器群时,WSD 会逐渐引导流量至新的服务器,直至服务器的状态完全稳定;

(3) 独特的监测技术能完整检测网络的健康状况,包括 IP、TCP、UDP、Application 及 Content;

(4) 当发生错误时,WSD 及时将使用者流量导向至正常运作的服务器;同时监测服务器群及其后的设备与资料库,以确保整个资料通道均正常;

(5) 两台 WSD 间能同时相互备份,形成完整的容错机制,使用者能享受永不停顿的网络服务;

(6) WSD 对外仅提供虚拟地址(VIP)用于用户访问,因此用户端无法得知实际服务器的地址,从而有效保护后台主机。

目前,该系统的 WSD 内部已连接的应用服务包括网站服务、网上报税服务、网上查询、网上投诉、全程服务、邮件服务等十几项;系统运用了 WSD 的负载均衡算法,对两台网上报税服务器及两台 SSL 加解密设备分别按所设置的比例值均衡分配流量,实现了集群功能。

3.5 SSL 高速加解密

网络安全系统采用两台 SSL 高速加解密设备 CT100,在不降低网络性能的情况下为用户提供快速的 SSL 应用,对网上报税的业务数据和企业信息进行加解密服务,确保信息快速安全地传输;在动态增强网络性能的同时,确保了高效、连续和安全地完成报税业务。

CT100 通过减轻网络 web 服务器执行时 CPU 的负载与运用 SSL 加密和解密计算技术,实现了纳税人在进行安全报税的同时获得高质量、快速和高效的服务。

同时,CT100 具有独特的缓存功能,它可以直接从缓存中提供常用的页,而不是返回到服务器中查找这些页,从而进一步增强了网络和服务器的性能和效率。

采用 SSL 方式报税时企业端的操作流程:

(1) 打开税务局网站,点击"电子申报"图标,该图标的链接地址为:

"https://www.＊＊＊.＊＊＊.cn/wssb/wssb/web.html";

(2) 跳出"安全警报"窗口,点击"确定";

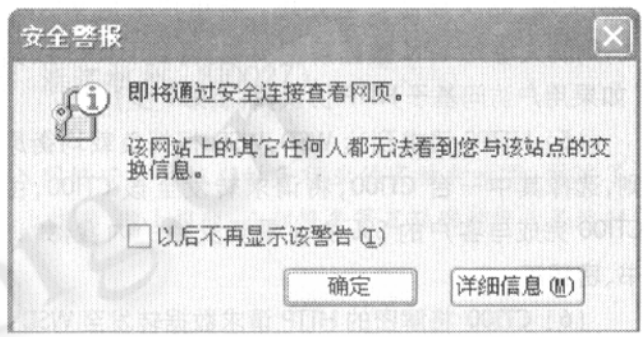

图 1　安全报警提示 1

(3) 弹出关于证书"安全警报"窗口,提示"是否继续",点击"是";

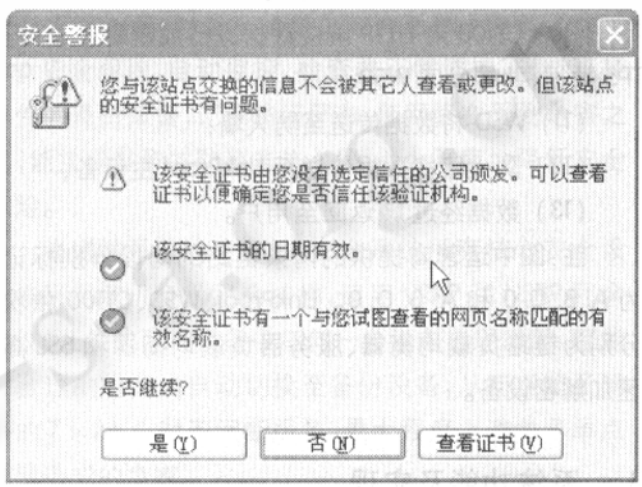

图 2　安全报警提示 2

(4) 进入"网上报税"网页,同时在页面右下角出现一个带锁的证书标记(如图 3);

(5) 自此,用户已可通过 SSL 加解密方式进行网上报税业务。

3.6 双机备份冗余结构

(1) 虚拟路由冗余协议(VRRP)。网络安全系统中 Link-Proof 和 WSD 通过应用虚拟路由冗余协议(Virtual Router Redundancy Protocol,简称 VRRP)实现设备间的冗余容错备份,避免系统的单点故障;通过对时间选项

的设置，保证主/备切换时间在 2 – 5 秒之内。同时主/备之间可进行会话表的复制，保证用户的会话不会出现过多的中断。

图 3　网上报税首页

VRRP 协议通过对共享多存取访问介质（如以太网）上终端 IP 设备的默认网关（Default Gateway）进行冗余备份，从而在其中一台路由设备宕机时，备份路由设备及时接管转发工作，向用户提供透明的切换，提高了网络服务质量。

（2）NetScreen 冗余协议（NSRP）。NetScreen 冗余协议（NSRP）是一种在 NetScreen 设备上支持的、可提供高可用性（HA）服务的专有协议。

NSRP 的基本原则是没有单一故障点。NetScreen 设备具有专用的物理冗余 HA 接口（HA1 和 HA2）或可以将两个通用接口绑定到 HA 区段，以提供 HA 接口冗余。同时可以创建冗余安全区段接口。

两台防火墙之间传递的 NSRP 信息都是通过两个 HA 接口传递的。为更好地分配超出带宽的带宽，HA1 处理 NSRP 控制消息而 HA2 处理网络数据消息。如果任一个端口在有 HA1 和 HA2 接口的 NetScreen 设备上发生故障，另一个活动端口会同时承担这两种信息流。

安全系统中通过使用 NSRP 创建两个虚拟安全设备（VSD）组，每个组都具有自己的虚拟安全接口（VSI），实现了将两台防火墙都配置为主动。即 NetScreen_A 充当 VSD 组 1 的主设备，并充当 VSD 组 2 的备份设备；NetScreen_B 充当 VSD 组 2 的主设备，并充当 VSD 组 1 的备份设备，形成双主动模式（即 Active – Active 模式）。由于设备冗余，因此不存在单一故障点。

3.7　入侵检测（IDS）

该系统选用了美国安氏公司的具有先进的三层分布式体系结构的领信入侵检测系统。入侵检测系统由网络传感器、事件收集器和控制台三部分组成，在网络和主机层面，将基于攻击特征分析和协议分析的入侵检测技术完美结合，监控分析网络传输和系统事件，自动检测和响应可疑行为，使用户在系统受到危害之前截断并防范非法入侵和内部网络误用，最大程度降低安全风险，保护税务网络系统安全。

该入侵检测系统具有业界最全面的入侵检测特征库，能识别预探测攻击、拒绝服务攻击、针对各种服务的攻击（如 DNS、FTP、SMTP、HTTP 等）、各种后门攻击、针对 Windows 和 Unix 的网络攻击、未授权访问企图等攻击类型。

该系统使用一台硬件网络传感器，监听所有流经服务器前端交换机的网络流量；事件收集器依据所设置的安全策略，实时地检测、报告可疑攻击并记录该事件。

4　结论

该互联网接入网络安全系统上线后，取得了良好的社会和经济效益。网上报税、网上认证、网站服务、邮件服务、全程服务、效能投诉等互联网涉税业务运行稳定、畅通、快捷；系统中所有设备都主备冗余，避免了单点故障；前端采用严密的安全防范措施，内部服务器未受到任何外来黑客的侵入；采用 SSL 加密方式传输网上报税数据，在不增加企业端负担的前提下，使企业端的安全性大为提高，同时使用方便，至今未发现报税数据被截取的攻击事件，保证了企业报税数据准确、及时地上报至税务端服务器，提高了税务局的形象和对外纳税服务的效率。

参考文献

1　Andrew S. Tanenbaum . 计算机网络（第三版）[M]，北京：清华大学出版社，1998.
2　William Stallings. SSL：Foundation for Web Security [M].
3　谢希仁. 计算机网络（第二版）[M]，大连：大连理工大学出版社，1996：261 – 299.
4　宗坤、唐三平，VPN 与网络安全[M]，北京：电子工业出版社，2002：120 – 201.