粟毅, 安小伟, 李振, 等. 门户网站 DDoS 模拟攻击及安全防护 [J]. 华北地震科学, 2020, 38(4): 28-33. doi:10.3969/j.issn.1003−1375.2020.04.005.
SU Yi, AN Xiaowei, LI Zhen, et al. Portal Web DDoS Simulated Attacks and Safety Protection[J]. North China Earthqauke Sciences, 2020, 38(4): 28-33. doi:10.3969/j.issn.1003−1375.2020.04.005.

门户网站 DDoS 模拟攻击及安全防护

粟 毅, 安小伟, 李 振, 吕 帅, 刘鹏飞

(云南省地震局, 昆明 650224)

摘要: 针对云南省地震局互联网门户网站系统进行分布式拒绝服务(DDoS)模拟攻击, 通过单台短时间内发送大量 SYN Flood 包分别检测网络与服务运行情况, 从交换机端口镜像获取数据包分析攻击特性, 从而检测网络流量数据安全防护能力; 结合安全软件、硬件资源针对门户网站系统安全提出防护措施建议, 对网络中存在的信息安全漏洞进行修复, 提高网络信息安全。

关键词: DDoS 攻击; 模拟攻击; 安全防护

中图分类号: P315-392 **文献标志码**: A **文章编号**: 1003−1375(2020)04−0028−06

doi:10.3969/j.issn.1003−1375.2020.04.005

0 引言

分布式拒绝服务 (distributed denial-of-service, DDoS) 攻击已成为网络安全的最大威胁之一, 是一种较难检测和实施的攻击方法[1]。通过在发生 DDoS 攻击时, 通知互联网服务提供商 (ISP) 将已发现的攻击元组流量在网络中短暂丢弃的方式, 可以在保证 DDoS 防御的前提下, 显著减少防御能力部署。仿真实验表明, 对已知的攻击元组流量丢弃合理的时长, 即可在仅检测 0.55% 攻击流量的前提下阻止 99. 9% 的攻击流量[2]。根据其周期性发送大量攻击流量的特性, 从对业务主机进行分布式拒绝服务 (DDoS) 攻击中, 深入剖析 DDoS 攻击概念和原理[3]。同时, 根据 DDoS 攻击与主机攻防实测, 采用模拟网络的方法对门户网站系统进行攻击模拟, 总结出业务系统主机安全的有效防护措施。

1 互联网业务系统

云南省地震局网络分为互联网和行业网, 两网进行了物理隔离, 互联网信道部署了若干对外提供的应用服务, 包括门户网站和 SSLVPN 服务、行业服务等。门户网站系统依托于网络信道支撑服务, 现有安全设备有 WEB 防火墙、入侵检测系统、网页防篡改系统、政府网站综合防护系统, 门户网站采用反向代理负载均衡模式部署。信息安全防护不能单独针对某业务系统及服务器做安全措施, 应全面分析网络中的传输数据、承载的各种业务应用及服务器操作系统等, 从网络层到应用层进行全面的信息安全防护。

2 DDoS 攻击与模拟与分析

在突飞猛进的信息化时代, 信息安全已然成为了目前面临的严峻问题[4]。常见的网络攻击如: 缓冲溢出攻击、蠕虫、木马、SQL 注入、网页篡改、DoS/DDoS、跨站脚本攻击等。其中, DDoS 攻击以成本低廉、攻击性强、检测困难等特点成为黑客常用的攻击手段之一, 本文主要以 DDoS 的攻击特性来进行模拟攻击。

2.1 DDoS 攻击类型

DDoS 分布式拒绝服务攻击根据攻击原理和方式的区别, 可以分为 4 个阶段, 即基于网络层攻击、传输层攻击、会话层攻击和较为常见的基于应用层的攻击。这 4 类攻击方式各有特点, 对网络安全造成了极大的危害。对于应用层 DDoS 攻击来说, 最常见的是基于 Web 服务器的攻击。

网络层攻击, 网络层攻击方式比较有代表性的是 UDP 反射攻击, 如 NTP Flood 攻击, 这类攻击特

收稿日期: 2020-04-28
第一作者简介: 粟毅(1981—), 男, 云南昭通人, 工程师, 主要从事网络管理、信息服务、数据共享、网络安全工作.
E-mail: suyiwy@163.com

性是利用大流量、短时间堵塞被攻击者的网络带宽, 导致用户的业务无法正常响应访问。

传输层攻击, 传输层攻击是使用较多的攻击类型, 攻击包括连接数攻击、SYN Flood 攻击等, 这类攻击通过占用服务器的连接池资源从而达到拒绝服务的目的。

会话层攻击, 比较典型的攻击类型是 SSL 连接攻击, 这类攻击占用服务器的 SSL 会话资源从而达到拒绝服务的目的。

应用层攻击, 比较典型的攻击类型包括 DNS flood 攻击、HTTP flood 攻击、游戏假人攻击等, 这类攻击占用服务器的应用处理资源、极大地消耗服务器处理性能, 从而达到拒绝服务的目的。

2.2　模拟 DDoS 网络攻击

以 SYN flood 攻击工具(图 1)来进行模拟攻击。SYN flood 攻击是目前网络攻击中比较常见的方式, 主要是利用 TCP 协议通信上的一个缺陷, 通过 TCP3 次握手的原理, 向服务所在的端口发送大量的伪造源地址的攻击报文, 造成目标服务器中的半开连接队列被占满, 网络造成堵塞, 从而阻止其他合法用户进行访问。

图 1　模拟用 SYN flood 工具

2.2.1　门户网站运行监控

模拟攻击开始时监控门户网站运行状况, 发送报文攻击进行至 20 min 时网站访问变慢, 同时查看网站并发连接数升至 10 000 后打开页面成功率下降为 16%(图 2), SSH 连接服务器出现延时; 进行至 35 min 时网站无法正常访问, 页面停留在加载状态(图 3), SSH 连接服务器失败, 此时大量的伪造源地址的攻击报文对网站服务运行造成了很大影响, 服务资源基本耗尽。

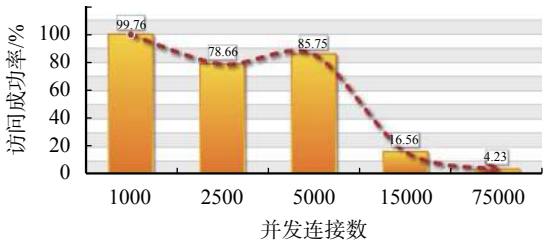

图 2　访问成功率

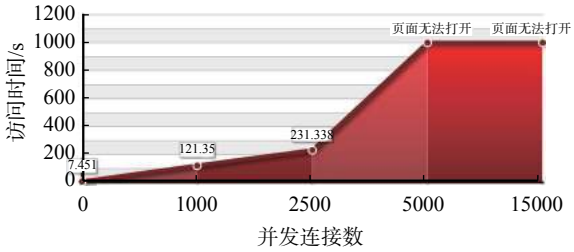

图 3　响应时间

2.2.2　网络运行监控

从网络防火墙上监控攻击过程中的网络资源占用量, 1 h 内连接并发数达到 23 万以上(图 4), CPU 占用率达到 90% 以上(图 5), 此时网络带宽已被大量连接占满, 同时防火墙资源占用量巨大, 设备高负荷运行, 网络运行处于瘫痪状态。

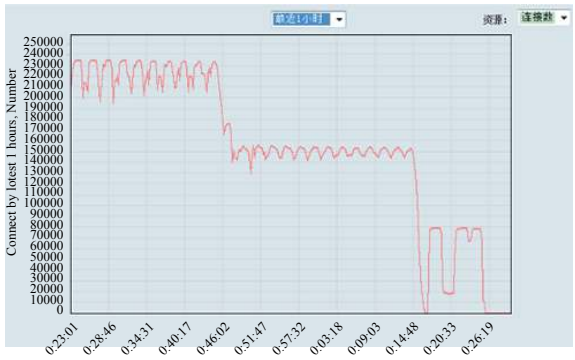

图 4　连接数变化情况

图 5　CPU 占用率

2.2.3 攻击行为分析

此时，我们利用 Ethereal 抓包工具获取网络信道中的数据包进行分析，从抓取的包中总结出以下几点报文特征。

1）报文量很大。分析报文可知，源地址 1 s 内模拟攻击服务器向目的地址门户网站发送了将近 10 000 次 SYN TCP 请求（图 6），在分析中发现没有 3 次握手信息，无正常的 TCP 连接，只有源地址不断地发出连接请求。

2）报文填充 Payload。正常 SYN 请求大小为 64 字节，并无 Payload（载荷），而抓到的数据中，报文均为 902 字节，并且每个包带有 payload（图 7），该 SYN 报文均为软件伪造报文，以 10 000 次/s 对门户网站服务器发出 SYN 请求。

3）无 ACK 回应。TCP 协议通讯之前会经过 3 次握手，请求方发出一个 SYN 信号来请求对方连接，对方收到请求并接受的时候就会发出 ACK 消息，在此次报文分析中无 ACK 回应。

4）占用大量端口。从报文分析可知，每个报文都占用不同的端口快速发送请求（图 8）。

根据上述抓包后的报文分析，可以得出攻击行为符合 SYN flood 攻击的特征，确定此次攻击的方式，DDoS 模拟攻击到此结束。

3 网络安全防护

在整个网络模拟攻击中，现有安全设备没有做详细的安全策略，网站服务器完全暴露在互联网络中，端口也没有做限制，这样极易发生网络攻击事件[5]。在整个网络安全中，安全设备的使用有着至关重要的作用，以硬件设备结合软件分析，能加大信息安全系数。

云南省地震局互联网信道安全防护措施现由安全设备、运营商服务、省公安厅联动等构成（图 9）。其中，硬件防护措施 3 套，包括下一代防火墙、WEB

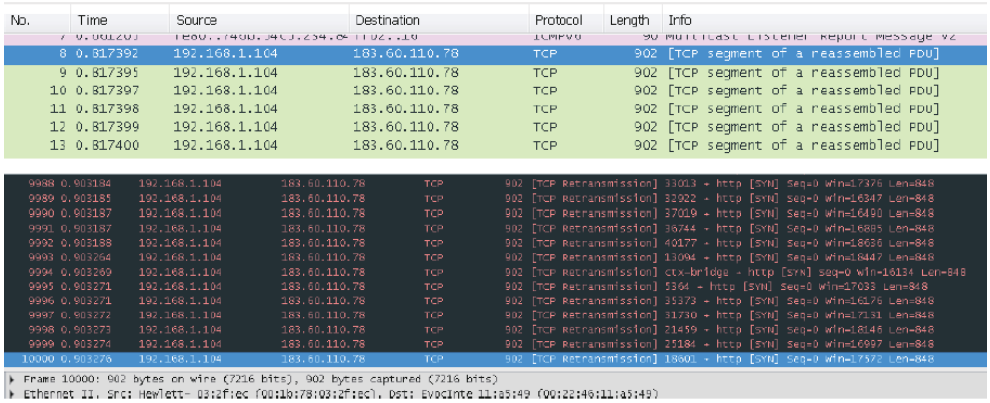

图 6 SYN TCP 请求

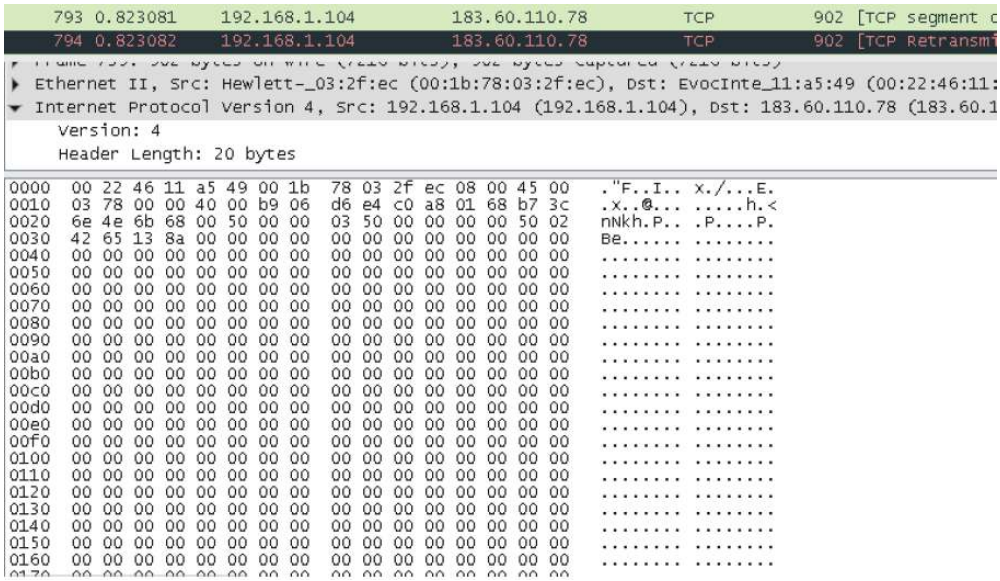

图 7 报文填充 payload

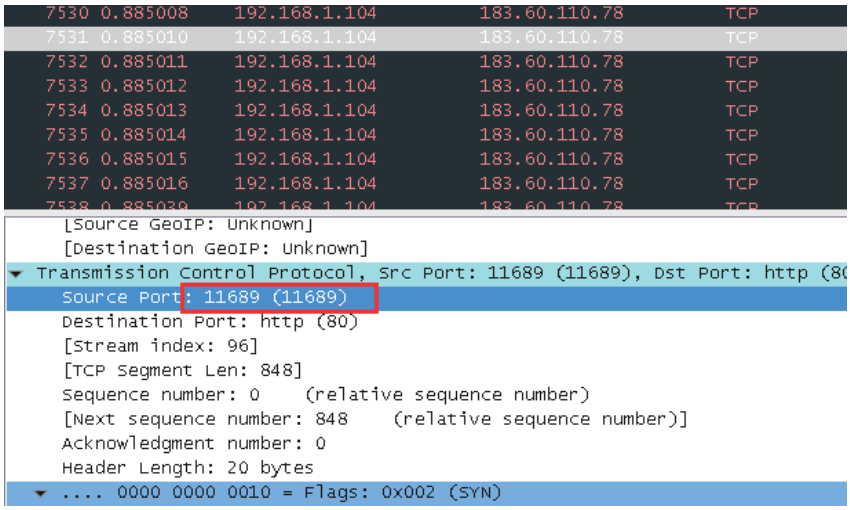

图 8　不同端口发送请求

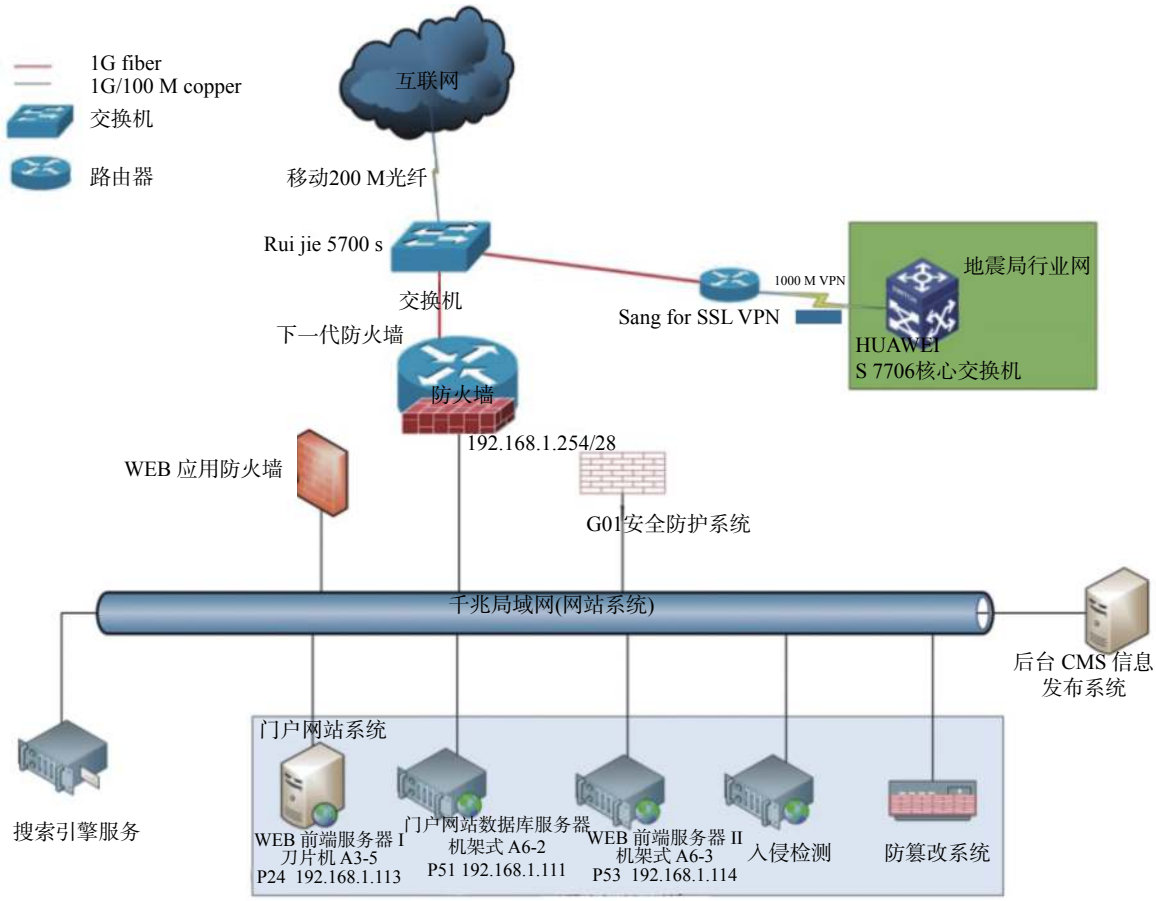

图 9　网络安全设备拓扑图

防火墙、防入侵检测系统(IDS), 互联网信道运营商提供链路级抗 DDoS 防护; 软件防护措施 2 套, 包括网页防篡改系统和省公安厅提供的政府网站综合防护系统(G01)。通过现有安全设备与社会安全防护力量相结合, 配置安全设备策略、联动各项防护措施、优化门户网站部署等方式, 最终提升互联网信道的安全防护能力。

3.1　防火墙安全策略

防火墙系统在网络中主要是过滤部分攻击, 关闭不使用的端口, 禁止特定端口的流出通信, 在防火墙安全策略中启用入口和出口抗攻击选项, 启用蠕虫过滤选项, 启用 IDS 的联动模块, 将防火墙和防入侵检测系统进行联动; 在安全规则中配置非 80 端口的访问限制, 配置服务器主机保护, 禁止 30 s

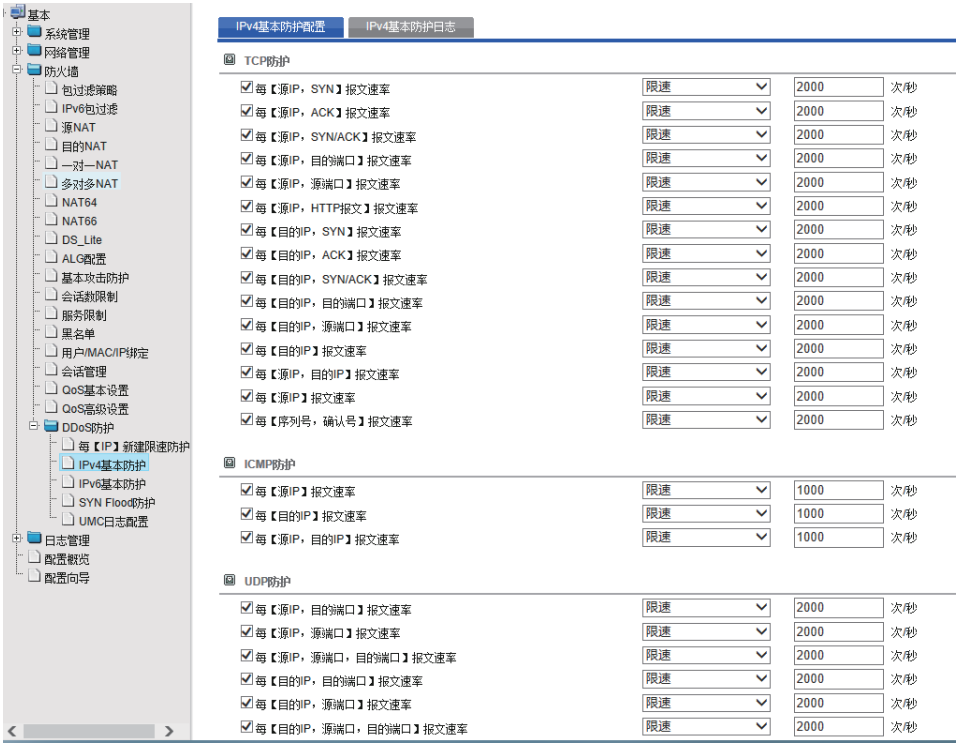

图 10 防火墙抗 DDoS 防护策略

内建立新的连接，每秒最多允许 2 000 次有效连接(图 10)；同时打开防火墙 DDoS 防护。

3.2 入侵检测系统（IDS）

入侵检测系统通过网络旁路部署，镜像交换机端口流量进行检测，可以将网络传输中的报文与设备特征中的攻击类型进行匹配，配置好 IDS 策略，发现网络流量中数据包的报头文件信息可疑和违背安全策略的数据传输时，则进行阻断或通过与防火墙进行联动防护[6]。配置安全策略时，可根据平常设备运行的状态设置设备正常情况的数值，如 CPU 利用率、内存利用率、报文流量等。当设备运行数值超出策略配置范围时识别为入侵行为，则切断此次 TCP 连接并产生告警信息。

3.3 Web 防篡改系统

通过网页防篡改系统将主网站静态网页全镜像到两台 Web 发布服务器上，两台 Web 发布服务器做负载均衡，同时对 Web 发布服务器进行实时监控，如发现非法删除、修改文件、非法新增等操作时，将主网站服务器中的文件同步到 Web 发布服务器进行覆盖修复原文件。配置时只需将 Web 服务器 IP 映射至互联网，主服务器用内网 IP 进行数据交换，用户在访问时不会访问到主服务器，达到隐藏后台网站发布系统的目的。

3.4 政府网站综合防护系统（G01）

政府网站综合防护系统(G01)是云南省公安厅网安大队提供的政府网站安全防护系统，该系统从常见的各种普通攻击防护到进阶版深入网站服务器安装插件，进行整个门户网站服务器包括操作系统、业务、端口等安全防护。根据不同的攻击方式进行 IP 限制、20 min 内禁止访问、拦截、告警，将可疑 IP 拉入黑名单，能清晰记录攻击行为和处理结果，为攻击溯源提供参考(图 11)。

4 网站反向代理服务应用

基于反向代理服务优势在于隐藏后端主服务器信息不被外界攻击，同时能提供良好的负载均衡能力，所有访问请求转发到负载节点提供访问，在所有负载节点发生故障时可通过故障转移功能指定一个备份节点 (standby node) 提供用户访问。反向代理以代理服务器来接受 Internet 上的连接请求，然后将请求转发给内部网络上的服务器，并将从服务器上得到的结果返回给 Internet 上请求连接的客户端，此时代理服务器对外就表现为一个，这是利用 Apache 自带的 Mod_proxy 模块使用代理技术来连接 Tomcat，实现反向代理的需求。云南省防震减灾网站两台 WEB 发布服务器按反向代理服务方式进行部署，隐藏门户网站实际 IP，提升网站安全性，通过与网络信道运营商建立重大突发事件(地震、网络攻击等)时网络信道保障机制，突发访问量增大的情况下，门户网站运行正常，在一定程

图 11　系统安全防护日志

度上缓解了网站系统压力。

5　结论

安全问题, 三分技术、七分管理。虽然可以通过部署高性能防火墙、入侵防御系统等相关防护类设备来起到一定的防护效果, 但还是需要加强人为管理, 通过持续的网站监测, 定期安全巡检、安全审计、实时应急响应服务来保障网络安全。同时, 在自身技术力量不足时应积极利用社会安全服务资源来解决安全问题。针对各种类型的应用对信息安全有不同的需求, 必须进行具体的分析才能制定出适合自身要求的总体信息安全解决方案。

参考文献:

[1] 张源良, 张宇. 一种针对 BGP 会话的低速率分布式拒绝服务攻击模拟研究 [J]. 智能计算机与应用, 2020, 10(2): 263-266, 271.
[2] 张锦辉, 张文秀. 网络设备参与的 DDoS 防御系统的构建与仿真 [J]. 信息技术与网络安全, 2019, 38(1): 1-6.
[3] 邹创勋, 李锫. DDOS 攻击实测与业务系统主机安全防护 [J]. 通信与信息技术, 2020(2): 38-42.
[4] 周利霞, 王晓磊, 杨奕, 等. 天津地震信息网络系统的安全建设 1[J]. 震灾防御技术, 2013, 8(3): 334-339.
[5] 曾薇, 杨乐, 谭颖. 网络存储技术在地震数据存储中的应用 [J]. 震灾防御技术, 2011, 6(3): 335-342.
[6] 李刚, 孙晶岩, 卞真付, 等. MPLS VPN 高速区域网络在天津地震监测系统中的应用 [J]. 震灾防御技术, 2012, 7(1): 92-99.

Portal Web DDoS Simulated Attacks and Safety Protection

SU Yi, AN Xiaowei, LI Zhen, LYU Shuai, LIU Pengfei
（Yunnan Earthquake Ageacy, Kunming 650224, China）

Abstract: The distributed denial of service (DDoS) simulation attack is carried out on the web portal system of Yunnan earthquake agency. Through sending a large number of SYN Flood packets in a short period of time, the network and service operation conditions are respectively detected, and the packet analysis attack characteristics are obtained from the port image of the switch, so as to test the security protection capability of network traffic data. Combined with security software and hardware resources, this paper proposes protective measures for portal system security, and fixes the information security holes existing in the network, so as to improve the network information security.

Key words: DDoS attack; simulated attacks; safety protection