# 代理服务器的安全性能指标及测试研究

## The safety indexes of agent server and their test studies

李常先　王 海　（莱阳农学院海都学院 山东莱阳市 265200）

**摘要**：虽然代理服务器的安全性在日常网络应用中已经引起广泛关注，但是有关安全代理服务器的性能指标和测试方法至今没有被系统的提出，使我们很难找到一种标准来衡量代理服务器安全性能的好坏。针对目前代理服务器的现状我们提出一些代理服务器安全基本性能和安全性能的关键指标，为代理服务器的安全性能评价提供客观依据。

**关键词**：代理服务器 安全性能 安全性 代理

代理服务器英文全称是 Proxy Server，其功能就是代理网络用户去取得网络信息。形象的说：它是网络信息的中转站。代理服务器是介于浏览器和 Web 服务器之间的一台服务器，使用代理服务器能大大提高浏览速度和效率，但在实际使用中我们更看重的是它所提供的安全功能。下面我们就代理服务器的安全性能加以分析研究。

## 1　代理服务器的安全性能指标

### 1.1　基本性能指标

(1) 最大并发连接数(Maximum number of concurrent connections)。是衡量代理服务器性能的一个重要指标，指代理服务器能够同时建立代理连接的最大数目。普遍认为，如果客户和服务器之间的连接对各种请求的平均带宽大于 320kb/s，则称其为顺畅连接(conforming connection)，最大顺畅连接数越大说明代理服务器的性能越好。

(2) 吞吐量(Throughput)。指网络设备在不丢失任何帧的情况下的最大转发速率，以太网吞吐量最大理论值称为线速，即指网络设备有足够的能力以全速处理最小的数据封包转发。吞吐量是代理服务器最重要的指标，可用平均速率或峰值速率表示，其值越大说明代理服务器性能越好。

(3) 时延(Latency)。指用户发送请求到代理服务器转发请求所花费的时间，时延越短说明代理服务器对数据的处理速度越快，其性能就越好。

(4) 丢包率(Frame Lose Rate)。也是衡量代理服务器性能指标的一个重要参数，指在稳态负载下由于缺少系统资源而没有转发的帧所占的比例，数据包丢失一般是由网络拥塞引起的。虽然以太网协议中规定的丢失重复发送保证了丢包不影响数据的正确性，但大量的丢失会降低网络的利用率和实用性能，甚至会引起网络瘫痪。

### 1.2　安全性能指标

代理服务器的安全由防御、检测、响应及恢复几部分的共同协作保证。防御系统的安全指标主要是访问控制的力度，采用不同的访问控制模型和策略，控制的力度就有所不同，一般来说，访问控制的力度越细，防御系统的安全性就越高，反之亦然。

响应系统的安全性主要体现为攻击事件发生后的处理。响应系统在接收到网络攻击的通知后，主要做两方面处理，一是报警，二是阻断，其中阻断成功率是响应系统安全性的重要指标，阻断成功指阻断恶意连接，并阻断正在发生的攻击事件或攻击事件将要发生的条件。阻断成功率越高，系统越安全。

恢复系统的安全性主要体现为对攻击事件的恢复程度和恢复时间，它们共同决定了恢复系统的性能，恢复时间少但恢复程度不高，或恢复程度高而恢复时间长，都不是好的恢复系统。一般来说恢复程度应该控制在 80% 以上，而恢复时间应该控制在安装系统所需时间的一半或更少。

总上所述我们可以发现检测系统的安全性能指标

主要有以下几个：

(1) 错误率。错误率是评价代理服务器安全性能的重要指标，是检测错误次数占标准测试数据总数的比例。错误包含两种情况：误警和漏警。一般来说，错误率越低，安全性越好。同样的错误率，漏警越少，安全性能越好。

(2) 准确率。准确率是指检测攻击事件的正确次数占标准测试数据总数的比例，准确率的高低直接影响了代理服务器的性能。

(3) 查全率。错误率和准确率还不能确切表明入侵事件被忽略的可能性，所以评测系统安全性能的另一个重要指标就是查全率——能正确地检测出来的入侵事件占标准测试数据中包含的入侵事件总数的比例。

(4) 自我恢复能力。这也是代理服务器的一个重要安全性能指标，无论在其他方面多好的代理服务器，只要自我恢复能力太差，则会造成系统无法正常使用，不能及时的处理攻击事件甚至一些正常业务，影响其服务性能。

由此可以看出，代理服务器的安全指标一般有防御、检测、响应及自我恢复几部分构成，一一般而言，只要通过测试上述指标我们就可以客观评价一个代理服务器的安全性。

## 2 安全代理服务器性能的测试

### 2.1 测试数据源

测试代理服务器的性能，需要一批合适的测试数据，测试数据的来源有两种：

(1) 标准测试数据。就是在某种标准的信息源中预先得到并整理好的数据，使用标准测试数据的方法叫做后台测试方法。它的优点是高效率、低成本，只要一组标准数据就可重复测试多个系统；缺点是不能检测出各种突发问题及系统的鲁棒性。

(2) 实际测试数据。指数据在检测现场得到，采用实际测试数据的方法叫做在线测试方法，它需要一个检测环境。它的优点是是能够检测出一些突发问题、最高检测速率和鲁棒性等；缺点是成本比较高。

### 2.2 基本性能的测试

对于基本性能的测试，即吞吐量、最大并发连接数、丢包率和时延等性能的测试，一般采取在线测试方法。有一些测试工具如 WebStress、SpecWeb99 等，可以模拟出真实的网络环境，对代理服务器进行压力测试，观察、统计上述性能的变化过程，就可得到这些性能的变化曲线，从而获得有关该代理服务器的综合性能。对不同的代理服务器分别进行上述测试过程，经过比较，就可评测出代理服务器的优劣，性能不好的代理服务器会引起网络的瓶颈，造成工作效率降低和投资的浪费。

### 2.3 安全性能的测试

对于防御系统安全性的测试，即对访问控制力度的测试，一般采取的步骤是：

(1) 用一组非法用户身份数据测试防御系统的认证功能，安全的情况是每一个非法的用户都不会被允许使用该代理服务器及其服务。

(2) 用合法的用户身份进行登录，并访问该用户无权访问的资源，如果系统能够阻挡 90% 以上的非法访问，就认为防御系统的安全性比较好。对于检测系统安全性能的测试，可以采用标准测试数据。标准测试数据包括若干不同类型的攻击、入侵和正常事件的数据，每一条数据都被标注为是某种攻击或正常事件。测试完毕后，将检测结果与数据标志比较，就可得出检测结果是否正确，下面给出过程描述。

假设标准测试数据 DATA 中有 N 条数据，其中有 A 条是攻击数据，B 条是正常数据：

$N=A+B$

用 DATA 测试安全代理服务器，检测结果为：

在 A 条攻击数据中只检测出 c 条($C<A$)，其余 D ($D=A-C$)条攻击被认为正常。

在 B 条正常数据中，有 E($E<B$)条被认为是攻击事件，其余 F($F=B-E$)条正常数据被正常识别。

不同的使用环境对安全性的要求不同，例如，对攻击不是很敏感的环境需要较低的误警率，对攻击敏感的环境需要较低的错误率。对于一个安全防御系统，查全率随误警率变化的曲线叫做 ROC 曲线，一般来说，查全率越高，误警率就越高。如图 4 是两个不同安全代理服务器安全性能的比较。

分析图 1 的曲线，可知：

(1) 两条曲线均为上升曲线，说明误警率增加，查全率也增加。

(2) 当查全率为 0 时，ROC 曲线沿横轴走(即 cl

的 OA1 段和 C2 的 OA2 段),说明没有检测到任何入侵,可是误警率不为 0,表示检测到的全是误警。

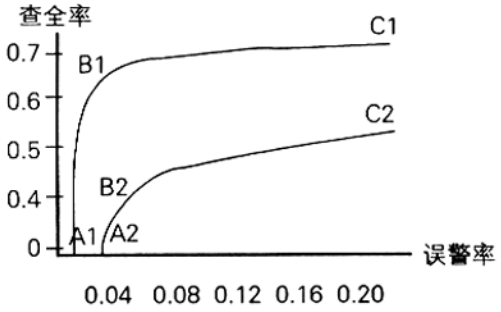


图 1　ROC 曲线比较

(3) 随着误警率逐渐增加,查全率有大幅增加,说明只要牺牲一点误警率,就可以大大改善查全率,此时,大部分常见攻击已经全部被检测出来,误警相对比较少。

(4) 如果误警率继续增加,查全率缓慢上升。此时 ROC 曲线较平坦,表示尽管误警率增加很大,查全率改善很小,说明常见的攻击已经全被检测出来,有少数新的攻击可能未被检测出来,所以误警相对也开始增加。

(5) 应该看到,两个安全代理服务器的最佳工作点应该是 B1 和 B2 附近。比较两个安全代理服务器,在同样误警率的任何情况下,c1 的查全率要比 C2 的查全率高,所以第一个安全代理服务器的安全性能要比第二个安全代理服务器的安全性能好。对于响应系统和恢复系统的测试,可与检测系统的测试同时进行,记录响应系统对那些非法数据,或者某个正在发生的攻击事件的阻断成功率,例如一个正在蔓延的病毒,观察响应系统是否能够阻止该病毒的传染,是否能够清除该病毒源,如果可以阻断 80% 以上,那么说明响应系统的安全性比较高。接着运行恢复系统,观察恢复程度和所需恢复时间,根据上文所列指标,就可评价该恢复系统的性能优劣。

### 2.4 综合性能的测试

前面分别给出了安全代理服务器基本性能和安全性能的评价指标和测试方法,但一般说来,基本性能和安全性能之间存在某些矛盾,安全性能的提高往往会使基本性能降低。因此安全代理服务器的目标是在加强安全性能的同时保证基本性能。综合性能的测试可以按以下几个步骤进行:

(1) 使用同一组数据,分别在无安全防护的代理服务器和安全代理服务器上进行测试,目的是测试加入安全性能使基本性能降低的幅度。此时安全代理服务器相比普通代理服务器,主要的不同就是应用各种安全策略,对输入的数据信息进行检测。一般来说,由于基本性能下降在 10% 之内时,不会给人造成很明显的感觉,所以都可以被接受。

(2) 分别对安全代理服务器使用正常数据和非正常数据,比较正常数据情况下基本性能和非正常数据情况下基本性能的差别。使用非正常数据相比使用正常数据,安全代理服务器的主要不同是响应系统和恢复系统的执行对基本性能的影响。

(3) 采集上述两步的数据,进行比较、分析、综合,确定安全代理服务器综合性能的优劣。一般来说,在保持同样或相近的安全性能情况下,基本性能下降幅度小的安全代理服务器的综合性能比较强。通过使用上述测试方法,可以客观地比较不同安全代理服务器之间各项性能的优劣。在实际情况中,要均衡利弊,根据具体使用情况选择适合的代理服务器。

## 3 结束语

本文给出了安全代理服务器性能评价指标和测试方法,为客观评估代理服务器的安全和性能提供了依据。

### 参考文献

1 Stephen Nottheutt. Inside Network Perimeter security [M], 北京:机械工业出版社,2003.56.
2 RFC1242, BenelmaarkingTerminologyfor-Network InterconneedonDevic [S].
3 吴克喜等,具有智能特征的防火墙——专家系统及其在网络安全管理中的应用[J].小型微型计算机系统,1999,20(6).
4 王春枝等,基于用户的代理服务器安全访问的开发[J],湖北工学院学报,2000,15(2):4—6.
5 东方网,美国国防部紧锣密鼓招黑客[DB/OL].
6 张千里等,网络安全新技术[M],北京:人民邮电出版社,2003.56—62,180～184.
7 张林辉,防火墙性能测试浅析[DB/OL],网络世界.
8 楚狂 等,网络安全与防火墙技术[M],北京:人民邮电出版社,2000.50.