《实验一 加解密算法的实现》实验报告

姓名	李宽宇	年级	21 级
学号	20215279	专业、班级	21 计卓 1 班
实验名称	实验三 拒绝服务攻击与防御仿真实验		
实验时间	2024.4.27	实验地点	DS3305
实验成绩		实验性质	□验证性 □设计性 □综合性

教师评价：

□算法/实验过程正确； □源程序/实验内容提交 □程序结构/实验步骤合理；

□实验结果正确； □语法、语义正确； □报告规范；

评语：

评价教师签名（电子签名）：

一、实验目的

1. 理解拒绝服务攻击的基本概念和常见拒绝服务攻击与防御技术。

2. 能基于具体场景中的现象和数据建立拒绝服务攻击的数学模型，得出合理的结论

3. 能识别问题中的关键因素，通过探索、优化和折中等方法，给出兼顾多个目标的防御方案。

4. 理解拒绝服务场景中攻击和防御的对抗特性，能利用基本的博弈论方法选择较优的攻防策略

二、实验项目内容

实验一：虚假 IP 地址攻击

在本任务中，你将扮演黑客，利用虚假 IP 地址攻击 Web 服务器。本任务的闯关要求是，在攻击成本不高于 50 的前提下，使网络服务质量降低到 40 或以下。已知条件如下：防火墙用于处理连接请求的带宽为

500,000 数据包/秒，正常用户的到达率为 100 个/秒，用户连接请求速率为 100 数据包/秒。

实验二：真实 IP 地址攻击

在本任务中，你将扮演黑客，利用真实 IP 地址攻击 Web 服务器。本任务的闯关要求是，在攻击成本不高于 50 的前提下，使网络服务质量降低到 90 或以下。已知条件如下：防火墙用于处理连接请求的带宽为 100,000 数据包/秒，正常用户的到达率为 100 个/秒，用户连接请求速率为 100 数据包/秒。

实验三：初级防御实验

在本任务中，你将扮演网络管理员，对虚假 IP 地址攻击进行防御。本任务的闯关要求是，在防御成本不高于 20 的前提下，使网络服务质量达到 90 或以上。已知条件如下：正常用户的到达率为 800 个/秒，用户连接请求速率为 100 数据包/秒。

实验四：中级防御实验

在本任务中，你将扮演网络管理员，对真实 IP 地址攻击进行防御。本任务的闯关要求是，在防御成本不高于 20 的前提下，使网络服务质量达到 90 或以上。已知条件如下：正常用户的到达率为 800 个/秒，用户连接请求速率为 100 数据包/秒。

实验五：综合防御实验

在本任务中，你将扮演网络管理员，对拒绝服务攻击进行防御。本任务的闯关要求是，在防御成本不高于 20 的前提下，使网络服务质量达到 80 或以上。已知条件如下：正常用户的到达率为 800 个/秒，用户连接请求速率为 100 数据包/秒。

实验六：连接成功率建模

当防火墙的处理带宽不足时，防火墙只能同意部分 TCP 连接请求。假设防火墙以概率 p 同意连接请求，且一般用户在请求连接时最多尝试三次。请问一般用户可成功连接的概率是多少？请用四则运算写出连接成功率的数学表达式。（格式举例： p+p*p*p，注意区分大小写）

实验七：服务速率建模

服务速率 假设每秒有 a 个新用户与网站服务器建立 TCP 连接。每个用户从建立连接到离开网站请求的总数据量为 w。 同时有 z 台肉机一直在向服务器发送请求。

为了缓解肉机的影响，防火墙规定，当一个客户端请求的数据量超过某个配额后， 相对其它用户，其请求被响应的概率为 q。假设防火墙用于处理服务请求的带宽为 s，请问经过一段时间后， 防火墙可稳定提

供给用户的服务速率(即防火墙可分配给每个用户的平均带宽)是多少？

请用四则运算写出服务速率的数学表达式 （表达式用小写的 a,q,s,w,z 的四则运算表示，如： w*s/(a*q+z)）。

实验八：攻防博弈

博弈论是研究冲突对抗条件下最优决策问题的理论，包含三个基本要素

参与人 （例如黑客、网络管理员）

策略集 （例如 {使用 DoS 攻击、不使用 DoS 攻击}）

收益函数 （例如 网络服务质量）

混合策略纳什均衡：在多人参与的博弈中，假设每个参与者按一定概率配置选择策略，如果任何一个参与人单独改变其概率配置都不会提高收益的数学期望，则该状态构成混合策略纳什均衡。

求解混合策略纳什均衡的一个例子。

假设两个参与人（参与人 1 和参与人 2），其策略集分别为{A, B}和{C, D}，其收益矩阵如下：

		参与人2 C	参与人2 D
参与人1	A	(2, 3)	(5, 2)
参与人1	B	(3, 1)	(1, 5)

矩阵每个格子中第一个数表示参与人 1 的收益，第二个数表示参与人 2 的收益，如:(2,3)表示参与人 1 的收益为 2，参与人 2 的收益为 3。

假设参与人 1 以概率 p 选择策略 A，以概率 1-p 选择策略 B；参与人 2 以概率 q 选择策略 C，以概率 1-q 选择策略 q 选择策略 D，求该博弈问题的混合策略纳什均衡。

			博弈方2 **q** C	博弈方2 **1-q** D
博弈方1	**p**	A	(2, 3)	(5, 2)
博弈方1	**1-p**	B	(3, 1)	(1, 5)

策略选择概率

解：该问题可用等值法进行求解。

以参与人 2 为例，它选择的概率 q 应该使得下面的情况成立，无论参与人 1 如何选择 p 值（即选择策略 A 的概率），其收益的期望值是相同的。

参与人 1 选择策略 A 的收益期望值： E(A) = 2q + 5(1-q)

参与人 1 选择策略 B 的收益期望值： E(B) = 3q + (1-q)

由 E(A) = E(B)可得 q = 0.8

同理，对于参与 1 而言，它选择的 p 值应使得参与人 2 使用策略 C 和 D 的收益期望值是相同的。

参与人 2 选择策略 C 的收益期望值： E(C) = 3p + (1-p)

参与人 2 选择策略 D 的收益期望值： E(D) = 2p + 5(1-p)

由 E(A) = E(B)可得 p = 0.8

故混合策略纳什均衡点为(0.8, 0.8)即参与人 1 以 0.8 的概率选择策略 A，参与人 2 以 0.8 的概率选择策略 B.

三、实验原理

拒绝服务攻击是指利用网络协议的缺陷或直接耗尽被攻击对象的资源，从而使被攻击对象无法正常提供服务的攻击，拒绝服务攻击也是当前最常见的网络攻击之一。

当用户访问网站时，网页浏览器与 Web 服务器之间采用 HTTP 协议进行通信，主要分成两个阶段：第一个阶段，浏览器与 Web 服务器之间建立 TCP 连接。第二个阶段，浏览器向服务器发出 HTTP 请求，服务器向浏览器返回 HTTP 响应。

虚假 IP 地址攻击任务发生在上述第一个阶段，攻击者采用虚假 IP 地址向 Web 服务器发出大量 TCP 连接请求，从而消耗服务器的计算资源，降低其服务质量。真实 IP 地址攻击任务发生在上述第二个阶段，攻击者采用真实 IP 地址向 Web 服务器发出大量服务请求，从而消耗服务器的计算资源，降低其服务质量。

DRR（Dynamic Rate Limiting）：动态速率限制是一种防御措施，用于限制特定 IP 地址或来源的流量速率。这可以防止恶意用户或攻击者通过发送大量请求或数据包来占用服务器资源或进行拒绝服务（DDoS）攻击。DRR 会动态地根据实时流量情况来调整速率限制，从而有效地保护服务器免受过载或恶意攻击的影响。

配额（Quotas）：配额是一种管理和控制资源使用的机制，可应用于服务器防火墙中。通过设置配额，管理员可以限制特定用户、应用程序或服务对服务器资源（如 CPU、内存、带宽等）的使用量。这有助于防止资源滥用、提高系统的稳定性和安全性。

Cookies：Cookies（Cookie-based 防御）是一种用于识别和跟踪用户会话的技术，在服务器防火墙中也有一定的防御作用。通过使用 Cookies，服务器可以识别合法的用户会话，并对来自未经授权的请求进行拦截或限制访问。例如，服务器可以基于 Cookies 来实现对登录状态的验证，从而防止未经授权的访问或会话劫持。

黑名单（Blacklisting）：黑名单是一种常见的防御工具，用于识别和阻止已知的恶意 IP 地址、域名、用户或应用程序。服务器防火墙可以通过黑名单机制来拦截来自黑名单中的来源的流量或请求，从而减少安全风险和攻击的可能性。黑名单通常会定期更新，以包含最新的威胁信息和恶意来源。

四、实验过程中遇到的问题及解决情况(主要问题及解决情况)

主要问题：实验八攻防博弈，参考了博弈问题的混合策略纳什均衡。算不出来提示的数值 0.66

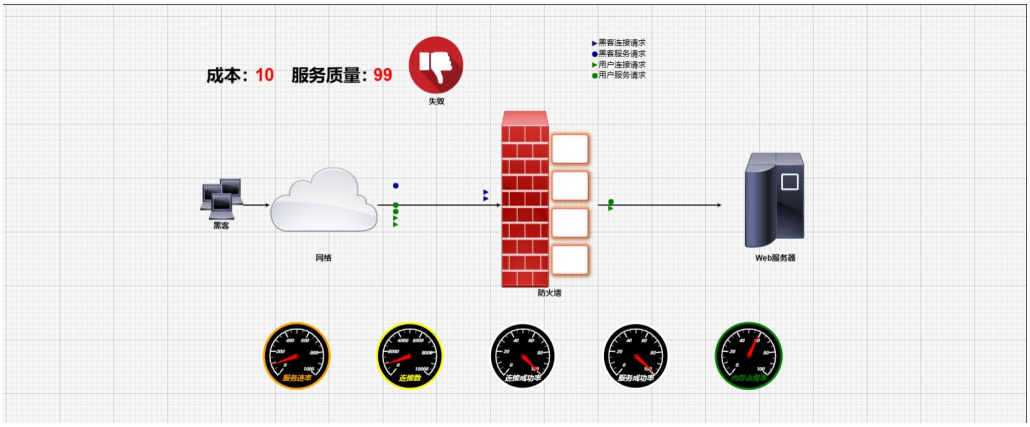
解决：实际上，实验八，应该是通过尝试，选取一个合适的值，而非计算出结果。参考资料的方法为混合策略纳什均衡点，表示两个策略的收益期望值是相同的，与防御最大收益没有关系。

五、实验结果及分析

实验一：虚假 IP 地址攻击

逐渐增加虚拟 IP 攻击台数，使攻击成本不超过 50，最终攻击成功。

(1)虚假 IP 攻击台数：10，虚假 IP 攻击速率 1000

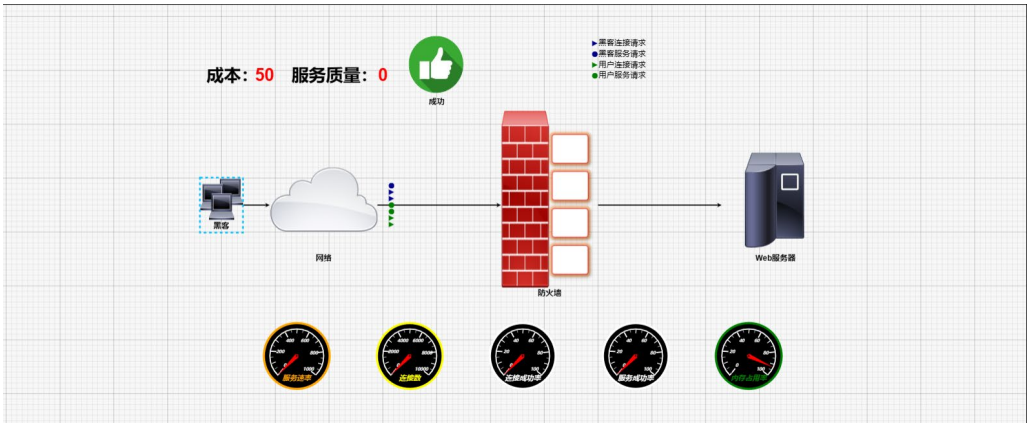


攻击失败，连接成功率和服务成功率均为 100%，服务器内存占用率为 60%

(2) 虚假 IP 攻击台数：40，虚假 IP 攻击速率 1000

攻击失败，连接成功率和服务成功率均为 100%，服务器内存占用率为 90%

(3) 虚假 IP 攻击台数：50，虚假 IP 攻击速率 1000



攻击成功，连接成功率和服务成功率均为 0%，连接数为 0，服务器内存占用率为 100%

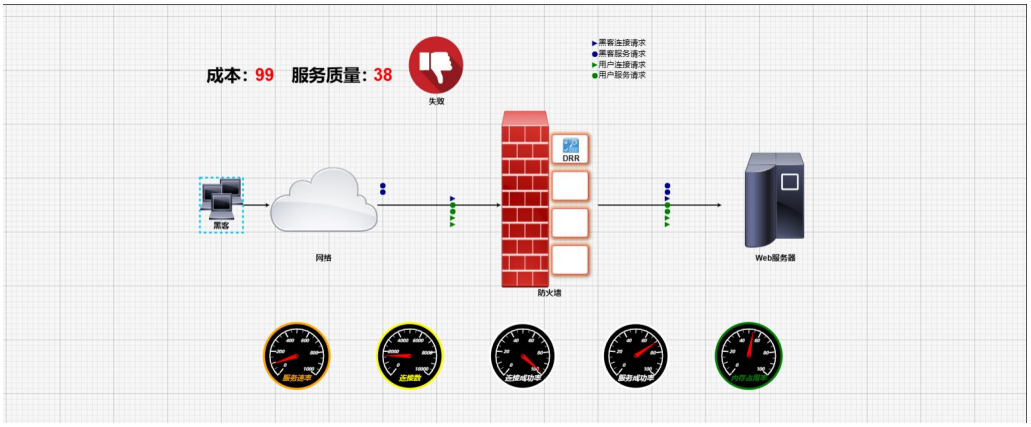
(4)结果分析

当服务器的内存占用率达到 100%时，会导致服务器无法再继续接受新的连接或处理新的请求。当内存占用率达到 100%时，服务器的内存资源已经完全耗尽，无法再为新的连接或请求分配足够的内存空间。这导致新的连接被拒绝或无法建立，从而使得连接数下降到 0。攻击者正是利用这一点，通过大规模的虚假 IP 攻击来消耗服务器的内存资源，最终导致连接数下降到 0，使服务器无法继续提供服务。

实验二：真实 IP 地址攻击

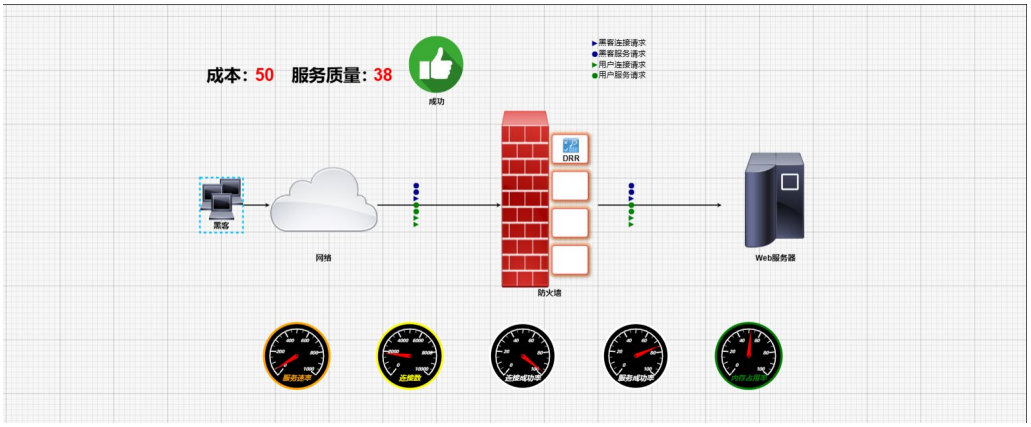
逐渐减少真实 IP 攻击速率，使攻击成本不超过 50，最终攻击成功。

(1)真实 IP 攻击台数：500，真实 IP 攻击速率 1000



服务质量 38，成本 99 过高，连接成功率 100%，服务成功率 60%

(2）真实 IP 攻击台数：500，真实 IP 攻击速率 100



服务质量 38，成本 50，符合要求，服务成功率 75%

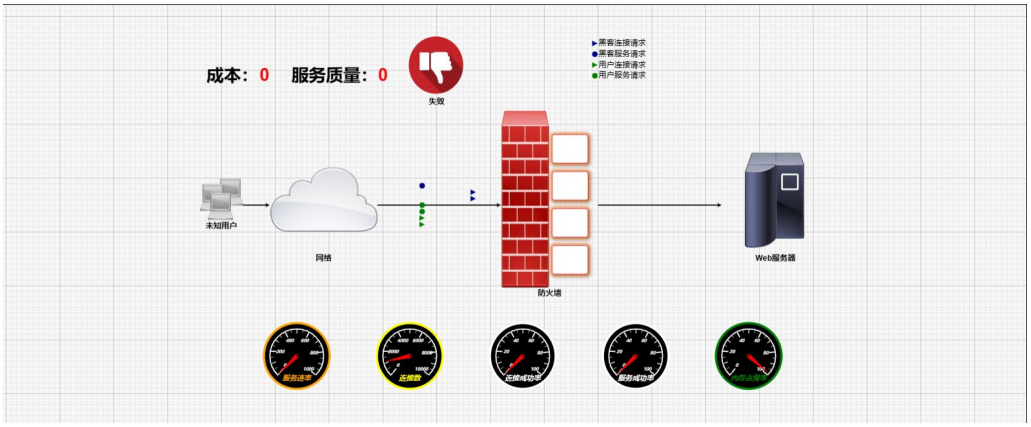
（3）结果分析

防火墙使用 DRR 工具限制黑客攻击速率，从动画中可以看出，经过防火墙的过滤，黑客请求和用户请求的速率都被限制到较低的相同值，因此维持较高的真实 IP 攻击速率(1000)没有意义，降低到 100 与用户请求速率一致即可。

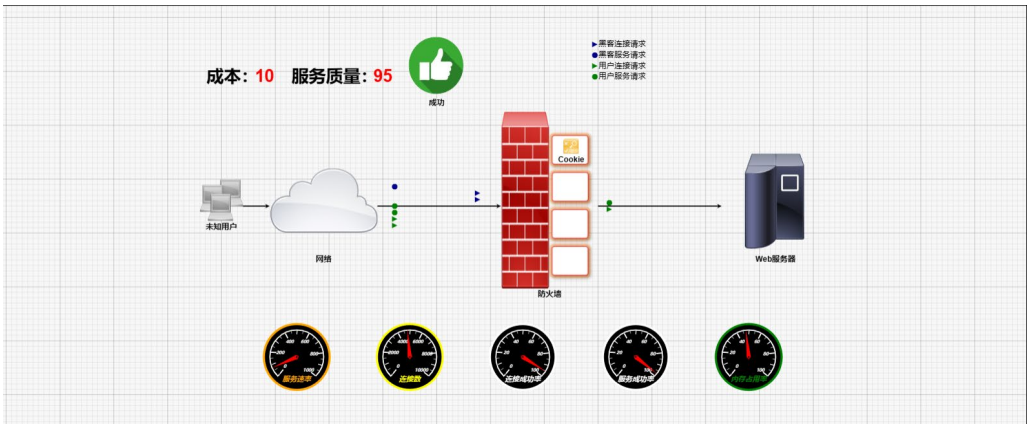
实验三：初级防御实验

依次尝试所有工具

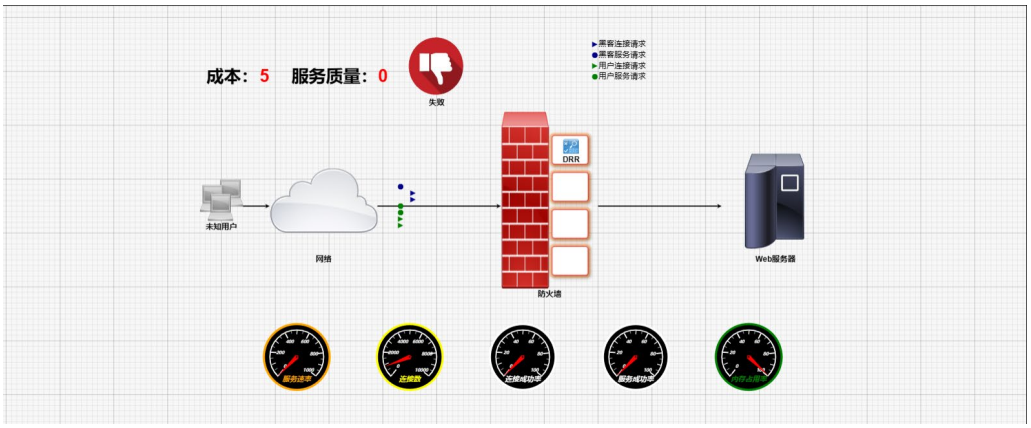
（1）不采取任何防御策略



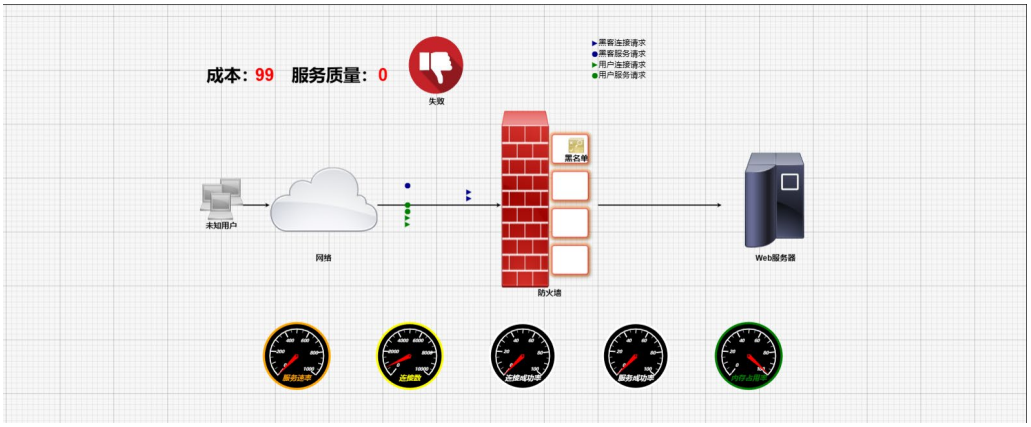
（2）只采用 cookies 工具



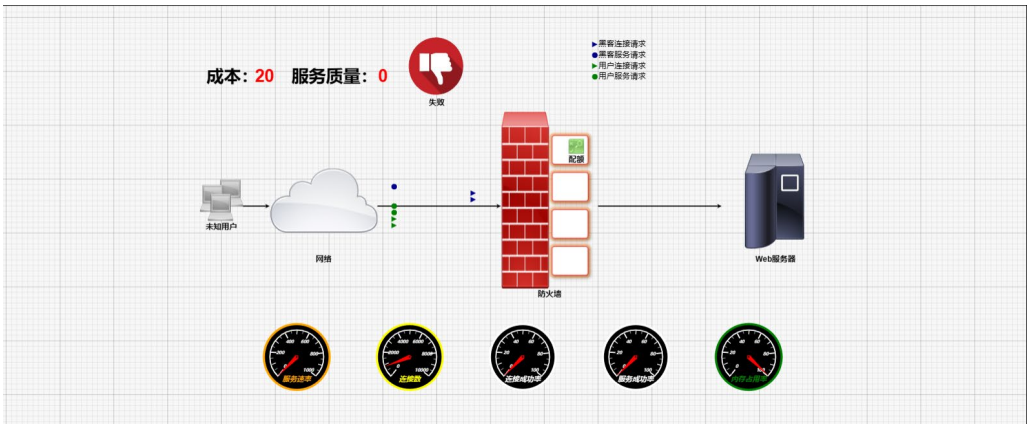
(3)只采用 DRR 工具



(4)只采用黑名单工具



(5)只采用配额工具

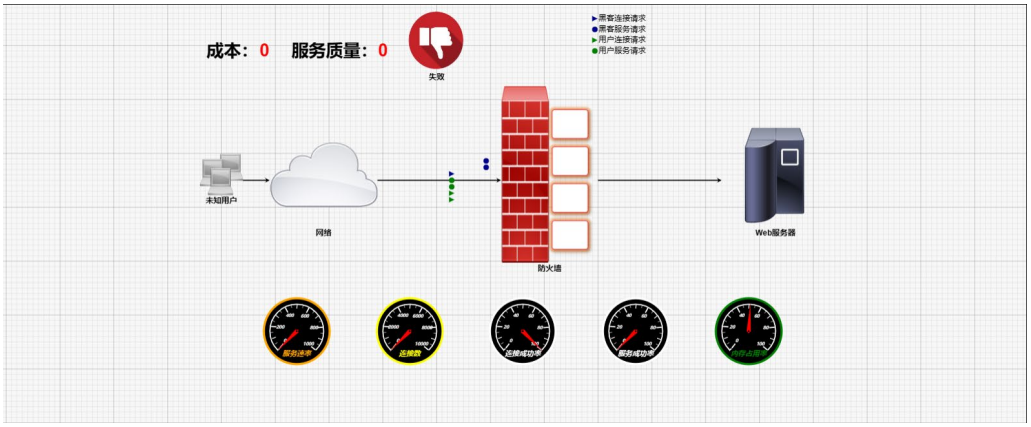


（6）结果分析

只有 cookies 工具将内存占用率从 100%降低到 50%，从而解决了服务质量低的问题。推测采用 SYN Flood 攻击（SYN 洪水攻击），旨在通过向目标服务器发送大量伪造的 TCP 连接请求（SYN 包），使服务器耗尽资源，无法响应合法用户的请求。攻击者发送大量的 TCP 连接请求，但不完成 TCP 三次握手过程（即不发送 SYN-ACK 响应），导致服务器在等待连接建立的过程中耗尽资源，例如内存。由于 TCP 连接资源有限，当服务器不断接收到大量未完成的连接请求时，正常的合法请求无法被处理，导致服务不可用。Cookies 工具并不直接用于应对 SYN Flood 攻击。Cookies 通过识别和跟踪用户会话，可以拒绝未登录状态的 SYN 包，从而防止服务器在等待连接建立的过程中耗尽资源。

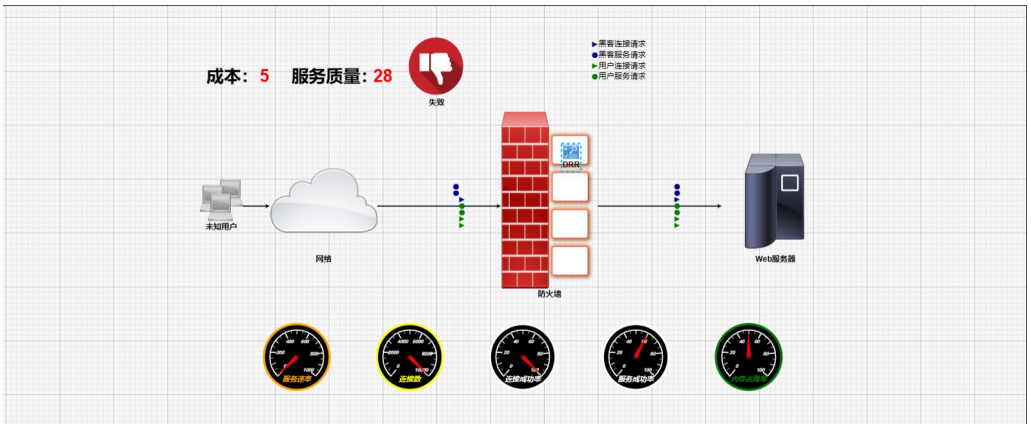
实验四：中级防御实验

(1)不采用工具进行防御



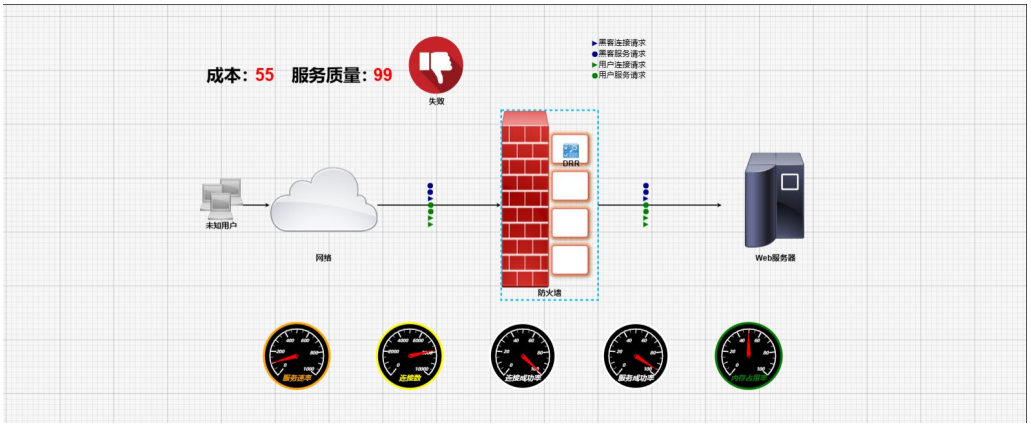
发现服务速率为 0，连接数为 0，连接成功率 100%，服务成功率 0%，内存占用率 50%，推测采用了真实 IP 地址攻击，且黑客服务请求速率非常高。应该使用 DRR 工具限制黑客攻击速率。

（2）使用 DRR 工具，DRR+连接请求带宽 500000+服务请求带宽 500000



此时，连接成功率达到 100，服务成功率 60%，服务质量 28，说明 DRR 起到了一定的作用。为了提高服务成功率，应该尽量调高服务请求带宽。

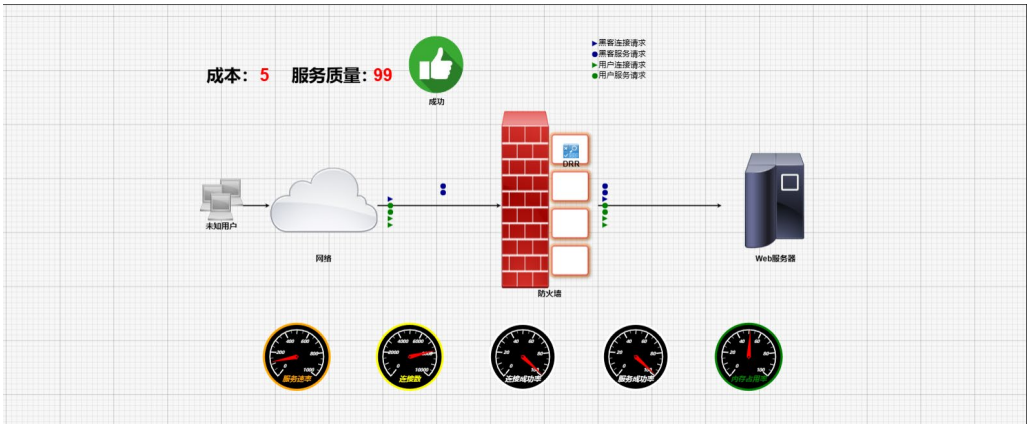
(3)DRR+连接请求带宽 500000+服务请求带宽 1000000



此时，服务质量 99，服务成功率和连接成功率均 100%，适当降低服务请

求带宽和连接请求带宽，以降低防御成本。

(4)DRR+连接请求带宽 100000+服务请求带宽 900000



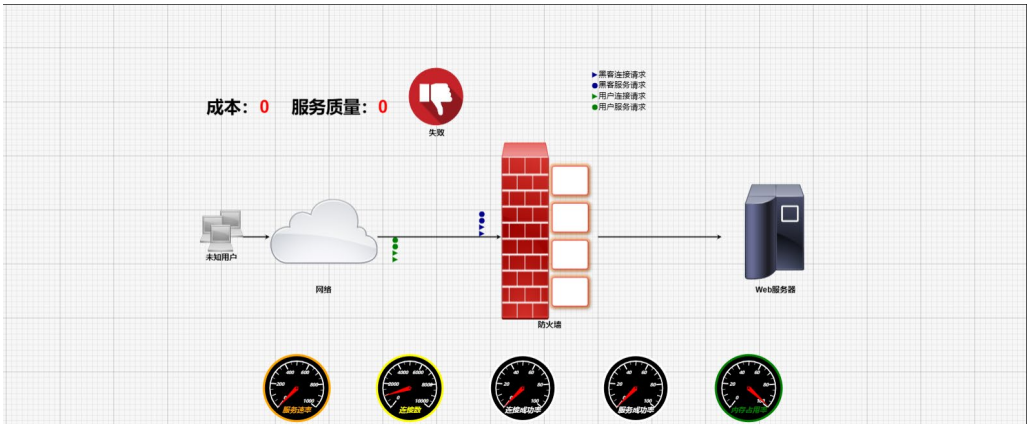
此时，服务质量 99，成本 5

（5）结果分析

连接成功率高，服务成功率低，说明黑客主要采用真实 IP 地址攻击。应该使用 DRR 工具限制黑客攻击速率。更具服务成功率和连接成功率，调整服务请求带宽和连接请求带宽，调高带宽可以提高成功率，但会增加成本。

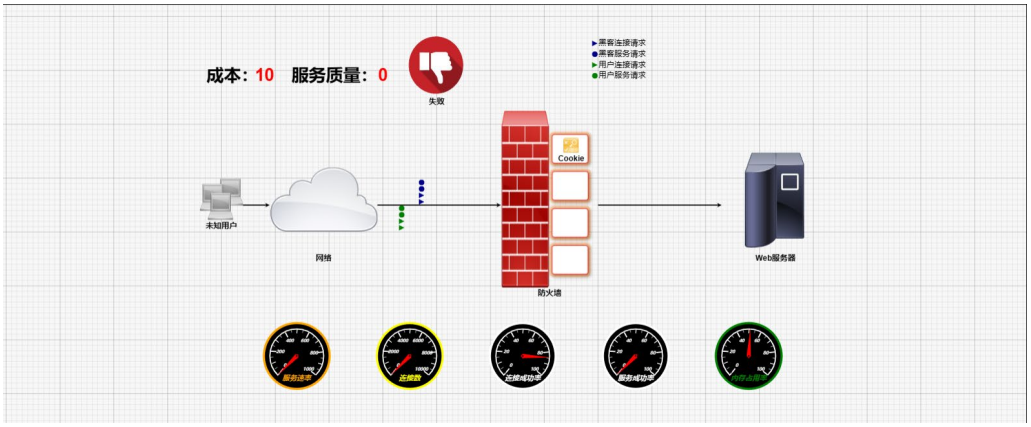
实验五：综合防御实验

(1)不采用工具进行防御



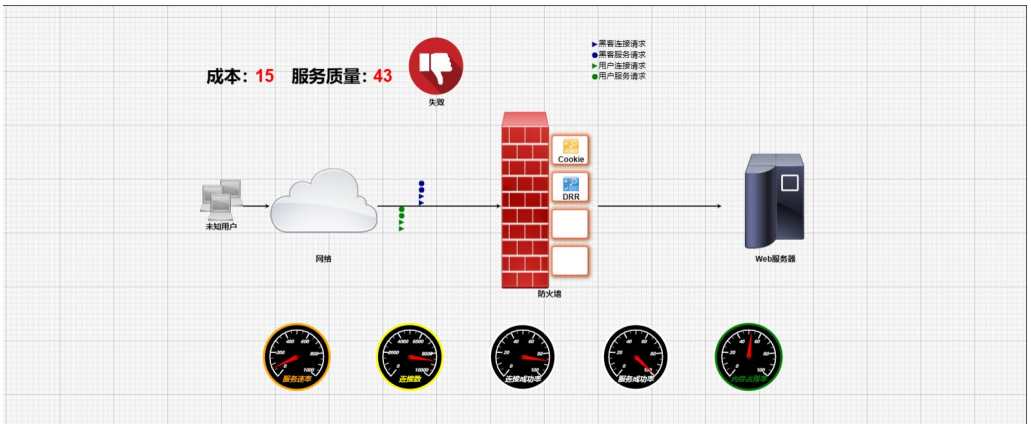
发现服务速率为 0，连接数不为 0，连接成功率 0%，服务成功率 0%，内存占用率 100%。首先，内存占用率 100%，推测黑客采用虚拟 IP 地址攻击。

（2）先采用 cookies 解决内存占用率的问题



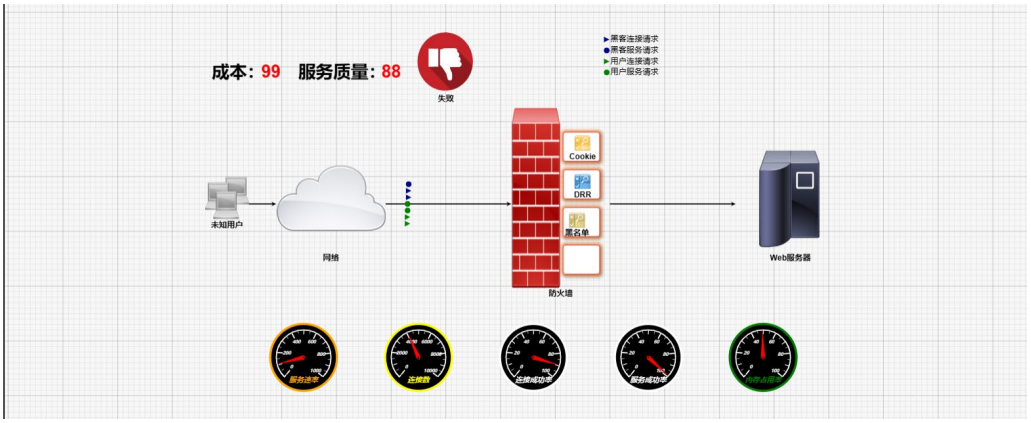
此时，cookies 工具已经起到了作用，将内存占用率降低下来。但是连接数为 0，连接成功率 80%，服务成功率 0。推测采用了真实 IP 地址攻击，且黑客服务请求速率非常高。应该再使用 DRR 工具限制黑客攻击速率

（3）cookies+DRR



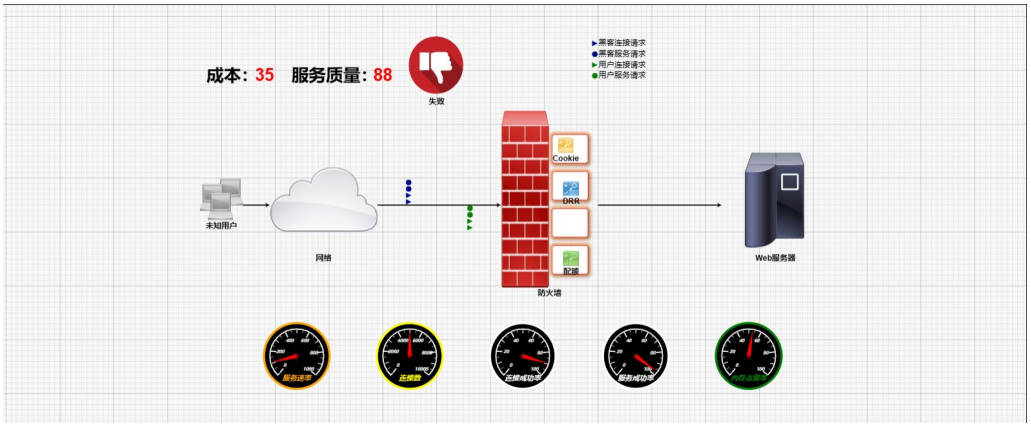
此时，服务质量 43，有了改善，但是连接数明显高于用户数量，应该进行限制

（4） cookies+DRR+黑名单



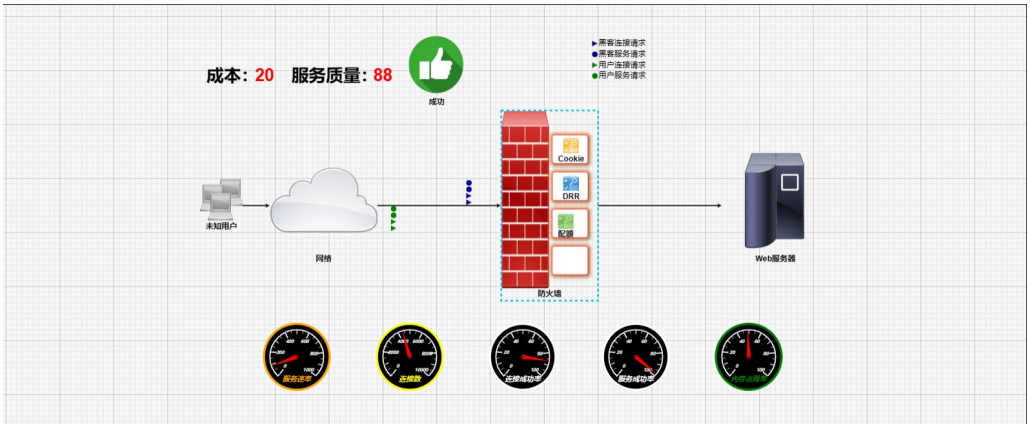
此时服务质量 88，成本 99，连接数已经明显降低

（5） cookies+DRR+配额



此时服务质量 88，成本 35，连接数已经明显降低，应该降低成本

（6）cookies+DRR+配额（惩罚因子 0.38）

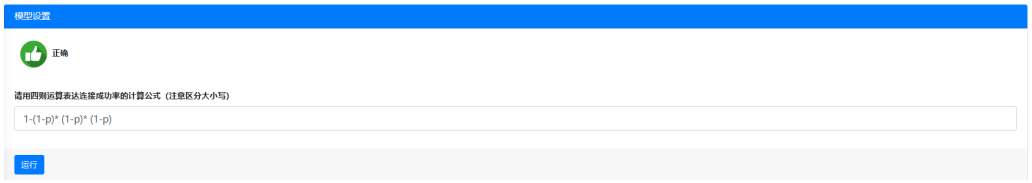


（7）结果分析

①内存占用率 100%，推测黑客采用虚拟 IP 地址攻击。采用 cookies 解决内存占用率的问题。②服务成功率 0。推测采用了真实 IP 地址攻击，且黑客服务请求速率非常高。应该再使用 DRR 工具限制黑客攻击速率。③连接数明显高于用户数量，应该进行限制，cookies+DRR+配额在保证较高服务质量的同时，成本低 cookies+DRR+黑名单。④将惩罚因子调高，使防御成本不超过 20。

实验六：连接成功率建模

一次失败率是 1 若三次都失败的概率是 (1-p)*(1-p)*(1-p) 则连接成功的概率为 1-(1-p)*(1-p)*(1-p)



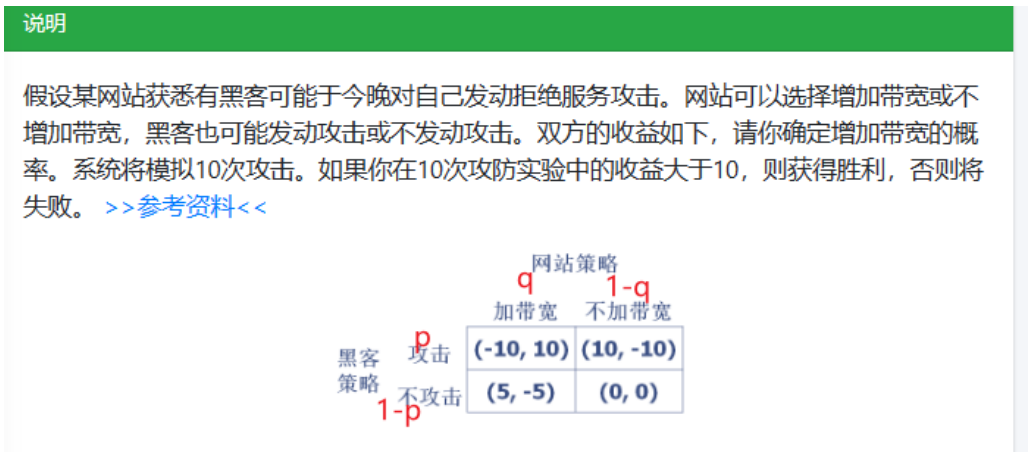
实验七：服务速率建模

第一步：在平衡时，每个用户的服务时间为 w/v，到达率为 a。因此，正在接受服务的用户人数为 a*w/v。

第二步：配额机制使得 z 个攻击者相当于 zq 个正常用户，因此 x+zq 个用户共享一部分带宽。服务速率可表示为 s/(x+z*q)。

第三步：将前面两个表达式构成一个方程组，即 x=aw/v，v=s/(x+zq)。通过解这个方程组，可以得到 v 的表达式。具体地，v=s/(aw/v+zq)。

实验八：攻防博弈



黑客：E(攻击) = -10q+10(1-q)

E(不攻击) = 5q+0(1-q)

E(攻击)= E(不攻击) =>q=0.4

网站：E(加带宽) = 10p-5(1-p)

E(不加带宽) = -10p+0(1-p)

E(加带宽)= E(不加带宽) =>p=0.2

分析和总结

1.虚拟 IP 地址攻击会提高服务器的内存占用率，当服务器的内存占用率达到 100%时，会导致服务器无法再继续接受新的连接或处理新的请求。当内存占用率达到 100%时，服务器的内存资源已经完全耗尽，无法再为新的连接或请求分配足够的内存空间。这导致新的连接被拒绝或无法建立，从而使得连接数下降到 0。攻击者正是利用这一点，通过大规模的虚假 IP 攻击来消耗服务器的内存资源，最终导致连接数下降到 0，使服务器无法继续提供服务。比如 SYN Flood 攻击（SYN 洪水攻击），旨在通过向目标服务器发送大量伪造的 TCP 连接请求（SYN 包），使服务器耗尽资源，无法响应合法用户的请求。攻击者发送大量的 TCP 连接请求，但不完成 TCP 三次握手过程（即不发送 SYN-ACK 响应），导致服务器在等待连接建立的过程中耗尽资源，例如内存。由于 TCP 连接资源有限，当服务器不断接收到大量未完成的连接请求时，正常的合法请求无法被处理，导致服务不可用。

2.真实 IP 地址攻击会降低服务成功率。拒绝服务（DDoS）攻击：攻击者可以通过发送大量的请求来超载服务器，使其无法正常工作。这可能导致网站或网络服务无法访问，从而影响业务运营。

3. 虚拟 IP 地址攻击可以通过 Cookies 工具进行防御。以 SYN Flood 攻击为例，Cookies 通过识别和跟踪用户会话，可以拒绝未登录状态的 SYN 包，从而防止服务器在等待连接建立的过程中耗尽资源。

4. 真实 IP 地址攻击可以通过 DRR 工具限制黑客攻击速率。动态速率限制是一种防御措施，用于限制特定 IP 地址或来源的流量速率。这可以防止恶意用户或攻击者通过发送大量请求或数据包来占用服务器资源或进行拒绝服务（DDoS）攻击。DRR 会动态地根据实时流量情况来调整速率限

制，从而有效地保护服务器免受过载或恶意攻击的影响。

5.攻击会通过抢占服务器资源（如 CPU、内存、带宽等）使得服务质量下降，可以通过配额机制解决。配额（Quotas）：配额是一种管理和控制资源使用的机制，可应用于服务器防火墙中。通过设置配额，管理员可以限制特定用户、应用程序或服务对服务器资源（如 CPU、内存、带宽等）的使用量。这有助于防止资源滥用、提高系统的稳定性和安全性。可以设置惩罚因子。带宽亦可以提高网络质量，但会极大的增加成本。