期末论文

防火墙观念和技术

卜忠礼

2021 年 4 月 10 日

随着计算机网络的普遍使用，计算机网络和 WEB 应用的安全问题日益严重，防火墙技术能够有效保障计算机网络和 WEB 应用的安全。防火墙实际上是一个分离器，一个限制器，也是一个分析器，有效地监控了数据包和流量，将不同的区域安全的分开。它是一种计算机硬件和软件的结合，从而保护内部网络或者应用免受非法攻击的侵入。

一、传统防火墙技术

为了保护内部网络免受攻击，并隐藏内网的拓扑结构，网络管理员可以利用三种防火墙技术：IP 地址转换（NAT），代理服务器，或者虚拟专用网络（VPN）。

NAT 是一种将私有 IP 地址转化为公网 IP 地址的技术。通过 NAT 协议，路由器或者防火墙能把未经注册的内部 IP 地址转换为已获注册的 Internet IP 地址，反之亦然。该协议解决两个问题，一方面可以隐藏内部的真实 IP 地址，使内部网络免受黑客的直接攻击，另一方面也可以解决公网 IP 地址不足的问题。NAT 有两个方式，正向 NAT 处理从内网出去的数据包和反向 NAT 处理从外网进入的数据包。无论是正向 NAT 还是反向 NAT，都可以采用负载均衡技术，一般是通过轮询方式实现的，以减轻每台服务器的访问压力。

代理技术的防火墙用代理服务器的方式运行，在内网和外网之间实现安全控制功能，起到应用服务的转接作用。一个内部网络的主机给一个外部服务器发送请求的话，当该请求到达代理服务器后，代理服务器对数据包的包头和信息进行检查，然后将内网的源地址改为自己的，最后将这个数据包发给外部的目的主机。外部主机应答的数据包也将发送到代理服务器，经过相反的过程，而外网并不清楚内网的拓扑结构。这是通过在代理服务器上安装特殊的代理代码来实现的，该代码一定有服务器端的代码，也可以包括 server 和 client 端代码。和包过滤技术相比，代理技术有较高安全性，还可以为安全检测和日志记录提供最详细的信息；代理服务器提供缓存功能，可以在提交重复请求时从缓存获取信息，提高网络性能。可是代理服务技术有它的缺点，比如不能支持所有的协议；在访问数据量大的情况下，代理技术会增加访问的延迟等。

VPN 可以在公用网络上建立专用网络，进行加密通信。举例来说，外地员工 A 需要访问公司 B 的内网，通过 B 的内部 VPN 服务器，A 和 B 能够进行加密通信。简单的说，当 A 访问 B 时，A 的数据包会被 A 的 VPN 程序进行封装，从而成为一个新的 VPN 数据包。如果黑客非法地拦截该数据包的话，他无法了解加密信息。当 VPN 的数据包到达 B 的 VPN 服务器时，B 可以把加密的数据包解包为原始信息。这样的通信虽然处于公网上，但 VPN 的封装过程相当于建立了一个专用的数据隧道，保证了数据能够安全传输。VPN 最大的缺点是它的复杂性，因为创建和部署 VPN 线路不容易，所以很多公司选择较简单的技术。

二、WEB 应用防火墙（WAF）

传统防火墙能保护内部网络，防止外部的非法影响，但是在越来越多的公司，个体，政府等机构广泛地采用 WEB 应用的同时，WEB 安全的需求也迅速地增加。为提高 WEB 应用的安全性，用户可使用 WEB 应用防火墙（简称为 WAF）来保障用户核心应用与业务持续稳定的运行。WAF 是集 WEB 防护，网页保护，负载均衡于一体的 WEB 整体安全防护设备的一款产品。WAF 是指通过执行一系列针对 HTTP/HTTPS 的安全策略专门为 WEB 应用提供保护的产品，主要用于防御针对网络应用层的攻击，比如 SQL 注入攻击，XSS，参数篡改等攻击行为。

传统统防火墙位于内部和外部网络之间，工作在 OSI 的网络层，对企业网络层数据进行保护，而 WAF 工作在 OSI 的应用层，对于现今常见的网络应用层攻击行为有很好的防御效果。相比较于传统防火墙，WAF 可以为 WEB 应用提供基于规则的保护、基于异常的保护、对 HTTP 请求进行异常检测、提供会话保护机制、提供正面规则集等。对于基于规则的保护，WAF 给 WEB 应用提供一系列的检测，能有效的防范已知和变形攻击的威胁。对于基于异常的保护，WAF 通过建立统计模型也能建立一个保护层，可是这种保护系统模型的构建比较困难，所以并不多见。WAF 还会对 HTTP 的请求进行异常检测，通过提供严格的 HTTP 协议验证能够完整的解析 HTTP 协议。WAF 也可以建立一个可靠的会话管理机制，有效防止 COOKIE 篡改和会话劫持攻击等。WAF 通过仅允许已知的有效输入通过，增强输入验证，提供正向安全模型（白名单），能够有效防止信息泄露、木马病毒植入等入侵行为。正是 WAF 有以上区别于传统防火墙的特点，使 WAF 具有很好的保护 WEB 应用程序的能力。

WAF 的主要功能包括：WEB 应用防护，通过 WAF 的主动安全防护技术，固话专用特征规则库，从而能抵御主要的攻击手段；文本保护，WAF 主要采用事件触发检测技术在网页被非法篡改时进行合法性检查，来实现文件保护；网页木马及后门检测，通过爬虫技术 WAF 能全面检查网站的各级页面中是否被植入恶意代码，避免网站成为恶意软件的分发渠道，并能提供本地后门扫描功能，将网站安全面临的风险降低。

一些重要的 WAF 安全策略包括：限制 HTTP 请求包的 HEAD 大小，以便减轻 DoS 和缓冲区攻击；限制 HTTP/HTTPS 请求方法，比如 GET，POST，DELETE 等选项；以及用户自定义的安全过滤规则，根据业务需求或者针对某些关键字定义过滤规则；WAF 还提供

WEB 应用的审计和固有弱点的屏蔽。但 WAF 本身有一定的局限性，比如它无法解决逻辑错误问题。

三、下一代防火墙（NGFW）

按照 2009 年著名咨询机构 Gartner 做的报告，为应对当前与未来新一代的网络安全威胁，防火墙需要再一次升级为“下一代防火墙”。下一代防火墙，简称 NGFW，是一款可以全面应对应用层威胁的高性能防火墙。NGFW 能够为用户提供有效的应用层一体化安全防护，帮助用户安全地开展业务并简化用户的网络安全架构。因为现今更多的通信量都只是通过少数几个端口及采用有限的几个协议进行，除此之外它的 IPS 系统还不能有效的识别与阻止应用程序的滥用，所以传统防火墙不能满足目前网络安全的需求。

NGFW 主要采用的一项技术叫做深度包检测技术（DPI）。它是一种基于应用的数据包检测和控制技术，当 IP 数据包，TCP 或 UDP 数据流通过基于 DPI 技术的系统时，该系统对数据包进行重组并进行整体控制。DPI 和传统杀毒软件系统在一定程度上比较相像，能识别的应用类型都必须是系统库已有的。当有数据包经过时，DPI 技术会对数据包进行解包，并与后台特征数据库中的特征进行比较。如果有新的应用出现，特征数据库也需要及时更新，来保持对大部分应用数据包特征的支持能力。综上可见，基于 DPI 技术的应用识别易于理解，升级方便，维护简单，精度高，健壮性好，且具有应用分类功能。

NGFW 主要采用的另一项技术是深度流检测技术（DFI）。当网络流量比较大的时候，DPI 无法对数据包进行有效检测，此时可以使用 DFI 技术。DFI 采用的是基于流量的应用识别技术，源于不同的应用类型在会话连接或数据流上的状态模式各有不同，正是基于这一系列流量的行为特征，建立流量特征模型，通过分析多种会话连接流的特征，从而实现鉴别应用的类型。它将流量特征分为两个层次：基本特征集合和组合特征集合，由于数据集是通过对网络流量实时提取获得的，因此真实地反映了网络的实时状态。网路流量异常模型是将基线模板应用于使用者所设定的监测范围内，流量异常检测模型主要凭借系统实时对网络中正常流量形成流量基线，再根据网络正常的网络流量模型来动态分析网络中的异常流量，以期最早时间发现网络中流量的激增和突减。

综上所述，对于未加密的数据包，DFI 技术检测的效率较 DPI 更高，但是没有 DPI 技术的检测精度高。而对于加密的数据包，DFI 检测效果受到较少的影响。

随着 WEB 应用越来越多，网络安全应用的风险问题越来越突出，因此对网络安全防护技术的要求也就越来越高。现在在许多种攻击手段日益变化的同时，针对它们的安全防护技术也在日益完善。计算机网络安全是一个相对的概念，是系统的工程。只有不断的研发计算机网络安全系统，才能使我们一直处于安全的计算机网络环境中。