中国防火墙的相关概念和技术

卜忠礼

2019 年 09 月 06 日

摘要

这是对于中国防火墙小文章的汇编，为他关于防火墙的目的，方法，和影响的独立研究被卜忠礼写了。这独立研究是四月的，从 2019 年 09 月到 2019 年 12 月。

This is a collection of small essays on the Great Firewall of China, written by Charlie Bushman（卜忠礼）as part of his independent study into the purpose, means, and effects of the Firewall，lasting four months from September 2019 to December 2019.

目录

1 相关概念

防火墙是互联网安全性的保护措施。它有两提法，网络防火墙和计算机防火墙的方面。网络防火墙保护内部网络，防止外部网络的不安全因素。，与计算机防火墙保护用户计算机，防止外部网络的不安全因素。全部“防火墙就是用来阻挡外部不安全因素影响的内部网络屏障。”两提法都滤除不符合规定的信息以便不安全的外信息不可能侵染用户的计算机或者网络。它们也有别的方法，比如，网络防火墙称筛选路由器，进入路由器的信息里找到匹配键词。计算机防火墙检查用户计算机输出的信息，并加上相应协议的标志，以便收到信息受到的计算机或网络可能决定信息是否安全安全不安全的信息。

2 重要性和特征

防火墙有一些特征，让防火墙对于计算机网络安全非常重要。~~以上特征，~~防火墙是数据必经之地，因此数据只有一条对外部网络路径。因为数据必经之地，防火墙能够控制网络流量的合法性，~~利用网络地址转换（NAT）~~监控网络通过的信息。防火墙还有完整信任关系的操作系统，从而有抗~~空~~攻击免疫力。

防火墙最重要的功能是记录计算机网络之中的数据信息，防止工作人员访问存在安全隐患的网站，和控制不安全服务。防火墙能够收集计算机网络的数据传输和信息访问，同时把收集的信息进行分类，以便找到安全隐患的数据信息。防火墙也能够对工作人员的操作进行实时监控，因此如果工作人员访问存在安全隐患的网站，防火墙就会发出警报~~，并重定向工作人员的计算机~~。其它~~三~~，防火墙能够降低由不安全服务造成的工作人员的实际操作风险，以拦截不安全的服务，防止对计算机网络非法攻击。

3 功能

防火墙的最基本的目的是极大地提高一个内部网络的安全性。为了达到这样的水平，所以防火墙具有~~一些~~有效防止威胁的功能，包括保护~~屏蔽~~内部网络免受外部威胁，强化网络安全策略，创建一个检查点，审计和日志记录，和控制网络的流量。这些功能能够保护内部网络，同时为内部网提供对外界网络的访问。

为了保护~~屏蔽~~内部网免受外部威胁，防火墙只允许精心选择的应用协议经过，如由于外部攻击者可能利用 NFS 协议来攻击内部网络，可以禁止 NFS 进出内部网络。它也可以防止基本路由的攻击，如 IP 选项中的源路由攻击，ICMP 重定向中的重定向路径等~~别的类型攻击~~并通知防火墙管理员。防火墙就可以隐蔽不安全信息~~有秘密信息~~的服务，如 Finger，DNS 等，还能将所有安全软件如口令，加密，身份认证等配置在防火墙上，因此防火墙的集中安全管理比分散到各个计算机上更经济。

防火墙创建一个检查点，在网络安全行业中称之为“阻塞点”，逼迫所有进出流量都通过这个检查点。如果内部网络有不止一个防火墙，各个防火墙就创建他自己的检查点，检查他自己的进出流量。防火墙也可以有效地审计和日志记录，因为防火墙都创建检查点，所以他们就能记录~~上~~所有的经过访问。这些记录的信息对管理人员非常重要，同时网络使用统计对网络需求和威胁等进行分析，防止威胁和对数据信息的上传和下载速度进行掌握。防火墙可以为更重要的服务配置更多带宽，因此如果网络有太小的带宽，防火墙能够确保重要服务有足够带宽。

4 安全性的区域和透明模式

防火墙定义五个根本安全性的区域，各个实现自己的目的，还有合适的安全优先级。低级安全区域是 untrust（不信任域），用来定义互联网等不安全的网络。中级安全区域是 DMZ（隔离区，安全优先级为 50），用来定义内部服务器所在网络。DMZ 作用是允许外部服务器访问一些不含机密信息的公用服务器，比如 web，mail，FTP 等，同时这外部的访问者不能接触内网中的信息，即使 DMZ 中服务器被外部攻击者危及，这些攻击者还不能存取内部网络的机密信息。高级安全区域是 trust（信任域，安全优先级为 85），用来定义内部用户所在的网路，一般来说这是公司的内部网。顶级安全两个区域是 local 和 management（本地和管理，安全优先级都为 100）。local 就是防火墙本身的区域，防火墙主动发出的报文都是从 local 区域中发出，防火墙响应并处理或者转发的报文都不是从 local 中发出。Management 允许管理员对防火墙设备进行配置，但需要 console 控制接口或一根双绞线链接到管理接口。

为了隔离该些区域并保护内部网络，防火墙有多种部署方式，其中透明模式（图 1）最简单。透明模式网络中，防火墙将过滤通过的 IP 数据包，但 IP 报文中的源或目的地址不会改变。客户端和服务器进行通信时防火墙转发通信，以用户不会感觉到防火墙的存在，因此透明模式也可叫做桥模式。透明模式网络中，防火墙的 trust 区域接口与公司内部网络相连，untrust 区域接口与外部网络相连，并且 trust 和 untrust 两个区域必须处于同一个子网中。

透明模式是在大多数情况下比较适合，如你的服务器需要使用真实互联网 IP 地址。透明模式中的服务器看起来像直接面对互联网一样，因此服务器能够直接访问外部网络但防火墙还能检测经过的报文。另一方面，如果一个公司需要保护同一子网上不同部门的主机可是他们的网络已经建成的话，网络拓扑结构无须做任何改变。透明模式的简单性和设置的便利让它是一个普通的选择。

5 防火墙的关键技术

为了保护内部网络免受攻击和隐藏内网的拓扑结构，网络管理员可以利用 IP 地址转换(NAT)，代理服务器，或者虚拟专用网络 (VPN)。这三个技术通过特殊的办法实现内网的比较高安全性。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 的两个方式，正向 NAT 和反向 NAT 分别是指从内网出去的数据包和是指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与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，经过反的过程，而外网并不清楚内网的拓扑结构。这样作用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。和包过滤技术的安全性比较，代理服务器提供的信息最详细，但是在访问数据量大的情况下，代理技术会增加访问的延迟。为降低这样延迟的几率，代理服务器而提供缓存功能，可是它也有别的问题，比如没有广泛的规则因此应用层代理不能支持所有的协议。

VPN 可以在公用网络上建立专用网络，进行加密通讯。举例来说，外地员工 A 需要存取公司 B 的内网，通过 B 的内部 VPN 服务器 A 和 B 能够进行加密通讯。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，他肯定不能了解它的信息。当 VPN 的数据包到达 B 的 VPN 服务器，B 可以把 VPN A 的数据包解包为 A 本来发送的。这样的通讯处于公网上，但 VPN 的封装过程建立一个专用的数据隧道。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，所以很多公司不能还是不管建立这么高安全水平的技术。

6 WEB 应用防火墙

传统防火墙能保护内部网络，防止外部的非法影响，但在越来越多公司，个体，政府等机构采用本 WEB 的应用的同时，WEB 安全的需求也极快地增加。为提高 WEB 应用的安全性开发者而可使用 WEB 应用防火墙，也被简称为 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。

传统防火墙位于内部和外部网络之间在网络层上，对企业网络层数据进行保护，反之 WAF 工作在 OSI 的应用层，对于现今常见的攻击行为有很好的防御效果。基于规则的攻击 WAF 给 WEB 应用提供一系列的测试，能有效的防范已知和变形已知攻击的安全问题。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，可是这样保护系统的构建比较困难，所以并不多看。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，为了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），在很短的时间内屏蔽各种各样的漏洞等。

通过 WAF 的主动安全技术，固话专用特征规则库，从而能抵御主要和变形攻击的攻击手段。WAF 也主要采用事件触发检测技术，爬虫技术和网页携带木马检测技术。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。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，那避免网站成为恶意软件的分发。WAF 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。WAF 还提供 WEB 应用的审计和固有弱点的屏蔽，可是他本身有一定的局限性，比如它无法解决逻辑问题以及现代的 WEB2.0 动态代码很难保护。

7 下一代防火墙

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。因为第一代防火墙更多的通讯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，所以现代第一代防火墙的防护有效性很差。

一个 NGFW 用的技术被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 和传统杀毒软件的系统在一定程度上比较相像，能识别的应用类型都必须时系统库已有的。DPI 技术，一旦有数据包经过，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。在这样情况下，如果有新的应用出现时，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技术能力。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。

另一方面，NGFW 也可利用深度流检测技术（DFI），如果对 DPI 来看，保护网络的流量比较大。DFI 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，正式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。网路流量异常模型时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，DFI 技术检测的效率较 DPI 更高以及加密的数据包对 DFI 检测有较少的影响，但是没有 DPI 技术的检测精度高。