

应用防火墙技术

随着网络的逐步普及，网络安全已成为 INTERNET 的焦点，它关系着 INTERNET 的进一步发展和普及，甚至关系着 INTERNET 的生存。安全技术在近几年也得到较大的反展，网络安全产品也走下神坛，变得日益普及。但是，在运用防火墙、入侵检测系统等等安全产品之后，为何网络攻击事件却层出不穷。从根本上说，新的攻击手段的迅速发展和对安全防范理解的误区造成了目前的问题。

在网络出现的初期，网络应用十分简单，如 FTP，MAIL 等很多都是简单的协议，而且是“一次性”交互，只是简单的传递信息。随着网络技术的普及和发展，网络上承载的应用越来越多，应用越来越复杂，针对应用层的攻击越来越多。

当前的企业网络正在面临着 Web 滥用、病毒泛滥和黑客攻击等安全问题，这些问题直接导致企业生产力下降。尽管大多数企业都安装了防火墙，但是攻击者知道正面攻破防火墙十分困难，于是从简单的端口扫描攻击转向通过应用层协议进入企业内部。具体来说，通过 Web、Web 邮件、聊天工具和 P2P 攻击企业网络。

几乎所有的企业防火墙都会打开 Web 端口，攻击者想方设法将病毒隐藏在下载软件或网页的恶意代码中，使不知情的用户执行了下载文件或恶意代码之后就会感染病毒。有的恶意代码还弹出欺骗性的提示信息引诱用户执行，这种方式非常隐蔽，并且能绕过防火墙过滤以及防毒机制的扫描。尽管企业能够防止病毒通过 SMTP 传播，但很多用户利用基于 Web 的邮件服务(如 hotmail、Yahoo)发送或接收文件，避开 SMTP 邮件扫描系统。

目前，利用网上随处可见的攻击软件，攻击者不需要对网络协议的深厚理解基础，即可完成诸如更换 web 网站主页，到取管理员密码，破坏整个网站数据等等攻击。而这些攻击过程中产生的网络层数据，和正常数据没有什么区别。

防火墙

防火墙技术发展已经非常成熟，也是目前网络安全技术中最实用和作用作大的技术。防火墙工作在网络层，完成下面的功能：

- ü 状态检测——这是非常有用和重要的功能，通过使用状态检测技术，可以实现单向的通讯保护。

- ü 地址转换——通过地址转换实现对内部地址的隐藏和保护
- ü 访问控制——实现网络层的访问控制，可以根据报文协议头部的信息实现对报文的过滤控制

使用代理的防火墙还能够完成对所代理协议的验证和加固保护功能，防止防火墙后面的协议漏洞暴露在攻击者面前。目前出现的集成杀毒的复合型防火墙能够检测流量中的附件是否感染病毒。

但是，作为目前应用最为广泛的 **http** 服务器等应用服务器，通常是部署在防火墙的 **DMZ** 区域，防火墙完全向外部网络开放 **http** 应用端口，这种方式对与 **http** 应用没有任何的保护作用。即使使用 **http** 代理型的防火墙，防火墙也只是验证 **http** 协议本身的合法性，完全不能理解 **http** 协议所承载的数据，也无从判断对 **http** 服务器的访问行为是否合法。一个最简单的例子就是在请求中包含 **SQL** 注入代码，或者提交可以完成获取他人用户认证信息的跨站脚本，这些数据不管是在传统防火墙所处理的网络层和传输层，还是在代理型防火墙所处理的协议会话层，都会认为是合法的。

明白了防火墙的工作原理，对于应用层攻击，传统防火墙显得无能为力也就不会感到奇怪了。

入侵检测

目前最成熟的入侵检测技术就是攻击特征检测。入侵检测系统首先建立一个包含目前大多已知攻击特征的数据库，然后检测网络数据中的每一个报文，判断是否含有数据库中的任何一个攻击特征，如果有，则认为发生响应的攻击，否则认为是合法的数据。

入侵检测系统作为防火墙的有利补充，加强了网络的安全防御能力。但是，入侵检测技术的作用存在一定的局限性。由于需要预先构造攻击特征库来匹配网络数据，对于未知攻击和不能有效提取攻击特征的攻击，入侵检测系统不能检测和防御。另外就是其技术实现的矛盾，如果需要防御更多的攻击，那么就需要很多的规则，但是随着规则的增多，系统出现的虚假报告（对于入侵防御系统来说，会产生中断正常连接的问题）率会上升，同时，系统的效率会降低。

对于应用攻击，入侵检测系统可以有效的防御部分攻击，但不是全部。

应用防火墙

网络面临的许多安全问题单靠防火墙是无法解决的，必须通过一种全新设计的高性能安全代理专用设备来配合防火墙。具体来说，利用防火墙阻挡外面的端口扫描攻击，利用应用安全防护技术，深层管理和控制由用户访问外部资源而引起的应用层攻击，解决针对应用的、具有破坏性的复杂攻击。

目前的应用防火墙实现了对网络应用保护，是传统安全技术的有效补充。应用防火墙可以阻止针对 Web 应用的攻击，而不仅仅是验证 Http 协议。这些攻击包括利用特殊字符或通配符修改数据的数据攻击，设法得到命令串或逻辑语句的逻辑内容攻击，以及以账户、文件或主机为主要目标的目标攻击。应用防火墙可以有效的阻止下列的应用攻击：

Top Vulnerabilities in Web Applications 2004		
A1	Unvalidated Input	Information from web requests is not validated before being used by a web application. Attackers can use these flaws to attack backend components through a web application.
A2	Broken Access Control	Restrictions on what authenticated users are allowed to do are not properly enforced. Attackers can exploit these flaws to access other users' accounts, view sensitive files, or use unauthorized functions.
A3	Broken Authentication and Session Management	Account credentials and session tokens are not properly protected. Attackers that can

		compromise passwords, keys, session cookies, or other tokens can defeat authentication restrictions and assume other users' identities.
A4	Cross Site Scripting (XSS) Flaws	The web application can be used as a mechanism to transport an attack to an end user's browser. A successful attack can disclose the end user's session token, attack the local machine, or spoof content to fool the user.
A5	Buffer Overflows	Web application components in some languages that do not properly validate input can be crashed and, in some cases, used to take control of a process. These components can include CGI, libraries, drivers, and web application server components.
A6	Injection Flaws	Web applications pass parameters when they access external systems or the local operating system. If an attacker can embed malicious commands in these parameters, the external system may execute those commands on behalf of the web application.
A7	Improper Error Handling	Error conditions that occur during normal operation are not handled properly. If an attacker can cause errors to occur that the web application does not handle, they can

		gain detailed system information, deny service, cause security mechanisms to fail, or crash the server.
A8	Insecure Storage	Web applications frequently use cryptographic functions to protect information and credentials. These functions and the code to integrate them have proven difficult to code properly, frequently resulting in weak protection.
A9	Denial of Service	Attackers can consume web application resources to a point where other legitimate users can no longer access or use the application. Attackers can also lock users out of their accounts or even cause the entire application to fail.
A10	Insecure Configuration Management	Having a strong server configuration standard is critical to a secure web application. These servers have many configuration options that affect security and are not secure out of the box.

业界标准的应用防火墙一般采用主动安全技术实现对应用的保护。主动安全技术是指建立正面规则集，也就是说明哪些行为和访问是合法的规则描述。对于接收到的应用数据（从网络协议还原出来的应用数据，不是数据报文头），判断是否符合合法规则。因为只允许通过已知的正常数据，这种方式可以防御所有的未知攻击。

下表是应用防火墙技术和传统安全产品功能的比较：

攻击类型	防火墙	入侵检测	应用防火墙
------	-----	------	-------

Unvalidated Input	不能防御	部分防御	全部防御
Broken Access Control	不能防御	不能防御	全部防御
Broken Authentication and Session Management	不能防御	不能防御	全部防御
Cross Site Scripting (XSS) Flaws	不能防御	部分防御	全部防御
Buffer Overflows	不能防御	部分防御	全部防御
Injection Flaws	不能防御	部分防御	全部防御
Improper Error Handling	不能防御	不能防御	全部防御
Insecure Storage	不能防御	不能防御	全部防御
Denial of Service	部分防御	部分防御	全部防御
Insecure Configuration Management	部分防御	部分防御	全部防御
Unknown Attacks	不能防御	不能防御	全部防御

应用防火墙技术是现有网络安全架构的一个重要的补充,并不是取代传统防火墙和入侵检测等安全设备。传统安全设备阻挡攻击者从正面入侵,着重进行网络层的攻击防护;而应用防火墙着重进行应用层的内容检查和安全防御,与传统安全设备共同构成全面,有效的安全防护体系。