防火墙技战法

从2016年开始，一场由公安部组织的网络安全攻防演练，目的是针对全国范围的真实网络目标为对象的实战攻防活动，旨在发现、暴露和解决安全问题，

检验我国各大企事业单位、部属机关的网络安全防护水平和应急处置能力。参加演练的单位不断增加，一般持续时间2-3周，一般护网演练在白天工作日进行，不过攻击方（红队）会不分昼夜和休息日进行。在以往国家级**“HVV”**行动期间，企业网站每天要遭受成百上千来自红队（攻击方）的网络攻击，在此背景下，防守方（蓝队）的工作就显得尤为困难，所以此时如果有一面很好的**“盾牌”**那无疑会给防守带来很大帮助，而防火墙、IPS\IDS无疑就是那面盾牌，今天就防火墙来着重讲一下。

一、黑名单

黑名单，指根据报文的源 VPN 和源 IP 地址进行过滤的一种方式。同 ACL 相比，由于进行匹配的域非常简单，可以以很高的速度实现报文的过滤，从而有效地将特定 IP 地址发送来的报文屏蔽，同时支持用户静态配置黑名单和防火墙动态生成黑名单。

**黑名单的特点**

防火墙的黑名单，其实就是用户电脑中安装的防火墙有阻止某些网络用户，或者网络IP进入此电脑的一种功能，只要用户在防火墙中设置了黑名单，一般来说，除非此网络用户可以破解用户的防火墙，否则来说，很难进入到电脑中，攻击用户的电脑，或者跟用户的电脑联网。所以通常来讲，HVV中采用防火墙封堵优先级。

防火墙除了有添加黑名单以外，还具有添加白名单的功能，顾名思义，白名单就是黑名单的对立面，是电脑用户设置的，认为可以添加信任的网络用户以及网络地址，在添加白名单后，防火墙会略过用户设置的白名单，一旦这些白名单中含有病毒，那么用户就会受到病毒的攻击。

攻击者的 IP 地址在黑名单中，从攻击者发出的所有报文都会被防火墙丢弃。

综上所述，它在HVV中的效果和作用无疑是非常重要且明显的。

**设备对黑名单的支持**

除了用户可以静态配置黑名单外，当设备发现特定 IP 地址在进行 IP 扫描攻击或端口扫描攻击时，会将发起攻击的 IP 主动插入到黑名单中。如果黑名单已使能的话，在此后的一定时间内，来自这个 IP 地址的任何报文，都可以被黑名单过滤掉。

用户可以配置静态和动态黑名单的老化时间。

无论命中了黑名单的数据包是否为 ACL 规则允许的访问，防火墙对此类数据包予以丢弃。

用户可以将黑名单配置信息导出到文件中，也可以通过文件导入黑名单配置。

1. 白名单

使用源 VPN 和 IP 地址来表示一个白名单项。白名单主要用在网络上的特定设备发出的合法业务报文具备 IP 扫描攻击和端口扫描攻击特性的场合，防止该特定设备被防火墙加入黑名单。

白名单只有静态的。

**白名单的特点**  
如果用户将某个主机的 VPN 和 IP 地址加入防火墙白名单，防火墙就不会对该主机发出的报文进行 IP 扫描攻击和端口扫描攻击检查，也不会将其 IP 地址生成动态黑名单，也不允许用户将白名单主机添加到静态黑名单中。

**设备对白名单的支持**  
当设备收到一个报文后，就会检查是否是来自于白名单项的报文。如果是，设备对该报文就不会进行 IP 扫描攻击和端口扫描攻击检查，也不会将源 IP 生成动态黑名单，但是其他安全过滤功能，比如 ACL 包过滤、 ASPF、流量统计和监控等，还是要进行，以达到防火墙的最大安全过滤效果。  
用户可以配置白名单的老化时间。  
用户可以将白名单配置信息导出到文件中，也可以通过文件导入白名单配置。

**黑、白名单的区别**

名单的概念与“黑名单”相对应。例如：在电脑系统里，有很多软件都应用到了黑白名单规则，操作系统、防火墙、杀毒软件、邮件系统、应用软件等，凡是涉及到控制方面几乎都应用了黑白名单规则。黑名单启用后，被列入到黑名单的用户（或IP地址、IP包、邮件、病毒等）不能通过。如果设立了白名单，则在白名单中的用户（或IP地址、IP包、邮件等）会优先通过，不会被当成垃圾邮件拒收，安全性和快捷性都大大提高。将其含义扩展一步，那么凡有黑名单功能的应用，就会有白名单功能与其对应。

白名单是设置能通过的用户，白名单以外的用户都不能通过。 黑名单是设置不能通过的用户，黑名单以外的用户都能通过。 所以多数情况下白名单比黑名单限制的用户要更多一些。

**黑、白名单的划分**

其实黑名单就是通过防火墙、IPS/IDS等设备查看出来的有恶意攻击手段的IP，通常此类IP不会单独只有一两次请求，大多都是某个时间段内大量的请求，又比如常见的红队IP阿里IP，而白名单就是客户资源池内或者客户内部自己使用的IP。

# 三、流量统计及监控 防火墙不仅要对数据流量进行监控，还要对内外部网络之间的连接发起情况进行检测，进行大量的统计计算与分析。防火墙的统计分析一方面可以通过专门的分析软件对日志信息进行事后分析，另一方面，防火墙系统本身可以完成一部分分析功能，具有一定的实时性。

比如，通过分析外部网络向内部网络发起的 TCP/UDP 连接数是否超过设定阈值，可以确定是否需要限制该方向发起新连接，或者限制向内部网络某一 IP 地址发起新连接。

防火墙的一个典型应用示例，当启动了外部网络到内部网络的基于 IP 地址的统计分析功能时，如果外部网络对 Web 服务器 129.1.9.1 发起的 TCP 连接数超过了设定的阈值，将限制外部网络向该服务器发起新连接，直到连接数降到正常范围。

**四、防火墙日志** 防火墙可以实时记录防火墙的动作和状态（例如实施了某种防火墙措施、检测到某种网络攻击等），并将信息记录到日志中。

对日志内容的分析和归档，能够使管理员检查防火墙的安全漏洞、何时何人试图违背安全策略、网络攻击的类型，实时的日志记录还可以用来检测正在进行的入侵。

当需要对防火墙的动作和状态进行记录，以便检查防火墙的安全漏洞、检测网络攻击和入侵等，可以配置防火墙日志功能。

**设备对防火墙日志的支持**

**黑名单日志**设备在发现有地址扫瞄、端口扫瞄等攻击的时候，在黑名单使能的情况下会动态生成黑名单日志。  
手动加入的黑名单同样也会生成黑名单日志。  
动态生成的黑名单、手动加入的静态黑名单到老化时间之后，会生成解除黑名单日志。

**攻击日志**

设备发现各种攻击类型后，会生成攻击日志，记录攻击类型和参数。

**流量监控日志**  
当系统全局、区域出入的会话数超过所配置的连接数阈值上限时，设备会生成流量监控日志，当会话数低于所配置的连接数阈值下限时，设备会生成流量恢复日志。

**流日志**  
设备的流日志是在会话表老化的情况下，封装流日志信息，发送到日志服务器。