防火墙架构

防火墙架构

企业的防火墙设计和安装是一项艰巨的工作。在设计过程中对防火墙的选择在以后的多年中对安全的意义深远。在这一系列文章中，我们将详细探讨防火墙的安装，希望对防火墙设计的过程会有帮助。

我们将会分四个部分来探讨。

如何选择防火墙

尽管新的安全技术不断发展进化，防火墙仍然是网络结构的关键部分。目前，企业可选择的防火墙种类很多。本小节将列出选择适合企业网络安全需要的防火墙时的五个常见问题。

- ❖ 如何选择防火墙

如何选择防火墙拓扑结构

当为一个企业开发边界保护策略时，最常见的问题是“我应该把防火墙设置在哪里，以发挥其最大效用？”本小节将介绍三种最常见的防火墙拓扑结构，包括防御主机，屏蔽子网和双重防火墙结构。

- ❖ 防火墙拓扑结构选择

如何在防火墙拓扑结构中配置系统

一旦你决定了哪一种拓扑结构最适合你的 IT 架构，就需要决定在选种的拓扑结构中系统的位置。本小节将介绍在防火墙拓扑结构中系统的位置，比如在防御主机，屏蔽子网和多宿防火墙等拓扑结构中的位置。

- 在防火墙拓扑结构中配置系统

如何利用防火墙日志功能

迅速而频繁的改变配置使得日常维护任务变得很难。在这篇文章中，我们将探讨防火墙日志功能，来维持良好的状态。

- 防火墙行为审计

如何选择防火墙

现在市场上有一些不同种类的防火墙。为你的组织选择一种防火墙是一项令人望而却步的工作——尤其是为一个充斥着流言和专利商标的行业。我们来看一下防火墙技术的基本知识以及为公司选择防火墙时，你可能会问到的五个问题。

1．为什么要使用防火墙？当然，这可能听起来似乎是一个简单的问题。你可能自己会解答，“因为我们需要！”但是重要的是你花费时间确定使用防火墙的技术目标。这些目标会决定选择过程。当一种简单的产品就能满足你的技术要求时，你就不想选择一种昂贵的、而功能丰富到迷惑管理员的防火墙。

2．防火墙如何能适合你的网络拓扑结构？这种防火墙是否存在于整个网络的周界，并直接与因特网相连接，或者是否适合公司其它地方的敏感局域网分段？它可以处理多大流量？它需要多少界面来分割流量？诸如这些的性能要求大大增加了推行新防火墙的总成本，这很容易造成购买产品的不足或过剩。

3．你需要运行哪种类型的流量检测器？流言就是从这里开始的。每个厂商对其流量检测技术都有一个不同的商标，但是基本上有三个不同的选择（按照复杂度和成本排序）：

- **封包过滤防火墙**（屏障式路由器防火墙）使用简单的规则，对遇到的每个数据包，按其本身的特点进行评价。它们不保存每个数据包的记录历史，进行基本的数据包组头检测。这种检测的简单性加快了其速度。这种防火墙是最便宜的选择，但同时他们也是最不灵活和漏洞最多的。你的运气比较好就是你已经拥有了可以运行封包过滤防火墙的设备——那就是你的路由器！
- **状态检测防火墙**（动态过滤包防火墙）更进了一步。它们跟踪三向 TCP 同步交换，确保数据包始终属于一个已建立的网段（比如，就没有设置 SYN 特征位），

以对防火墙检测到的上一个活动做出反应。开放最初连接的要求，受到了状态检测防火墙规则数据库的限制。

- **应用代理防火墙**拥有最高级的性能。在状态检测防火墙的基础上，它们突破了客户机与服务器之间的连接。客户机与防火墙相连，防火墙可以分析请求（包括数据包内容的应用层检测）。如果防火墙的规则显示信息传输可以进行，那么防火墙就会与服务器建立连接，继续在通信过程中扮演的媒介的角色。当防火墙与网络地址翻译协议（Network Address Translation）相结合时，这两个主机甚至都不会防范其它主机的存在——它们都相信它们正在直接与防火墙交流。

4．你的公司更适合采用设备解决方案还是软件解决方案？

设备一般更易于安装。一般情况下你只要插进合适的以太网电缆，进行基本的网络配置，就准备好配置防火墙规则了。另一方面，软件防火墙比较难安装，并且需要调节。它们也缺少防火墙操作系统通常所固有的安全性。如何权衡？你可以猜一下！设备更昂贵一些。

5.哪种操作系统最能满足你的要求？

即使设备可以运行操作系统，在你防火墙管理职业生涯中，你有时可能会需要使用该操作系统。如果你是Linux系统操作员，你可能不想选择一种基于 Windows系统的防火墙。另一方面，如果你不了解/var/log的/dev/null， 你就可能想要避开使用基于Unix系统的解决方案。

虽然，我不知道你的需求，就不能给你建议一种具体的防火墙，但是回答这些问题的过程可以帮助你打定主意，做出正确的选择。有了这些答案，在选择购买防火墙时，你应该能够明智地评价当前市场上各种产品的成本/优点了。

(作者：Mike Chapple 译者：李娜娜 来源：TT中国)

防火墙拓扑结构选择

当为一个企业开发边界保护策略时，最常见的问题是“我应该把防火墙设置在哪里，以发挥其最大效用？”在本节中，我们会探讨一下三个基本的选择，并分析每种情况下的最佳模式。

我们开始之前，请注意本节中我们只处理防火墙的设置问题。无论谁想要建立一个边界保护策略，都应该计划采用一个深度防御方法，该方法可以利用包括防火墙、带有封包过滤功能的边界路由器以及入侵探测系统等的多种安全设备。

第一种选择：防御主机

第一种最基本的选择是使用防御主机。在这种设置中（下图 1 所示），防火墙设置在因特网和受保护网络之间。它可以过滤所有进入或离开网络的流量。

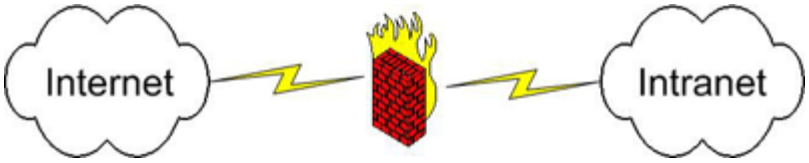

图 1：防御主机

防御主机拓扑结构适合于相对简单的网络（比如，那些不提供任何公共因特网服务的网络。）要切记的关键因素是它仅提供一个单一的边界。一旦有人设法渗透到边界之中，那么他们就已经可以不受任何限制地（至少从边界保护的角度来说）进入到受保护的网络之中。如果你仅仅使用防火墙来保护整主要用来上网的企业网络，这种设置是可行的。但是，如果你的主机是 Web 站点或 e-mail 服务器，这种配置就不够用了。

第二种选择：屏蔽子网

第二种选择是使用一种屏蔽子网，比防御主机方法而言，可以提供更多的优点。这种方法使用带有三个网卡的单一防火墙（通常是指三宿主机防火墙）。这种拓扑结构的一个例子如图 2 所示。

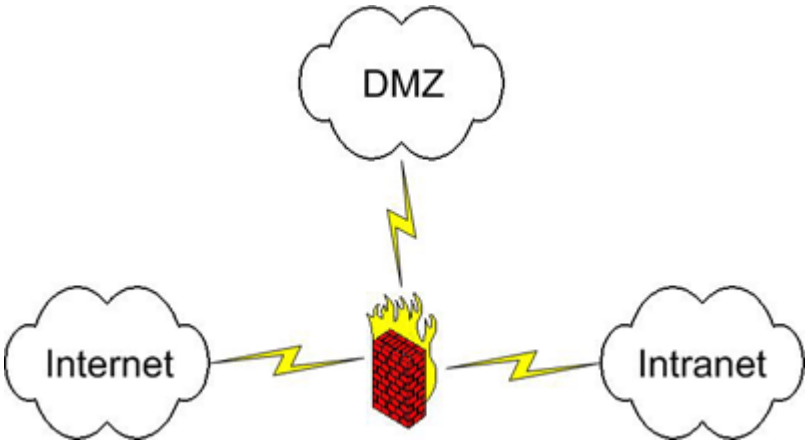

图 2：屏蔽子网

屏蔽子网提供了这样一种解决方案：企业可以为因特网用户安全地提供服务。任何负责公共服务的服务器都被设置在隔离区(DMZ)，隔离区是被防火墙分割开因特网和所信任的网络。因此，如果恶意用户设法攻破防火墙，他或她也无法进入企业内部的互联网（前提是正确配置防火墙）。

第三种选择：双重防火墙

最安全（也是最贵的）选择是在采用两个防火墙的屏蔽子网，。这种情况下，隔离区（DMZ）设置在两个防火墙之间，如图 3 所示。

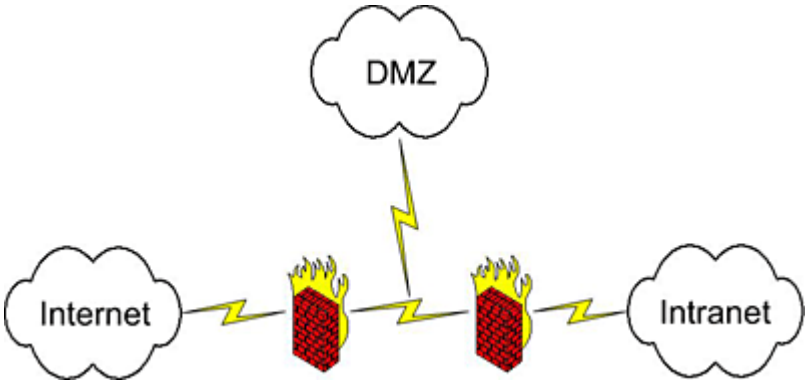

图 3：双重防火墙

使用双重防火墙，公司还可以通过 DMZ 为因特网用户提供服务，但是需要增加一层保护。安全架构师从两个不同的经销商的防火墙技术，然后用来实施这一计划，这种情况相当常见。当恶意个人发现某个软件有可以利用的漏洞时，这种做法就增强了安全性。

高端防火墙在这些方面也有一些变化。基本的防火墙模式通常有三界面界限，高端防火墙则可以有许多物理和虚拟界面。比如，Secure Computing 公司的 Sidewinder G2 防火墙可以有 20 个物理界面。通过使用 VLAN，标记物理界面，就可以增加额外的虚拟界面。这对你来说意味着什么？有了大量的界面，你就可以在网络中采用不同的安全区。比如，你可能会有下面的界面配置：

- 安全区 1：因特网
- 安全区 2：受限工作站
- 安全区 3：普通工作站
- 安全区 4：公共隔离区
- 安全区 5：内部隔离区
- 安全区 6：中心服务器

这种构架中，你可以使用任何一种上述三种拓扑结构，并有了极大地灵活性。

这是关于防火墙构架的简单入门知识。现在你已经掌握了基本概念，那么你就能够在不同情况下，帮助选择合适的防火墙拓扑结构。

(作者：Mike Chapple　译者：李娜娜　来源：TT 中国)

在防火墙拓扑结构中配置系统

在前面的文章中，我们探讨了选择防火墙拓扑结构的基础知识。我们讲到了防御主机，屏蔽子网和更安全的多防火墙结合之间的区别。一旦你决定了哪一种拓扑结构最适合你的 IT 架构，就需要决定在选种的拓扑结构中系统的位置。

在我们讨论的这个话题时，我们将会使用安全区的概念，详细说明我们的要求。处于我们的目的，要考虑一个安全区，将所有系统和防火墙的单个界面连接起来，直接连接或者通过非防火墙的网络设备。

防御主机

首先，我们看一个最简单的例子：防御主据。在这种情况下，所有进入或离开网络的流量都通过防火墙，而且只有两个界面：直接和因特网连接的公共界面以及和企业内网连接的私密界面。这使我们要考虑两个安全区，安置系统就很简单了。我们只要简单地把所有我们想要保护地系统放到私密区。

在防御主机的拓扑结构中，我们假定，你不打算对因特网提供任何公共服务。如果确实需要提供公共服务（比如 DNS，SMTP 和 HTTP），就应该严肃地考虑使用替补的拓扑结构。如果不可能，就要面对一个艰难的选择：应该把公共服务器放在公共区还是私密区？如果放在公共区，他们就不能获得来自防火墙的任何保护，就更容易受到攻击。另外一方面，如果放在私密区，在公共服务器受到攻击的情况下，就会增加其他更多的敏感系统被攻击的可能性。在作决定时，需要认真平衡风险和优点。

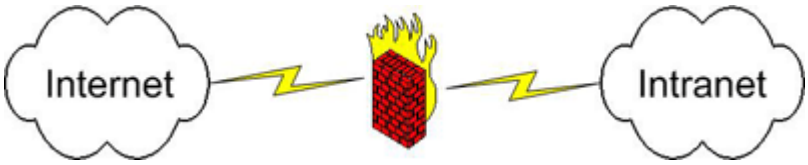

图 1：防御主机

屏蔽子网

屏蔽子网是应用最广泛的防火墙拓扑结构，它在某种程度上也很直接。我们增加一个附加区，也就是屏蔽子网（或者 DMZ），它包含所有提供公共服务的主机。在这种情况下，公共区就直接和因特网连接，并且没有受企业控制的主机。私密区的包含因特网用户没有商业性访问的系统，例如，用户工作站，内部文件服务器和其他非公共设备。DMZ 包含所有可能向因特网提供服务的系统。这个区包含公共的应用服务器，SMTP 服务器，DNS 服务器和其他类似的服务器。你的 IMAP/POP 服务器可能在这个区，也可能不在，这取决于你的安全策略。

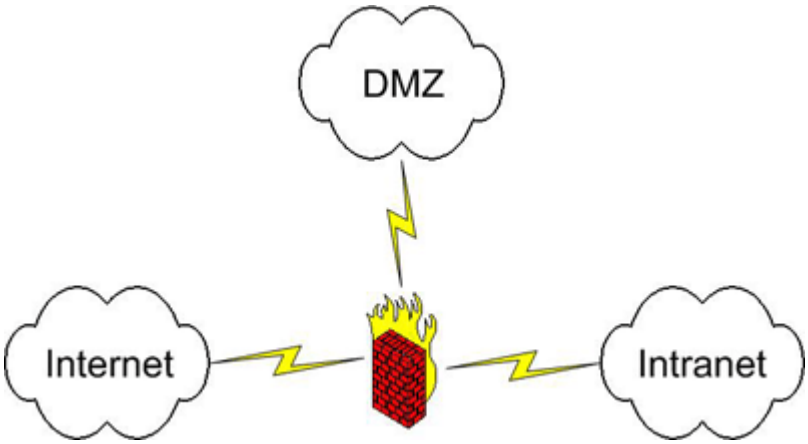

图 2 ：屏蔽子网

多宿防火墙

最后一种情况，有多于 3 个界面的多重防火墙，它是最有意思的挑战。在这种情况下，有不止 3 个区，所以就有了大量更加细分的系统。必须使这些细分的系统在企业中基于详细的安全目标。要做的分区之一是把工作站放入不同的区域，便于隔离敏感系统。例如，你可能把所有的属于会计的系统放在一个区中，而把行政工作站放在另一个区中，其他的工作站放在第三个区中。你可能还想区分为因特网提供服务的系统。例如，向一般公众提供服务（比如公司网站）的系统可能和只向注册用户（比如 Web 邮件服务器）提供服务的系统放在不同的区域。

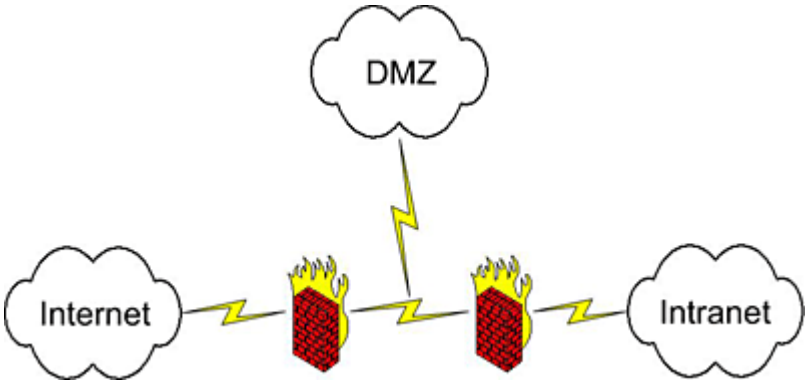

图 3：多宿防火墙

最后，决定还要你来做。既然你已经读了这篇文章了，脑子里就应该有很多想法了吧。坐下来，写到纸上，和同事讨论一下这些选择，再开发适合你的企业的系统布置策略。

（作者：Mike Chapple　译者：Tina　来源：TT 中国）

防火墙行为审计

一旦你通过了防火墙的选择和架构设计阶段的挑战，你就安装了 DMZ，对吧？你的 Rulebase 应该还很稳定，永远也不需要改变配置。我们只能梦想！在实际的防火墙管理中，我们面对的是持续的改变要求和厂商对我们的防火墙可执行操作的补丁之间的平衡。迅速而频繁的改变配置使得日常维护任务变得很难。在这篇文章中，我们将探讨防火墙日志功能，以维持良好的状态。

我们来看四的实际的部分，在这里基础的日志分析可以提供有价值防火墙管理数据：

1. 监测规则行为

系统管理员趋向于尽快了解新规则，但是在一条规则不再需要的时候，他们就不着急让你知道了。监测规则行为可以提供一些有价值的信息，协助管理 Rulebase。如果一条频繁使用的规则突然之间变得安静了，就应该研究一些这条规则是否还需要。。如果不再需要了，就从 Rulebase 中把它删除。遗留下来的规则堆积起来，会增加不必要的复杂性。这些年，我有机会分析很多防火墙产品的 Rulebase，我估计至少 20%的一般防火墙的 Rulebase 都是不必要的。我见过这个比例高达 60%的系统。

2. 流量

还要监控不正常流量日志。如果一个服务器通常的流量很低，突然要负担通过放火墙的大部分流量（不管是在整个链接中，还是通过的字节），那么就需要深入研究一下了。如果在有些情况下，预料到会出现“flash crowds”，他们通常是系统错误配置或进程攻击的征兆。

3. 违反规则

插卡防火墙拦截的流量，可能会发现有趣的信息。这一点对于来自网络内部的流量尤其准确。这种活动的通常原因是系统错误配置或者用户不知道流量限制，但是违反规则分析也可能会发现企图通过设备的恶意流量。

4．拒绝探针

如果你曾经分析过连接到互联网的防火墙的日志，就会知道研究从互联网直接连到你的网络的探针是没有用的。它们太过频繁了，经常出现死胡同。尽管如此，你可能没有考虑过分析来自内部可信赖网络的探针日志。这些机器有趣，应为他们最可能出现的是被攻击的系统探求扫描互联网主机，或者内部用户正在运行扫描工具。这两种情况都值得关注。

你的防火墙审计日志是真正的网络安全的金矿。使用审计日志，会对你有帮助的。

(作者：Mike Chapple　译者：Tina　来源：TT 中国)