构建 DMZ 保护网络安全

构建 DMZ 保护网络安全

DMZ（Demilitarized Zone）即俗称的隔离区或非军事区，与军事区和信任区相对应，作用是把 WEB，e-mail，等允许外部访问的服务器单独接在该区端口，使整个需要保护的内部网络接在信任区端口后，不允许任何访问，实现内外网分离，达到用户需求。DMZ 可以理解为一个不同于外网或内网的特殊网络区域，DMZ 内通常放置一些不含机密信息的公用服务器，比如 Web、Mail、FTP 等。

DMZ 基础知识

网络 DMZ 通过创建屏蔽子网，将受信任网络从不受信任网络中区分出来，并进行隔离。通过将系统分段，并创建只有中间层次的信任存在的 DMZ，该系统对连续攻击具有更强劲的抵抗力，即使在其它部分都无法正常工作的情况下也能保护重要资源。DMZ 可以发挥作用，是因为在没有路由的情况下，网络流量不能在两个分支网络之间传输。

- 分而克之——DMZ 作用解析

DMZ 的构建

DMZ 的构建，可以保护内网安全。本小节将讨论如何构建稳定而安全的 DMZ。

- 如何配置执行 DMZ
- 如何建立稳定的 DMZ
- 设计不同访问级别的 DMZ
- 单一防火墙的 DMZ 还是双重防火墙的 DMZ?

DMZ 具体应用

DMZ 内通常要放置一些不含机密信息的公用服务器和其他应用程序等，那么应该如何具体应用呢，本节以 VPN 和服务器为例介绍 DMZ 的具体应用。

- DMZ 和 VPN 如何共存？
- 服务器配置在 DMZ 外部
- 采用 Windows 认证访问 Linux DMZ

DMZ 应用中存在的风险

虽然 DMZ 的设置可以保护内网安全，但是处于某些特殊的需要而做的某些设置仍会带来风险。

- 在 DMZ 中放置企业用户有什么风险
- 在 DMZ 中放置邮件服务器的风险

分而克之——DMZ 作用解析

网络 DMZ 通过创建屏蔽子网，将受信任网络从不受信任网络中区分出来，并进行隔离。通过将系统分段，并创建只有中间层次的信任存在的 DMZ，该系统对连续攻击具有更强劲的抵抗力，即使在其它部分都无法正常工作的情况下也能保护重要资源。DMZ 可以发挥作用，是因为在没有路由的情况下，网络流量不能在两个分支网络之间传输。

你的 Web 服务器、FTP 服务器、电子邮件服务器以及内部 DNS 服务器应当配置在这个 DMZ 内，或者“边界网络”中，还需要有额外的网络防御，比如入侵检测系统（IDS）。将这些公共服务安置在 DMZ 内，你就可以把这些安置在与你的内部网络不同的支网中。诸如数据库服务器之类的后端系统应当设置在内部网络之中。任何配置在 DMZ 的机器仍然处在危险之中，但是如果一个入侵者危及 DMZ 的安全，那么他就不能自动进入内部网络。

DMZ 的每个访问接入点都对网络流量进行阻挡和过滤，仅允许去往或来自特定网络地址、经由特定端口的活动通过。应当非常小心，确保与 DMZ 的交互行为不暴露在内部网络中。每一网段之间的障碍受到防火墙和路由器的控制和屏蔽，并受到文件访问控制列表、功能强大的认证与加密技术的保护。为了最终实现 DMZ 的安全，将每项服务设置在自己的 DMZ 段，配置防火墙策略来满足每个服务器的要求。

网络布置

我们将探讨两种 DMZ 网络布置方式。第一种是三宿主边界网络，它适合于低预算、不能与关键内部网络相连接的 Web 站点。第二种是背靠背边界网络，它用于电子商务和其它关键任务的 Web 站点。

三宿主边界网络

这个拓扑结构使用单一的防火墙将因特网、边界网络和企业内网隔离开来。通常也称为单一屏蔽式子网，由于 DMZ 是由一个带有三个网卡的防火墙限定范围的：一个网卡与因特网相连接、一个与 DMZ 连接、一个与企业内网连接（见图 1）。这种网络布置的缺点是单一故障点。当端口对由单一防火墙护卫的边界网络开放时，不可避免地减弱了边界安全性。如果入侵者危及这种拓扑中的防火墙，那么他就既可以进入 DMZ 的服务器，也可以进入企业的内网的服务器。

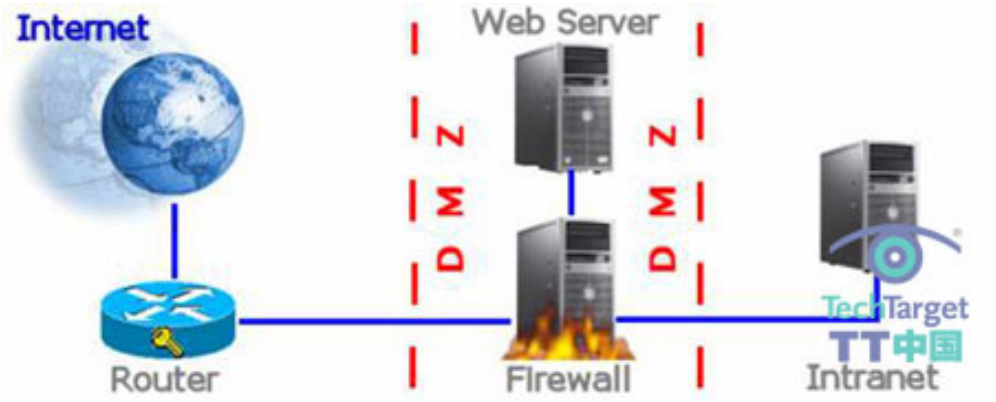

图 1　三宿主边界网络

需要注意的是，这种拓扑结构详细说明了如何使用因特网和 DMZ 之间的安全路由器。应当锁定该路由器上的端口。为了保证 Web 服务器的正确功能，需要打开一些端口，比如用于 HTTP 的端口 80 和 HTTPS 的端口 443。

背靠背边界网络

图 2 中显示的是背靠背边界网络拓扑结构，它被广泛认为是最安全的网络布置之一。边界网络使用两个防火墙，一方面与因特网分离开来，另一方面与内部网络区分开来。每个防火墙有两个网络适配器。当内部防火墙有一个网络适配器与边界网络相连接，并且另一个与内部网络相连接时，外部防火墙有一个网络适配器与因特网相连接，另一个与边界网络相连接（如图 2 所示）。这就提供了一层额外保护。如果一个来自因特网的入侵者危及到边界网络的安全，他不能自动访问内部网络资源，因为在入侵者和网络其余部分之间有另一道屏障。

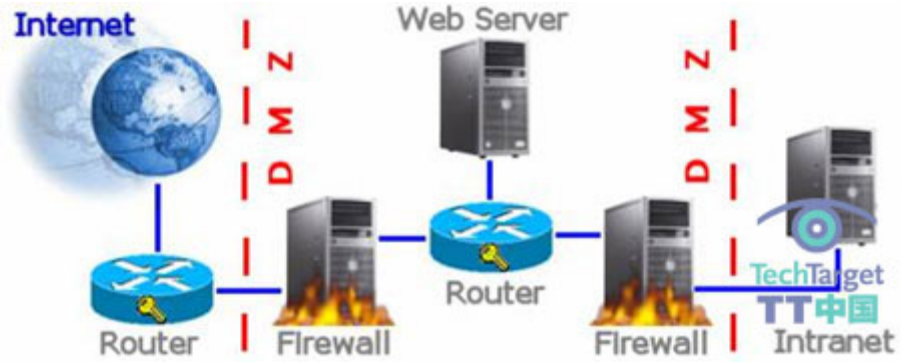

图 2　使用两个防火墙的双重屏蔽子网或背靠背边界网络

请注意，另一个安全路由器将网络分割成不同的部分，这些部分组成整个外围网络。尽管锁定这个路由器没有锁定与因特网连接的路由器重要，但是也可以确保关闭不重要的端口，以获得更多的安全。

外部防火墙可以阻止外部攻击，并管理所有进入 DMZ 的因特网访问。内部防火墙管理进入内部网络的 DMZ 访问。与面对因特网的防火墙规则相比，这个防火墙应当拥有不同的规则，仅允许内部具体应用服务访问进入特定的系统，并阻止自发输入端口 80 的网络流量进入内部网络。换句话说，内部防火墙应当仅传递来自 DMZ 服务器的、需要与某个内部系统进行通信的输入流量。比如，如果一个 Web 服务器通过 SQL 与数据库通信时，打开防火墙的 TCP 端口，传递 SQL 请求和响应，并且阻止其它任何流量。当构成防火墙的不同部分用在 DMZ 的每一边时，安全性得到进一步增强。黑客不太可能使用相同的方式对两个系统进行攻击。

为了安全起见，对网络进行分割时，要总是选择物理分割法。虚拟局域网（VLAN）是一个网段，逻辑上由转换器定义并控制，该转换器可以将其端口分配到两个或者更多虚拟局域网段，而不是将其所有端口分配到同一个物理网段。尽管这样可以降低购买多个交换器的成本，但分割的网段是虚拟的。可以删除这种分割，并且很容易就可以绕过交换器所提供的安全。

（作者：Michael Cobb　译者：李娜娜 来源：TT 中国）

如何配置执行 DMZ？

问：设置 DMZ 有什么局限？需要什么样的工具？

答：DMZ（demilitarized zones）是和中立面的网络对等。他们为面向公众的服务提供独立的网络分段，例如 Web 和邮件服务。保护你的网络中的私密内容不向这些服务器公开，因为公众可以访问这些服务器，使他们更容易受到攻击。

创建DMZ的标准方法包括使用有三个网络界面的放火墙。更多内容和解释请阅读《选择合适的放火墙拓扑结构》（链接：http://www.searchsecurity.com.cn/showContent_6466.htm）。

（作者： Mike Chapple 译者：Tina 来源：TT 中国）

如何建立稳定的 DMZ

问：可以保护 DMZ 网络应用服务器和 Web 服务器的机制有哪些？处于这样的目的，可以使用什么软件产品？

答：你的问题很重要。我是“深度防护”概念的忠实信徒。这种原则支持安全分层的方法，这种方法是用许多独立的安全控件，防护任何一层的失败带来的问题。你所问的，从本质上来说，就是“为了弥补网络防火墙，我需要设置那一层的安全措施？”

在建立安全的 DMZ 的时候，有几种值得思考的不同的技术。通常使用的几种有：

- 服务器杀毒软件。杀毒软件非常常见，现在已经不需要考虑，但是它仍然值得提出来。确定所有的服务器上都有活跃的杀毒软件，并且每天都更新 signature files。杀毒软件应该由中央管理，这样在数据中心，就可以完整地看看杀毒环境。
- 入侵检测/防护系统。一个良好的 IDS/IPS 可以监控网络上恶意行为的迹象。在任何层面防护中，它都是重要组件。
- 文件完整性监控软件。绊网（Tripwire），著名的文件文正性监控包，例如，监控文件系统的变化，并把这些变化和企业的安全策略相比较。它可以提醒管理员未经授权的文件变更，这种变更可能是恶意行为的迹象。
- 漏洞扫描系统。它是在 DMZ 中的网络上的“安全巡警”，巡查偶尔没有关闭的大门。漏洞扫描器测试服务期的安全配置，并对潜在漏洞发出警告。

这些是有助于深度防护状态的安全控件的几个例子。还有很多种的可能，你的混合选择取决于你的安全要求和可用资源（财政和人力）。

（作者：Mike Chapple 译者：Tina 来源：TT 中国）

设计不同访问级别的 DMZ

问：我需要为我们本地的不同访问级别的用户，消费者，合作伙伴和应用服务器，设计 DMZ 方面的一些信息。在我的局域网上有超过 1100 个工作站，我也想要为本地的用户定义不同的访问级别。谢谢您的任何指导。

答：通常在任何和互联网连接的公司中，DMZ 是需要设计的第一站。在这个区中，不要设置任何的 e-mail,数据库和对公司来说很重要的其它数据。

设置为认证而连接的服务器。当这些设备通过 DMZ 连接回，比如说数据库区的时候，创建一个只有这些设备的网络子网。这就把其他的内部系统和外部分离开来，并提供分层的方法。现在，任何需要访问，比如 e-mail 和其他数据（共享文档，文件等）的人，要把他们放在远离 DMZ 的另外的网络中。我总是建议在 DMZ 的两面都设置防火墙，并在外部设置 IDS 系统-----一个在 DMZ 内部，一个在数据库区，其他的或多或少都在所有的区中。

安全问题必须要以分层的方法解决。第一步是在流量进入 DMZ 前进行过滤。所以路由器只能把端口 80 和 443 接入 DMZ。然后，DMZ 将只允许 DMZ e-mail，SMTP 中的任何应用程序的流量。不要 FTP,因为它不安全。DMZ 应该只允许后面的通向设备的合法流量。

(作者：Ed Yakabovicz 译者：Tina 来源：TT 中国)

单一防火墙的 DMZ 还是双重防火墙的 DMZ？

对这个问题有所思考的人，估计已经接受了这种想法：使用 DMZ（隔离区或非军事区） 可以为部分的机器提供更安全和强大的保护功能，而不是简单地在整个网络前面放置一个传统的防火墙，将所有的通信都转入内部网络。接受这点观点固然不错，不过，有一个问题：你是采用简单的路由，将 DMZ 区域设置在单一的防火墙一侧呢？还是多花一些钱，实现最大的安全保护，使用两个防火墙，将 DMZ 区域设置在其间?

采用传统的单一防火墙 DMZ 架构，可以合理地保护面向公众的服务器。这些服务器将保护敏感的内部网络不受恶意的外部用户入侵。在这种情况下，防火墙将监视从外部流入的全部通信，以确定这种通信是应该转到 DMZ 网络（至少有一台机器具有转发通信的功能），还是应该传送到受保护的内部网络。同时，传统的 DMZ 还检查从内部网络发往外部网络的全部通信，以确定是否让这种通信通过。一，是否允许要求网络和邮件服务的内部数据包从受保护的内部网络发送到 DMZ 网络；二，是否需要对来自内部请求的应答通过 DMZ 区域进入受保护的网络；三，是否允许这些通信进入互联网。你可能知道这种结构是一种双宿网关结构，因为这种防火墙有两个接口，一个通向 DMZ，另一个通向内部网络。

进一步而言，双重防火墙 DMZ 架构（亦称为子网防火墙）增加了另一个防御层，将内部网络与庞大而邪恶的外部世界隔离开来。通过在面向公众的主机前配置设置一个防火墙和在内部网络前再增加一个防火墙，这样为主机提供进一步的安全保护。使用这种架构，受保护的网络和互联网之间的通信必须要经过这两个防火墙。这些防火墙将为你对外开放的服务器提供最初的第一线防御，防止恶意通信的入侵。

所以，你得自己做出选择，希望下面这些问题能够对你有所帮助：

- 从性能的角度说，你能够承受让外部通信经过两个防火墙而不是一个防火墙而带来的性能损失吗?

- 你能够监视通过这个网络的两个线路的通信吗?
- 你应该从哪里监视该通信?
- 你需要一直拥有从被攻破状态立即恢复到正常状态的能力吗?这种能力应该包括在一个防火墙系统关闭的时候保持另一个防火墙运行和通信畅通。
- 你有必备数量的网络端口吗?
- 你是否有购买两个防火墙的足够预算?或者这项开支不被批准?

总的来说，:传统的 DMZ 结构为提供公共服务的机器增加了一层额外的保护，但是，这需要额外的操作和维护工作。双重防火墙 DMZ 的选择是最安全的，不过，其部署和运行的成本也是最贵的。

(作者：Jonathan Hassell 译者：Shirley 来源：TT 中国)

DMZ 和 VPN 如何共存？

问：如果你有一个 VPN 防火墙路由器，它会受到 DMZ 服务器配置的影响吗？换句话说，DMZ 服务器和 VPN 可以共存吗？

答：DMZ 和 VPN 当然可以共存。实际上，它们是设计在一起工作的。

在典型的防火墙设置情形中，防火墙把网络分为明显的三个区：互联网，专用网和 DMZ。来自互联网的带内连接只允许连到 DMZ 中的服务器上；在互联网和专用网之间不允许直接的连接。提供公共服务的服务器（例如，Web 服务器和 SMTP 服务期）放置在 DMZ 内部，而为互联网用户提供服务的服务则存在于专用网上。

VPN 为远程用户提供了专用资源的访问权。用户经过 VPN 认证，然后就可以通过 VPN 连接访问专用网上的互联网资源。

（作者：Mike Chapple　译者：Tina 来源：TT 中国）

服务器配置在 DMZ 外部

问：我们的 Web、FTP（文件传输协议）和 DNS（域名系统）服务器都是设置在 DMZ 内部的，并且只允许几个特定的端口从外部区域进行访问。如果我还把服务器放在内部，然后允许外部访问端口，这样有什么不同？特别是我们在思科的 PIX 防火墙上使用相同的命令，允许端口从较低的安全区域访问较高的安全区域。

答：不错的问题。把服务器放置在 DMZ 内部，而不是网络内部，是为了防御来自网络内部或外部的攻击。研究表明，大部分的安全事故是由内部引起的。内部和外部的访问使用同样的规则有意义吗？分离服务器和 DMZ 的另外一个原因是，为了帮助保护内部网络。比如，现在，在端口 80 上，有很多的正在运行的攻击，而你需要为 Web 服务器开放开放端口 80 。通过把服务器放置砸 DMZ 内部，就可以对 DMZ 开放端口 80，但是可能会对内部网络关闭。如果在内部网络上有服务器，就不能关闭端口。你总是需要拒绝任何流量，然后允许需要的内容。通过把服务器放置在 DMZ 内部，在应用安全公理的时候米就有了更多的间隔尺寸。

(作者：Stephen Mencik 译者：Tina 来源：TT 中国)

采用 Windows 认证访问 Linux DMZ

问：我正在设计一个新的包括一个 DMZ（隔离区或非军事化区）网络，在一个防火墙后配置的是 Linux Web 服务器和 Windows BackOffice。我希望使用 Linux 运行 DMZ 一边的公司内部网（intranet）。但是，我想限制员工访问 Internet，并限制通过防火墙后采用 Windows Server 2003 登陆认证。我能这么做吗？如果可以，我如何设置防火墙？是不是有人能给我一些相关的指引呢？

答：这是当今问得很多的一个问题，答案其实并不是很复杂。你需要做的就是配置一个代理服务器。我建议你采用 Squid 来代理你的流量，并使用 Samba 认证来自 Windows 2003 登录认证数据库的流量。

（作者：Mark Hinkle　译者：Shirley 来源：TT 中国）

在 DMZ 中放置企业用户有什么风险

问：当设置防火墙的时候，你建议把企业用户放在 DMZ 中吗?

答：不。按照设计，DMZ 是作为中间位置的（所以它名字是 demilitarized zone），公共服务和专用服务都和这里相连。传统的防火墙设置创建了三个区域：不受信任区（在边界防火墙中通常是互联网）、信任区（企业内网）和用于提供公共服务的 DMZ。它们通常被用于为企业提供一个独立层，保护他们的内网系统不向外部暴露。

必须要呈现在不受信任区的企业服务，比如 Web 服务器和 SMTP 服务器，应该放在 DMZ 中。在受到攻击的情况下，这种安排确保内部用户和系统有一道防火墙保护他们，隔离受感染的服务器。把企业用户（属于企业内网的人）放在 DMZ 中，就没有了这一层保护，使他们有存在于不受信任区的系统上的风险。

(作者：Mike Chapple　译者：Tina 来源：TT 中国)

在 DMZ 中放置邮件服务器的风险

问：目前，我们的内部邮件服务器和其他设备一样放在防火墙后面的计算机上。我们的数据库管理员想要把邮件服务器转移到 DMZ 中，这样数据库就可以和邮件系统连接了。很明显，他想要的功能，只能在邮件服务器在 DMZ 中时工作。这样做有什么风险吗?如果有，我应该怎样排除或减轻这种风险。

答：任何时候，对互联网开放企业系统，都存在风险。尽管如此，如果恰当地建立系统，就可以减轻风险。开始可以使用两个网络适配器。一个用于 DMZ，另一个用于内部访问。确定在网卡上设置了端口过滤，并且只允许必需流量通过。如果把 Web 邮件从邮件服务器上分离转移到另外的服务器上，也会（对把 IIS，即互联网信息服务隔离在 DMZ 外）有所帮助。彻底检查所有的 NTFS 许可，查找安全漏洞。例如，在所有可能的位置，把“Everyone Group”替换为“Authenticated Users”。同样，要总是确定系统不断进行不定更新。

(作者：Ben Wright　译者：Tina 来源：TT 中国)