样的设备观察到一个可疑的分组时，或一系列可疑的分组时，它能够防止这些分组进入该机构网络。或者仅仅是因为觉得该活动可疑，该设备虽说能够让这些分组通过，但要向网络管理员发出告警，网络管理员然后密切关注该流量并采取适当的行动。当观察到潜在恶意流量时能产生告警的设备称为**入侵检测系统**（Intrusion Detection System，IDS）。滤除可疑流量的设备称为**入侵防止系统**（Intrusion Prevention System，IPS）。在本节中我们一起学习 IDS 和 IPS 这两种系统，因为这些系统的最为有趣的技术方面是它们检测可疑流量的原理（而不是它们是否发送告警或丢弃分组）。我们因此将 IDS 系统和 IPS 系统统称为 IDS 系统。

IDS 能够用于检测多种攻击，包括网络映射（例如使用 nmap 进行分析）、端口扫描、TCP 栈扫描、DoS 带宽洪泛攻击、蠕虫和病毒、操作系统脆弱性攻击和应用程序脆弱性攻击。（参见 1.6 节有关网络攻击的概述内容。）目前，数以千计的机构应用了 IDS 系统。这些已部署的系统有许多是专用的，Cisco、Check Point 和其他安全装备厂商在市场上销售这些系统。但是许多已部署的 IDS 系统是公共域系统，如极为流行的 Snort IDS 系统（我们将简要讨论它）。

一个机构可能在它的机构网络中部署一个或多个 IDS 传感器。图 8-36 显示了一个具有 3 个 IDS 传感器的机构。当部署了多个传感器时，它们通常共同工作，向一个中心 IDS 处理器发送有关可疑流量活动的信息，中心处理器收集并综合这些信息，当认为适合时向网络管理员发送告警。在图 8-36 中，该机构将其网络划分为两个区域：一个高度安全区域，由分组过滤器和应用程序网关保护，并且由 IDS 系统监视；一个较低度安全区域（称之为**非军事区**（DeMilitarized Zone，DMZ)），该区域仅由分组过滤器保护，但也由 IDS 系统监视。注意到 DMZ 包括了该机构需要与外部通信的服务器，如它的公共 Web 服务器和它的权威 DNS 服务器。

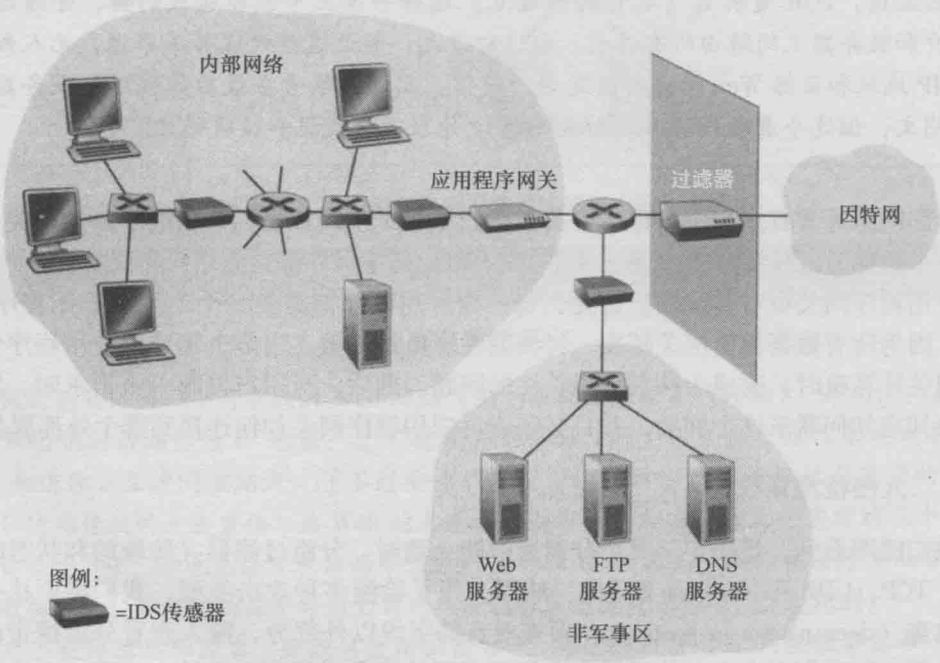

图 8-36 部署一个过滤器、一个应用程序网关和多个 IDS 传感器的机构

此时你也许想知道，为什么使用多个 IDS 传感器？为什么在图 8-36 中不只是在分组过滤器后面放置一个 IDS 传感器（或者甚至与分组过滤器综合）？我们将很快看到，IDS 不