

安全域边界控制方案

为保证内部网络的安全可靠运行，一般单位通常采取以下两种方式对内、外网实施安全隔离。

1. 内、外网物理隔离

内、外网进行物理隔离，严格来讲就是，内、外网之间根本不能连通，不能相互通信，专职人员必须通过使用物理隔离的计算机，才能够访问内、外网。

2. 内、外网逻辑隔离

内、外网逻辑隔离，主要是通过划分 VLAN（Virtual Local Area Network，虚拟局域网）等技术手段，隔离一些特殊的群体，以实施更有针对性的安全防护，实现内部网络的相对独立性。同时在内、外网连接处，一般都安装防火墙和入侵检测等系统对内网提供保护。

但是，非法外联和非法接入等行为，很容易对物理隔离或逻辑隔离的内部网络造成安全威胁。

● 安全风险分析：

- 1) 内部人员可通过 Modem 拨号、ADSL 拨号或手机无线拨号等方式，非法连接到互联网等外部网络，造成内部网络安全保障措施失效，可能会造成病毒感染、敏感信息泄密等安全事件；
- 2) 在内、外网物理隔离的涉密信息系统内部，工作人员也可能把内网计算机连接到外部网络上，形成非法的网络出口，从而为外部黑客非法入侵提供途径，容易造成安全隐患；
- 3) 外部移动笔记本电脑等，通过非法接入内部网络的交换设备，访问内部信息系统中的计算机和服务器资源，造成可能的信息失泄密；
- 4) 在某些情况下，外部移动笔记本计算机还可以通过直连线，直接跟内部网络中的计算机相连，建立对等网络连接，从而造成信息泄密。

● 解决方案：

中安源可信网络安全平台基于密码技术，对 IP 数据包进行重构，在协议层

实现了对非法外联和非法内接行为提供了有效的防范手段,安装了系统的计算机不论通过何种方式,均不能非法外联到互联网。任何没有授权的计算机,都不能通过网络交换设备接入单位内部网络,也不能通过网线直连的方式接入到单位内部的任何一台计算机上获取数据。

具体功能描述如下:

- 1) 应用密码技术对 IP 包进行重构,使得非法外联的计算机无法与外界的计算机进行正常的网络通信,只能与指定范围内的计算机和服务之间进行通信,从而可有效切断一切非法外联行为;
- 2) 通过 IP 包重构技术,不管是什么形式的非法接入行为,包括交换设备接入和直连线对等网接入,外来的计算机都不能跟内网的计算机进行正常的网络通信,可有效切断一切非法接入行为;
- 3) 通过非法接入阻断技术,可以主动阻断未经认证或者未部署安全系统的计算机接入到内部网络中;
- 4) 通过安全网关,可以建立安全服务器区(OA 服务器、文件服务器等),仅经过管理员授权的计算机和用户才能访问此区域内的服务器,从而保护重要的服务器不被非法访问,防止内部敏感信息泄密;
- 5) 可以直接禁止计算机上的网络设备,包括网卡、红外、蓝牙、WLAN、Modem 等设备的运行;
- 6) 通过 IP 绑定技术,可以防止用户随意更改计算机 IP 地址,规避一些安全管理风险;
- 7) 对非法外联和非法内接行为提供详细的日志记录,并在发生安全事件时通过报警、短信、电子邮件、声音等多种方式通知安全管理员。

● 系统部署示意图:

