# 旁路模式解决方案

旁路模式有三种部署模式，采用路由将流量转发到防火墙进行处理，防火墙将镜像流量模拟处理，单纯的IDS监听模式。

## 路由式旁路转发

逻辑拓扑如下：



防火墙旁路挂在服务器区的路由器上。两个防火墙做成HA（这不是必须的）。实际上的逻辑拓扑如下：



防火墙与核心交换机之间启用trunk，路由器通过路由方式将流量转发到防火墙上进行处理，处理后的流量再返回到核心路由上。

**该种模式与串接并无不同地方，只是流量是通过路由器进行控制和转发。**

主要功能

|  |  |  |
| --- | --- | --- |
| **主要功能** | **展现** | **阻断** |
| **防火墙** | **是** | **是** |
| **IPS** | **是** | **是** |
| **防病毒** | **是** | **是** |
| **网站过滤** | **是** | **是** |
| **应用识别与控制** | **是** | **是** |
| **邮件过滤** | **是** | **是** |
| **数据防泄漏** | **是** | **是** |
| **流量控制** | **是** | **是** |
| **日志** | **是** |  |

## 防火墙模拟处理镜像流量

部署拓扑如下



在交换机上部署镜像接口，把往返的流量镜像到防火墙上。在防火墙上做单臂策略，将往返的流量视为经过防火墙然后出去的数据流。

该模式的功能与防火墙相同，但是无法策略阻断和防止攻击，也就是说不能主动去做什么事情，只能发现问题。

主要功能

|  |  |  |
| --- | --- | --- |
| **主要功能** | **展现** | **阻断** |
| **防火墙** | **是** | **否** |
| **IPS** | **是** | **否** |
| **防病毒** | **是** | **否** |
| **网站过滤** | **是** | **否** |
| **应用识别与控制** | **是** | **否** |
| **邮件过滤** | **是** | **否** |
| **数据防泄漏** | **是** | **否** |
| **流量控制** | **是** | **否** |
| **日志** | **是** |  |

## IDS监听模式

部署拓扑如下



在交换机上部署镜像接口，把往返的流量镜像到防火墙上。防火墙启用IDS监听模式，对镜像的数据流进行分析。该功能主要用于IDS类，其他功能无法实现。

主要功能

|  |  |  |
| --- | --- | --- |
| **主要功能** | **展现** | **阻断** |
| **防火墙** | **否** | **否** |
| **IPS** | **是** | **可以发reset阻断** |
| **防病毒** | **否** | **否** |
| **网站过滤** | **否** | **否** |
| **应用识别与控制** | **否** | **否** |
| **邮件过滤** | **否** | **否** |
| **数据防泄漏** | **否** | **否** |
| **流量控制** | **否** | **否** |
| **日志** | **是** |  |