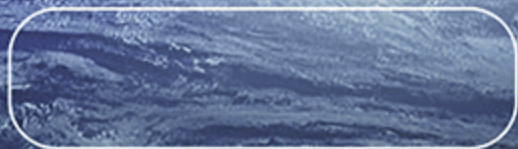


# 神州数码防火墙工作原理





# 目录

- 防火墙概述
- 神州数码防火墙核心技术
- 神州数码防火墙工作原理详解
- 神州数码防火墙部署与应用场景



# 目录

- 神州数码防火墙性能优化与管理
- 神州数码防火墙面临挑战及发展趋势

01

# 防火墙概述



# 防火墙定义与作用

## 防火墙定义

防火墙是一种网络安全设备，用于监控和控制网络之间的通信流量，根据预先设定的安全策略，允许、拒绝或限制数据包的通过。

## 防火墙作用

防火墙可以有效地保护内部网络免受外部攻击，防止未经授权的访问和数据泄露，同时也可以对内部网络进行访问控制和流量管理。





# 神州数码防火墙产品简介



神州数码防火墙是神州数码公司自主研发的一款高性能、高可靠性的网络安全产品，具有多种安全特性和功能，可满足不同规模和需求的网络环境。

神州数码防火墙支持多种安全策略，包括访问控制、应用识别、内容过滤、VPN等，可以有效地保护网络边界安全，提高网络整体安全性。



# 防火墙在网络安全中地位

防火墙是网络安全的重要组成部分，是网络安全的第一道防线，可以有效地防止外部攻击和内部泄露。

防火墙可以与其他安全设备和技术相结合，形成多层次、全方位的安全防护体系，提高网络的整体安全性和可靠性。同时，防火墙也是网络安全管理和监控的重要手段之一，可以帮助网络管理员实时监控网络流量和安全事件，及时发现和处理安全问题。

02

# 神州数码防火墙核心技术

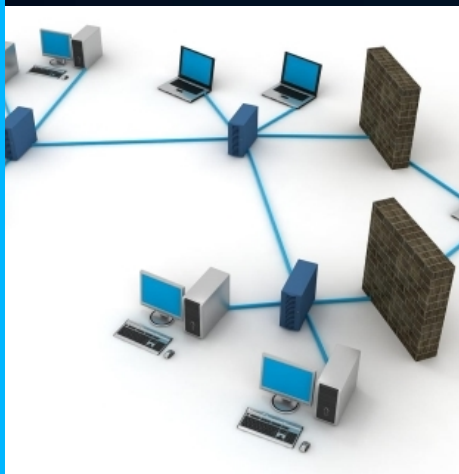






# 包过滤技术

基于数据包的源地址、  
目的地址、端口号等  
信息进行过滤



阻止不符合规则的数  
据包通过防火墙

可配置访问控制列表  
( ACL ) 实现细粒度  
控制





# 代理服务技术



代理服务器作为客户端和服务  
器之间的中介



客户端请求先发送到代理服务  
器，再由代理服务器转发给目  
标服务器



代理服务器可对请求和响应进  
行检查、修改或缓存等操作



# 状态监测技术

1

跟踪连接状态，判断数据包是否属于合法连接

2

识别并阻止恶意攻击，如SYN洪水攻击、端口扫描等

3

结合包过滤技术实现更高效的访问控制





# VPN支持及加密技术



支持IPSec VPN、SSL VPN等多种VPN协议



提供数据加密、身份认证、访问控制等安全功能



保障远程访问和数据传输的安全性

03

# 神州数码防火墙工作原理详解





# 数据流通过程描述



## 数据包接收

神州数码防火墙监听网络接口，接收进出的数据包。

## 数据包解析

对接收的数据包进行深度解析，提取源/目的IP、端口号、协议类型等信息。

## 安全策略匹配

将解析后的数据包与预先定义的安全策略进行匹配。

## 动作执行

根据匹配结果执行相应的动作，如允许、拒绝、重定向等。

# 访问控制策略实施方式

## 基于IP地址的访问控制

根据源/目的IP地址进行访问控制。



## 基于端口号的访问控制

根据源/目的端口号进行访问控制。



## 基于协议类型的访问控制

根据协议类型（如TCP、UDP等）进行访问控制。



## 综合访问控制策略

结合以上多种方式进行综合访问控制。



以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：  
<https://d.book118.com/056105241114010124>