Table of Contents

[1. 概述/简介 3](#_Toc134174833)

[1.1 概念 3](#_Toc134174834)

[1.2 类型 4](#_Toc134174835)

[1.3 安全原理 5](#_Toc134174836)

[2. 华为防火墙 7](#_Toc134174837)

[2.1 面板，功能 9](#_Toc134174838)

[2.1.1 仪表盘Dashboard 9](#_Toc134174839)

[2.1.2 监控 Monitor 9](#_Toc134174840)

[2.1.3 政策 Policy 9](#_Toc134174841)

[2.1.4 对象/安全配置文件 Object 9](#_Toc134174842)

[2.1.5 网络 Network 9](#_Toc134174843)

[2.1.6 系统 System 9](#_Toc134174844)

[2.2 常用指令 9](#_Toc134174845)

[3. 飞墙 FortiOS 10](#_Toc134174846)

[3.1 面板，功能 11](#_Toc134174847)

[3.1.1 仪表盘 12](#_Toc134174848)

[3.1.2 网络 12](#_Toc134174849)

[3.1.3 安全配置文件 12](#_Toc134174850)

[3.1.4 无线&交换机控制器 12](#_Toc134174851)

[3.1.5 系统管理 12](#_Toc134174852)

[3.1.6 Security Fabric 12](#_Toc134174853)

[3.1.7 日志&报表 12](#_Toc134174854)

[3.1.8 其他 12](#_Toc134174855)

[3.2常用指令 12](#_Toc134174856)

[4. NSX-T 13](#_Toc134174857)

[4.1 面板，功能 14](#_Toc134174858)

[4.1.1 主页Home 14](#_Toc134174859)

[4.1.2 网络Networking 14](#_Toc134174860)

[4.1.3 安全Security 14](#_Toc134174861)

[4.1.4 清单 Inventory 14](#_Toc134174862)

[4.1.5 计划和故障排除 Plan & Troubleshoot 14](#_Toc134174863)

[4.1.6 系统 System 14](#_Toc134174864)

[5. 总结 15](#_Toc134174865)

# 1. 概述/简介

防火墙是一种安全设备，通常用于保护计算机网络免受未经授权的访问和网络攻击。它可以过滤网络流量，根据特定规则阻止或允许流量通过。防火墙可以位于网络边缘，例如企业网络的边界或互联网边缘，并充当网络和外部世界之间的“门卫”。

防火墙可以根据不同的规则进行配置，以控制哪些网络流量可以通过，哪些不允许通过。这些规则可以基于源IP地址、目标IP地址、端口号、协议类型等参数进行设置。防火墙也可以执行其他安全功能，如网络地址转换（NAT）和虚拟专用网络（VPN）。

防火墙在保护计算机网络免受未经授权的访问和网络攻击方面非常重要。它可以帮助企业和个人用户保护敏感信息和数据，并减轻网络攻击对网络和系统的影响。

## 1.1 概念

防火墙（Firewall）是一种安全设备，通常位于网络的边缘，用于保护计算机网络免受未经授权的访问和网络攻击。防火墙可以控制网络流量，根据特定的规则允许或阻止流量通过。

防火墙的基本功能是过滤网络流量。当网络上的数据包通过防火墙时，防火墙会根据预先定义的规则来决定是否允许数据包通过。这些规则可以基于源IP地址、目标IP地址、端口号、协议类型等参数进行设置。

例如，一个企业可能会将规则设置为只允许来自指定IP地址的流量通过防火墙。另一个企业可能会设置规则，只允许特定的端口通过，如HTTP（端口号80）或HTTPS（端口号443）。

除了过滤网络流量，防火墙还可以执行其他安全功能，如网络地址转换（NAT）和虚拟专用网络（VPN）。

* 网络地址转换（NAT）是一种技术，它允许企业使用较少的公共IP地址来连接到互联网。当内部计算机发送请求时，NAT会将内部IP地址转换为公共IP地址，以使请求能够通过互联网。
* 虚拟专用网络（VPN）是一种安全的远程访问技术，它可以允许用户从远程位置访问企业网络，同时保持网络和数据的安全性。VPN使用加密技术来保护数据在互联网上的传输过程中不被窃取或篡改。

总之，防火墙在保护计算机网络免受未经授权的访问和网络攻击方面非常重要。它可以帮助企业和个人用户保护敏感信息和数据，并减轻网络攻击对网络和系统的影响。

## 1.2 类型

防火墙可以按不同的方式进行分类，例如按照部署位置、技术实现方式、功能等方面进行分类。以下是常见的防火墙类型分类：

* 基于部署位置的分类：
  + 网络边界防火墙（Network Boundary Firewall:）：安装在网络边界的设备，保护内部网络和互联网之间的通信。该防火墙可以安装在企业的边缘，阻止来自外部网络的未经授权的访问。例如，企业可以使用Cisco ASA、Fortinet FortiGate、Juniper SRX等品牌的设备来保护其网络边界。
  + 主机防火墙（Host-based Firewall）：安装在单个计算机上的软件防火墙，保护单个计算机的安全。Windows和Mac OS X都内置了防火墙功能。企业也可以使用第三方防火墙软件，如Norton Internet Security、McAfee Total Protection等，来保护计算机的安全。
  + 应用程序防火墙 （Application Firewall）：专门保护应用程序的防火墙，监控特定应用程序的流量并阻止未经授权的访问。这种防火墙专门保护某些应用程序。例如，企业可以使用F5 Networks的应用程序防火墙来保护其Web应用程序。
* 基于技术实现方式的分类：
  + 基于硬件的防火墙 (Hardware-based firewall)：使用专门的硬件设备来实现防火墙功能，通常比软件防火墙更高效。这种防火墙通常使用专用硬件设备，如Cisco ASA、Fortinet FortiGate、Juniper SRX等品牌的设备。这些设备能够在网络层和应用层提供安全保护。
  + 基于软件的防火墙 (Software-based firewall)：这种防火墙通常是一种软件程序，例如Windows和Mac OS X自带的防火墙，或者企业可以使用第三方软件，如Norton Internet Security、McAfee Total Protection等。
  + 代理防火墙 (Proxy Firewall)：通过代理方式监视和过滤网络流量，它可以检查更深层次的网络协议。例如，企业可以使用Squid作为Web代理来保护其网络安全。
  + 状态检测防火墙 (Stateful Inspection Firewall)：使用状态检测技术来检查网络连接的状态，确定是否允许特定的流量通过。例如，企业可以使用Checkpoint防火墙来保护其网络安全。
* 基于功能的分类：
  + 包过滤防火墙：根据源地址、目标地址、端口号和协议等信息过滤网络数据包。
  + 应用程序过滤防火墙：监控应用程序的流量，并根据特定的应用程序规则过滤流量。
  + 内容过滤防火墙：检查数据包中的内容，防止传输有害的信息或恶意代码。
  + VPN防火墙：提供安全的远程访问方式，通过VPN建立安全的通信渠道。
  + IDS/IPS防火墙：IDS（入侵检测系统）/IPS（入侵预防系统）可以监控网络流量并识别潜在的攻击行为，并根据特定的规则自动预防或阻止攻击。

总之，选择哪种类型的防火墙应该根据实际需求和网络拓扑结构来进行决策，以达到最佳的网络安全保护效果。

## 1.3 安全原理

防火墙的安全原理可以概括为以下几个方面：

* 区分信任和不信任的网络：防火墙通过将网络划分为信任和不信任的两个部分，防止不信任的网络访问信任的网络，从而保护内部网络的安全。
* 策略过滤：防火墙通过过滤网络流量，只允许符合预定义安全策略的流量通过，从而防止未经授权的访问和攻击。
* 端口过滤：防火墙可以过滤特定的端口，只允许预定义的端口进行通信，从而防止一些常见的攻击方式，如端口扫描、网络钓鱼等。
* NAT（网络地址转换）：防火墙可以将内部网络的私有IP地址转换为公网IP地址，从而保护内部网络的隐私和安全。
* VPN（虚拟专用网络）：防火墙可以提供安全的VPN通信，使远程用户和分支机构可以安全地访问内部网络资源。

总之，防火墙的安全原理是通过限制不信任的网络流量，仅允许预定义的安全流量通过，从而保护内部网络的安全性和隐私性。防火墙可以通过不同的功能和技术实现这些安全策略，例如：区分网络、过滤网络流量、端口过滤、NAT和VPN等。

# 2. 华为防火墙

华为防火墙是一种网络安全设备，主要用于保护企业网络免受恶意攻击和数据泄露，其主要功能、应用和优缺点如下：

功能：

* 防火墙：防止未授权的访问，对网络流量进行控制和过滤，保障网络的安全
* 入侵检测和防御系统(IDS/IPS)：检测和预防网络入侵攻击，保护网络不受外部攻击。
* 虚拟专用网络(VPN)：建立安全的远程连接，实现分支机构和远程用户的远程访问。
* 数据泄露防护：检测和防止敏感数据在网络中的泄露。
* 应用控制：控制和过滤网络应用，防止未经授权的应用使用。
* 内容过滤：控制和过滤网络内容，防止非法和有害信息的传播。
* 反病毒：检测和预防计算机病毒的传播，保障网络的安全。

应用：

* 企业网络安全：华为防火墙可以保护企业网络免受外部攻击和内部威胁，保障企业数据的安全性和完整性。
* 电子商务：华为防火墙可以保护电子商务网站和应用免受黑客攻击和数据泄露，确保交易信息的保密性和安全性。
* 金融业：华为防火墙可以保护金融机构的客户数据免受外部攻击和内部威胁，保障金融业的信息安全。

优点：

* 强大的安全保护：华为防火墙提供了多种安全功能，可以有效地保护企业网络的安全。
* 灵活的部署方式：华为防火墙支持多种部署方式，可以根据不同的应用场景和需求进行选择。
* 多种管理方式：华为防火墙提供了多种管理方式，包括Web界面、命令行界面和SNMP协议，方便管理员进行设备的配置和管理。
* 可靠性高：华为防火墙支持冗余配置和热备插拔功能，确保设备在故障或维护升级时的连续性和稳定性。

缺点：

* 配置灵活性较低：华为防火墙的功能非常丰富，但这也使得其相对于其他品牌的防火墙来说更加复杂。需要有较高的技术水平才能完全掌握其所有功能。导致在一些特定场景下，其配置灵活性可能较低。例如，有些配置需要通过命令行完成，而不是在Web界面中完成。
* 部署成本高：华为防火墙的价格相对较高，需要一定的资金才能购买和部署。另外，由于其复杂性，可能需要额外的培训和人力成本。
* 支持服务可能有限：由于华为防火墙在国内市场的知名度和用户数量较少，因此其支持和服务可能相对有限，不能像其他品牌的防火墙那样及时得到支持。
* 依赖华为设备：如果企业使用的其他设备不是华为品牌，那么与华为防火墙的集成可能会面临一些挑战。在这种情况下，可能需要花费更多的时间和精力来解决问题。

## 2.1 面板，功能

### 2.1.1 仪表盘Dashboard

### 2.1.2 监控 Monitor

### 2.1.3 政策 Policy

### 2.1.4 对象/安全配置文件 Object

### 2.1.5 网络 Network

### 2.1.6 系统 System

## 2.2 常用指令

# 3. 飞墙 FortiOS

飞墙防火墙是一种网络安全设备，主要用于保护企业网络免受恶意攻击和数据泄露，其主要功能、应用和优缺点如下：

功能：

* 防火墙：防止未授权的访问，对网络流量进行控制和过滤，保障网络的安全。
* 入侵检测和防御系统(IDS/IPS)：检测和预防网络入侵攻击，保护网络不受外部攻击。
* 虚拟专用网络(VPN)：建立安全的远程连接，实现分支机构和远程用户的远程访问。
* 数据泄露防护：检测和防止敏感数据在网络中的泄露。
* 应用控制：控制和过滤网络应用，防止未经授权的应用使用。
* 内容过滤：控制和过滤网络内容，防止非法和有害信息的传播。
* 反病毒：检测和预防计算机病毒的传播，保障网络的安全。

应用：

* 企业网络安全：飞墙防火墙可以保护企业网络免受外部攻击和内部威胁，保障企业数据的安全性和完整性。
* 电子商务：飞墙防火墙可以保护电子商务网站和应用免受黑客攻击和数据泄露，确保交易信息的保密性和安全性。
* 金融业：飞墙防火墙可以保护金融机构的客户数据免受外部攻击和内部威胁，保障金融业的信息安全。

优点：

* 高速数据处理：飞墙防火墙采用高性能硬件，可以实现高速数据处理，保证网络的流畅性和稳定性。
* 灵活的部署方式：飞墙防火墙支持多种部署方式，可以根据不同的应用场景和需求进行选择。
* 多种管理方式：飞墙防火墙提供了多种管理方式，包括Web界面、命令行界面和SNMP协议，方便管理员进行设备的配置和管理。
* 丰富的安全功能：飞墙防火墙提供了多种安全功能，可以有效地保护企业网络的安全。

缺点：

* 学习曲线陡峭：飞墙相对于其他品牌的防火墙，可能有较为陡峭的学习曲线。对于一些不熟悉飞墙的管理员，学习和配置可能需要一定的时间和经验。
* 部署复杂：飞墙的部署可能相对复杂，需要一定的专业知识和技能才能顺利完成。对于没有相关经验的管理员，可能会增加部署和配置的难度。
* 需要配合其他设备使用：飞墙可能需要配合其他设备一起使用，如IPS/IDS、VPN等，这可能会增加整个系统的复杂度和成本。
* 服务和支持：飞墙在国内市场的知名度和用户数量相对较少，相应的服务和支持可能不如其他品牌的防火墙成熟和完善。

## 3.1 面板，功能

### 3.1.1 仪表盘

### 3.1.2 网络

### 3.1.3 安全配置文件

### 3.1.4 无线&交换机控制器

### 3.1.5 系统管理

### 3.1.6 Security Fabric

### 3.1.7 日志&报表

### 3.1.8 其他

## 3.2常用指令

# 4. NSX-T

NSX是一种网络虚拟化和安全平台，主要用于帮助企业构建和管理虚拟化网络和云环境，其主要功能、应用和优缺点如下：

功能：

* 虚拟化网络：将物理网络转化为虚拟网络，提供灵活、可扩展、安全的网络基础设施。
* 安全性：提供多层次的安全保障，包括防火墙、入侵检测和防御系统、虚拟私有网络等。
* 自动化：提供自动化管理和协作，实现自动化流程和资源管理。
* 多云集成：支持多种公有云和私有云的集成，为企业提供更强的扩展性和灵活性。
* SD-WAN：提供全球性的SD-WAN解决方案，实现高效、可靠、安全的网络连接。
* 容器网络：提供容器网络解决方案，支持多种容器和Kubernetes平台。

应用：

* 企业网络安全：NSX可以为企业提供更加安全、可靠和可扩展的网络基础设施。
* 云计算：NSX可以帮助云服务提供商构建和管理虚拟化网络和云环境，提高云计算的安全性和可靠性。
* 多云环境：NSX可以帮助企业将多个公有云和私有云进行集成，实现更加灵活和高效的网络管理。

优点：

* 网络虚拟化：NSX可以将物理网络转化为虚拟网络，提供更加灵活和可扩展的网络基础设施。
* 多层次的安全性：NSX提供多层次的安全保障，包括防火墙、入侵检测和防御系统、虚拟私有网络等，保障网络的安全性。
* 自动化：NSX提供自动化管理和协作，实现自动化流程和资源管理，提高了企业的效率和生产力。
* 多云集成：NSX支持多种公有云和私有云的集成，为企业提供更强的扩展性和灵活性。
* SD-WAN：NSX提供全球性的SD-WAN解决方案，实现高效、可靠、安全的网络连接。

缺点：

* 学习成本高：NSX相对于传统网络设备，学习曲线可能比较陡，需要学习和掌握较高的技术水平。
* 部署复杂：NSX部署和配置较为复杂，需要专业人员进行管理和维护。
* 依赖VMware环境：只能在VMware虚拟化环境中使用。如果企业不使用VMware，那么需要额外的成本和努力来集成NSX。
* 需要额外的硬件支持：在某些情况下，NSX可能需要额外的硬件支持才能实现最佳性能，这可能会增加部署和管理成本。

## 4.1 面板，功能

### 4.1.1 主页Home

### 4.1.2 网络Networking

### 4.1.3 安全Security

### 4.1.4 清单 Inventory

### 4.1.5 计划和故障排除 Plan & Troubleshoot

### 4.1.6 系统 System

# 5. 总结

华为防火墙、飞墙和NSX都是网络安全领域中的重要产品。它们各有特点和适用场景。

华为防火墙是华为公司生产的一种硬件设备，旨在提供网络安全防护功能，如流量过滤、攻击检测和防御等。华为防火墙具有高性能和高可靠性的特点，能够满足大型企业和服务提供商的需求。

飞墙是中国移动公司开发的一种网络安全产品，可提供流量清洗、DDoS防护、DNS劫持等功能。与华为防火墙不同的是，飞墙是基于软件实现的，可以部署在虚拟化环境中。

NSX是VMware公司推出的一种软件定义网络（SDN）产品，可以提供网络虚拟化和安全功能。NSX具有多种安全功能，如虚拟化的防火墙、网络安全组（NSX Distributed Firewall）、安全网关等，适用于数据中心和云环境。

表格 1：华为防火墙，飞墙，NSX-T的简单对比：

|  |  |  |  |
| --- | --- | --- | --- |
| 产品名称 | 类型 | 主要功能 | 使用场景 |
| 华为防火墙 | 硬件设备 | 流量过滤，攻击检测和防御 | 大型企业和服务商的网络安全防护 |
| 飞墙 Fortigate | 软件 | 流量清洗，DDoS防护，DNS劫持等等 | 虚拟化环境的网络安全防护 |
| NSX-T | 软件定义网络 | 网络虚拟化和安全功能， 如虚拟防火墙，网络安全组，安全网关等 | 数据中心，云环境 |

以上是针对华为防火墙、飞墙和NSX的一个简单的比较。可以看到，它们的类型、主要功能和适用场景都有所不同。华为防火墙是一种硬件设备，适用于大型企业和服务提供商的网络安全防护；飞墙是一种基于软件实现的网络安全产品，适用于虚拟化环境中的网络安全防护；而NSX则是一种软件定义网络产品，适用于数据中心和云环境，提供更多的网络虚拟化和安全功能。

Top of Form

总体来说，华为防火墙和飞墙是专门针对网络安全防护的硬件和软件产品，适用于企业和服务提供商等需要高性能、高可靠性网络防护的场景。而NSX则是一种软件定义网络产品，提供了更多的网络虚拟化和安全功能，适用于云环境和数据中心等场景。